Computing group cohomology rings from the Lyndon-Hochschild-Serre spectral sequence

Graham Ellis

Mathematics Department, National University of Ireland, Galway, Ireland

Paul Smith [1]

Mathematics Department, National University of Ireland, Galway, Ireland

Abstract

We describe a method for computing presentations of cohomology rings of small finite p-groups. The description differs from other accounts in the literature in two main respects. First, we suggest some techniques for improving the efficiency of the obvious linear algebra approach to computing projective resolutions over a group algebra. Second, we use an implementation of the multiplicative structure of the Lyndon-Hochschild-Serre spectral sequence for determining how much of a projective resolution needs to be computed in order to obtain a presentation of the cohomology ring.

Key words:
Computational algebra, cohomology rings, finite p-groups, kernels of derivations
1991 MSC: 20J06

[1] This author was supported by Marie Curie fellowship MTKD-CT-2006-042685
Email addresses: graham.ellis@nuigalway.ie (Graham Ellis), pas1001@cantab.net (Paul Smith).
URL: http://hamilton.nuigalway.ie (Graham Ellis).

1 Introduction

A standard approach to calculating the cohomology ring $H^*(G, \mathbb{F}_p)$ of a finite group G with coefficients in the field $\mathbb{F}_p$ of p elements is to first calculate the cohomology $H^*(Syl_p(G), \mathbb{F}_p)$ of a Sylow p-subgroup and then use the result (attributed to J. Tate in [3]) that $H^*(G, \mathbb{F}_p)$ is isomorphic to the subring of G-stable elements in $H^*(Syl_p(G), \mathbb{F}_p)$. If the Sylow subgroup is not too large then, for any given $N \geq 0$, one can use elementary linear algebra on a computer to describe

$$H^*_N(Syl_p(G), \mathbb{F}_p) = H^*(Syl_p(G), \mathbb{F}_p)/H^{>N}(Syl_p(G), \mathbb{F}_p)$$

as a finite dimensional structure constant algebra. It is then straightforward to obtain a presentation of $H^*_N(Syl_p(G), \mathbb{F}_p)$ as a graded commutative algebra (or commutative algebra when $p = 2$). Removing all relations of degree $> N$, one obtains a presentation of an infinite dimensional graded commutative algebra $\hat{H}^*_N(Syl_p(G), \mathbb{F}_p)$. A result discovered independently by Golod [11], Venkov [19] and Evens [8] implies that $\hat{H}^*_N(Syl_p(G), \mathbb{F}_p) \cong H^*(Syl_p(G), \mathbb{F}_p)$ for sufficiently large N.

Our aim in this article is to give a self-contained account of the efficient computation of a ring presentation for $H^*(Syl_p(G), \mathbb{F}_p)$. The account overlaps with those in [2,12], but differs in the following three respects. (i) We suggest some efficiencies that can be applied to the obvious linear algebra approach (taken for instance in [2]) to computing the structure constant algebra $H^*_N(Syl_p(G), \mathbb{F}_p)$. However, even with these efficiencies it seems that the linear algebra approach is probably less powerful than the non-commutative Gröbner basis methods of [12]. (ii) We demonstrate that a constructive version of a homological perturbation lemma of Wall [20] can be used to automate computations of the additive and multiplicative structure of the Lyndon-Hochschild-Serre spectral sequence. These computations are used to determine a value of N sufficient for obtaining a presentation of $H^*(Syl_p(G), \mathbb{F}_p)$. The additive structure of the spectral sequence and the structure constant algebra $H^*_N(Syl_p(G), \mathbb{F}_p)$ have been implemented by the first author for all primes p. The multiplicative structure on the spectral sequence, and a function for determining suitably large N, have been implemented by the second author for the prime p equal to 2 using SINGULAR's Gröbner basis techniques for commutative rings; this implementation could be routinely extended to primes $p > 2$ using SINGULAR's tools for Gröbner bases in graded commutative rings but this has not yet been done. (iii) We illustrate computational functionality and performance of the approach using functions implemented as part of the first author's homological algebra package HAP [5].

Other approaches to determining sufficiently large N are given in [2][1] and have been used with the MAGMA system to determine the mod 2 cohomology

rings of all groups of order 64. In fact MAGMA contains, as standard, functions for calculating a presentation for the ring $\hat{H}^*_N(Syl_p(G), \mathbb{F}_p)$ (though not for determining suitable N). Recently a variant of the approach in [1] has been used to compute the rings for all groups of order 128 [13][15].

A major impetus for the paper was the following paragraph by J. Carlson [2]:

> "... the cohomology ring, $H^*(G, \mathbb{F})$, is an infinite object but any calculation of it is necessarily finite. So the question is: when do we know that we are done? One method would be to check the calculated answer against various spectral sequences that might be available. For groups which are not too large, this method is not impractical. Indeed, Rusin's [17] impressive calculations of the mod-2 cohomology rings of the 51 groups of order 32 were performed using the Eilenberg-Moore spectral sequence. However, many of the cohomology rings of the 267 groups of order 64 are much more complicated. Indeed, the method is not very appealing since there are choices to be made in the spectral sequences that always seem ad hoc and the calculations must be completed by hand. It would be much better to have a method which could be implemented on a computer."

Our HAP [5] implementation is an extension to the GAP system for computational algebra and can be used to obtain results such as the following presentation of the mod 2 cohomology ring $H^*(Syl_2(M_{12}), \mathbb{F}_2)$ for the sylow 2-subgroup of the Mathieu group M_{12}.

```
gap> P := SylowSubgroup(MathieuGroup(12), 2);;
gap> Mod2CohomologyRingPresentation(P);
Graded algebra GF(2)[ x_1, x_2, x_3, x_4, x_5, x_6, x_7 ] /
[ x_2*x_3, x_1*x_3, x_3*x_4, x_1^2*x_2+x_1*x_2^2+x_2^3+x_2*x_4+
  x_2*x_5, x_2^2*x_4+x_2*x_6, x_1^2*x_4+x_1*x_6+x_2*x_6+x_4^2+
  x_4*x_5, x_2^4+x_1*x_2*x_5+x_1*x_6+x_2*x_6+x_4*x_5,
  x_1^2*x_6+x_1*x_2*x_6+x_2^2*x_6+x_2*x_4*x_5+x_4*x_6,
  x_1*x_2^4+x_2^5+x_2^3*x_5+x_1*x_2*x_6+x_1*x_4*x_5+x_2*x_4*x_5+
  x_2*x_5^2+x_4*x_6, x_2^3*x_6+x_1*x_4*x_6+x_1*x_5*x_6+
  x_3^2*x_7+x_3*x_5*x_6+x_4^2*x_5+x_6^2
 ] with indeterminate degrees [ 1, 1, 1, 2, 2, 3, 4 ]
```

The group $Syl_2(M_{12})$ has order 64. Some larger groups can be handled by the implementation. For example, it takes about 25 minutes on a 2.66GHz Intel PC with 2Mb of memory to compute the (well-known) Poincaré series for the dihedral group of order 4096.

The implementation [5] can, in principle, be used to compute the structure constant algebra $H^*_N(Syl_p(G), \mathbb{F}_p)$ for any prime p and finite group G. For $p = 2$ the implementation can also, in principle, compute a presentation for $H^*(Syl_2(G), \mathbb{F}_2)$. Our algorithm for determining a presentation works for ar-

bitrary primes but, as yet, is not implemented for $p \geq 3$.

The implementation [5] can also be used to make some mod p cohomology computations for non prime-power groups. For instance, the following computes a rational function whose coeficient of x^n equals the dimension of $H^n(PSL_5(\mathbb{F}_2), \mathbb{F}_3)$ for at least all $0 \leq n \leq 20$. (In the case of non prime-power groups the implementation does not yet guarantee equality for all $n \geq 0$.)

```
gap> N:=20;; PoincareSeriesPrimePart(PSL(5,2),3,N);
(x^8-2*x^7+3*x^6-3*x^5+3*x^4-3*x^3+3*x^2-2*x+1)/
(x^10-2*x^9+3*x^8-4*x^7+4*x^6-4*x^5+4*x^4-4*x^3+3*x^2-2*x+1)
```

The paper is organized as follows. In Section 2 we describe a standard linear algebraic approach to computing the ring $H^*_N(Syl_p(G), \mathbb{F}_p)$. Our description emphasises the role of contracting homotopies as a means of removing seemingly ad hoc choices from the implementation. In Section 3 we describe a memory efficient method for performing Gaussian elimination in a vector space endowed with the structure of a free $\mathbb{F}G$-module. A constructive version of a lemma of Wall [20] is used in Section 4 to determine the differentials in the Lyndon-Hochschild-Serre spectral sequence. In Section 5 we give a Gröbner basis method for computing the homology of a page in the spectral sequence. Sections 4 and 5 yield a computer method for choosing a value of N for which $\hat{H}^*_N(Syl_p(G), \mathbb{F}_p) = H^*(Syl_p(G), \mathbb{F}_p)$; the method is different to the those described by Carlson [2] and Benson [1] and has been implemented by the second author in GAP (for $p = 2$) with calls to SINGULAR [14]. This part of the implementation together with the experimental results in Section 6 form the second author's contribution to the paper.

Throughout we use both $\mathbb{F}$ and $\mathbb{F}_p$ to denote the field of p elements and $\mathbb{K}$ to denote an arbitrary integral domain.

2 Computing $H^*_N(Syl_p(G), \mathbb{F}_p)$

The first N terms of a free $\mathbb{K}G$-resolution R^G_* of $\mathbb{K}$ can be represented on a computer by storing:

- the $\mathbb{K}G$-rank of the kth free module R^G_k $(k \leq N)$.
- the image of the ith free $\mathbb{K}G$-generator of R^G_k under the boundary homomorphism $d_k \colon R^G_k \to R^G_{k-1}$ $(k \leq N)$.
- the image of the ith free $\mathbb{K}$-generator of R^G_k under a contracting homotopy $h_k \colon R^G_k \to R^G_{k+1}$ $(0 \leq k \leq N-1)$.

The contracting homotopy satisfies, by definition, $h_{k-1}d_k + d_{k+1}h_k = 1$ and needs to be specified on a set of free $\mathbb{K}$-module generators of R^G_k since it is not G-equivariant. The homotopy can be used to make algorithmic the following frequent element of choice.

> *For $x \in \ker(d_k\colon R^G_k \to R^G_{k-1})$ choose an element $\tilde{x} \in R^G_{k+1}$ such that $d_{k+1}(\tilde{x}) = x$.*

One sets $\tilde{x} = h_k(x)$. In particular, for any group homomorphism $\phi\colon G \to G'$, the homotopy provides an explicit induced ϕ-equivariant chain map $\phi_*\colon R^G_* \to R^{G'}_*$. The homotopy can also be used to construct the composition product in cohomology.

For a small group G one can naively represent an element of the group ring $\mathbb{K}G$ as a vector of length $|G|$ over $\mathbb{K}$. An element in a free $\mathbb{K}G$-module $(\mathbb{K}G)^r$ can be represented as a vector of length $r \times |G|$ over $\mathbb{K}$. To compute a free $\mathbb{K}G$-resolution R^G_* of $\mathbb{K}$ one can set $R^G_0 = \mathbb{K}G$, define $d_0\colon \mathbb{K}G \to \mathbb{K}$, $\Sigma\lambda_g g \mapsto \Sigma\lambda_g$, and then recursively

(1) determine a $\mathbb{K}$-basis for $\ker d_n$ (using Gaussian elimination if $\mathbb{K}$ is a field, and Smith Normal Form if $\mathbb{K} = \mathbb{Z}$),
(2) determine a small subset $\{v_1, \ldots, v_r\} \subset \ker d_n$ whose $\mathbb{K}G$-span equals $\ker d_n$,
(3) set $R^G_{n+1} = (\mathbb{K}G)^r$,
(4) define $d_{n+1}\colon (kG)^r \to R^G_n$ by sending the ith free generator to v_i.

The construction of a contracting homotopy $h_n\colon R^G_n \to R^G_{n+1}, x \mapsto \tilde{x}$ essentially boils down to solving a matrix equation $d_{n+1}(\tilde{x}) = x$ where $\tilde{x}$ is unkown and x is a known vector in the image of d_{n+1}. The most costly part of the recursive procedure is Step 2. If $\mathbb{K} = \mathbb{F}$ and if G is a p-group then the radical of $\ker d_n$ is the vector space spanned by vectors $v - g \cdot v$ where v ranges over an $\mathbb{F}$-basis for $\ker d_n$ and g ranges over generators for G; any basis for the complement of the radical yields a minimal set $\{v_1, \cdots v_r\}$ with $\mathbb{F}G$-span equal to $\ker d_n$. Even when G is not a p-group this method can be used to find a set whose $\mathbb{F}P$-span equals $\ker d_n$, where P is a Sylow p-subgroup of G; one can then use naive methods to reduce the size of this set to a smaller one with $\mathbb{F}G$-span equal to $\ker d_n$. (Other, more elaborate, methods for constructing free $\mathbb{K}G$-resolutions for large or infinite groups G and for $\mathbb{K} = \mathbb{Z}$ are described in [6][7].)

Having constructed a free $\mathbb{K}G$-resolution of $\mathbb{K}$ with contracting homotopy, it is straighforward to implement routines for computing $\mathrm{Ext}^n_{\mathbb{K}G}(\mathbb{K}, \mathbb{K})$ and for computing the composition product $\mathrm{Ext}^m_{\mathbb{K}G}(\mathbb{K}, \mathbb{K}) \times \mathrm{Ext}^n_{\mathbb{K}G}(\mathbb{K}, \mathbb{K}) \to \mathrm{Ext}^{m+n}_{\mathbb{K}G}(\mathbb{K}, \mathbb{K})$. We are particularly interested in $H^n(G, \mathbb{F}) = \mathrm{Ext}^n_{\mathbb{F}G}(\mathbb{F}, \mathbb{F})$.

The above discussion underlies functions for computing the graded structure constant algebra $H^*_N(Syl_p(G), \mathbb{F}_p)$ which have been implemented in [5]. As an indication of the (limited) potential of these functions, we mention that it takes around thirty minutes to compute structure constants for the ring $H^*_{12}(Syl_2(M_{23}), \mathbb{F}_2)$ and determine a minimal set of eighteen generators: three in dimension 1, two in degree 2, one in degree 3, three in degree 4, three in degree 5, two in degree 6, one in degree 7 and three in degree 8.

3 Gaussian elimination with group actions

Let G be a finite p-group. The representation of free $\mathbb{F}G$-modules as vector spaces over $\mathbb{F}$ can require significant amounts of memory. Consider for instance the group $G = Syl_2(M_{23})$ of order 128. A minimal free $\mathbb{F}_2G$-resolution R^G_* has 445 free generators in degree 19 and 508 free generators in degree 20. Thus at least $445 \times 508 \times 128^2/2^{23} = 442$Mb are needed to represent the boundary homomorphism $d_{20}\colon R^G_{20} \to R^G_{19}$ as an $\mathbb{F}_2$-homomorphism and even more are needed to compute it. The implementation in [5] just manages to compute d_{20} on a processor with 2GB of memory.

A G-equivariant linear homomorphism $d\colon (\mathbb{F}G)^n \to (\mathbb{F}G)^m$ is determined by its value

$$d(e_j) = a_{1j}f_1 + a_{2j}f_2 + \cdots + a_{mj}f_m$$

on generators $e_1, \ldots, e_n$ for the free module $(\mathbb{F}G)^n$ (where f_i are generators for $(\mathbb{F}G)^m$ and $a_{ij} \in \mathbb{F}G$). The equivariant homomorphism is represented by an $m \times n$ matrix $A = (a_{ij})$ which is a factor of $|G|$ smaller than the matrix needed to represent d as a non-equivariant homomorphism. In order to benefit from the smaller representation we need an efficient equivariant method for computing a minimal set of $\mathbb{F}G$-generators for the kernel of d.

One recursive approach to computing a minimal generating set for the $\mathbb{F}G$-module $\ker d$ involves the $\mathbb{F}G$-module π generated by the m elements $a_{i1} \in \mathbb{F}G$ in the first column of A. Viewing π as an $\mathbb{F}$-subspace of $\mathbb{F}^{|G|}$ we can use Gaussian elimination to find a linearly independent susbet $\{a_{i1}\}_{i\in I}$ of the first column which constitutes an $\mathbb{F}$-basis for the complement of $\mathbb{I}G \cdot \pi$ where $\mathbb{I}G$ is the kernel of the augmentation map $\mathbb{F}G \to \mathbb{F}$. Therefore $(a_{i1})_{i\in I}$ is a minimal $\mathbb{F}G$-generating set for π. By re-ordering rows if necessary, we can assume that $I = \{1, 2, \ldots, t\}$. We can then take $\mathbb{F}G$-linear combinations of the first t rows of A from subsequent rows to produce a new matrix (a'_{ij}) such that $a'_{i1} = 0$ for $t + 1 \leq i \leq m$. Form a matrix E whose rows are an $\mathbb{F}$-basis for the $\mathbb{F}G$-span of the first t rows in A. The matrix E involves at most $tn|G|^2 \log_2(p)$ bits of information and so we should be able to use Gaussian elimination to reduce E to echelon form. Let $e_{1*}, \ldots, e_{t'*}$ be an $\mathbb{F}G$-generating set for the $\mathbb{F}$-span of those rows of the echelon form of E which are zero in the first $|G|$ coordinates.

Let A' be the matrix obtained by appending to (a'_{ij}) the vectors $e_{1*}, \ldots, e_{t'*}$. For $w \in (\mathbb{F}G)^n$ we have $Aw = 0$ if and only if $A'w = 0$. For convenience we decompose A' into submatrices B, C, D as follows.

$$A' = \left(\begin{array}{c|ccc} a_{11} & a_{12} & \cdots\cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{t1} & a_{t2} & \cdots\cdots & a_{tn} \\ \hline 0 & a'_{t+1,2} & \cdots\cdots & a_{t+1,n} \\ \vdots & \vdots & & \vdots \\ 0 & a'_{m,2} & \cdots\cdots & a_{m,n} \\ 0 & e_{12} & \cdots\cdots & e_{1n} \\ \vdots & \vdots & & \vdots \\ 0 & e_{t'2} & \cdots\cdots & e_{t'n} \end{array}\right) = \left(\begin{array}{c|c} B & C \\ \hline 0 & D \end{array}\right)$$

Using the canonical isomorphism $(\mathbb{F}G)^n \cong \mathbb{F}G \oplus (\mathbb{F}G)^{n-1}$ the matrices B and D correspond to module homomorphisms $d_B\colon \mathbb{F}G \to (\mathbb{F}G)^t$ and $d_D\colon (\mathbb{F}G)^{n-1} \to (\mathbb{F}G)^{m-t+t'}$. By recursion we can find minimal $\mathbb{F}G$-generating sets X_B, X_D for $\ker d_B$ and $\ker d_D$ respectively. Any $x \in X_B$ can be extended to a generator $\overline{x} = (x, 0, \ldots, 0) \in \ker(d)$. We can also extend any $x \in X_D$ to a generator $\overline{x} \in \ker(d)$ since the echelon form of E provides an explicit injective homomorphism $\ker d_D \to \ker d$ which we use to map $x \in X_D$ to $\overline{x} \in \ker(d)$. The set $X = \{\overline{x}\colon x \in X_B \cup X_D\}$ is a generating set for the module $\ker d$.

The generating set X will not in general be minimal. One possibility is to use a version of G-reduction (see below) to minimize it. Alternatively, X can be used to construct minimal $\mathbb{F}G$-resolutions as follows. Suppose we have k terms of a minimal $\mathbb{F}G$-resolution R^G_* of $\mathbb{F}$. Using the preceding method we can extend the resolution to a possibly non-minimal resolution with $k+2$ terms.

$$\oplus_{X'}\mathbb{F}G \to \oplus_X \mathbb{F}G \to R^G_k \to R^G_{k-1} \to \cdots$$

The extended resolution can then be used to compute $H_{k+1}(G, \mathbb{F})$. The $\mathbb{F}$-rank of $H_{k+1}(G, \mathbb{F})$ is equal to the $\mathbb{F}G$-rank of the module R^G_{k+1} in a minimal resolution, and using this we can eliminate redundant generators from X to construct $k+1$ terms of a minimal resolution.

A direct implementation of the above recursive G-equivariant method for finding module generators of the kernel of $d\colon (FG)^n \to (FG)^m$ runs into the following problem. The recursion produces a sequence of $\mathbb{F}G$-matrices $A, A', A'', \ldots, A^{(i)}, \ldots$ each representing a homomorphism $d^{(i)}\colon (FG)^n \to (FG)^{m_i}$ with kernel equal to $\ker d$. The problem is that the number of rows of $A^{(i)}$ can

become prohibitively large. To overcome this we introduce the following definition.

Definition. A matrix A over $\mathbb{F}G$ will be said to be *G-reduced* if, for each column of A, those non-zero entries of the column that are the first non-zero entry of their row form a *minimal* generating set for some $\mathbb{F}G$-submodule of the group algebra $\mathbb{F}G$.

Using just linear algebra in the vector space $\mathbb{F}^{|G|} \cong \mathbb{F}G$, a sequence of row operations can be applied to any $\mathbb{F}G$-matrix A to convert it to a G-reduced form. Note that if A is in G-reduced form then the number of rows in A is crudely bounded by nt where n is the number of columns of A and t is the maximum number of elements needed to generate a submodule of $\mathbb{F}G$. (For the dihedral group of order 32 one can directly compute $t = 2$. For $G = Syl_2(M_{23})$ of order 128 we are unable to compute t; considering just the modules in the radical series of G shows that $t \geq 16$ and this may well be an accurate bound on t.)

When implementing the above recursive method for finding generators of $\ker d$ each $A^{(i)}$ can be converted to G-reduced form. This should overcome the potential problem of a prohibitively large number of rows.

The above method has not yet been fully implemented. However, some of its ideas have been implemented by the second author in [18] and used on a computer with 2Gb available to obtain 24 terms of a minimal $\mathbb{F}_2G$-resolution for $G = Syl_2(M_{23})$. With the same amount of memory the method of Section 2 can only compute 20 terms (and requires 5Gb of memory to compute 24 terms).

4 Computing spectral sequence differentials

Suppose that G is a group, possibly infinite, for which we have some $\mathbb{K}G$-resolution

$$S_*: \cdots \to S_n \to S_{n-1} \to \cdots \to S_0 \to \mathbb{K},$$

but that S_* is not $\mathbb{K}G$-free. Suppose that for each m we have a free $\mathbb{K}G$-resolution A_{m*} of the module S_m.

$$A_{m*}: \to A_{m,n} \to A_{m,n-1} \to \cdots \to A_{m,0} \to S_m.$$

The following constructive version of a lemma of Wall [20] was given in [7] and explains how we can compute a free $\mathbb{K}G$-resolution R^G_* of $\mathbb{K}$ with $R^G_n =$

$\bigoplus_{p+q=n} A_{p,q}$.

Lemma 1 *[20][7] Let A_{pq} $(p,q \geq 0)$ be a bigraded family of free $\mathbb{K}G$-modules. Suppose that there are $\mathbb{K}G$-module homomorphisms $d_0 \colon A_{p,q} \to A_{p,q-1}$ such that $(A_{p,*}, d_0)$ is an acyclic chain complex for each p. Set $S_p = H_0(A_{p,*}, d_0)$ and suppose further that there are $\mathbb{K}G$-homomorphisms $\delta \colon S_p \to S_{p-1}$ for which (S_*, δ) is an acyclic chain complex. Then there exist $\mathbb{K}G$-homomorphisms $d_k \colon A_{p,q} \to A_{p-1,q+k-1}$ $(k \geq 1, p > k)$ such that*

$$d = d_0 + d_1 + \cdots \colon R_n^G = \bigoplus_{p+q=n} A_{pq} \to R_{n-1}^G = \bigoplus_{p+q=n-1} A_{pq}$$

is a differential on a free $\mathbb{K}G$-resolution of $\mathbb{K}$. Suppose that there exist $\mathbb{K}$-homomorphisms $h_0 \colon A_{p,q} \to A_{p,q+1}$ such that $d_0 h_0 d_0(x) = d_0(x)$ for all $x \in A_{p,q+1}$. Then we can construct d_k by first lifting δ to $d_1 \colon A_{p,0} \to A_{p-1,0}$ and recursively defining $d_k = -h_0(\sum_{i=1}^{k} d_i d_{k-i})$ on free generators of the module A_{pq}. Furthermore, if $H_0(S_*) \cong \mathbb{K}$ and each S_p is a free $\mathbb{K}$-module, we can construct $\mathbb{K}$-module homomorphisms $h \colon R_n^G \to R_{n+1}^G$ satisfying $dhd(x) = d(x)$ by setting $h(a_{pq}) = h_0(a_{pq}) - hd^+h_0(a_{pq}) + \epsilon(a_{pq})$ for free generators a_{pq} of the module A_{pq}. Here $d^+ = \sum_{i=1}^{p} d_i$ and, for $q \geq 1$, $\epsilon = 0$. For $q = 0$ we define $\epsilon = h_1 - h_0 d^+ h_1 + hd^+ h_1 + hd^+ h_0 d^+ h_1$ where $h_1 \colon A_{p,0} \to A_{p+1,0}$ is a $\mathbb{K}$-linear homomorphism induced by a contracting homotopy on S_*.

When $\mathbb{K} = \mathbb{Z}$ or $\mathbb{K} = \mathbb{F}$ this lemma provides a practical divide-and-conquer strategy for computing a free $\mathbb{K}G$-resolution R_*^G for a group G posessing a normal subgroup Z. We set $Q = G/Z$ and compute a free $\mathbb{K}Q$-resolution S_*^Q of $\mathbb{K}$, and a free $\mathbb{K}Z$-resolution T_*^Z of $\mathbb{K}$. The resolution S_*^Q is a non-free $\mathbb{K}G$-resolution. A free $\mathbb{K}G$-resolution A_{m*} for S_m^Q can be constructed as $A_{m*} = \bigoplus_{X_m}(T_* \otimes_{\mathbb{K}Z} \mathbb{K}G)$ where X_m is the free $\mathbb{K}Q$-basis for S_m^Q.

(As an aside remark we note that since Lemma 1 constructs a contracting homotopy on the resolution, the divide-and-conquer strategy can be applied recursively to any finite subnormal sequence $Z_1 \leq Z_2 \leq \cdots \leq G$. For instance, a recursive implementation of Lemma 1 provided in [5] can establish the existence of an 8-dimensional free $\mathbb{Z}G$-resolution (all modules of degree ≥ 9 being trivial) for the free nilpotent group $G = G_{2,4}$ of class 4 on two generators. This resolution can be used to show that the integral cohomology ring $H^*(G_{2,4}, \mathbb{Z})$ has 3-torsion in degrees 4 and 5 but no other torsion. The resolution can be used to show that $H^*(G_{2,4}, \mathbb{Z})$ is generated by two classes in degree 1, six classes in degree 2, ten classes in degree 3, eight classes in degree 4 and four classes in degree 5.)

Let G be a group with normal subgroup Z, and let R_*^G be a free $\mathbb{K}G$-resolution R_*^G of $\mathbb{K}$ constructed using Lemma 1. The chain complex $C_* = R_*^G \otimes_{\mathbb{K}G} \mathbb{K}$

obtained by tensoring R_*^G with the trivial module $\mathbb{K}$ admits a filtration

$$F_0C_* \leq F_1C_* \leq F_2C_* \leq \cdots \leq C_*$$

defined by $F_mC_n = \oplus_{p+q=n, p\leq m}(A_{pq} \otimes_{\mathbb{K}G} \mathbb{K})$. This filtration gives rise to the Lyndon-Hochschild-Serre homology spectral sequence.

Let us recall details of the spectral sequence arising from an (arbitrary) filtration. Let $C_* = (C_n, d_n)$ be any chain complex of $\mathbb{K}$-modules. Let F_pC_n be a submodule of C_n (for $p, n \geq 0$). Suppose that each $F_{p-1}C_n$ is a submodule of F_pC_n. Suppose also that the homomorphism $d_n\colon C_n \to C_{n-1}$ restricts to a homomorphism $d_n\colon F_pC_n \to F_pC_{n-1}$ (for $p \geq 0, n \geq 1$). We summarize this situation by saying that we have a *filtration* $F_0C_* \leq F_1C_* \leq F_2C_* \leq \cdots \leq C_*$ on the chain complex C_*.

Define $Z_{p,q}^r = \{a \in F_pC_{p+q} \mid d_{p+q}(a) \in F_{p-r}C_{p+q-1}\}$. Define

$$E_{p,q}^r = \frac{Z_{p,q}^r \ + \ F_{p-1}C_{p+q}}{d_{p+q+1}(Z_{p+r-1,q-r+2}^{r-1}) \ + \ F_{p-1}C_{p+q}}.$$

Thus the elements of $E_{p,q}^r$ are cosets $[a]$ and any such coset can be represented by an element $a \in Z_{p,q}^r$.

There is a homomorphism

$$d_{p,q}^r\colon E_{p,q}^r \to E_{p-r,q+r-1}^r$$

which can be defined as follows. For any element $[a] \in E_{p,q}^r$ choose a representative $a \in Z_{p,q}^r$. Then define

$$d^r([a]) = [d_{p+q}(a)].$$

In this definition it is essential to choose the representative a in $Z_{p,q}^r$. (Suppose that an element $[a] \in E_{p,q}^r$ is represented by $a \in F_pC_{p+q}$ but that a does not lie in $Z_{p,q}^r$. Then, by solving a linear matrix equation, one can find $\epsilon \in F_{p-1}C_{p+q}$ such that $a' = a + \epsilon \in Z_{p,q}^r$. Since $\epsilon \in F_{p-1}C_{p+q}$ one has $[a] = [a']$.) There is an isomorphism

$$E_{p,q}^{r+1} \cong \frac{\ker d_{p,q}^r}{\text{image}\, d_{p+r,q-r+1}^r} \quad .$$

In the case when the filtration arises from a normal subgroup $Z \leq G$ Evens [9] showed that there exists some positive integer ρ such that

$$E_{p,q}^\rho \cong E_{p,q}^\infty \quad (p, q \geq 0).$$

If $\mathbb{K} = \mathbb{F}$ then

$$H_n(G, \mathbb{F}) = \bigoplus_{p+q=n} E_{p,q}^\rho \quad (n \geq 0).$$

For a finite p-group G we have $H_n(G,\mathbb{F}) \cong H^n(G,\mathbb{F})$ for $n \geq 0$. The advantage of working with cohomology is that the cup product $H^p(G,\mathbb{F}) \times H^q(G,\mathbb{F}) \to H^{p+q}(G,F)$ exists and defines the structure of a graded anti-commutative $\mathbb{F}$-algebra on $H^*(G,\mathbb{F})$. In cohomology the Lyndon-Hochschild-Serre spectral sequence arises from a group G, normal subgroup Z, and the resulting filtration of cochain complexes

$$C^* = F^0C^* \geq F^1C^* \geq F^2C^* \geq \cdots$$

defined by $F^mC^n = \oplus_{p+q=n, p\geq m}\mathrm{Hom}_{\mathbb{F}G}(A_{pq},\mathbb{F})$ where $A_{p,q}$ are the components of the $\mathbb{F}G$-resolution of Lemma 1. It is shown in [8] that the cohomology differential

$$d_r^{p,q}\colon E_r^{p,q} \to E_r^{p+r,q-r+1}$$

can be viewed as a derivation of $\mathbb{F}$-algebras $d_r\colon E_r^{*,*} \to E_r^{*,*}$. Since

$$E_{r+1}^{*,*} \cong \frac{\ker d_r}{\mathrm{image}\, d_r}$$

we can compute succesive pages of the cohomology spectral sequence by using Gröbner basis methods to compute kernels and images of derivations (see below). For some integer $\rho \geq 2$ we have that $E_\rho^{*,*} = \mathrm{Gr}H^*(G,\mathbb{F})$ is the graded algebra associated to a filtration on $H^*(G,\mathbb{F})$. This means that $d_r = 0$ for $r > \rho$. It is possible to determine the value of ρ by finding a finite set of generators for the algebra $\ker d_\rho$ and then verifying that $d_r(x)$ is trivial for each generator x and $\rho < r < q+1$ where q is the largest integer for which $E_r^{p,q}$ contains a generator. Additively the associated graded algebra is isomorphic to the $H^*(G,\mathbb{F})$. Although the isomorphism does not in general preserve multiplication it can be used to derive an integer N such that $\hat{H}_N^* \cong H^*(G,\mathbb{F}_p)$.

Indeed, the maximum degree of a minimal generator (resp. relation) of $H^*(G,\mathbb{F})$ is no greater than that of $\mathrm{Gr}H^*(G,\mathbb{F})$. Evens' proof [8] of the finite generation of $H^*(G,\mathbb{F}_p)$ for a finite p-group G uses this fact, with Z equal to a central subgroup of order p, together with induction on the order of G.

To illustrate the idea consider the quaternion group G of order 8. There is a central extension $1 \to C_2 \to G \to C_2 \times C_2 \to 1$ which yields the spectral sequence

$$E_2^* = H^*(C_2 \times C_2,\mathbb{F}) \otimes H^*(C_2,\mathbb{F}) \Longrightarrow H^*(G,\mathbb{F}).$$

By induction on the order of groups we can assume we know that $H^*(C_2 \times C_2,\mathbb{F}) \cong \mathbb{F}[x,y]$ and $H^*(C_2,\mathbb{F}) \cong \mathbb{F}[x]$. Hence $E_2^* \cong \mathbb{F}[x,y,z]$. From the resolution constructed using Lemma 1 the computer can determine values of the derivation $d_2\colon E_2^* \to E_2^*$ on all generators of the ring E_2^*, namely $d_2(x) = d_2(y) = 0$ and $d_2(z) = x^2 + xy + y^2$. Using the method described in Section 5 we can compute

$$E_3^* = \ker(d_2)/\mathrm{image}(d_2) = \mathbb{F}[x,y,z^2]/ < x^2 + xy + y^2 > .$$

The resolution from Lemma 1 yields the differential on E_3^* from which we compute

$$E_4^* = \mathbb{F}[x, y, z^2]/ < x^2 + xy + y^2,\ y^3 > .$$

The computation can be repeated until we are certain that $E_4^* = E_\infty^*$. We then observe that all generators and relations in E_∞^* have degree at most 3. We conclude that $\hat{H}_3^*(G, \mathbb{F}_p) \cong H^*(G, \mathbb{F}_p)$ and we use 3 terms of a projective $\mathbb{F}G$-resolution to compute a presentation for the cohomology ring. In this example the presentation coincides with that for E_4^*.

5 Computing homology of derivations

For convenience we assume that $p = 2$ throughout this section. The extension of the theory to primes $p > 2$ is routine and left to the reader. (We have implemented the theory only for $p = 2$, taking advantage of SINGULAR's tools for Gröbner bases in commutative rings which apply in this case. The SINGULAR system [14] also handles graded commutative rings and could be used to implement the theory for $p \geq 2$.)

Consider the polynomial ring $R = \mathbb{F}[x_1, ..., x_n]$ and let I be an ideal in R. Set $E = R/I$ and suppose that we are given some derivation $d\colon E \to E$ (by which we mean an $\mathbb{F}$-linear homomorphism satisfying $d(uv) = ud(v) + vd(u)$ for $u, v \in E$). Our goal is to compute an ideal $J \leq \mathbb{F}[u_1, ..., u_t]$ for which there is an explicit commutative ring isomorphism

$$\ker(d)/\text{image}(d) \cong F[u_1, ..., u_t]/J\ .$$

This computation is precisely what is needed to recursively determine the infinity page E_∞ of the Lyndon-Hochschild-Serre cohomology spectral sequence.

The kernel of the derivation d is not in general an ideal in E. Therefore we can not directly apply SINGULAR's [14] Gröbner basis functions to obtain a presentation for $\ker(d)$. We need to consider the subring $S = \mathbb{F}[x_1^2, x_2^2, ..., x_n^2]$ in R. The ring S lies in the kernel of d and, moreover, R is a free S-module with basis the 2^n square-free monomials in R.

We can consider the R-module I as an S-module, and we denote this S-module by I_S. A finite generating set X for the R-module I can be converted to a finite generating set X_S for the S-module I_S. The set X_S is the product of X with the set of all square-free monomials. The derivation $d\colon E \to E$ can be viewed as a homomorpism

$$d_S\colon S^{2^n}/I_S \to S^{2^n}/I_S$$

of S-modules. The SINGULAR function `modulo(d,I)` can be used to compute a generating set $Y_S = \{y_1, ..., y_t\}$ for an S-module $K_S \leq S^{2^n}$ that yields an isomorphism $K_S/I_S \cong \ker(d_S)$ of S-modules. (The y_i can be viewed as elements of R.)

We now introduce the polynomial ring $R' = \mathbb{F}[x_1, ...x_n, u_1, ..., u_t]$ and the ideal $K \leq R'$ generated by the set

$$Y = X \cup \{u_1 - y_1, ..., u_t - y_t\} \ .$$

Thus $E = R/I$ is isomorphic to the quotient ring R'/K, and the isomorphism maps generators of $\ker(d)$ to the elements represented by $u_1, ..., u_t$. The SINGULAR function `eliminate(K,X)` can be used to eliminate the variables $x_1, ..., x_n$ from the set Y to produce a set of elements in $\mathbb{F}[u_1, ..., u_t]$ that generates an ideal $J' \leq \mathbb{F}[u_1, ..., u_t]$ with $\mathbb{F}[u_1, ..., u_t]/J \cong \ker(d)$.

If $d^2 = 0$ then the image of d is an ideal in $\ker(d)$ and it is straightforward to extend the generating set for J' so as to generate an ideal J with $\mathbb{F}[u_1, ..., u_t]/J \cong \ker(d)/\text{image}(d)$.

Example. Let $R = \mathbb{F}[x, y]$, $I = \langle xy^2 \rangle$ and consider the derivation $d\colon R/I \to R/I$ defined by $d(x) = 0, d(y) = x$. Then $X = \{xy^2\}$, $S = \mathbb{F}[x^2, y^2]$ and $X_S = \{xy^2, x^2y^2, xy^3, x^2y^3\}$. SINGULAR produces a set $Y_S = \{x^2, y^2, x, y^3\}$ representing S-module generators for $\ker(d)$. We now set $R' = \mathbb{F}[x, y, u_1, u_2, u_3, u_4]$ and consider the ideal $K = \langle xy^2, u_1 - x^2, u_2 - y^2, u_3 - x, u_4 - y^3 \rangle$. SINGULAR eliminates x and y from the generating set for K to produce the ideal $J' = \langle u_3u_4, u_1u_4, u_3^2 + u_1, u_2u_3, u_1u_2, u_2^3 + u_4^2 \rangle$ with $\mathbb{F}[u_1, u_2, u_3, u_4]/J' \cong \ker(d)$. Finally, $d^2 = 0$ and we obtain $\ker(d)/\text{image}(d) \cong \mathbb{F}[u_2, u_4]/\langle u_2^3 + u_4^2 \rangle$. □

When applying the method to large examples, two simple techniques can be used to improve efficiency. First, the generating set for the ideal K can be large and very redundant. This might pose a problem when computing a Gröbner basis for K. Elimination of obvious redundances among the generators of K can help to overcome the problem. Second, in many examples the subring S can be increased in size subject to the constraints that $S \subset \ker(d)$ and R is a free S-module.

6 Experimental results

The second author has used the above methods to re-compute the mod 2 cohomology rings of all groups of order 32 (originaly computed by Rusin [17]) and many of the groups of order 64 (originaly computed by Carlson [2]) on a dual-core 2.66MHz Intel PC with an initial memory cap of 512Mb.

The mod 2 cohomology rings of 48 of the 51 groups of order 32 were computed in a total of 73 seconds, and needed no more than six terms of a resolution and no more than six pages for the spectral sequence to converge. Two further groups (numbers 8 and 44 in the GAP small groups library) required resolutions of length nine and ten pages of the spectral sequence, and needed a total of two minutes for the computation of their cohomology rings. The only problematic group was number 50 in the GAP library. This is an extraspecial group and the resolution and cohomology ring for Q are expensive to compute using the general method of Section 2. For this group the mod 2 cohomology ring required 30 minutes.

Precisely 67 of the 267 groups of order 64 are direct products of smaller groups and their cohomology rings can be obtained quickly as tensor products of the cohomology rings of the smaller groups. The cohomology rings of 135 of the remaining groups were obtained in 38 minutes; these required at most ten pages of the spectral sequence, though most required just six or fewer pages. We have computed the cohomology rings for four further groups and this took a further two hours. We do not yet have results for 39 of the groups of order 64. For 24 of these groups the memory limit of 512Mb was insufficient, either (a) to compute the resolution and cohomology ring for Q and G, or (b) to compute a Gröbner basis (using an elimination ordering) as part of the computation of a ring presentation for the homology of a derivation or a sheet of the spectral sequence. The current version of the code for computing the homology of derivations in the spectral sequence takes a mathematical short cut at one point which may produce an incorrect answer, but once the answer is computed its correctness is tested; for 15 groups this internal test failed and the computation of a sufficiently large N aborted.

Some groups of order greater than 64 can be handled. For example, the (well-known) mod 2 cohomology ring for the dihedral group of order 4096 was easily computed.

A detailed analysis of the computation of the mod 2 cohomology ring for the group $G = Syl_2(M_{12})$ of order 64 is instructive. The spectral sequence calculation required resolutions up to degree 5 for the centre $Z = C_2$ and quotient $Q = G/Z$; it also required the computation of the cohomology ring for Q. It converged at the page $E^6 = E^\infty$. The ring presentation obtained for E^∞ involved relations of largest degree $N = 6$. This value of N was then used to compute the mod 2 cohomology ring $\hat{H}^*_N(Syl_p(G), \mathbb{F}_p) = H^*(G, \mathbb{F})$ as described in Section 2. The complete calculation took roughly 6 seconds and brokes down as follows. The computation of the E^∞ page of the spectral sequence took a small proportion of the total computation time. This is typical, the exceptions coming in cases where the calculation of the homology of the derivation involves very large Gröbner bases requiring considerable time and memory. This example is also typical in that more computation time is devoted

Task	**time (secs)**
Computing resolutions and cohomology rings for Z and Q	2.9
Computing twisted tensor product resolution for G	0.5
Computing spectral sequence derivations	0.2
Computing homologies of derivations	0.3
Other related spectral sequence computations	0.2
Total for computing spectral sequence	**4.1**
Computing 6 terms of a minimal resolution for G	0.5
Computing presentation for $H^*(G, \mathbb{F}_2)$ from the resolution	1.4
Total for computing mod 2 cohomology ring	**6.089**

to determining a suitable integer N than to calculating the presentation for the structure contant algebra $\hat{H}^*_N(G, \mathbb{F})$.

7 Conclusions

The experimental results demonstrate that the standard spectral sequence proof [8] of the finite generation of cohomology rings of finite groups provides a practical alterative algorithm for computing (or verifying previously computed) mod p cohomology rings for many small finite p-groups G. An implementation of the method has been made available as a GAP package, and no knowledge of homological algebra is required by a user wishing to compute cohomology rings with the package. Comparison with the computations in [13] suggests that the spectral sequence method is probably, in many cases, not as efficient as D. Benson's completion criterion given in [1]. Though in some cases the spectral sequence completion criterion yields a lower value of N than that produced by Benson's criterion; this could be useful when dealing with certain large groups. The spectral sequence approach involves an algorithm for computing the homology of a derivation on a graded commutative ring over the field of p-elements. This algorithm, which so far been implemented only for $p = 2$, may be of independent interest.

The generality of the spectral sequence method makes it applicable in other contexts. For example, given a connected CW-space X with $\pi_1 X$ and $\pi_2 X$ finite p-groups and $\pi_n(X) = 0$ for $n \geq 3$, the cohomology spectral sequence of the fibration $K(\pi_2 X, 2) \to X \to K(\pi_1 X, 1)$ can, in principle, be used to determine a presentation for the cohomology ring $H^*(X, \mathbb{F})$. Work on implementing this fibration method is in progress and involves an OpenMath interface developed in [16] between the HAP homological algebra package [5] and the KENZO

system [4] for computational simplicial topology.

References

[1] D.J. Benson, "Dickson invariants, regularity and computation in group cohomology", *Illinois J. Math.* 48(1), (2004), 171-197.

[2] J. Carlson, "Calculating group cohomology: tests for completion", *J. Symbolic Computation*, vol. 31, issue 1-2 (2001), 229-242.

[3] H. Cartan & S. Eilenberg, *Homological Algebra*, Princeton Univ. Press 1956.

[4] X. Dousson, J. Rubio, F. Sergeraert and Y. Siret, The KENZO system for constructive simplicial topology, Institute Fourier, Grenoble, 1999.

[5] G. Ellis, HAP – Homological Algebra programming, Version 1.8 (2008), an official package for the GAP computational algebra system. (`http://www.gap-system.org/Packages/hap.html`)

[6] G. Ellis, "Computing group resolutions", *J. Symbolic Computation* 38 (2004), no. 3, 1077-1118.

[7] G. Ellis, J. Harris and E. Sköldberg, "Polytopal resolutions for finite groups", *J. reine angewandte Mathematik*, 598 (2006) 131-137.

[8] L. Evens, "The cohomology ring of a finite group", *Trans. American Math. Soc.* 101 (1961), 224-239.

[9] L. Evens, "The spectral sequence of a finite group extension stops", *Trans. American Math. Soc.* 212 (1975), 269-277.

[10] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.9; 2006. (`http://www.gap-system.org`)

[11] E. Golod, "The cohomology ring of a finite p-group", *Dokl. Akad. Nauk SSSR* 125 (1959), 703-706.

[12] D.J. Green, Gröbner bases and the computation of group cohomology, Lecture Notes in Math. 1828, (Springer 2004), pp138.

[13] D.J. Green & S.A. King, "The computation of the cohomology rings of all groups of order 128", arXiv:1001.2577

[14] G.-M. Greul, G. Pfister and H. Schönemann, SINGULAR computer algebra system for polynomial computations, `http://www.singular.uni-kl.de`

[15] S. King, Computations of the mod p cohomology rings of groups of order at most 128, `http://users.minet.uni-jena.de/~king/cohomology`

[16] A. Romero, G. Ellis & J. Rubio, "Interoperating between computer algebra systems: computing homology of groups with Kenzo and GAP", ISAAC Proceedings 2009, pp8.

[17] D. Rusin, "The cohomology groups of order 32", *Math. Comput.*, 53 (1989), 359-385.

[18] P. Smith, HAPPRIME, version 0.4 (2008), a deposited package for the GAP computational algebra system.
(`http://www.gap-system.org/Packages/happrime.html`)

[19] B. Venkov, "Cohomology algebras for some classifying spaces", *Dokl. Akad. Nauk. SSR* 127 (1959), 943-944.

[20] C.T.C. Wall, "Resolutions of extensions of groups", *Proc. Cambridge Philos. Soc.* 57 (1961), 251-255.