

# Lazard and PORC

Bettina Eick

TU Braunschweig – Germany

L'Aquila, July 2023, Talk 2

# Higman's PORC conjecture

## Higman's PORC conjecture

# Classifying of $p$ -groups by order

## Aims

- **(Strong)** Determine up to isomorphism a complete and irredundant list of groups of order  $p^n$ .

# Classifying of $p$ -groups by order

## Aims

- **(Strong)** Determine up to isomorphism a complete and irredundant list of groups of order  $p^n$ .
- **(Weaker)** Determine the number  $f(n, p)$  of isomorphism types of groups of order  $p^n$ .

# Classifying of $p$ -groups by order

## Aims

- **(Strong)** Determine up to isomorphism a complete and irredundant list of groups of order  $p^n$ .
- **(Weaker)** Determine the number  $f(n, p)$  of isomorphism types of groups of order  $p^n$ .
- **(Variation)** Investigate  $f(n, p)$  as a function in  $n$  or as a function in  $p$ .

# PORC

## PORC

A function  $f$  is PORC if it is a Polynomial On Residue Classes:

- there exist  $s, m \in \mathbb{N}$  and polynomials  $f_0, \dots, f_{m-1}$  so that

# PORC

## PORC

A function  $f$  is PORC if it is a Polynomial On Residue Classes:

- there exist  $s, m \in \mathbb{N}$  and polynomials  $f_0, \dots, f_{m-1}$  so that
- $f(p) = f_i(p)$  for all  $p > s$  prime with  $p \equiv i \pmod{m}$ .

# Example

## Example for a PORC function

$$p \mapsto 2p + 61 + (p - 1, 4) + 2(p - 1, 3)$$

choose  $s = 2$ , use  $m = 12$

- $f_1(p) = 2p + 61 + 10$
- $f_3(p) = 2p + 61 + 4$
- $f_5(p) = 2p + 61 + 6$
- $f_7(p) = 2p + 61 + 8$
- $f_9(p) = 2p + 61 + 6$
- $f_{11}(p) = 2p + 61 + 4$



# Higman (1960)

## PORC Conjecture (Higman 1960)

The function  $f(n, p)$  for fixed  $n$  as a function in  $p$  is PORC.

# Groups of order $p^n$ , $p > 5$

	Number	Comment
$p^1$	1	
$p^2$	2	
$p^3$	5	
$p^4$	15	
$p^5$	$2p + 61 + (p - 1, 4) + 2(p - 1, 3)$	Bagnera 1898
$p^6$	$3p^2 + 39p + 344 + 24(p - 1, 3) + 11(p - 1, 4) + 2(p - 1, 5)$	Newman, O'Brien, Vaughan-Lee 2004
$p^7$	$3p^5 + \dots$	O'Brien, Vaughan-Lee 2005

# The Lazard correspondence

## The Lazard correspondence

# Lazard

## Lazard

Let  $p > c$ :

- The Lazard correspondence associates to each group  $G$  of order  $p^n$  and  $p$ -class  $c$  a Lie ring  $L$  of order  $p^n$  and  $p$ -class  $c$  and vice versa.

# Lazard

## Lazard

Let  $p > c$ :

- The Lazard correspondence associates to each group  $G$  of order  $p^n$  and  $p$ -class  $c$  a Lie ring  $L$  of order  $p^n$  and  $p$ -class  $c$  and vice versa.
- The translation is done by the Baker-Campbell-Hausdorff formula and its inverse.

# Lazard

## Lazard

Let  $p > c$ :

- The Lazard correspondence associates to each group  $G$  of order  $p^n$  and  $p$ -class  $c$  a Lie ring  $L$  of order  $p^n$  and  $p$ -class  $c$  and vice versa.
- The translation is done by the Baker-Campbell-Hausdorff formula and its inverse.
- The correspondence preserves isomorphism.

# Advantage

## Advantage

Lie  $p$ -rings are slightly easier to study.

# Classification

## O'Brien and Vaughan-Lee (2005)

- Determined all nilpotent Lie rings of order at most  $p^7$  for all primes  $p > 5$  up to isomorphism.



# Classification

## O'Brien and Vaughan-Lee (2005)

- Determined all nilpotent Lie rings of order at most  $p^7$  for all primes  $p > 5$  up to isomorphism.
- Classification is mainly by hand and checked by computer.

# Result 1

## Result 1

The PORC conjecture holds for  $n \leq 7$ .

## Result 2

### Result 2

The classification is available in GAP in the LiePRing package.

# The LiePRing Package of GAP

## The LiePRing Package of GAP

# Classification

## Database of LiePRings

```
gap> List([1..7], x -> Length(LiePRingsByLibrary(x)));  
[ 1, 2, 5, 15, 75, 542, 4773 ]
```

```
gap> L := LiePRingsByLibrary(5)[55];  
<LiePRing of dimension 5 over prime p with parameters [ x ]>  
gap> NumberOfLiePRingsInFamily(L);  
1/2*p-1/2
```

# Classification

## Database of LiePRings

```
gap> List(LiePRingsByLibrary(5), NumberOfLiePRingsInFamily);  
[ 1, 1, 1, 1, 1, 1, 1/2*p+1/2, 1, 1, 1, 1/2*p-1/2, 1, 1, 1,  
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1/2*(p-1,3)-1/2,  
  1/2*(p-1,3)-1/2, 1, 1, 1, 1/2*(p-1,4)-1, 1/2*(p-1,4)-1,  
  1, 1/2*(p-1,3)-1/2, 1/2*(p-1,3)-1/2, 1, 1, 1, 1, 1, 1,  
  1, 1, 1, 1, 1, 1, 1, 1, 1/2*p+1/2, 1, 1, 1/2*p-1/2, 1,  
  1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 ]  
gap> Sum(last);  
2*p+2*(p-1,3)+(p-1,4)+61
```

# Classification

## Database of LiePRings

```
gap> L := LL[70];  
<LiePRing of dimension 5 over prime p>  
gap> ViewPCPresentation(L);  
[12,11] = 15  
  
gap> K := SpecialisePrimeOfLiePRing(L, 5);  
<LiePRing of dimension 5 over prime 5>  
gap> PGroupByLiePRing(K);  
<pc group of size 3125 with 5 generators>  
  
gap> K := SpecialisePrimeOfLiePRing(L, 37);  
<LiePRing of dimension 5 over prime 37>  
gap> PGroupByLiePRing(K);  
<pc group of size 69343957 with 5 generators>
```

# Classification

## Database of LiePRings

```
gap> L := LL[55];
<LiePRing of dimension 5 over prime p with parameters [ x ]>
gap> ViewPCPresentation(L);
p*12 = x*15
p*13 = 14 + 15
[12,11] = 14
[13,11] = 15
gap> LiePRingsInFamily(L, 5);
[ <LiePRing of dimension 5 over prime 5>,
  <LiePRing of dimension 5 over prime 5> ]
gap> LiePRingsInFamily(L, 11);
[ <LiePRing of dimension 5 over prime 11>,
  <LiePRing of dimension 5 over prime 11>,
  <LiePRing of dimension 5 over prime 11>,
  <LiePRing of dimension 5 over prime 11>,
  <LiePRing of dimension 5 over prime 11> ]
```



# Classification

## Database of LiePRings

```
gap> LL := LiePRingsByLibrary(7);  
gap> L := LL[122];  
<LiePRing of dim 7 over prime p with parameters [x,y,z]>  
gap> L!.LibraryConditions;  
[ "x ne 0, [x,y,z]~[ax,a^2y,az] if a^4=1", "" ]  
gap> Length(LiePRingsInFamily(L, 11));  
605  
gap> Length(LiePRingsInFamily(L, 37));  
12321  
gap> NumberOfLiePRingsInFamily(L);  
 $-1/8*p^3*(p-1,4)+3/4*p^3+1/8*p^2*(p-1,4)-3/4*p^2$ 
```

# Classification

## Database of LiePRings

```
gap> Filtered(LL, x -> Length(ParametersOfLiePRing(x))>8);  
[ <LiePRing of dimension 7 over prime p with parameters  
  [ x, y, z, t, j, k, m, n, r, s, u, v ]>,  
  <LiePRing of dimension 7 over prime p with parameters  
  [ x, y, z, t, j, k, m, n, r, s, u, v ]> ]  
  
gap> NumberOfLiePRingsInFamily(last[1]);  
p^5+p^4+4*p^3+6*p^2  
+p*(p-1,3)+15*p+3/2*(p-1,3)+1/2*(p+1,3)+14
```

# Algorithms

## Computations with LiePRings

```
gap> L;
<LiePRing of dim 7 over prime p with parameters [x,y,z]>
gap> LiePLowerCentralSeries(L);
[ <LiePRing of dim 7 over prime p with parameters [x,y,z]>,
  <LiePRing of dim 5 over prime p with parameters [x,y,z]>,
  <LiePRing of dim 4 over prime p with parameters [x,y,z]>,
  <LiePRing of dim 3 over prime p with parameters [x,y,z]>,
  <LiePRing of dim 2 over prime p with parameters [x,y,z]>,
  <LiePRing of dim 0 over prime p with parameters [x,y,z]> ]
gap> List(last, BasisOfLiePRing);
[ [ 11, 12, 13, 14, 15, 16, 17 ],
  [ 13, 14, 15, 16, 17 ],
  [ 14, 15, 16, 17 ],
  [ 15, 16, 17 ],
  [ 16, 17 ],
  [ ] ]
```

# What next?

What next?

# Open Problems

My favourite open problems:

- Invent a generic Lie p-ring generation algorithm

# Open Problems

My favourite open problems:

- Invent a generic Lie p-ring generation algorithm
- Takes as input an generic LiePRing

# Open Problems

My favourite open problems:

- Invent a generic Lie p-ring generation algorithm
- Takes as input an generic LiePRing
- Determines parametrised presentations for descendants

# How to do that?

## What are the problems

- Use the ideas of p-group generation:



# How to do that?

## What are the problems

- Use the ideas of  $p$ -group generation:
- Step (1): Compute the  $p$ -cover, the  $p$ -multiplier, the  $p$ -nucleus

# How to do that?

## What are the problems

- Use the ideas of  $p$ -group generation:
- Step (1): Compute the  $p$ -cover, the  $p$ -multiplier, the  $p$ -nucleus
- Step (2): Compute orbits and stabilizer of the automorphism group action