Group cohomology and efficient methods for group algebras of large p-groups

David J. Green
Friedrich-Schiller-Universität Jena

ICMS 2016

Berlin, 11th July 2016

seit 1558

Group cohomology: cochains

Let G be a finite group, M a $\mathbb{Z}G$-module.

Definition: n-cochain

$$C^n(G,M) := \{f\colon G^n \to M \mid f(g_1,\ldots,1,\ldots,g_n) = 0\}.$$

Elements of C^n called *(normalized standard) n-cochains*.

Example: 1-cocycles

Call $f\colon G \to M$ a 1-cocycle if $f(g_1g_2) = g_1f(g_2) + f(g_1)$.

- So if action on M trivial then

$$\text{1-cocycle} \equiv \text{homomorphism } (G,\cdot) \to (M,+).$$

seit 1558

Coboundary map

More generally:

Coboundary map $\delta^n \colon C^n(G, M) \to C^{n+1}(G, M)$

$$\begin{aligned}\delta^n f(g_1, \ldots, g_{n+1}) &= g_1 f(g_2, \ldots, g_{n+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) \\ &\quad + (-1)^{n+1} f(g_1, \ldots, g_n)\,.\end{aligned}$$

One then shows that $\delta^{n+1} \circ \delta^n = 0$.

seit 1558

Cohomology

- Cocycles $Z^n(G,M) = \ker\left(C^n \xrightarrow{\delta} C^{n+1}\right)$.
- Coboundaries $B^n(G,M) = \mathrm{Im}\left(C^{n-1} \xrightarrow{\delta} C^n\right)$.

Example: 2-cocycles

$f\colon G^2 \to M$ a 2-cocycle if

$$f(g_1,g_2) + f(g_1g_2,g_3) = g_1 f(g_2,g_3) + f(g_1,g_2g_3)\,.$$

This is an associativity condition, c.f. group extensions.

- Since $\delta^{n+1} \circ \delta^n = 0$, have $B^n \subseteq Z^n$.
- So can define cohomology $H^n(G,M) := \dfrac{Z^n(G,M)}{B^n(G,M)}$.

seit 1558

Some applications I

Low dimensional cohomology: classification problems

$H^2(G, M)$ classifies group extensions $1 \to M \xrightarrow{i} \Gamma \xrightarrow{\pi} G \to 1$.

- Choose $\sigma\colon G \to \Gamma$ with $\sigma(1) = 1$ and $\pi\sigma = \mathrm{Id}_G$.
- σ unlikely to be a homomorphism. Define $f\colon G^2 \to M$ by

$$i(f(g_1, g_2))\sigma(g_1 g_2) = \sigma(g_1)\sigma(g_2)\,.$$

- Γ associative $\Rightarrow f \in Z^2(G, M)$: the extension class.

Interactions with algebraic topology

If G acts trivially on M then $H^n(G, M) \cong H^n_{\mathrm{sing}}(BG, M)$

seit 1558

Some applications II

Commutative algebra

- If $M = R$, a commutative ring with trivial G-action, then

$$H^*(G, R) := \bigoplus_{n \geq 0} H^n(G, R)$$

a graded ring, commutative in the graded sense:

$$x \in H^r \, , \; y \in H^s \; : \; yx = (-1)^{rs} xy \, .$$

- Quillen, Duflot, Benson-Carlson, Symonds: Commutative algebra of $H^*(G, \mathbb{F}_p)$ reflects the p-local group theory of G.

seit 1558

Homological algebra

How to compute cohomology?

- Description using normalized standard cochains just right for applications . . .
- But totally impractical for calculations: Grows way too fast.

Solution: Homological algebra!

- Normalized standard cochains are cochains on one free resolution of the trivial module . . .
- But any other projective resolution will do.

- E.g. Cyclic group, order n.
  - r-th term in the normalized standard resolution free of rank $(n-1)^r$.
  - But Cartan-Eilenberg give a periodic resolution.
- Computationally one wants resolution to be as small as possible.

seit 1558

Computing cohomology

Low dimensional, with non-trivial M

Holt, e.g. in GAP.

Medium-dimensional, with $M = \mathbb{Z}$

Geometric constructions for small resolutions, by Ellis and others.

All dimensions, for p-groups with $M = \mathbb{F}_p$

- Construct the *minimal* resolution using linear algebra (Carlson) or non-commutative Gröbner bases (King-G.).
- Carlson and Benson give "tests for completion" that tell you when you have gone far enough.

seit 1558

The importance of p-groups

Let R be a commutative ring.

Transfer theory

- $|G| \cdot H^n(G, R) = 0$ for all $n \geq 1$.
- So $H^{>0}(G, R)$ splits as direct sum of p-local pieces.

Stable elements (Artin-Tate)

$H^{>0}(G, R)_{(p)}$ the *stable* elements in $H^{>0}(P, R)$.

- P a Sylow p-subgroup of G
- Stable means that $x \in H^n(P, R)$ satisfies a condition on its restriction to $P \cap P^g$, for each $g \in G$.

Holt (1985): Testing stability is computationally feasible.
Start at $N_G(P)$ and climb up a tower of subgroups to G.

seit 1558

Mod-p cohomology of p-groups

From now on: Want $H^n(P, \mathbb{F}_p)$ for P a p-group

- Coefficients a field $\Rightarrow \exists$ *minimal* projective resolution.
- And since P a p-group: projective $=$ free.
- Free modules are easier to compute with!
- Need to iterate following key step:

Key step

- Given: A map $d\colon (\mathbb{F}_p P)^s \to (\mathbb{F}_p P)^r$.
- Want: Minimal generators for $\ker(d)$.

seit 1558

Performing the key step

The representation question

How to represent group algebra $\mathbb{F}_p P$ and the d on a computer?

Carlson: Linear algebra

- $\mathbb{F}_p P$ is a $|P|$-dimensional vector space over $\mathbb{F}_p$.
- Group generators act on $\mathbb{F}_p P$. Record action matrices.
- Represent d by its matrix. Dimensions: $s|P| \times r|P|$.
- Kernel is nullspace of this matrix.
- For minimal generators, use group generator matrices to compute radical of kernel.

seit 1558

Sage package p_group_cohomology

Gröbner bases with action matrices

- Like Carlson, store those group generator action matrices.
- So calculations in $\mathbb{F}_p P$ are instantaneous.
- But store d as list of module generator images: $s \times r\,|P|$.
- Kernel: Two-speed Buchberger with elimination ordering.
- Minimal generators: Weak version of Faugère F5.
- Have to use a *local* ordering.

Requires a **local** term ordering

- For minimal generators, need algebra generators in radical.
- Gröbner basis for $\mathbb{F}_p P$ too big with a well-ordering.

seit 1558

Acheivements

Carlson (2003)

All 267 groups of order 64.

King-G. (2011)

All 2328 groups of order 128.

Adem-Carlson-Karagueuzian-Milgram (2001)

Sylow 2-subgroup (order 2^9) of Higman-Sims group HS.

King-Ellis-G. (2011)

Sylow 2-subgroup (order 2^{10}) of Conway group Co_3.

seit 1558

Still wide open I

Sylow 2-subgroup (order 2^9) of unitary group $SU_3(8)$

- Essential ideal might have nilpotency class > 2.
- Benson's test: Completion only attained in degree 46.
- n-th term in minimal resolution grows as n^2.
- Already ptifully slow in degree 22.
- Oehme: Eilenberg-Moore spectral sequence does not collapse at E_2.
- Complicated ring structure: Sylow 2-subgroup of $SU_3(4)$ was hardest group of order 64.

seit 1558

Still wide open II

Sylow 2-subgroup (order 2^{10}) of Mathieu group M_{24}

- n^{th} term in minimal resolution grows as n^5.
- 12^{th} term free of rank 1,298; and 13^{th} has rank 1,726.
- So storing this d requires 287 MB.
- Still finding new generators in these degrees, and . . .
- Generator in deg n $\Rightarrow$ completion no earlier than deg $2n$.

Difficulties in these two cases:

- Size of "basic unit" $\mathbb{F}_p P$.
- Need large initial segment of minimal resolution.
- And the resolution grows too fast.

seit 1558

What about larger p-groups?

If $|P|$ much bigger than 2^{10} then ...

- Can't hope to compute ring $H^*(P, \mathbb{F}_p)$ any time soon.
- But for small n can try for $H^n(P, \mathbb{F}_p)$.
- $H^4(G, \mathbb{Z})$, $H^4(G, \mathbb{F}_p)$: applications in conformal field theory.

By the way: If you're wondering about odd primes ...

- We haven't even finished $|P| = 3^5$ yet!
- Basic unit $\mathbb{F}_p P$ larger, and you need to go a lot further.

seit 1558

Twisting the Drinfeld double

The twisted quantum double $D^\eta(G)$

Dijkgraaf-Pasquier-Roche: A quasi-Hopf algebra defined by G and a 3-cocycle $\eta \in Z^3(G, \mathbb{C}^\times)$.

Dimension shifting

- Short exact sequence $0 \to \mathbb{Z} \to \mathbb{C} \xrightarrow{\exp(2\pi i\_)} \mathbb{C}^\times \to 1$ induces long exact sequence in cohomology.
- Combine this with $|G|\, H^n(G, \mathbb{C}) = 0$ to get $H^n(G, \mathbb{C}) = 0$,

$$\text{whence} \qquad H^n(G, \mathbb{C}^\times) \cong H^{n+1}(G, \mathbb{Z})\ \forall\, n \geq 1\,.$$

So $H^4(G, \mathbb{Z})$ parametrizes twisted quantum doubles of G.

seit 1558

Connectivity of cohomology

Definition: Cohomological connectivity

Set $n_0(G,R) := \min\{n \geq 1 \mid H^n(G,R) \neq 0\}$, $n_0(G) = n_0(G,\mathbb{Z})$.

Properties of connectivity

- $H^1(G,\mathbb{Z}) = 0$ and $H^2(G,\mathbb{Z}) \cong \mathrm{Hom}(G,\mathbb{C}^\times)$. Hence

$$n_0(G) \geq 2\,; \quad \text{equality} \Leftrightarrow [G,G] \lneq G\,.$$

- So G simple $\Rightarrow n_0(G) \geq 3$.
- Milgram (2000): $n_0(M_{23}) = 6$: highest known connectivity.

$$H^6(M_{23},\mathbb{Z}) \cong \mathbb{F}_7 \qquad H^7(M_{23},\mathbb{Z}) \cong \mathbb{F}_2\,.$$

seit 1558

Connectivity mod p

Cohomology sequence induced by $0 \to \mathbb{Z} \xrightarrow{p\times} \mathbb{Z} \to \mathbb{F}_p \to 0$

- If $H^{n-1}(G, \mathbb{Z}) = 0$ then

$$H^{n-1}(G, \mathbb{F}_p) = \{x \in H^n(G, \mathbb{Z}) \mid px = 0\}.$$

- So $n_0(G) = 1 + \min\{n_0(G, \mathbb{F}_p) \mid p \text{ a prime dividing } |G|\}$.
- That's how Milgram did M_{23}.

Can still aim to determine $n_0(G)$ even if Sylow subgroups large.

seit 1558

Questions

Janko group J_4: action matrices not an option

- Known: $n_0(J_4, \mathbb{Z}[\frac{1}{2}]) = 6$.
- Mason (2007) asks whether $n_0(J_4) = 6$.
- To decide, need $H^n(J_4, \mathbb{F}_2)$ for $n \leq 4$.
- Sylow 2-subgroup has order 2^{21}.
- **Action matrices not an option!** Each weighs 550GB.

Monster group M

- Mason, Ganter: 2- and 3-primary parts of $H^4(M, \mathbb{Z})$?
- If non-zero, then $H^3(M, \mathbb{F}_2)$, $H^3(M, \mathbb{F}_3)$ non-zero.
- Sylows have size 2^{46}, 3^{20}.

seit 1558

Cohomology without action matrices?

That's easy . . .

You just need a Gröbner basis for $\mathbb{F}_p P$.

One approach: Power-commutator presentations

- Standard method in computational p-group theory.
- If $|G| = p^n$, then n generators $g_1, \ldots, g_n$.
- Each p^{th} power and each commutator decribed in terms of later generators.
- C.f. Jennings series of P, and Loewy layers of $\mathbb{F}_p P$.
- R. Müller-G.: Turn pc-presentation of P into Gröbner basis for $\mathbb{F}_p P$, with generators in radical.

seit 1558

Does it work for J_4?

Good news

Construction of $\mathbb{F}_2 P$ nearly instantaneous.

- Use GAP for group theory; then construct $\mathbb{F}_2 P$ in Plural from Sage.
- Group algebra has 21 weighted generators; ordering negwdeglex; highest weight 8.

Bad news

Can't even get second term in resolution, let alone the fourth.

- Elimination for kernel of map $(\mathbb{F}_2 P)^5 \to \mathbb{F}_2 P$ takes forever: support explodes.

seit 1558

Potential workaround?

Try presenting $\mathbb{F}_2 P$ with minimal generators (5 rather than 21).

- Need more work to get Gröbner basis for $\mathbb{F}_2 P$.
- Longest standard monomial has length 71.
- Gröbner basis will be shorter.