Computational Group Cohomology: Using SINGULAR in Sage

Simon King
National University of Ireland, Galway
joint work with G. Ellis (NUIG) and D. J. Green (Jena)

Juli 14, 2010

Outline

Group Cohomology

G finite group, p prime dividing $|G|$. $H^*(G) := H^*(G; \mathbb{F}_p)$

- Finitely presentable graded commutative $\mathbb{F}_p$–algebra.
- $\phi : G_1 \to G_2 \rightsquigarrow \phi^* : H^*(G_2) \to H^*(G_1)$,
  $\rightsquigarrow$ restriction $r_U^G : H^*(G) \to H^*(U)$ for $U \leq G$.
- G determines $H^*(G)$ up to isomorphism.

Wanted:

Software, using *general* methods, to compute

- minimal presentation of $H^*(G)$,
- depth, Poincaré series, a–invariants, ...
- higher structures (Massey products, Steenrod action)

for as many finite groups as possible.

Computing cohomology

Topology

Construct *Classifying spaces*. Tailor made. Not algorithmic.

Spectral Sequences

- Lyndon–Hochschild–Serre: extrasp. 2–groups [Quillen 1971]
- Eilenberg–Moore: groups of order 32 [Rusin 1989]

But not general enough, and difficult to implement.

Ring approximations in increasing degree

- Prime power groups: Projective resolutions, general homological algebra.
- Otherwise: Stable element method.

Minimal resolutions for prime power groups

D. Green [2001]: Initial segments of a minimal free $\mathbb{F}_p G$-resolution can be computed using n. c. Gröbner Basis techniques for *finite* $\mathbb{F}_p G$-modules.

- *Negative* monomial orders (for minimality).
  No problem, the algebra is nilpotent.
- *Two-speed* replacement rules: *Type I* precedes *Type II*.
  Idea: Type I is for $\mathbb{F}_p G$, Type II is for $\mathbb{F}_p G$-modules.

Resolutions for *p*-groups are computed by C-programs of D. Green.
Could Letterplace do the job as well?

Stable element method (Cartan–Eilenberg)

If $U < G$ contains a Sylow p-subgroup of G, then r_U^G is injective.

Stability under $g \in G$

Let $c_g : H^*(U) \to H^*(U^g)$ be induced by conjugation with g^{-1}.
$x \in H^*(U)$ is stable under g $:\iff$ $\mathrm{r}^U_{U\cap U^g}(x) = \mathrm{r}^{U^g}_{U\cap U^g}(c_g^*(x))$

Characterisation of $H^*(G)$ as subring of $H^*(U)$

An element of $H^*(U)$ is in $\mathrm{r}_U^G(H^*(G))$ if and only if it is stable under double coset representatives of $U \setminus G/U$.

GAP bug: After catching 200 GAP errors, one runs into recursion depth trap.

Cue SINGULAR!

Next step of a ring approximation

Let $\alpha_n : \tau_n H^*(G) \to H^*(G)$ the degree-n-approximation.

- Compute standard monomials of $\tau_n H^*(G)$ in degree-$(n+1)$.
- Compute $\alpha_n(\tau_n H^{n+1}(G))$ using a resolution / a computation in $H^*(U)$.
- Comparison of $\alpha_n(\tau_n H^{n+1}(G))$ with $\tau_n H^{n+1}(G)$ reveals degree-$(n+1)$ relations of $H^*(G)$.
- Comparison of $H^{n+1}(G)$ with $\alpha_n(c)$ reveals degree-$(n+1)$ generators of $H^*(G)$.

SINGULAR provides the Gröbner bases.

... of course much faster than self made implementation.

Implementing the Stable Elements method

Let $P < G$ be a Sylow p-subgroup and
$P = U_0 < U_1 < \ldots < U_k = U < G$ a subgroup tower.
Shall we represent $H^*(G) < H^*(P)$ in terms of a resolution for P?
No! Computing resolutions is expensive, and the required degree for $H^*(G)$ is much higher than for $H^*(P)$.

Recursive approach: We know $H^*(U)$ etc.!

- Represent the rings $H^*(U)$ and $H^*(U \cap U^g)$ and the maps $\mathrm{r}^{U}_{U \cap U^g}$, $\mathrm{r}^{U^g}_{U \cap U^g}$ and c_g in SINGULAR.
- Compute $H^{n+1}(G)$ as the stable subspace of $H^{n+1}(U)$.
- Proceed from $\tau_n H^*(G)$ to $\tau_{n+1} H^*(G)$ as sketched above.

A memory leak

Formulating the stability conditions in degree n requires mapping a basis of $H^n(U)$. Mapping ideals reveals a leak:

```
> ring r = 2,(x(1..5)),dp;
> ideal I = maxideal(7);
> ideal J;
> int i;
> map m = r,x(1)-x(2),x(2)-x(3),x(3)-x(4),x(4)-x(5),x(5)-x(1);
> for (i=1;i<=100;i++)J=m(I); print(memory(2));
1183744
1708032
1713632
1721576
1729520
1737464
...
9333544
9336192

9338840
```

$\rightsquigarrow$ Map one polynomial after the other, but that's slower.

Interface overhead

Two ways to solve the stability conditions:

1. Ship lists of coefficients from SINGULAR to Sage, formulate and solve linear equations, ship the result back to SINGULAR. The interface is a serious bottle neck!
2. Keep all data in SINGULAR and solve conditions by interreduction.
   Much faster, but memory consumption (apparently no leak) is a problem.

$\rightsquigarrow$ Would be nice to be able to use `libSingular` – but we'd need graded commutative rings, and we'd like to use library methods in `libSingular` (already done?).

Benson's Completeness criterion

Need to test whether $\alpha_n : \tau_n H^*(G) \to H^*(G)$ is an isomorphism.

J. F. Carlson [$\sim$ 2000]

Complicated criterion that relies on a conjecture

D. J. Benson [2004]

- If n is big enough, *filter regular parameters* $\mathcal{P}$ for $H^*(G)$ can be constructed in $\tau_n H^*(G)$.
- Using the *filter degree type* of $\mathcal{P}$, compute upper bound α for the regularity of $\tau_n H^*(G)$.
- If $n > \alpha + \sum_{\zeta \in \mathcal{P}} (|\zeta| - 1)$ then α_n is isomorphism.

Problems: Computation of filter degree type; parameter degree

Modified Benson criterion

D. Green, S. K. [2009]

- For p-groups: Improved construction of filter regular parameters (smaller degrees).
- Existence result for filter regular parameters $\mathcal{P}'$ of $\tau_n H^*(G;k)$ in small degrees, for some finite extension field k of $\mathbb{F}_p$.
- If $n > \alpha + \sum_{\zeta\in\mathcal{P}'}(|\zeta|-1)$ then α_n is isomorphism.

$G = P = \mathrm{Syl}_2(Co_3)$ (order 1024)

Benson: Parameter degrees 8, 12, 14, 15 (applies in degree 46).
Our construction: Parameter degrees 8,4,6,7 (applies in degree 22).
Existence proof: Parameter degrees 8,4,2,2 over finite extension field. We detect completion in degree 14, which is perfect.

How to find filter regular parameters

From maximal elementary abelian subgroups...

Dickson invariants: Explicit formula for elements $\zeta_{i,V} \in H^*(V)$ for all maximal p-elementary abelian subgroups $V < G$.
Degree grows like $p^{rk_p(G)}$ (Benson)
or like $p^{rk_p(G)-rk(C(G))}$ (Green – K. if G is p-group)
These elements simultaneously lift to elements $\zeta_i \in H^*(G)$ that form a filter-regular HSOP.

... to elements $\zeta_i \in \tau_n H^*(G)$

If $n \geq \deg(\zeta_{i,V})$, then we may lift by linear algebra.
For $n << \deg(\zeta_{i,V})$: May use SINGULAR.
Intersect full preimages of restriction maps. Hand-made for $p > 2$.
Wish SINGULAR had *graded-commutative* rings!

Constructive improvements

If a parameter is decomposable: Replace it by a small factor.
The last parameter can be replaced by any other (smaller) parameter.
The result is still a filter regular HSOP!

Inconstructive improvements

If $\tau_n H^*(G)/\langle\zeta_1, \ldots, \zeta_i\rangle$ is finite over degree-d standard monomials: There is a finite field extension k of $\mathbb{F}_p$, so that $H^*(G, k)$ has a f.r. HSOP formed by $\zeta_1, \ldots, \zeta_i$ and elements of degree d.

Testing filter regularity using SINGULAR

Need to compute annihilators. Computing quotients hand-made, since crashes happened for $p > 2$.
Experimental: Use Hilbert-driven computations for $p = 2$.

Criteria without filter regularity

P. Symonds [2009]

Let $\mathcal{P} \subset \tau_n H^*(G)$ yield parameters for $H^*(G)$.
If $n > \sum_{\zeta\in\mathcal{P}} (|\zeta| - 1)$ and $\tau_n H^*(G)$ is generated in degree $\leq n$ as a module over $\langle\langle\mathcal{P}\rangle\rangle$ then α_n is an isomorphism.

S. K. [2010]: Criterion for non prime power groups

1. If $H^*(U)$ is generated in degree $\leq n$ as a module over $\mathrm{im}(\mathrm{r}_U^G \circ\alpha_n)$ then α_n is surjective.
   No need to compute stable subspace in degree $> n$!
2. Let α_n be surjective, $\exists$ parameters $\mathcal{P}'$ of $\tau_n H^*(G; k)$, $n \geq N = \sum_{\zeta\in\mathcal{P}'} |\zeta| - depth(H^*(U; \mathbb{F}_p))$.
   α_n is isomorphism iff $p(\tau_n H^*(G), t) \cdot \prod_{\zeta\in\mathcal{P}'} (1 - t^{|\zeta|})$ is a polynomial of degree $\leq N$. Idea due to Peter Symonds.

Computational results with our optional SPKG

NEEDS REVIEW! Hint...

All 267 groups of order 64 and all 2328 groups of order 128

Order 64 first done by J. Carlson [1997-2001, 8 months comp. time].
We need about 30 minutes for order 64, about 2 months for order 128.

Interesting non prime power groups

http://www.nuigalway.ie/maths/sk/Cohomology/rings/
Modular cohomology for different primes of (among others)

- Co_3: $H^*(Co_3; \mathbb{F}_2)$ is Cohen-Macaulay. Use tower of 4 subgroups!
- HS, Janko groups (not J_4), Mathieu groups (not M_{24})
- McL: correcting result of Adem-Milgram
- $Sz(8)$: minimal presentation of $H^*(Sz(8); \mathbb{F}_2)$ has 102 generators of maximal degree 29 and 4790 relations of maximal degree 58.

SINGULAR wishlist

Some of it may already be in the devel version.

- Student project: Implement Green's algorithm in Letterplace.
- Fix the leak in mapping ideals.
- Genuine graded commutative rings (with dim, Hilbert-driven approach, kernel/preimage...)
- `libPlural`
- Usage of SINGULAR library functions on `libSingular`.
- Faster transition of SINGULAR improvements to Sage.

THANK YOU FOR YOUR ATTENTION!
(and for implementing the wishlist...)