Journal of Algebra 325 (2011) 352–363

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

The computation of the cohomology rings of all groups of order 128 ☆

David J. Green [a], Simon A. King [b,*]

[a] *Mathematical Institute, University of Jena, D-07737 Jena, Germany*
[b] *Mathematics Department, National University of Ireland, Galway, Ireland*

ARTICLE INFO

Article history:
Received 25 January 2010
Available online 15 September 2010
Communicated by Jon Carlson

MSC:
primary 20J06
secondary 20-04, 20D15

Keywords:
Modular group cohomology
Finite p-groups
Regularity
Filter regular parameters

ABSTRACT

We describe the computation of the mod-2 cohomology rings of all 2328 groups of order 128. One consequence is that all groups of order less than 256 satisfy the strong form of Benson's Regularity Conjecture.

1. Introduction

Computing large numbers of group cohomology rings allows one to test existing conjectures and to look for new patterns. Carlson's computations [13, Appendix] for all 267 groups of order 64 led to the refutation of the Essential Conjecture [16, p. 96], and inspired further work on the significance of the local cohomology of group cohomology rings: see pp. 6–8 of [5], and its appendix.

Here we announce the computation of the mod-2 cohomology rings of all 2328 groups of order 128. The results are available in human-readable form at our website [17]. They can be read into the computer using our package [19] for the Sage [25] computer algebra system.

We also give some first applications. Theorem 7.7 verifies the strong form of Benson's Regularity Conjecture for all groups of order less than 256. We study the statistical effectiveness of Duflot's

☆ King was supported by DFG grant GR 1585/4-1 during most of this research, and by Marie Curie grant MTKD-CT-2006-042685 while this paper was written. Both authors received travel assistance from grants GR 1585/4-1 and -2.

* Corresponding author.
E-mail addresses: david.green@uni-jena.de (D.J. Green), simon.king@nuigalway.ie (S.A. King).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2010.08.016

lower bound for the depth in Section 6. And we investigate the local cohomology of these cohomology rings, observing that although the a-invariants are normally weakly increasing, there are 15 exceptions amongst the 2595 groups of order 64 or 128: see Table 1 on page 359.

Following J.F. Carlson [10], we compute mod-p cohomology rings of p-groups from a suitably large initial segment of the minimal projective resolution, using a completeness criterion to tell when we are done. For a project of this scale it was necessary to detect completion as soon as possible, as each extra stage in the minimal resolution is costly. We derive in Theorem 3.3 a computationally efficient variant of Benson's test for completion [7, Theorem 10.1]. Benson's test involves finding filter-regular systems of parameters. In Sections 2 and 3 we develop methods for constructing such parameters in reasonably low degrees, and demonstrating their existence in even lower degrees.

We implemented our cohomology computations in the open source computer algebra system Sage [25]. King rewrote large parts of Green's cohomology program [16]. He developed extensive Cython code that implements the theoretical improvements presented in this paper and makes use of various components of Sage, most notably SINGULAR [18]. Our Sage package is available online [19] and contains the cohomology ring for each group of order 64. The cohomology ring of each group of order 128 is automatically downloaded from a web repository when it is required. The cohomology rings and induced homomorphisms can then easily be transformed into objects of SINGULAR.

2. Constructing filter-regular parameter systems

We recall the key concepts from Benson's paper [7]. Let k be a field of characteristic $p > 0$. Throughout this paper, let $A = \bigoplus_{n\geqslant 0} A_n$ be a connected Noetherian graded commutative k-algebra. That is, $A_0 = k$ and A is finitely generated.

Elements of A will always be understood to be homogeneous. If $x \in A_n$ then we write $|x| = n$. Recall that the elements of positive degree form a maximal ideal, which we shall denote by A_+.

Definition. (See [7, §3].)

a) A sequence of elements $h_1, \dots, h_r \in A_+$ is called *filter-regular* if for each $1 \leqslant i \leqslant r$ the annihilator of h_i in the quotient ring $A/(h_1, \dots, h_{i-1})$ has bounded degree (i.e., it is a finite dimensional k-vector space).
b) A system of parameters $h_1, \dots, h_r$ which is filter-regular is said to have *type* $(d_0, d_1, \dots, d_r) \in \mathbb{Z}^{r+1}$ if

$$d_0 \geqslant -1, \quad d_{i-1} - 1 \leqslant d_i \leqslant d_{i-1} \quad \text{for each } 1 \leqslant i \leqslant r,$$

and the annihilator of h_{i+1} in $A/(h_1, \dots, h_i)$ lies in degrees $\leqslant d_i + \sum_{j=0}^{i} |h_i|$ for all $0 \leqslant i \leqslant r$, where $h_{r+1} = 0$.
c) A system of parameters is *strongly quasi-regular* if it is filter-regular of type $(0, -1, \dots, -r)$. If it has type $(-1, -2, \dots, -r, -r)$ then it is *very strongly quasi-regular*.

Lemma 2.1. *Let $h_1, \dots, h_r$ be a sequence of homogeneous elements in A_+. Let d be the Krull dimension of A. Then the following are equivalent*:

a) *$h_1, \dots, h_r$ is a filter-regular system of parameters.*
b) *$h_1, \dots, h_r$ is a filter-regular sequence, $r \leqslant d$, and $A/(h_1, \dots, h_r)$ is a finite dimensional k-vector space.*
c) *$h_1, \dots, h_r, 0$ is a filter-regular sequence and $r \leqslant d$.*

Remark. If A has bounded degree, then *every* sequence in A is filter-regular.

Proof. Recalling what filter-regularity means for the term $h_{r+1} = 0$, one sees the equivalence of the last two statements. The first implies the second, since then $r = d$ and $A/(h_1, \dots, h_r)$ has Krull dimension zero. And the second implies the first, for A is a finite module for $k[h_1, \dots, h_r]$, and so if $h_1, \dots, h_r$ were algebraically dependent then the Krull dimension would have to be less than $r \leqslant d$. □

Remark. By Benson's [7, Theorem 4.5] all filter-regular parameter systems for A have the same type. By his Corollary 4.8 and Symonds' Theorem [26], every cohomology ring $H^*(G,k)$ has a strongly quasi-regular parameter system.

2.1. The weak rank-restriction condition

Benson's test requires an explicit filter-regular system of parameters in $H^*(G,k)$. One approach is to find classes whose restrictions to each elementary abelian subgroup are (powers of) the Dickson invariants [7, Corollary 9.8]. This is straightforward, but the degrees involved can be inconveniently large. Restricting to the case of a p-group, we shall see in Lemma 2.3 that one can use the Dickson invariants for a complement of the centre instead: these lie in lower degree.

Definition. (C.f. [7, §8].) Let G be a p-group with $p\text{-rk}(G) = K$. Set C to be $\Omega_1(Z(G))$, the greatest central elementary abelian subgroup of G. Homogeneous elements $\zeta_1, \ldots, \zeta_K \in H^*(G)$ satisfy the *weak rank restriction condition* if for each elementary abelian subgroup $V \geqslant C$ of G the following holds, where $s = \text{p}-\text{rk}(V)$:

> The restrictions of $\zeta_1, \ldots, \zeta_s$ to V form a homogeneous system of parameters for $H^*(V)$; and the restrictions of $\zeta_{s+1}, \ldots, \zeta_K$ are zero.

Lemma 2.2. *If $\zeta_1, \ldots, \zeta_K \in H^*(G)$ satisfy the weak rank restriction condition then they constitute a filter-regular system of parameters.*

Proof. By a well-known theorem of Quillen (see e.g. [6, §5.6]), $\zeta_1, \ldots, \zeta_K$ is a system of parameters for $H^*(G)$. The proof of [7, Theorem 9.6] applies equally well to parameters satisfying the weak rank restriction condition: if $E \leqslant G$ is elementary abelian of rank i, then for $V = \langle C, E\rangle$ one has $V \geqslant C$ and $C_G(V) = C_G(E)$. And since $p\text{-rk}(V) \geqslant i$, the restrictions of $\zeta_1, \ldots, \zeta_i$ to $H^*(C_G(E))$ form a regular sequence, by the same Duflot-type argument. □

Lemma 2.3. *Let G be a p-group. Set with $K = p\text{-rk}(G)$, $C = \Omega_1(Z(G))$ and $r = p\text{-rk}(C)$. Then there exist $\zeta_1, \ldots, \zeta_K \in H^*(G)$ satisfy the following conditions*:

a) *The restrictions of $\zeta_1, \ldots, \zeta_r$ form a regular sequence in $H^*(C)$.*
b) *For each rank $r+s$ elementary abelian subgroup $V \geqslant C$ of G the restrictions of $\zeta_{r+s+1}, \ldots, \zeta_K$ to V are zero, and for $1 \leqslant i \leqslant s$ the restrictions of ζ_{r+i} to V is a power of the ith Dickson invariant in $H^*(V/C)$.*

Any such system $\zeta_1, \ldots, \zeta_K$ is a filter-regular system of parameters for $H^*(G)$.

Remark. By the ith Dickson invariant we mean the one which restricts nontrivially to dimension i subspaces, but trivially to smaller subspaces. That is, if $i < j$ then the ith Dickson invariant lies in lower degree than the jth Dickson invariant.

Proof. Evens showed [13, p. 128] that $H^*(C)$ is a finitely generated module over the image of restriction, so $\zeta_1, \ldots, \zeta_r$ exist. The ζ_{r+i} are specified by their restrictions to elementary abelian subgroups. These restrictions satisfy the compatibility conditions for genuine restrictions. Thus, on raising these defining restrictions by sufficiently high pth powers, the ζ_{r+i} do indeed exist, by a result of Quillen [6, Corollary 5.6.4]. Last part: The weak rank restriction condition is satisfied. □

Remark. Lemma 2.3 is a recipe for constructing filter-regular parameters. By Kuhn's work [20], $\zeta_1, \ldots, \zeta_r$ may be found amongst the generators of $H^*(G)$.

Moreover one can replace ζ_K by any element that completes a system of parameters, as every parameter is filter-regular in the one-dimensional case.

Example. The Sylow 2-subgroup of Co_3 has order 1024. The Dickson invariants lie in degrees 8, 12, 14 and 15, so they can only be used for Benson's test in degree 46. Lemma 2.3 yields filter regular parameters in degrees 8, 4, 6 and 7, and the last parameter can be replaced by one in degree 1. This allows one to use Benson's test in degree 17. In Section 3 we will improve this to 14.

2.2. New filter-regular sequences from old

Finding filter-regular parameters in low degrees makes the computations easier. The two following methods can be used to lower the degrees once filter-regular parameters have been found. They are factorization (Lemma 2.5) and nilpotent alteration (Lemma 2.7).

Lemma 2.4. *Suppose that $p_1, \dots, p_r \in A_+$ are filter-regular. Suppose that $p_1 x \in (p_2, \dots, p_r)$ and that x lies in sufficiently high degree. Then $x \in (p_2, \dots, p_r)$.*

Proof. This is clear for $r = 1$. We proceed by induction on r. So suppose that $r \geqslant 2$ and $p_1 x = \sum_{i=2}^{r} p_i w_i$.

Since w_r is in sufficiently large degree, there are $v_1, \dots, v_{r-1} \in A$ with $w_r = \sum_{i=1}^{r-1} p_i v_i$. Then $p_1(x - p_r v_1) \in (p_2, \dots, p_{r-1})$, and we are done by induction. □

Lemma 2.5. *Suppose that $p_1, \dots, p_r \in A_+$ is a filter-regular sequence, and that $f_1, \dots, f_r \in A_+$ satisfy $f_i \mid p_i$ for each i. Then $f_1, \dots, f_r$ is filter-regular too. Hence if $p_1, \dots, p_r$ is a filter-regular system of parameters, then so is $f_1, \dots, f_r$.*

Proof. By induction on r it suffices to prove that $f_1, p_2, \dots, p_r$ is filter-regular. We do this by induction on r. If $f_1 = p_1$ then we are done, so we may assume that $p_1 = f_1 g_1$ with $f_1, g_1 \in A_+$. If $f_1 x = 0$ then $p_1 x = 0$, so x is in bounded degree and the case $r = 1$ is done. Now suppose that $r \geqslant 1$. Observe that we may assume that both $f_1, p_2, \dots, p_{r-1}$ and $g_1, p_2, \dots, p_{r-1}$ are filter-regular.

Suppose that $p_r x \in (f_1, p_2, \dots, p_{r-1})$ and that x is in large degree. Then $p_r g_1 x \in (p_1, p_2, \dots, p_{r-1})$ and $g_1 x$ is in large degree, so by filter-regularity of $p_1, \dots, p_r$ we have $g_1 x \in (p_1, \dots, p_{r-1})$.

Hence for some $w \in A$ we have $g_1(x - f_1 w) \in (p_2, \dots, p_{r-1})$. So $x - f_1 w \in (p_2, \dots, p_{r-1})$ by Lemma 2.4, as $g_1, p_2, \dots, p_{r-1}$ is filter regular. Therefore $x \in (f_1, p_2, \dots, p_{r-1})$, as required. The last part follows from Lemma 2.1. □

Lemma 2.6. *Suppose that $p_1, \dots, p_r \in A_+$, and that $m_1, \dots, m_r \geqslant 1$. Then $p_1, \dots, p_r$ is filter-regular if and only if $p_1^{m_1}, \dots, p_r^{m_r}$ is.*

Proof. One direction follows by Lemma 2.5. For the other it suffices to prove that if $p_1, \dots, p_r$ is filter-regular, then $p_1^m, p_2, \dots, p_r$ is too. This is true for $m = 1$, so assume that $m \geqslant 2$ and that it is true for $m - 1$. Suppose that x has sufficiently large degree and satisfies $p_r x \in (p_1^m, p_2, \dots, p_{r-1})$. So there is $y \in A$ with

$$p_r x \in p_1^m y + (p_2, \dots, p_{r-1}).$$

Since $p_r x \in (p_1^m, p_2, \dots, p_{r-1}) \subseteq (p_1, \dots, p_{r-1})$ and x has sufficiently large degree, we have $x \in (p_1, \dots, p_{r-1})$ by filter-regularity of $p_1, \dots, p_r$. So there is $z \in A$ with $x \in p_1 z + (p_2, \dots, p_{r-1})$. Hence $p_1(p_r z - p_1^{m-1} y) \in (p_2, \dots, p_{r-1})$.

From Lemma 2.4 we deduce that $p_r z - p_1^{m-1} y \in (p_2, \dots, p_{r-1})$ and hence

$$p_r z \in \left(p_1^{m-1}, p_2, \dots, p_{r-1}\right).$$

As $p_1^{m-1}, p_2, \dots, p_r$ is filter-regular by assumption, and as z lies in sufficiently high degree, we deduce that $z \in (p_1^{m-1}, p_2, \dots, p_{r-1})$. Combining this with $x \in p_1 z + (p_2, \dots, p_{r-1})$, we see that $x \in (p_1^m, p_2, \dots, p_{r-1})$. □

Lemma 2.7. *Suppose that $f_1, \dots, f_r$ and $g_1, \dots, g_r$ are two sequences in A_+ with the property that each $g_i - f_i$ is nilpotent. Then $f_1, \dots, f_r$ is a filter regular sequence if and only if $g_1, \dots, g_r$ is.*

Proof. By nilpotence there is $N_i \geqslant 1$ such that $(g_i - f_i)^{N_i} = 0$. Choose $e_i \geqslant 1$ such that $p^{e_i} \geqslant N_i$, then $g_i^{m_i} = f_i^{m_i}$ for $m_i = p^{e_i}$. Now apply Lemma 2.6. □

Remark 2.8. Lemmas 2.5 and 2.7 work well together. Quotienting out the nilpotent generators reduces computational complexity and often makes it easier to factorize the parameters, reducing the degrees.

Example. For group number 38 of order 243, Lemma 2.3 yields parameters in degrees 6, 6, 12 and 16. The parameter in degree 12 has a factor in degree 2, and the last parameter can also be replaced by one in degree 2. Benson's test then detects completion in degree 20, which is perfect.

3. Existence of filter-regular parameters in low degrees

We give a non-constructive method that detects filter-regular parameters in low degrees (Proposition 3.2), and adapt Benson's test accordingly (Theorem 3.3).

Lemma 3.1. *Let $d \geqslant 1$. Suppose that A is a finitely generated module over $A(d)$, the subalgebra generated by A_d. Then there is a finite field extension L/k and an $x \in L \otimes_k A_d$ such that $\mathrm{Ann}_{A_L}(x)$ is finite-dimensional as a vector space.*

Proof. Choose an infinite field K that is algebraic over k. Let $x_1, \dots, x_n$ be a k-basis of A_d. By assumption, $A_K = K \otimes_k A$ is finite over $K[x_1, \dots, x_n]$. Noether normalisation [2, p. 69] means that there are K-linear combinations $y_1, \dots, y_r$ of the x_i such that A_K is finite over the *polynomial* subalgebra $K[y_1, \dots, y_r]$. Note that each $y_j \in (A_K)_d$. Let $Y \subseteq (A_K)_d$ be the K-vector space with basis the y_i.

Denote by A_K^+ the irrelevant ideal. As A_K is Noetherian we have $\mathrm{Ass}(A_K) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$, a finite set. Suppose that $Y \subseteq \mathfrak{p}_i$ for some i. If $x \in A_K^+$ then x is integral over $K[y_1, \dots, y_r]$ and therefore x^s lies in the ideal (Y) of A_K for some $s \geqslant 1$. So $x \in \mathfrak{p}_i$ and therefore $\mathfrak{p}_i = A_K^+$.

That is, if $\mathfrak{p}_i \neq A_K^+$ then $\mathfrak{p}_i \cap Y$ is a proper K-subspace of Y. As K is infinite, Y is not a union of finitely many proper subspaces. So there is an $x \in Y$ which lies in no $\mathfrak{p}_i$, except possibly A_K^+. Suppose $a \in \mathrm{Ann}_{A_K}(x)$, then $x \in \mathrm{Ann}_{A_K}(a)$, so $x \in \mathrm{Ann}_{A_K}(ab) \in \mathrm{Ass}\, A_K$ for some $b \in A_K$. Hence $\mathrm{Ann}_{A_K}(ab) = A_K^+$, and therefore $ab \in \mathrm{Ann}_{A_K}(A_K^+)$. But $\mathrm{Ann}_{A_K}(A_K^+)$ is finite dimensional, as A_K is Noetherian and connected. So there is a $N \geqslant 1$ such that $|c| \leqslant N$ for every $c \in \mathrm{Ann}_{A_K}(A_K^+)$. But then $|a| \leqslant N$, so $\mathrm{Ann}_{A_K}(x)$ is finite dimensional too.

Finally write x as a K-linear combination of the k-basis $x_1, \dots, x_n$ of A_d. Let $L \supseteq k$ be the field generated by the coefficients. Then L/k is finite. □

Proposition 3.2. *Let $d \geqslant 1$. Suppose that A is a finitely generated module over $A(d)$, the subalgebra generated by A_d. Then there is a finite extension K/k and a filter-regular system of parameters $x_1, \dots, x_n$ for A_K with $|x_i| = d$ for every i.*

Proof. If $\dim(A) = 0$ then $\dim_k(A) < \infty$ and we are done, with $n = 0$. If $\dim(A) \geqslant 1$ then by Lemma 3.1 there is a finite extension L/k and an $x_1 \in (A_L)_d$ such that $\mathrm{Ann}_{A_L}(x_1)$ is finite dimensional. This means that $\dim(A_L/(x_1)) < \dim(A)$. The result follows by induction over the Krull dimension. □

3.1. A variant of Benson's test for completion

Benson's test for completion [7, Theorem 10.1] makes two separate uses of a filter-regular system of parameters for $H^*(G, k)$. First one determines the filter degree type. Then one obtains a degree bound by combining the type with the sum of the parameter degrees.

Determining the type calls for explicitly constructed parameters, which are often in high degree. We now show that one can use a different parameter system at each of the two stages. This allows us to detect completion earlier using Proposition 3.2, as an existence proof is all that is needed for the degree sum.

Following Benson [7, §10] we write $\tau_N H^*(G,k)$ for the approximation to the graded commutative ring $H^*(G,k)$ obtained by taking all generators and relations in degree $\leqslant N$. Recall that if K/k is a field extension then $H^*(G,K) \cong K \otimes_k H^*(G,k)$, and hence $\tau_N H^*(G,K) \cong K \otimes_k \tau_N H^*(G,k)$. The following result is based on Theorem 10.1 of Benson's paper [7].

Theorem 3.3. *Let G be a finite group, k a field of characteristic p, and K/k a field extension. Suppose that $r = p\text{-}\mathrm{rk}(G) \geqslant 2$. Suppose that $\zeta_1, \ldots, \zeta_r \in \tau_N H^*(G,k)$ and $\kappa_1, \ldots, \kappa_r \in \tau_N H^*(G,K)$ have the following properties*:

a) *Each system is a filter-regular homogeneous system of parameters in its respective ring. Let $(d_0, \ldots, d_r)$ be the type of $\zeta_1, \ldots, \zeta_r$.*
b) *The images of the ζ_i form a homogeneous system of parameters in $H^*(G,k)$.*
c) *Set $n_i = |\kappa_i|$ and $\alpha' = \max_{0 \leqslant i \leqslant r-2}(d_i + i)$. Then $n_i \geqslant 2$ for all i, and*

$$N > \max\bigl(\alpha', 0\bigr) + \sum_{j=1}^{r} (n_j - 1). \tag{1}$$

Then the map $\tau_N H^*(G,k) \to H^*(G,k)$ is an isomorphism.

Moreover, if a Sylow p-subgroup of G has centre of p-rank at least two, then in Eq. (1) *we only have to require $\geqslant$.*

Proof. Since $H^*(G,K) \cong K \otimes_k H^*(G,k)$, the ζ_i are a filter-regular system of parameters of type $(d_0, \ldots, d_r)$ in $\tau_N H^*(G,K)$ as well. By (i) $\Rightarrow$ (iii) in Theorem 4.5 of [7], it follows that $a^i_{\mathfrak{m}}(\tau_N H^*(G,K)) \leqslant d_i$ for each $0 \leqslant i \leqslant r$. Hence $\alpha' \geqslant \alpha$ for α as in Benson's Theorem 10.1. Since the ζ_i are a system of parameters for $H^*(G,K)$, so are the κ_i. Hence applying Benson's Theorem 10.1 to the κ_i we deduce that $\tau_N H^*(G,K) \cong H^*(G,K)$ and therefore $\tau_N H^*(G,k) \cong H^*(G,k)$. The last part follows from the corrected version[1] of Benson's Remark 10.6(v). □

Example. For the Sylow 2-subgroup of Co_3, the computer finds filter-regular parameters in degrees 8, 4, 6, 1. Killing the first two parameters and then applying Proposition 3.2 shows that there are filter-regular parameters in degrees 8, 4, 2, 2. So Theorem 3.3 allows us to apply Benson's test in degree 14 (which is perfect).

4. Notes on the implementation

Our strategy for computing the cohomology of all groups of order 128 was to combine improved theoretical methods (Proposition 3.2, Lemma 2.3 and Lemma 2.5) with an efficient implementation.

The first author's package [16] was not powerful enough, nor was it in a form suitable for distribution. The C routines for minimal projective resolutions [16] were however serviceable enough, and reimplementing them from scratch would have been costly. We still needed GAP [15] for the group-theoretic work, and in addition we now needed a commutative algebra system such as SINGULAR [18].

The Sage project [25] perfectly matched our needs. It provides a common interface for and contains a distribution of several independent computer algebra systems, including SINGULAR [18] and GAP. Sage is based on Cython [3], which is a compiled version of Python. It makes linking against C-code easy, and it yields a huge speed-up compared with interpreted code. Sage is free open source software, so that it is more easy for us to make our results publicly available.

[1] It is the *centre* of the Sylow p-subgroup which should have rank at least two.

The second author implemented the (Yoneda) product and several other homological algebra constructions in Cython [3]. He also implemented the computation of the ring structure and of the completeness criterion provided by Theorem 3.3. For this purpose, fast Gröbner basis computations in graded commutative rings are particularly important. This is provided by SINGULAR [18].

Our project resulted in an optional Sage package, called the p-Group Cohomology Package [19], with constituents as described above. The package also provides general Massey products and restricted Massey powers. The latest version features Persistent Group Cohomology, introduced by Graham Ellis and the second author [14].

5. Experimental results

We computed the mod-2 cohomology rings of all 2328 groups of order 128. The results – omitted here for space reasons – may be consulted online [17] and read into our cohomology package [19]. Further cohomology computations include:

- Some further 2-groups, including the Sylow 2-subgroups of HS and Co_3;
- All but six groups of order dividing 3^5, together with some of order 3^6; and
- All groups of order dividing 5^4.

Each computation includes a minimal ring presentation, the Poincaré series and the depth. Our results agree with Carlson's for the groups of order 64 [13, Appendix], and with the first author's for groups of order 64, 3^4 and 5^4 [16].

The first complete computation for order 128 was in Summer 2008, using Lemmas 2.5 and 2.3 to improve Benson's criterion. Split over several processors, the real time used adds up to roughly 10 months. Adding in the existence result for low-degree parameters (Proposition 3.2), reduced the computation time to a total of about 2 months, on a Sun X4450 machine with 2.66 GHz.

Our package can now compute the cohomology of all groups of order 64 in about 20 minutes on a Mac Pro desktop machine running at 2.6 Ghz with 8 GB RAM (Darwin Kernel Version 10.0.0) in 64 bit mode.

5.1. Extremal cases

We highlight some order 128 groups whose cohomology is extremal in various ways. We adopt the numbering of the Small Groups library [8].

The improved Benson criterion (Theorem 3.3) is very efficient. In 1779 out of 2328 cases it already applies in the degree of the last generator or relation. The worst performance is for $2^4 \times D_8$ (number 2320): the presentation is complete from degree 2 onwards, but this is only detected 4 degrees later.

Number 836 is the Sylow 2-subgroup of one double cover of $Sz(8)$. Its cohomology ring has 65 minimal generators and 1859 minimal relations. This is the largest presentation by far: the other groups have at most 39 generators and at most 626 relations. But it is group number 562 which has the highest generator degree (17) and the highest relation degree (34).

The longest computation took about 11 days. Surprisingly, the group concerned (number 2327) was 2_-^{1+6}: the cohomology of this extraspecial group has been known since 1971 [24] and is easy to write down. The computations for groups number 2298 and 2300 took about a week each.

Remark. Other groups of order 128 have been studied before too. Adem and Milgram [1] determined the cohomology of group 931, and Maginnis [21] treated group 934: these are the Sylow subgroups of the sporadic groups M_{22} and J_2.

5.2. a-invariants

Benson–Carlson duality and Symonds' regularity theorem are two instances of the significance of the local cohomology of $H^*(G)$ [5]. Regularity measures the offset of the vanishing line of (bigraded) local cohomology. The a-invariants give more detailed vanishing information.

Table 1
The fifteen groups of orders 64 and 128 whose a-invariants are not weakly increasing.

$\lvert G\rvert$	Group	$a^0_{\mathfrak{m}}$	$a^1_{\mathfrak{m}}$	$a^2_{\mathfrak{m}}$	$a^3_{\mathfrak{m}}$	$a^4_{\mathfrak{m}}$	$a^5_{\mathfrak{m}}$	Note
64	0242	$-\infty$	$-\infty$	-3	-5	-4		Sylow in $L_3(4)$
128	0391	$-\infty$	$-\infty$	-3	-5	-4		
	0741	$-\infty$	-4	-5	-3			
	0749	$-\infty$	-3	-7	-3			
	0836	$-\infty$	-4	-5	-4	-4		Sylow in one $2.Sz(8)$
	0931	$-\infty$	$-\infty$	-3	-4	-4		Sylow in M_{22}
	0934	$-\infty$	$-\infty$	-3	-5	-4		Sylow in J_2
	1411	$-\infty$	$-\infty$	$-\infty$	-4	-6	-5	
	1931	$-\infty$	$-\infty$	-3	-5	-4		
	2005	$-\infty$	$-\infty$	-3	-5	-4		
	2191	$-\infty$	$-\infty$	-4	-6	-4		
	2258	$-\infty$	$-\infty$	$-\infty$	-4	-6	-5	Sylow in $2 \times L_3(4)$
	2261	$-\infty$	$-\infty$	-3	-5	-4		
	2272	$-\infty$	$-\infty$	-3	-5	-4		
	2300	$-\infty$	$-\infty$	-3	-4	-4		

Let k be a field and R a connected finitely presented graded commutative k-algebra. Let M be a finitely generated graded R-module, and $\mathfrak{m}$ the ideal in R of all positive degree elements. Recall that the a-invariants of M are defined by

$$a^i_{\mathfrak{m}}(M) = \max\bigl\{m \mid H^{i,m}_{\mathfrak{m}}(M) \neq 0\bigr\},$$

with $a^i_{\mathfrak{m}}(M) = -\infty$ if $H^i_{\mathfrak{m}}(M) = 0$. Benson provides a recipe for computing the a-invariants from a filter-regular system of parameters [7, Lemma 4.3].

We computed these invariants for all groups of orders 64 and 128. Interestingly, amongst the 2595 groups of these orders there are only 15 cases where the a-invariants are not weakly increasing. These are listed in Table 1.

6. Depth and the Duflot bound

Several results relate the group structure of a finite group G to the commutative algebra of its mod-p cohomology ring $H^*(G)$. For the Krull dimension and depth we have the following inequalities, where S denotes a Sylow p-subgroup of G:

$$p\text{-rk}\bigl(Z(S)\bigr) \leqslant \operatorname{depth} H^*(S) \leqslant \operatorname{depth} H^*(G) \leqslant \dim H^*(G) = p\text{-rk}(G). \tag{2}$$

The first inequality is Duflot's theorem [13, §12.3]. The second is Benson's [4, Theorem 2.1] and "must be well known". The third is automatic for finitely generated connected k-algebras. The last equality is due to Quillen [13, Corollary 8.4.7].

Definition. Let G, p, S be as above. The Cohen–Macaulay defect $\delta_p(G)$ and the Duflot excess $e_p(G)$ are defined by

$$\delta(G) = \dim H^*(G) - \operatorname{depth} H^*(G) \qquad e(G) = \operatorname{depth} H^*(G) - p\text{-rk}\bigl(Z(S)\bigr).$$

It follows from Eq. (2) that

$$\delta(G), e(G) \geqslant 0, \quad \delta(G) \leqslant \delta(S), \quad e(G) \geqslant e(S). \tag{3}$$

The term Cohen–Macaulay defect (sometimes deficiency) is already in use.

Question 6.1. How (for large values of n) are the p-groups of order p^n distributed on the graph with $\delta(G)$ on the x-axis and $e(G)$ on the y-axis?

Table 2
Distribution of the groups of order N by defect δ and excess e.

$N = 64$

e \ δ	0	1	2	3
3	0			
2	5	1		
1	45	22	1	
0	69	103	21	0

$N = 128$

e \ δ	0	1	2	3
3	1			
2	27	10		
1	256	220	32	
0	353	1123	292	14

$N = 3^4$

e \ δ	0	1	2
2	0		
1	2	1	
0	6	6	0

$N = 5^4$

e \ δ	0	1	2
2	0		
1	0	0	
0	6	7	2

Examples. Every abelian group has $(\delta, e) = (0, 0)$. So does every p-central group, such as the Sylow 2-subgroup of $SU_3(4)$.

Quillen showed that the extraspecial 2-group 2_+^{1+2n} has Cohen–Macaulay cohomology [24]. So this group has $(\delta, e) = (0, n)$. For odd p, Minh proved [23] that p_+^{1+2n} has $(\delta, e) = (n, 0)$. With one exception: 3_+^{1+2} has $(\delta, e) = (0, 1)$ [22].

One way to produce groups with small $e(G)/\delta(G)$ ratio is by iterating the wreath product construction. By passing from H to $H \wr C_p$ one multiplies the p-rank by p but increases the depth by one only [12].

Table 2 lists the number of groups with each value of (δ, e), for various orders.

Remarks 6.2. The group of order 64 with $(\delta, e) = (1, 2)$ is group number 138. The one with $(\delta, e) = (2, 1)$ is number 32.

The 14 groups of order 128 with $(\delta, e) = (3, 0)$ are investigated in Proposition 7.6 below. The one with $(\delta, e) = (0, 3)$ is the extraspecial group 2_+^{1+6}.

The group of order 81 with $(\delta, e) = (1, 1)$ is the Sylow 3-subgroup of S_9. One of the groups of order 625 with $(\delta, e) = (2, 0)$ is the Sylow 5-subgroup of the Conway group Co_1.

Question 6.3. Is the Duflot bound sharp for most groups of a given order p^n? That is, do most groups of order p^n lie on the bottom row $e = 0$ of the δ/e-graph? If so, is this effect more pronounced for large primes p?

7. The strong form of the regularity conjecture

Benson conjectured [7] and Symonds proved [26] that $H^*(G, k)$ has Castelnuovo–Mumford regularity zero. Equivalently, the cohomology ring $H^*(G, k)$ always contains a strongly quasi-regular system of parameters. Kuhn has applied Symonds' result to the study of central essential cohomology [20]. The following stronger form of the conjecture remains open.

Conjecture 7.1. *(See Benson p. 175 of [7].) Let G be a finite group, p a prime number and k a field of characteristic p. The cohomology ring $H^*(G, k)$ always contains a very strongly quasi-regular system of parameters.*

We are going to verify the conjecture for all groups of order < 256. We use the Cohen–Macaulay defect $\delta(G)$ to reduce to the case $|G| = 128$, and verify it there by machine computation.

Theorem 7.2 *(Benson). If $\delta(G) \leqslant 2$ then Conjecture* 7.1 *holds for G. This is the case for every group of order* 64.

Proof. This is Theorem 1.5 of [7]. Carlson [11,13] observed that every group of order 64 has $\delta(G) \leqslant 2$ See also the tabular data in [5, Appendix]. □

So we are only interested in groups with $\delta(G) \geqslant 3$. Now, $\delta(G)$ has a group-theoretic upper bound. Let $S \leqslant G$ be a Sylow p-subgroup. Then by Eq. (2)

$$\delta(G) \leqslant \delta_0(G) := p\text{-rk}(G) - p\text{-rk}\big(Z(S)\big).$$

Lemma 7.3. *Let G be a finite group and p a prime.*

a) *If $\delta_0(G) \geqslant 3$ then $p^5 \mid |G|$, and if $p = 2$ or $p = 3$ then $p^6 \mid |G|$.*
b) *If $\delta_0(G) \geqslant 4$ then $p^6 \mid |G|$, and if $p = 2$ or $p = 3$ then $p^7 \mid |G|$.*
c) *If $p = 2$ and $\delta_0(G) \geqslant 4$ then $2^8 \mid |G|$.*

Proof. Clearly $\delta_0(G) = \delta_0(S)$, so we may assume that G is a p-group.

a): If $\delta_0(G) \geqslant 3$ then $G \neq 1$ and so $p\text{-rk}(Z(G)) \geqslant 1$, whence $p - \text{rk}(G) \geqslant 4$. Moreover, G must be non-abelian, so $|G| \geqslant p^5$.

Suppose that $|G| = p^5$. Then $Z(G)$ is cyclic of order p, and there is an elementary abelian subgroup V of order p^4. By maximality, $V \trianglelefteq G$. Let $a \in G \setminus V$. Then $G = \langle a, V \rangle$ and the conjugation action of a on V is nontrivial of order p. So the minimal polynomial of the action divides $X^p - 1 = (X-1)^p$. Consider the Jordan normal form of this action. Each block contains an eigenvector, which must lie in $Z(G)$. So as $Z(G)$ is cyclic, there is just one Jordan block, of size 4. But for $p = 2$ the size 3 Jordan block does not square to the identity, so each block must have size $\leqslant 2$. Similarly there can be no size 4 block for $p = 3$, since it does not cube to the identity. The proof of b) is analogous.

c): We assume that $|G| = 128$ and derive a contradiction. Let $V \leqslant G$ be elementary abelian of rank $r = p\text{-rk}(G)$, then $r \geqslant 4 + p\text{-rk}(Z(G))$. Since G is non-abelian, $r = 5$ or 6. If $r = 6$ then we are in a similar situation to a): the Jordan blocks must have size < 3, so we need at least three; but there can be at most two, since $p - \text{rk}(Z(G)) \leqslant 2$.

So $r = 5$ and $p - \text{rk}(Z(G)) = 1$. Pick $V \lneq H \lneq G$, so $[G : H] = [H : V] = 2$. As V is maximal elementary abelian in H, we have $C \leqslant V$ for $C = \Omega_1(Z(H))$. The Jordan block argument means that C has rank $\geqslant 3$. Applying this argument to the action of G/H on C then yields $p - \text{rk}(Z(G)) \geqslant 2$, a contradiction. □

Remark 7.4. For $p \geqslant 5$ consider the action of a size 4 Jordan block on a rank four elementary abelian. This yields a group of order p^5 with $\delta_0 = 3$, since

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & \binom{n}{1} & \binom{n}{2} & \binom{n}{3} \\ 0 & 1 & \binom{n}{1} & \binom{n}{2} \\ 0 & 0 & 1 & \binom{n}{1} \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Corollary 7.5. *If $|G| < 256$ then $\delta(G) \leqslant 3$, with equality only if $|G| = 128$.*

Proof. Since $\delta(G) \leqslant \delta_0(G)$ and $|G| < 256$, Lemma 7.3 says that $p = 2$ and $64 \mid |G|$. So since $\delta(G) \leqslant \delta(S)$ and $|G| < 256$, it suffices to exclude the case $|G| = 64$. But this follows from Carlson's computations (see Theorem 7.2). □

Lemma 7.3(c) tells us that if $|G| = 128$ and $\delta(G) = 3$ then $\delta_0(G) = 3$.

Proposition 7.6. *Only* 57 *groups of order* 128 *satisfy $\delta_0(G) = 3$, and of these only* 14 *satisfy $\delta(G) = 3$. Each of these* 14 *groups satisfies Conjecture* 7.1.

In the Small Groups Library [8], *these* 14 *groups have the numbers* 36, 48, 52, 194, 515, 551, 560, 561, 761, 780, 801, 813, 823 *and* 836.

Table 3
For each group of order 128 with $\delta_0(G) = 3$, we give its number in the Small Groups library, the Krull dimension K and depth d of $H^*(G)$, the rank $r = K - 3$ of $Z(G)$ and the Cohen–Macaulay defect $\delta = K - d$. Underlined entries have $\delta = 3$.

gp	K	d	r	δ
36	5	2	2	3
48	5	2	2	3
52	4	1	1	3
194	5	2	2	3
513	5	3	2	2
515	5	2	2	3
527	4	2	1	2
551	5	2	2	3
560	4	1	1	3
561	4	1	1	3
621	5	3	2	2
623	4	2	1	2
630	5	3	2	2
635	4	2	1	2
636	4	2	1	2
642	4	2	1	2
643	4	2	1	2
645	4	3	1	1
646	4	2	1	2
740	4	2	1	2
742	4	2	1	2
753	5	3	2	2
761	5	2	2	3
764	4	2	1	2
780	4	1	1	3
801	4	1	1	3
813	4	1	1	3
823	4	1	1	3
836	4	1	1	3

gp	K	d	r	δ
850	5	3	2	2
852	4	2	1	2
853	4	2	1	2
854	4	2	1	2
859	4	2	1	2
860	4	2	1	2
866	4	2	1	2
928	4	3	1	1
929	4	2	1	2
931	4	2	1	2
932	4	2	1	2
934	4	2	1	2
1578	6	4	3	2
1615	4	3	1	1
1620	4	2	1	2
1735	5	3	2	2
1751	4	2	1	2
1753	4	3	1	1
1755	5	4	2	1
1757	4	3	1	1
1758	4	3	1	1
1759	4	3	1	1
1800	4	2	1	2
2216	5	4	2	1
2222	5	3	2	2
2264	5	3	2	2
2317	4	3	1	1
2326	4	4	1	0

Proof. The invariant δ_0 is purely group theoretic. Determining it for each of the 2328 groups of order 128 yields only 57 cases with $\delta_0(G) = 3$. The rest follows by inspecting our cohomology computations: as discussed above, determining the filter degree type is an integral part of our computations. Table 3 lists each of these groups together with its defect. □

Theorem 7.7. *Conjecture* 7.1 *holds for every group of order less than* 256.

Proof. Follows from Theorem 7.2, Corollary 7.5 and Proposition 7.6. □

Remark 7.8. Testing Conjecture 7.1 further requires more high defect groups. Carlson [9] showed that if there are essential classes in $H^*(G)$, then equality holds in $\delta(G) \leqslant \delta_0(G)$. This method shows that groups number 35, 56 and 67 of order 3^6 have $\delta(G) = 3$; and group 299 of order 256 has $\delta(G) = 4$. In each case there is an essential class in degree $\leqslant 4$.

Acknowledgments

The idea for Theorem 3.3 arose during a discussion with Dave Benson. We thank the referee for advice on the structure of the paper.

This work was supported by the German Science Foundation (DFG), project numbers GR 1585/4-1 and -2.

We are grateful to William Stein for giving us the opportunity to work on the `sage.math` computer, which is supported by National Science Foundation Grant No. DMS-0821725.

References

[1] A. Adem, R.J. Milgram, The cohomology of the Mathieu group M_{22}, Topology 34 (2) (1995) 389–410.
[2] M.F. Atiyah, I.G. Macdonald, Introduction to Commutative Algebra, Addison–Wesley Publishing Co., Don Mills, Reading, MA–London–Ontario, 1969.
[3] S. Behnel, R. Bradshaw, G. Ewing, Cython: C-extensions for python, programming language, http://www.cython.org/, 2008.
[4] D. Benson, Modules with injective cohomology, and local duality for a finite group, New York J. Math. 7 (2001) 201–215.
[5] D. Benson, Commutative algebra in the cohomology of groups, in: L.L. Avramov, M. Green, C. Huneke, K.E. Smith, B. Sturmfels (Eds.), Trends in Commutative Algebra, in: Math. Sci. Res. Inst. Publ., vol. 51, Cambridge Univ. Press, Cambridge, 2004, pp. 1–50, available at http://www.msri.org/communications/books/Book51.
[6] D.J. Benson, Representations and Cohomology. II, second ed., Cambridge Stud. Adv. Math., vol. 31, Cambridge Univ. Press, Cambridge, 1998.
[7] D.J. Benson, Dickson invariants, regularity and computation in group cohomology, Illinois J. Math. 48 (1) (2004) 171–197.
[8] H.U. Besche, B. Eick, E.A. O'Brien, A millennium project: Constructing small groups, Internat. J. Algebra Comput. 12 (5) (2002) 623–644, http://www-public.tu-bs.de:8080/~hubesche/small.html.
[9] J.F. Carlson, Depth and transfer maps in the cohomology of groups, Math. Z. 218 (3) (1995) 461–468.
[10] J.F. Carlson, Calculating group cohomology: Tests for completion, J. Symbolic Comput. 31 (1–2) (2001) 229–242.
[11] J.F. Carlson, The Mod-2 Cohomology of 2-Groups, Department of Mathematics, University of Georgia, Athens, GA, 2001, http://www.math.uga.edu/~lvalero/cohointro.html.
[12] J.F. Carlson, H.-W. Henn, Depth and the cohomology of wreath products, Manuscripta Math. 87 (2) (1995) 145–151.
[13] J.F. Carlson, L. Townsley, L. Valeri-Elizondo, M. Zhang, Cohomology Rings of Finite Groups, Algebr. Appl., vol. 3, Kluwer Academic Publishers, Dordrecht, 2003.
[14] G. Ellis, S.A. King, Persistent homology of groups, J. Group Theory (2010), in press, arXiv:1006.2237 [math.GR].
[15] The GAP Group, GAP–Groups, Algorithms, and Programming, Version 4.4.12, 2008, http://www.gap-system.org.
[16] D.J. Green, Gröbner Bases and the Computation of Group Cohomology, Lecture Notes in Math., vol. 1828, Springer-Verlag, Berlin, 2003.
[17] D.J. Green, S.A. King, The cohomology of finite p-groups, website, http://users.minet.uni-jena.de/cohomology/, 2008.
[18] G.-M. Greuel, G. Pfister, H. Schönemann, Singular 3-1-0—A computer algebra system for polynomial computations, http://www.singular.uni-kl.de, 2009.
[19] S.A. King, D.J. Green, p-group cohomology package, 2009, Peer-reviewed optional package for Sage [25], http://sage.math.washington.edu/home/SimonKing/Cohomology/.
[20] N.J. Kuhn, Primitives and central detection numbers in group cohomology, Adv. Math. 216 (1) (2007) 387–442.
[21] J. Maginnis, The cohomology of the Sylow 2-subgroup of J_2, J. Lond. Math. Soc. (2) 51 (2) (1995) 259–278.
[22] R.J. Milgram, M. Tezuka, The geometry and cohomology of M_{12}. II, Bol. Soc. Mat. Mexicana (3) 1 (2) (1995) 91–108.
[23] P.A. Minh, Essential cohomology and extraspecial p-groups, Trans. Amer. Math. Soc. 353 (5) (2001) 1937–1957.
[24] D. Quillen, The mod-2 cohomology rings of extra-special 2-groups and the spinor groups, Math. Ann. 194 (1971) 197–212.
[25] W. Stein, et al., Sage mathematics software (version 4.2.1), the Sage development team, 2009, http://www.sagemath.org.
[26] P. Symonds, On the Castelnuovo-Mumford regularity of the cohomology ring of a group, J. Amer. Math. Soc. 23 (2010) 1159–1173.