<table>
<thead>
<tr>
<th>Title</th>
<th>Fast decomposition of $p$-groups in the Roquette category, for $p &gt; 2$ (Research on finite groups and their representations, vertex operator algebras, and algebraic combinatorics)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Bouc, Serge</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (2014), 1872: 113-121</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2014-01</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/195487">http://hdl.handle.net/2433/195487</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

京都大学
Fast decomposition of $p$-groups in the Roquette category, for $p > 2$

Serge Bouc

Abstract: Let $p$ be a prime number. In [9], I introduced the Roquette category $\mathcal{R}_p$ of finite $p$-groups, which is an additive tensor category containing all finite $p$-groups among its objects. In $\mathcal{R}_p$, every finite $p$-group $P$ admits a canonical direct summand $\partial P$, called the edge of $P$. Moreover $P$ splits uniquely as a direct sum of edges of Roquette $p$-groups.

In this note, I would like to describe a fast algorithm to obtain such a decomposition, when $p$ is odd.


Keywords: $p$-group, Roquette, rational, biset, genetic.

1. Introduction

Let $p$ be a prime number. The Roquette category $\mathcal{R}_p$ of finite $p$-groups, introduced in [9], is an additive tensor category with the following properties:

- Every finite $p$-group can be viewed as an object of $\mathcal{R}_p$. The tensor product of two finite $p$-groups $P$ and $Q$ in $\mathcal{R}_p$ is the direct product $P \times Q$.

- In $\mathcal{R}_p$, any finite $p$-group has a direct summand $\partial P$, called the edge of $P$, such that

$$P \cong \bigoplus_{N \triangleleft P} \partial(P/N) .$$

Moreover, if the center of $P$ is not cyclic, then $\partial P = 0$.

- In $\mathcal{R}_p$, every finite $p$-group $P$ decomposes as a direct sum

$$P \cong \bigoplus_{R \in \mathcal{S}} \partial R ,$$

where $\mathcal{S}$ is a finite sequence of Roquette groups, i.e. of $p$-groups of normal $p$-rank 1, and such a decomposition is essentially unique. Given the group $P$, such a decomposition can be obtained explicitly from the knowledge of a genetic basis of $P$.

- The tensor product $\partial P \times \partial Q$ of the edges of two Roquette $p$-groups $P$ and $Q$ is isomorphic to a direct sum of a certain number $\nu_{P,Q}$ of copies of the edge $\partial(P \circ Q)$ of another Roquette group (where both $\nu_{P,Q}$ and $P \circ Q$ are known explicitly).
• The additive functors from $\mathcal{R}_p$ to the category of abelian groups are exactly the rational $p$-biset functors introduced in [4].

The latter is the main motivation for considering this category: any structural result on $\mathcal{R}_p$ will provide for free some information on such rational functors for $p$-groups, e.g. the representation functors $R_K$, where $K$ is a field of characteristic 0 (see [2], [3], and L. Barker's article [1]), the functor of units of Burnside rings ([6]), or the torsion part of the Dade group ([5]).

The decomposition of a finite $p$-group $P$ as a direct sum of edges of Roquette $p$-groups can be read from the knowledge of a genetic basis of $P$. The problem is that the computation of such a basis is rather slow, in general. For most purposes however, the full details encoded in a genetic basis are useless, and it would be enough to know the direct sum decomposition.

Hence it would be nice to have a fast algorithm taking any finite $p$-group $P$ as input, and giving its decomposition as direct sum of edges of Roquette groups in the category $\mathcal{R}_p$. This note is devoted to the description of such an algorithm, when $p > 2$.

2. Rational $p$-biset functors

2.1. Recall that the characteristic property of the edge $\partial P$ of a finite $p$-group in the Roquette category $\mathcal{R}_p$ is that for any rational $p$-biset functor $F$

$$\partial F(P) = \hat{F}(\partial P),$$

where $\partial F(P)$ is the faithful part of $F(P)$, and $\hat{F}$ denotes the extension of $F$ to $\mathcal{R}_p$. Also recall the following criterion ([7], Theorem 3.1):

\begin{itemize}
  \item if the center of $P$ is non cyclic, then $\partial F(P) = \{0\}$.
  \item if $E \leq P$ is a normal elementary abelian subgroup of rank 2, and if $Z \leq E$ is a central subgroup of order $p$ of $P$, then the map

$$\text{Res}_{C_P(E)}^P \oplus \text{Def}_{P/Z}^P : F(P) \rightarrow F(C_P(E)) \oplus F(P/Z)$$

is injective.
\end{itemize}
2.3. Let $K$ be a commutative ring in which $p$ is invertible. When $P$ is a finite group, denote by $\text{CF}_K(P)$ the $K$-module of central functions from $P$ to $K$. The correspondence sending a finite $p$-group $P$ to $\text{CF}_K(P)$ is a rational $p$-biset functor:

**2.4. Proposition**: If $P$ and $Q$ are finite $p$-groups, if $U$ is a finite $(Q, P)$-biset, and if $f \in \text{CF}_K(P)$, define a map $\text{CF}_K(U) : \text{CF}_K(P) \to \text{CF}_K(Q)$ by

$$\forall s \in Q, \text{CF}_K(U)(f)(s) = \frac{1}{|P|} \sum_{u \in U, x \in P} f(x)_u.$$

With this definition, the correspondence $P \mapsto \text{CF}_K(P)$ becomes a rational $p$-biset functor, denoted by $\text{CF}_K$.

**Proof**: A straightforward argument shows that $\text{CF}_K(U)(f)$ is indeed a central function on $Q$, hence the map $\text{CF}_K(U)$ is well defined. It is also clear that this map only depends on the isomorphism class of the biset $U$, and that for any two finite $(H, G)$-bisets $U$ and $U'$, we have

$$\text{CF}_K(U \sqcup U') = \text{CF}_K(U) + \text{CF}_K(U').$$

Moreover if $U$ is the identity biset at $P$, i.e. if $U = P$ with biset structure given by left and right multiplication, then for $f \in \text{CF}_K(P)$ and $s \in P$

$$\text{CF}_K(U)(f)(s) = \frac{1}{|P|} \sum_{u \in U, x \in P} f(x)_u = \frac{1}{|P|} \sum_{u \in P} f(s^u) = f(s),$$

hence $\text{CF}_K(U)$ is the identity map.

Now if $R$ is a third finite $p$-group, and $V$ is a finite $(R, Q)$-biset, then for any $t \in R$, setting $\lambda = \text{CF}_K(V) \circ \text{CF}_K(U)(f)(t)$, we have that

$$\lambda = \frac{1}{|Q|} \sum_{v \in V, s \in Q} f(x),$$

$$= \frac{1}{|Q||P|} \sum_{(v,u) \in V \times U} f(x),$$

$$= \frac{1}{|Q||P|} \sum_{(v,u) \in V \times U, s \in Q, x \in P} \{s \in Q \mid tv = vs, su = ux\} f(x).$$
\[
\lambda = \frac{1}{|Q||P|} \sum_{(v_{Q}u) \in V \times_{Q} U, x \in P, t(v_{Q}u) = (v_{Q}u)x} |Q : Q_{v} \cap uP||Q_{v} \cap _{u}P| f(x)
\]
\[= \frac{1}{|P|} \sum_{(v_{Q}u) \in V \times_{Q} U, x \in P, t(v_{Q}u) = (v_{Q}u)x} f(x) = CF_{K}(V \times_{Q} U)(f)(t) .
\]

Hence \( CF_{K}(V) \circ CF_{K}(U) = CF_{K}(V \times_{Q} U) \), and \( CF_{K} \) is a \( p \)-biset functor.

To prove that this functor is rational, we use the criterion given by Theorem 2.2. Suppose first that the center \( Z(P) \) of \( P \) is non-cyclic. Let \( E \) denote the subgroup of \( Z(P) \) consisting of elements of order at most \( p \). Then saying that \( \partial CF_{K}(P) = \{0\} \) amounts to saying that for any \( f \in CF_{K}(P) \), the sum

\[
S = \sum_{Z \leq E} \mu(1, Z) \text{Inf}_{P/Z}^{P} \text{Def}_{P/Z}^{P} f
\]

is equal to 0, where \( \mu \) denotes the Möbius function of the poset of subgroups of \( P \) (or of \( E \)). Equivalently, for any \( s \in P \)

\[
S(s) = \sum_{Z \leq E} \mu(1, Z) \frac{1}{|P|} \sum_{aZ \in P/Z, x \in P \atop saZ = aZx} f(x) = 0 .
\]

This also can be written as

\[
S(s) = \sum_{Z \leq E} \mu(1, Z) \frac{1}{|P||Z|} \sum_{a \in P, z \in P \atop saZ = aZx} f(x)
\]

\[
= \frac{1}{|P|} \sum_{Z \leq E} \frac{\mu(1, Z)}{|Z|} \sum_{a \in P, z \in Z} f(s^a.z)
\]

\[
= \frac{1}{|P|} \sum_{Z \leq E} \frac{\mu(1, Z)}{|Z|} \sum_{a \in P, z \in Z} f((sz)^a)
\]

\[
= \sum_{Z \leq E} \frac{\mu(1, Z)}{|Z|} \sum_{z \in Z} f(sz)
\]

\[
= \sum_{z \in E} \left( \sum_{z \in E \atop Z \leq E} \frac{\mu(1, Z)}{|Z|} \right) f(sz)
\]

2.5. Lemma: Let \( E \) be an elementary abelian \( p \)-group of rank at least 2. Then for any \( z \in E \)

\[
\sum_{z \in Z \leq E} \frac{\mu(1, Z)}{|Z|} = 0 .
\]
**Proof**: For \( z \in E \), set \( \sigma(z) = \sum_{z \in Z \leq E} \frac{\mu(1, Z)}{|Z|} \). Assume first that \( z \neq 1 \), i.e. \( |z| = p \). If \( Z \ni z \) is elementary abelian of rank \( r \), then \( \mu(1, Z) = (-1)^r p^{(r+1)}/2 \), hence \( \frac{\mu(1, Z)}{|Z|} = (-1)p = -\frac{1}{p} \mu(1, Z/<z>) \). Hence setting \( \overline{Z} = Z/<z> \) and \( \overline{E} = E/<z> \),

\[
\sigma(z) = -\frac{1}{p} \sum_{1 \leq \overline{Z} \leq \overline{E}} \mu(1, \overline{Z}) = 0
\]

since \( |\overline{E}| > 1 \). Now

\[
\sum_{z \in E} \sigma(z) = \sigma(1) + \sum_{e \in E - \{1\}} \sigma(z) = \sum \sum_{z \in Z, z \in Z \leq E} \frac{\mu(1, Z)}{|Z|} = \sum_{1 \leq \overline{Z} \leq \overline{E}} \mu(1, Z) = 0
\]

hence \( \sigma(1) = 0 \), completing the proof of the lemma.

It follows that \( S(s) = 0 \), hence \( S = 0 \), as was to be shown.

For the second condition of Theorem 2.2, suppose that \( E \) is a normal elementary abelian subgroup of \( P \) of rank 2, and that \( Z \) is a central subgroup of \( P \) of order \( p \) contained in \( E \). Let \( f \in CF_K(P) \) which restricts to 0 to \( CP(E) \), and such that

\[
\forall sZ \in P/Z, \quad (Def_{P/Z}^{P}f)(sZ) = \frac{1}{|P|} \sum_{z \in Z} f(sz) = 0
\]

Thus \( f(s) = 0 \) if \( s \in CP(E) \). Assume that \( s \notin CP(E) \). Then for \( e \in E \), the commutator \( [s, e] \) lies in \( Z \). Moreover the map \( e \in E \mapsto [s, e] \in Z \) is surjective. it follows that for any \( z \in Z \), there exists \( e \in E \) such that \( s^e = sz \). Thus \( f(sz) = f(s^e) = f(s) \). Hence \( Def_{P/Z}^{P}f(s) = f(s) = 0 \). Hence \( f = 0 \), as was to be shown.

\[\square\]

3. Action of \( p \)-adic units

Let \( \mathbb{Z}_p \) denote the ring of \( p \)-adic integers, i.e. the inverse limit of the rings \( \mathbb{Z}/p^n\mathbb{Z} \), for \( n \in \mathbb{N} - \{0\} \). The group of units \( \mathbb{Z}_p^\times \) is the inverse limits of the unit groups \( (\mathbb{Z}/p^n\mathbb{Z})^\times \), and it acts on the functor \( CF_K \) in the following way: if \( \zeta \in \mathbb{Z}_p^\times \) and \( P \) is a finite \( p \)-group, choose an integer \( r \) such that \( p^r \) is a multiple of the exponent of \( P \), and let \( \zeta_{p^r} \) denote the component of \( \zeta \) in \( (\mathbb{Z}/p^r\mathbb{Z})^\times \). For \( f \in CF_K(P) \), define \( \hat{\zeta}_P(f) \in CF_K(P) \) by

\[
\forall s \in P, \quad \hat{\zeta}_P(f)(s) = f(s^{\zeta_{p^r}})
\]
Then clearly $\hat{\zeta}_{P}(f)$ only depends on $\zeta$, and this gives a well defined map

$$\hat{\zeta}_{P} : \text{CF}_{K}(P) \rightarrow \text{CF}_{K}(P).$$

One can check easily (see [8] Proposition 7.2.4 for details) that if $Q$ is a finite $p$-group, and $U$ is a finite $(Q, P)$-biset, then the square

\[
\begin{array}{ccc}
\text{CF}_{K}(P) & \xrightarrow{\hat{\zeta}_{P}} & \text{CF}_{K}(P) \\
\downarrow \text{CF}_{K}(U) & & \downarrow \text{CF}_{K}(U) \\
\text{CF}_{K}(Q) & \xrightarrow{\hat{\zeta}_{Q}} & \text{CF}_{K}(Q)
\end{array}
\]

is commutative. In other words, we have an endomorphism $\hat{\zeta}$ of the functor $\text{CF}_{K}$. It is straightforward to check that for $\zeta, \zeta' \in \mathbb{Z}_{p}^{x}$, we have $\zeta \zeta' = \zeta \circ \zeta'$, and that $\hat{1}$ is the identity endomorphism of $\text{CF}_{K}$. So this yields an action of the group $\mathbb{Z}_{p}^{x}$ on $\text{CF}_{K}$.

It follows in particular that when $n \in \mathbb{N} - \{0\}$, and $P$ is a finite $p$-group, if we set

$$F_{n}(P) = \{ f \in \text{CF}_{K}(P) \mid \forall s \in P, f(s^{1+p^{n}}) = f(s) \},$$

then the correspondence $P \mapsto F_{n}(P)$ is a subfunctor of $\text{CF}_{K}$: indeed $F_{n}$ is the subfunctor of invariants by the element $1 + p^{n}$ of $\mathbb{Z}_{p}^{x}$.

It follows that $F_{n}$ is a rational $p$-biset functor, for any $n \in \mathbb{N} - \{0\}$, hence it factors through the Roquette category $\mathcal{R}_{p}$. In particular, for any finite $p$-group $P$, if $P$ splits as a direct sum

$$P \cong \bigoplus_{R \in \mathcal{S}} \partial R$$

of edges of Roquette groups in $\mathcal{R}_{p}$, then there is an isomorphism

$$F_{n}(P) \cong \bigoplus_{R \in \mathcal{S}} \partial F_{n}(R).$$

### 3.1. Notation:
For a finite $p$-group $P$, and an integer $n \in \mathbb{N} - \{0\}$, let $l_{n}(P)$ denote the number of conjugacy classes of elements $s$ of $P$ such that $s^{1+p^{n}}$ is conjugate to $s$ in $P$. Also set $l_{0}(P) = 1$.

With this notation, for any finite $p$-group $P$, and any $n \in \mathbb{N} - \{0\}$, the $K$-module $F_{n}(P)$ is a free $K$-module of rank $l_{n}(P)$. In particular, if $P = C_{p^{m}}$ is cyclic of order $p^{m}$, then $F_{n}(P)$ has rank $l_{n}(P) = p^{\min(m,n)}$. Thus if $m > 0$, ...
then $\partial F_n(C_{p^m})$ has rank $p^\min(m,n) - p^\min(m-1,n)$, since $C_{p^m} \cong \partial C_{p^m} \oplus C_{p^{m-1}}$ in $\mathcal{R}_p$.

### 3.2. Theorem:
Assume that a $p$-group $P$ splits as a direct sum

$$P \cong 1 \oplus \bigoplus_{m=1}^{\infty} a_m \partial C_{p^m}$$

of edges of cyclic groups in the Roquette category $\mathcal{R}_p$, where $a_m \in \mathbb{N}$. Then

$$\forall m \geq 1, \quad a_m = \frac{l_m(P) - l_{m-1}(P)}{p^{m-1}(p-1)}.$$

**Proof:** For any $n \in \mathbb{N} - \{0\}$, we have

$$l_n(P) = 1 + \sum_{m=1}^{\infty} a_m (p^\min(m,n) - p^\min(m-1,n)) = 1 + \sum_{m=1}^{n} a_m (p^m - p^{m-1}).$$

For $n \in \mathbb{N} - \{0\}$, this gives $l_n(P) - l_{n-1}(P) = a_n (p^n - p^{n-1})$.

### 3.3. Corollary:
Suppose $p > 2$. If $P$ is a finite $p$-group, then

$$P \cong 1 \oplus \bigoplus_{m=1}^{\infty} \frac{l_m(P) - l_{m-1}(P)}{p^{m-1}(p-1)} \partial C_{p^m}$$

in the Roquette category $\mathcal{R}_p$.

**Proof:** Indeed for $p$ odd, all the Roquette $p$-groups are cyclic, hence the assumption of Theorem 3.2 holds for any $P$.

### Appendix

#### 3.1. A GAP function:
The following function for the GAP software ([10]) computes the decomposition of $p$-groups for $p > 2$, using Corollary 3.3:

```gcode
# GAP function for computing Roquette decomposition of p-groups
# input is a p-group g
# output is a list of pairs of the form [p^n, a_n]
# where a_n is the number of summands of g
# isomorphic to the edge of the cyclic group of order p^n
```

```gcode
# GAP code
```
roquette_decomposition:=function(g)
local prem,cg,s,i,x,y,z,pn,u;
if IsTrivial(g) then return [[1,1]];fi;
prem:=PrimeDivisors(Size(g));
if Length(prem)>1 then
  Print("Error : the group must be a p-group\n");
  return fail;
fi;
pream:=pream[1];
if prem=2 then
  Print("Error : the order must be odd\n");
  return fail;
fi;
cg:=ConjugacyClasses(g);
s:=[ ];
for i in [2..Length(cg)] do
  x:=cg[i];
  y:=Representative(x);
  pn:=1;
  u:=y;
  repeat
    pn:=pn*prem;
    u:=u^prem;
    z:=y*u;
    until z in x;
  Add(s,pn);
  od;
s:=Collected(s);
s:=List(s,x->[x[1],x[2]*prem/(prem-1)/x[1]]);
s:=Concatenation([[1,1]],s);
return s;
end;

3.2. Example :

gap> 1:=AllGroups(81);;
gap> for g in 1 do
> Print(roquette_decomposition(g),"\n");
> od;
[[1,1],[3,1],[9,1],[27,1],[81,1]]
[[1,1],[3,4],[9,12]]
[[1,1],[3,7],[9,3]]
[[1,1],[3,7],[9,3]]
[[1,1],[3,4],[9,12]]
[[1,1],[3,4],[9,3]]
[[1,1],[3,8]]
[[1,1],[3,5],[9,1]]
[[1,1],[3,5],[9,1]]
[[1,1],[3,5],[9,1]]
For example, the group on line 6 of the previous list, isomorphic to the semidirect product $C_{27} \rtimes C_3$, is isomorphic to $1 \oplus 4\partial C_3 \oplus 4\partial C_9$ in $\mathcal{R}_3$.

References


Serge Bouc - CNRS-LAMFA, Université de Picardie, 33 rue St Leu, 80039, Amiens Cedex 01 - France.
email : serge.bouc@u-picardie.fr
web : http://www.lamfa.u-picardie.fr/bouc/