
Technische Universität
Carolo-Wilhelmina Braunschweig

Institut Computational Mathematics

# On the classification of algebras

Morten Wesche

September 19, 2016

# Introduction

*Higman (1950) published the papers Enumerating p-groups I and II and introduced the so-called "PORC"-functions. (PORC stands for* ***P****olynomial* ***O****n* ***R****esidue* ***C****lasses.) A function $f$ is called PORC if there exists a natural number $N$ and polynomials $f_0, \ldots, f_{N-1}$ such that $f(x) = f_a(x)$ for all $x \in N \cdot \mathbb{Z} + a$. So, $f$ behaves like a polynomial for all $x$ in the same residue class modulo $N$.*
*Higman (1950) proofed that the number $f_d(q)$ of isomorphism classes of algebras of fixed dimension $d$ over an arbitrary field with $q$ elements can be described by a PORC-function in $q$. He conjectured that the number $g_n(p)$ of isomorphism types of $p$-groups of order $p^n$ is given by a PORC-function in $p$. It is a still open problem in group theory. Vaughan-Lee (2013) sketched a method to compute the PORC-functions for $f_d(q)$ and he determined them for $d \leq 4$.*
*This paper will give an introduction to Higman's PORC theory and the basic ideas of the classification of finite dimensional algebras over finite fields.*

# Contents

# 1 Basic definitions and examples

**Definition 1.1:** ***Algebra***
*An algebra $\mathcal{A}$ of dimension $d$ over a field $\mathbb{K}$ is a $d$-dimensional vector space over $\mathbb{K}$ equipped with a bilinear mapping $\mathbb{K}^d \times \mathbb{K}^d \to \mathbb{K}^d$ called multiplication.*
*If the multiplication is associative[1], then $\mathcal{A}$ is called associative. If the multiplication is Jacobian[2], then $\mathcal{A}$ is called a Lie-algebra.*

**Remark 1.2**
*It is **not** assumed that an algebra contains an identity element.*

**Example 1.3**

1. *Let $V$ be any finite dimensional vector space over any field $\mathbb{K}$. Equipping $V$ with the trivial multiplication $V \times V \to V$, $(x, y) \mapsto 0$, gives an algebra. It is easy to see, that it is an associative and commutative algebra.*
2. *Let $V = M_n(\mathbb{K})$ be the vector space of all $n \times n$ matrices with entries in the field $\mathbb{K}$. Equipping $V$ with the standard multiplication of matrices, one gets an associative algebra. It is not commutative.*
3. *Let $V = \mathbb{R}^3$ equipped with the cross product: $\times : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3, (x, y) \mapsto x \times y$. As this multiplication is Jacobian, $(\mathbb{R}^3, \times)$ is a Lie-algebra.*
   *There are a lot of applications for this algebra: In maths it can be used for the calculation of the distance of skew lines or the volume of polyhedra. In physics it is used for computing an angular momentum or the Lorentz force.*

**Definition 1.4:** $f_d(\mathbb{K})$
*Let $f_d(\mathbb{K})$ be the number of isomorphism types of algebras of dimension $d$ over the field $\mathbb{K}$.*

**Remark 1.5**
*Two algebras are isomorphic if there exists a bijective base transformation preserving their structure.*

**Central Question:**
**What can be said about $f_d(\mathbb{K})$ depending on $d$ and $\mathbb{K}$?**

**Example 1.6**
*Independently from the chosen field, there are two isomorphism types of one dimensional algebras: The algebra $\mathcal{A}_1$ with zero multiplication $\cdot : \mathcal{A}_1 \times \mathcal{A}_1 \to \mathcal{A}_1$, $(x, y) \mapsto 0$, and the algebra $\mathcal{A}_2$ with non-zero multiplication.*
*When increasing the dimension to two, there are already infinitely many algebras[3] if the field is not finite (see [Goze and Remm, 2011]). However, if the field is finite with $|\mathbb{K}| = p^e = q$, then the number of isomorphism types can be given by polynomials (see [Vaughan-Lee, 2013]).*

| | $d = 1$ | $d = 2$ |
|---|---|---|
| $\lvert\mathbb{K}\rvert = \infty$ | 2 | $\infty$ |
| $\lvert\mathbb{K}\rvert = p^e = q$ | 2 | $\begin{cases} q^4 + q^3 + 4q^2 + 3q + 6, & p = 2 \\ q^4 + q^3 + 4q^2 + 4q + 6, & p = 3 \\ q^4 + q^3 + 4q^2 + 4q + 7, & p \geq 5 \end{cases}$ |

Table 1: Number of isomorphism types of algebras for small dimension $d$

[1] Associative: for all $a, b, c \in \mathcal{A}$ holds $(ab)c = a(bc)$.
[2] Jacobian: for all $a, b, c \in \mathcal{A}$ holds $(ab)c + (bc)a + (ca)b = 0$.
[3] For instances, take the algebras with basis $\mathcal{A}_k = \langle a, b \mid a^2 = 0, ab = 0, ba = b, b^2 = ka \rangle$ for an element $k \in \mathbb{K} \setminus \{0\}$. These algebras are pairwise non-isomorphic.

**Remark 1.7**
*For a finite field $\mathbb{K}$ with $|\mathbb{K}| = p^e = q$ write $f_d(\mathbb{K}) = f_d(q)$.*

**Theorem 1.8** ***(Higman)***
*For a fixed $d \in \mathbb{N}$ the function $f_d(q)$ is PORC.*

**Definition 1.9: *PORC***
*A function $f$ is called PORC (**P**olynomial **O**n **R**esidue **C**lasses), if there exists a natural number $N \in \mathbb{N}$ and a set of polynomials $f_0, \ldots, f_{N-1}$ such that*

$$f(x) = f_a(x) \quad \text{for all} \quad x \in N \cdot \mathbb{Z} + a.$$

**Remark 1.10**
*A function, that is PORC modulo $N$, behaves like a polynomial for all $x$ of the same residue class modulo $N$.*

**Example 1.11**
*Let $p \geq 5$ be a prime. How many irreducible polynomials of degree three of the form $x^3 - c$ exist in $\mathbb{F}_p[x]$, where $\mathbb{F}_p$ is the finite field with $p$ elements? In other words: How many elements $c \in \mathbb{F}_p$ exist, such that the polynomial $x^3 - c$ has no roots in $\mathbb{F}_p$?*
*It is obvious, that $c \neq 0$ must hold. Therefore, one can assume to choose $c$ from the unit group $\mathbb{F}_p^*$. Therefore, this group shall be looked at in more detail.*
*First of all, fix an element $\vartheta = \vartheta_p$ which generates this unit group of $\mathbb{F}_p$, hence it is $\langle\vartheta\rangle = \mathbb{F}_p^*$. Its order is $p-1$ and one can find an integer $k$ with $0 \leq k < p-1$ such that $c = \vartheta^k$.*
*Next, define the subgroup $\mathcal{H} = \langle\vartheta^3\rangle \leq \mathbb{F}_p^*$. Depending on $p$, $\mathcal{H}$ can or cannot be a trivial subgroup. Additionally, as $x = 0$ cannot be a root of $x^3 - c$, one can write $x = \vartheta^l$ with $0 \leq l < p-1$. So, findig the roots of $x^3 - c = 0$ is equivalent to finding all solutions of $\vartheta^{3l} = \vartheta^k$.*

1. *Let $p \equiv 1 \bmod 3$. Therefore, the subgroup $\mathcal{H}$ is a proper subgroup of index 3 in $\mathbb{F}_p^*$. With $x^3 = \vartheta^{3l} \in \mathcal{H}$ the equation $3l = k$ can just be solved with $k \equiv 0 \bmod 3$. There are $(p-1)/3$ such elements $\vartheta^k$.*
   *As there is a total of $p-1$ polynomials of the form $x^3 - c$ with $c \neq 0$ and as there are $(p-1)/3$ reducible polynomials, there remain $2(p-1)/3$ irreducible polynomials of the desired form.*
2. *Let $p \equiv 2 \bmod 3$. Then it is $\mathcal{H} = \mathbb{F}_p^*$ So, for any $l$, there is a $k$ such that the equation $\vartheta^{3l} = \vartheta^k$ holds. So the polynomial $x^3 - c \in \mathbb{F}_p[x]$ is always reducible and there are no irreducible polynomials of the desired form.*

*Depending on the residue class of $p$ modulo 3 one has two different polynomials. Therefore, the number is PORC. Putting all this together, one has*

$$\begin{aligned}
&|\{f(x) = x^3 - c \in \mathbb{F}_p[x] \mid f(x) \text{ is irreducible}\}| \\
=&\begin{cases} 2(p-1)/3, & p \equiv 1 \bmod 3 \\ 0, & p \equiv 2 \bmod 3 \end{cases} \\
=&\frac{\gcd(p-1,3)-1}{3} \cdot (p-1).
\end{aligned}$$

# 2 Enumerating algebras

**Remark 2.1**
*For the rest of this paper let $\mathbb{K}$ always be a finite field with $|\mathbb{K}| = p^e = q$.*

**Proposition and Definition 2.2: *Structure constants***
*The multiplication of a $d$-dimensional algebra with basis $\mathcal{B} = \{b_1, \ldots, b_d\}$ is completely determined by a set of structure constants $\lambda_{ijk} \in \mathbb{K}$, $1 \leq i, j, k \leq d$, via*

$$b_i b_j = \sum_{k=1}^{d} \lambda_{ijk} b_k.$$

**Example 2.3**

1. *In case of an algebra with zero multiplication, it is $\lambda_{ijk} = 0$ for all $i, j, k$.*
2. *In the case of the matrix algebra $M_n(\mathbb{K})$ first fix a basis: Let this be $\mathcal{B} = \{e_{ij} \mid 1 \leq i, j \leq n\}$, where $e_{ij}$ denotes that $n \times n$ matrix, which has a one in row $i$ at column $j$ and whose other entries are zero. It is known that $e_{ij}e_{kl} = \delta_{jk}e_{il}$ holds. Here, $\delta_{jk}$ denotes the Kronecker delta, which evaluates to one, if both indices are equal, and which evaluates to zero otherwise. Then, using the double indices, the structure constants are*

$$\lambda_{i_1 i_2,\, j_1 j_2,\, k_1 k_2} = \begin{cases} 1, & \text{if } i_2 = j_1,\ i_1 = k_1,\ j_2 = k_2, \\ 0, & \text{otherwise.} \end{cases}$$

3. *The structure constants of the algebra $(\mathbb{R}^3, \times)$ are given as follows (when using the canonical vector space base $\{e_1, e_2, e_3\}$:*

$$\begin{aligned} &\lambda_{123} = \lambda_{312} = \lambda_{231} = 1, \\ &\lambda_{132} = \lambda_{213} = \lambda_{321} = -1, \\ &\lambda_{ijk} = 0 \ \text{ otherwise.} \end{aligned}$$

Writing a set of structure constants as a vector $v \in \mathbb{K}^{d^3}$ (the elements $\lambda_{ijk}$ are arranged lexicographically), then the action of a basis transformation $G \in \mathrm{GL}(d, \mathbb{K})$ is given by $v \cdot G \otimes G \otimes G^{-1}$, where "$\otimes$" stands for the Kronecker product. The number of isomorphism types is therefore equal to the number of orbits of elements of $\mathbb{K}^{d^3}$ under the action of $\mathrm{GL}(d, \mathbb{K})$. Using the lemma of Burnside, Cauchy, and Frobenius, one gets

$$\begin{aligned} f_d(q) &= \frac{1}{|\mathrm{GL}(d, \mathbb{F}_q)|} \sum_{g \in \mathrm{GL}(d, \mathbb{F}_q)} |\mathrm{Fix}_g| \\ &= \frac{1}{|\mathrm{GL}(d, \mathbb{F}_q)|} \sum_{\substack{\text{conjugacy classes} \\ \mathrm{cl} \subset \mathrm{GL}(d, \mathbb{F}_q)}} |\mathrm{cl}| \cdot |\mathrm{Fix}_{g(\mathrm{cl})}| \\ &= \sum_{\substack{\text{conjugacy classes} \\ \mathrm{cl} \subset \mathrm{GL}(d, \mathbb{F}_q)}} |C_{\mathrm{GL}(d, \mathbb{K})}(g(\mathrm{cl}))| \cdot |\mathrm{Fix}_{g(\mathrm{cl})}|. \end{aligned}$$

It is $\mathrm{Fix}_g = \{v \in \mathbb{K}^{d^3} \mid v \cdot G \otimes G \otimes G^{-1} = v\}$, the length of a class cl is denoted by $|\mathrm{cl}|$, a representative of cl is given by $g(\mathrm{cl})$, and $C_{\mathrm{GL}(d,\mathbb{K})}(g(\mathrm{cl})) = \{x \in G \mid gx = xg\}$ is the centraliser of the element $g = g(\mathrm{cl})$ in $\mathrm{GL}(d, \mathbb{K})$.

**Remark 2.4**
$\mathrm{Fix}_g$ *is the eigenspace of $G \otimes G \otimes G^{-1}$ belonging to the eigenvalue 1.*

**Problem:**
**The conjugacy classes still depend on $q$. While increasing $q$, the number of conjugacy classes of $\mathrm{GL}(d, \mathbb{K})$ increases, too.**

# 3 Improvement of the lemma of Burnside, Frobenius, and Cauchy

The main work of improving the application of the lemma is done by Charles Green, Graham Higman, and Michael Vaughan-Lee.
Green published the paper *The characters of the finite general linear groups* (see [Green, 1955]) and there he defined the so called "type" of a matrix. This classification is based on the rational canonical form of a matrix, but is far coarser than the classification into conjugacy classes. The most important result is that the "types" do not depend on the field.
Graham Higman published his very well known papers *Enumerating p-groups I and II* (see [Higman, 1960a], [Higman, 1960b]). Although working with $p$-groups, he gives some theorems for algebras too. For instance, he proofed that the number of isomorphism types of algebras of fixed dimension over a finite field is PORC.
Michael Vaughan-Lee then developed algorithms to really determine the PORC functions. In his paper *Enumerating algebras over a finite field* (see [Vaughan-Lee, 2013]) he publishes the PORC functions for algebras of dimension $d \leq 4$. (In the case $d = 2$ the polynomials are of degree 4, for $d = 3$ they are of degree 18, and for $d = 4$ they are of degree 48.) The used algorithms are described in his paper *Choosing elements from finite fields* (see [Vaughan-Lee, 2012a]).

Charles Alexander Green[4]
(26 February 1926 – 7 April 2014)

Graham Higman[5]
(19 January 1917 – 8 April 2008)

Michael Vaughan-Lee[6]

**Work by Green:**

- $|\mathrm{Fix}_{g(\mathrm{cl})}|$ does not depend on $g(\mathrm{cl})$, but on the "type" of the class only.
- The number of different "types" within $\mathrm{GL}(d, \mathbb{K})$ depends on $d$ only, not on $q$.

**Work by Higman:**

- $|\mathrm{Fix}_{g(\mathrm{cl})}|$ is a polynomial in $q$.
- $|C_{\mathrm{GL}(d,\mathbb{K})}(g(\mathrm{cl}))|$ is a polynomial in $q$.
- The number of elements of a fixed "type" in $\mathrm{GL}(d, \mathbb{K})$ is PORC.

**Work by Vaughan-Lee:**

- Development of algorithms to determine expicitly the PORC functions in small cases of $d$.

[4] Picture taken from https://static.independent.co.uk/s3fs-public/styles/story_large/public/thumbnails/image/2014/07/20/19/sandy-green.jpg
[5] Picture taken from https://upload.wikimedia.org/wikipedia/commons/2/2d/Graham_Higman.jpg
[6] Picture taken from https://www.lincoln.ac.uk/home/media/universityoflincoln/schoolofmathematicsandphysics/Professor-Michael-Vaughan-Lee.jpg

# 4 The PORC-conjecture

When looking at Higman's papers *Enumerating p-groups I and II* one gets directly another possible question: How many isomorphism types of groups of order $p^n$ exist?
Let the number of those isomorphism classes be $g_n(p)$. Higman formulated his famous PORC conjecture dealing with this number.

**Conjecture 4.1** ***(Higman's PORC conjecture)***
*For fixed $n \in \mathbb{N}$, the function $g_n(p)$ giving the number of isomorphism types of groups of order $p^n$ is PORC.*

The problem is solved for $n \leq 7$. For instance, those polynomials can be found at http://groupprops.subwiki.org/wiki/Higman's_PORC_conjecture or in [Vaughan-Lee, 2012b] (for $n \leq 5$). However, it is an still open problem for $n \geq 8$.

# References


[Goze and Remm, 2011] Goze, M. and Remm, E. (2011). 2-dimensional algebras. *Afr. J. Math. Phys.*, 10(1):81–91.

[Green, 1955] Green, J. A. (1955). The characters of the finite general linear groups. *Trans. Amer. Math. Soc.*, 80:402–447.

[Higman, 1960a] Higman, G. (1960a). Enumerating $p$-groups. I. Inequalities. *Proc. London Math. Soc. (3)*, 10:24–30.

[Higman, 1960b] Higman, G. (1960b). Enumerating $p$-groups. II. Problems whose solution is PORC. *Proc. London Math. Soc. (3)*, 10:566–582.

[Vaughan-Lee, 2012a] Vaughan-Lee, M. (2012a). Choosing elements from finite fileds.

[Vaughan-Lee, 2012b] Vaughan-Lee, M. (2012b). Graham Higman's PORC conjecture. *Jahresber. Dtsch. Math.-Ver.*, 114(2):89–106.

[Vaughan-Lee, 2013] Vaughan-Lee, M. (2013). Enumerating algebras over a finite field. *Int. J. Group Theory*, 2(3):49–61.