LE MATEMATICHE
Vol. LXXVI (2021) – Issue I, pp. 3–18
doi: 10.4418/2021.76.1.1

COMPUTING A MINIMAL RESOLUTION OVER THE STEENROD ALGEBRA

C. NASSAU

We describe an algorithm that allows to compute a minimal resolution of the Steenrod algebra. The algorithm has built-in knowledge about vanishing lines for the cohomology of sub Hopf algebras of the Steenrod algebra which makes it both faster and more economical than the generic approach.

1. Introduction

Let A denote the Steenrod algebra at a prime p and let $k = \mathbb{F}_p$. The cohomology of A is, by definition, the Ext group $\mathrm{Ext}_A(k,k)$. It features prominently in algebraic topology as the E_2 term of the Adams spectral sequence for the computation of the stable homotopy groups of the sphere (see [8]).

Machine computations of the cohomology of A have a long history and there is considerable current activity in the field. While there are other legitimate approaches (e.g. the May spectral sequence [8, Ch. 3.2] or the Lambda algebra [9]) the most promising route for purely mechanical computations seems to be the computation of the minimal resolution of the ground field k as pioneered by Bruner [2]. The main obstacle here is the enormous size of the resolution: a computation for $p = 2$ up to topological dimension 200, for example, will require the computation of kernels and cokernels of matrices over k with hundreds

Received on October 10, 2019

AMS 2010 Subject Classification: 55-04, 55T15, 16-04, 18G10, 18G15
Keywords: Steenrod algebra, resolution, algorithm

of thousands of rows and columns (see [6, Abb. 2.14] for a chart showing the growth rate of the resolution). Carrying out such computations in a reasonable time seems well beyond the capabilities of current computing technology.

The author's contribution to this story is the discovery of a powerful shortcut based on vanishing lines for the cohomology of subalgebras of A. The author lectured about these results in Oberwolfach in 1997 and these shortcuts became the basis of his PhD dissertation [6]. For reasons long lost in time an English language account of these results has never been published. This note is meant to remedy that omission.

We have chosen not to give detailed proofs of the main theorems since this would require the introduction of cumbersome notation that would obscure the simple idea behind our approach. The mathematics involved is completely elementary and a reader who works out the examples that we give in Lemmas 2.2, 2.3 and 2.4 will have no problems filling in the details in the more general cases.

2. The algorithm

We will assume $p = 2$ throughout to simplify the exposition. All results generalize to odd primes in a straightforward way (for details see [6] or [7]).

We let C_* denote the minimal resolution that we wish to compute. Every C_s is a free A-module with a chosen set of generators $G_s \subset C_s$. The differential $d : C_s \to C_{s-1}$ is described by keeping a list of the $d(g_k)$ for $g_k \in G_s$.

One works by double induction on the internal degree t of the Steenrod algebra and the homological degree s of the resolution. At each step C_* is a partially complete resolution below some bidegree (s,t): one has $H(C_*)_{p,q} = 0$ if $p < s$ or $q < t$, but in (s,t) itself the homology $H(C_*)_{s,t}$ might be non-zero. If it is non-zero we introduce new generators in C_{s+1} that kill the offending homology classes. We can describe this procedure more formally as follows:

Input: A partial resolution below bidegree (s,t)
Result: An extension of the resolution to (s,t)
$M \longleftarrow$ compute matrix of $d : C_{s,t} \to C_{s-1,t}$
$K \longleftarrow$ basis of kernel of M
$N \longleftarrow$ compute matrix of $d : C_{s+1,t} \to C_{s,t}$
$Q \longleftarrow$ basis of quotient $K/\operatorname{im} N$, i.e. of $H(C_*)_{s,t}$
for $q \in Q$ **do**
    $x \longleftarrow$ pick a representative of q
    Introduce new generator $g \in C_{s+1,t}$ with $dg = x$.
end

Algorithm 1: The naive algorithm

This is the basic algorithm as it applies to any connected, graded algebra. To see how this can be improved given more specific knowledge about the algebra, consider the sequence

$$\mathrm{Sq}^1 C_* \xhookrightarrow{\text{incl.}} C_* \xrightarrow{\mathrm{Sq}^1\cdot} \mathrm{Sq}^1 C_* \tag{1}$$

Lemma 2.1. *This sequence is exact.*

Proof. For a generator $g_s \in G_s$ and a Milnor basis element $\mathrm{Sq}(r_1, r_2, \ldots)$ one has

$$\mathrm{Sq}^1 \cdot \mathrm{Sq}(r_1, r_2, \ldots) g_s = \begin{cases} \mathrm{Sq}(r_1+1, r_2, \ldots) g_s & (\text{if } r_1 \equiv 0 \bmod 2) \\ 0 & (\text{if } r_1 \equiv 1 \bmod 2) \end{cases}$$

The exactness is then easy to check. □

We look at the long exact sequence associated to (1).

Lemma 2.2. *If C_* is a partially complete resolution below (s,t) and if $t-s>1$ the map $H(C_*)_{s,t} \to H\left(\mathrm{Sq}^1 C_*\right)_{s,t+1}$ is an isomorphism.*

Proof. The associated long exact sequence in homology contains

$$H\left(\mathrm{Sq}^1 C_*\right)_{s,t} \longrightarrow H(C_*)_{s,t} \longrightarrow H\left(\mathrm{Sq}^1 C_*\right)_{s,t+1} \longrightarrow H\left(\mathrm{Sq}^1 C_*\right)_{s-1,t} \tag{2}$$

so it suffices to show that the left and right hand groups are zero.

Let $A(0)$ denote the exterior algebra $\mathbb{F}_2\{1, \mathrm{Sq}^1\}$. If C_* were already a complete resolution one would have $H\left(\mathrm{Sq}^1 C_*\right)_{p,q} = \mathrm{Ext}^{p,q-1}_{A(0)}(k)$ since $\mathrm{Sq}^1 C_* \cong k \otimes_{A(0)} C_*$ (up to a degree shift of 1) and C_* would function as an $A(0)$-resolution of k. For a partial resolution that identification holds true through a range and one can check that it applies to the boundary terms in (2). Since $\mathrm{Ext}^{p,q}_{A(0)} = 0$ for $q-p>0$ that proves the Lemma. □

The Lemma shows that for $t-s>1$ the computation of Q in Algorithm 1 can be carried out in $\mathrm{Sq}^1 C_*$ which is approximately only half as big as C_*.

This alone does not quite suffice for the completion of the inductive step, though: the algorithm needs a representative cycle x from $C_{s,t}$, but a computation of $H(\mathrm{Sq}^1 C_*)_{s,t+1}$ will only produce a cycle $\mathrm{Sq}^1 x'$ in $\mathrm{Sq}^1 C_*$. The explicit description of the map $\mathrm{Sq}(R) \mapsto \mathrm{Sq}^1 \mathrm{Sq}(R)$ in Lemma 2.1 shows that it is straightforward to pick a choice for x' given $\mathrm{Sq}^1 x'$: we just need to lower the first entry by one. However, writing $x = x' + \mathrm{Sq}^1 x''$ we then still need to determine the unknown component x''.

Lemma 2.3. *If $t-s>0$ we can determine $\mathrm{Sq}^1 x''$ by solving $d\left(\mathrm{Sq}^1 x''\right) = -dx'$ in $\mathrm{Sq}^1 C_*$.*

Proof. Firstly, one has $\mathrm{Sq}^1 dx' = d\,\mathrm{Sq}^1 x' = 0$, so dx' lies in $\mathrm{Sq}^1 C_{s-1,t-1} = \left(\mathrm{Sq}^1 C_*\right)_{s-1,t}$ by the exactness of (1). Arguing as in Lemma 2.2 we find that $H\left(\mathrm{Sq}^1 C_*\right)_{s-1,t}$ computes $\mathrm{Ext}_{A(0)}^{s-1,t-1}(k)$. The assumption $t-s>0$ guarantees that this vanishes, so there is indeed a $\mathrm{Sq}^1 x'' \in \mathrm{Sq}^1 C_{s-1,t-1}$ with boundary $-dx'$. □

Together Lemmas 2.2 and 2.3 show that for $t-s>1$ one can trade the single homology calculation in Algorithm 1 against one homology calculation in $\mathrm{Sq}^1 C_*$ and the solution of one lifting problem in $\mathrm{Sq}^1 C_*$. In large dimensions this is a considerable improvement: the matrix that represents the differential in $\mathrm{Sq}^1 C_*$ will need roughly just a quarter of the space that would be required to store the full differential; even though two such matrices are needed, they are needed sequentially, so the same space can be reused; and the linear algebra routines for the computation of kernel and quotient will run a lot faster since their running times are typically more than quadratic in the size of the input matrices.

The real power of this trick, however, is that it can be iterated. Consider the short exact sequences

$$\begin{aligned} \mathrm{Sq}(1,1)C_* &\xhookrightarrow{\text{incl.}} \mathrm{Sq}^1 C_* \xrightarrow{\mathrm{Sq}(0,1)\cdot} \mathrm{Sq}(1,1)C_* \\ \mathrm{Sq}(3,1)C_* &\xhookrightarrow{\text{incl.}} \mathrm{Sq}(1,1)C_* \xrightarrow{\mathrm{Sq}^2\cdot} \mathrm{Sq}(3,1)C_* \end{aligned} \tag{3}$$

The homology of $\mathrm{Sq}(1,1)C_*$ and $\mathrm{Sq}(3,1)C_*$ is approaching $\mathrm{Ext}_B^{p,q}(k)$ where B is, respectively, the exterior algebra E on Sq^1 and $\mathrm{Sq}(0,1)$ or the subalgebra $A(1)$ (as usual we let $A(n)\subset A$ denote the sub Hopf algebra spanned by $\mathrm{Sq}^1,\ldots,\mathrm{Sq}^{2^n}$). These both vanish if $q>3p$ and there is the following straightforward generalization of Lemma 2.2 and 2.3.

Lemma 2.4. *Let C_* be a partially complete resolution below (s,t) and assume $t>3(s+1)$. Then the map $C_*\to \mathrm{Sq}(3,1)C_*$ with $x\mapsto \mathrm{Sq}(3,1)x$ induces an isomorphism $H(C_*)_{s,t}\cong H(\mathrm{Sq}(3,1)C_*)_{s,t+6}$. Furthermore, any cycle $\mathrm{Sq}(3,1)x_0\in \mathrm{Sq}(3,1)C_{s,t}$ can be completed to a cycle $x=x_0+x_1+\cdots+x_7$ in $C_{s,t}$ by solving 7 subsequent lifting problems in $\mathrm{Sq}(3,1)C_*$.*

Proof. To establish the claimed isomorphism one needs to look at the long exact sequences

$$H\Big(\mathrm{Sq}^1 C_*\Big)_{s,t} \longrightarrow H\Big(C_*\Big)_{s,t} \longrightarrow H\Big(\mathrm{Sq}^1 C_*\Big)_{s,t+1} \longrightarrow H\Big(\mathrm{Sq}^1 C_*\Big)_{s-1,t}$$

$$H\Big(\mathrm{Sq}(1,1)C_*\Big)_{s,t+1} \longrightarrow H\Big(\mathrm{Sq}^1 C_*\Big)_{s,t+1} \longrightarrow H\Big(\mathrm{Sq}(1,1)C_*\Big)_{s,t+4} \to H\Big(\mathrm{Sq}(1,1)C_*\Big)_{s-1,t+1}$$

$$H\Big(\mathrm{Sq}(3,1)C_*\Big)_{s,t+4} \to H\Big(\mathrm{Sq}(1,1)C_*\Big)_{s,t+4} \to H\Big(\mathrm{Sq}(3,1)C_*\Big)_{s,t+6} \to H\Big(\mathrm{Sq}(3,1)C_*\Big)_{s-1,t+4}$$

The terms at the end compute, respectively, $\mathrm{Ext}_{A(0)}^{p,t-1}$, $\mathrm{Ext}_{E}^{p,t-3}$ and $\mathrm{Ext}_{A(1)}^{p,t-2}$ for $p = s, s-1$. Using $\mathrm{Ext}_B^{p,q} = 0$ for $q > 3p$ one finds that they all vanish if $t > 3(s+1)$. This establishes the isomorphism $H(C_*)_{s,t} \cong H(\mathrm{Sq}(3,1)C_*)_{s,t+6}$. To recover a cycle $x \in C_{s,t}$ from knowledge of the cycle $\mathrm{Sq}(3,1)x \in \mathrm{Sq}(3,1)C_{s,t}$ we arrange our short exact sequences in the form of a tree:

$$
\begin{tikzcd}
 & & & & & & & C \arrow[drrrr, two heads] & & & & & & & \\
 & & & C' \arrow[urrrr, tail] \arrow[drr, two heads] & & & & & & & & C' \arrow[drr, two heads] & & & \\
 & C'' \arrow[urr, tail] \arrow[dr, two heads] & & & & C'' \arrow[dr, two heads] & & & & C'' \arrow[urr, tail] \arrow[dr, two heads] & & & & C'' \arrow[dr, two heads] & \\
C''' \arrow[ur, tail] \arrow[d, dash] & & C''' \arrow[d, dash] & & C''' \arrow[ur, tail] \arrow[d, dash] & & C''' \arrow[d, dash] & & C''' \arrow[ur, tail] \arrow[d, dash] & & C''' \arrow[d, dash] & & C''' \arrow[ur, tail] \arrow[d, dash] & & C''' \arrow[d, dash] \\
(3,1) & & (1,1) & & (3,0) & & (1,0) & & (2,1) & & (0,1) & & (2,0) & & (0,0)
\end{tikzcd}
$$

Here we have written $C' = \mathrm{Sq}^1 C$, $C'' = \mathrm{Sq}(1,1)C$, $C''' = \mathrm{Sq}(3,1)C$ and we have suppressed various suspensions from the notation. The recovery process begins at the bottom right with the choice of an x_0 such that $\mathrm{Sq}(3,1)x_0$ is the given $\mathrm{Sq}(3,1)x$. The label $(0,0)$ is meant to indicate that we can choose the summands $\mathrm{Sq}(r_1,\ldots)g$ in x_0 to have $(r_1,r_2) \equiv (0,0) \bmod (4,2)$. The first step looks for an x_1 such that $\mathrm{Sq}(1,1)(x_0+x_1)$ becomes a cycle in $\mathrm{Sq}(1,1)C_*$. We can require the summands of x_1 to have $(r_1,r_2) \equiv (2,0) \bmod (4,2)$ since an odd r_1 or r_2 would cause the summand to be mapped to zero in $\mathrm{Sq}(1,1)C_*$. This procedure continues until we eventually have recovered a full cycle $x = x_0 + \cdots + x_7$.

At each step this process requires the exactness of $\mathrm{Sq}(3,1)C_{s-1,t+6-p}$ for some $p = 1,\ldots,6$. These groups relate to $\mathrm{Ext}_{A(1)}^{s-1,t-p}$ which are again zero for $t > 3(s+1)$ by assumption. The offsets p result from the implicit suspensions that we have suppressed from the notation. These p are just the dimensions of the $\mathrm{Sq}(s_1,s_2)$ for the labels (s_1,s_2). These labels will show up again in Lemma 2.5 under the name "signature". $\square$

The important points to remember are

1. A vanishing result for various $\mathrm{Ext}_B^{s,*}$ and $\mathrm{Ext}_B^{s-1,*}$ is used to reduce the homology calculation in $C_{s,t}$ to a homology calculation in a space of much smaller dimensions.

2. Similar vanishing results for various $\mathrm{Ext}_B^{s-1,*}$ are required to use the same reduction to recover the full cycle.

3. The lifting problems for the recovery of the full cycle are enumerated by the Milnor basis elements $\mathrm{Sq}(R)$ in B and they take place in degree $t-|\,\mathrm{Sq}(R)|$.

To give a more formal account of the algorithm we start with a sub Hopf algebra[1] $B\subset A$. Recall from [4, Ch. 15, Thm. 6] that such a B is described by a profile function $p:\mathbb{N}\to\mathbb{N}\cup\{\infty\}$. A vector space basis of B is given by those Milnor basis elements $\mathrm{Sq}(R)$ such that $0\le r_j<2^{p(j)}$.

We will always assume B to be finite, since a computation in a finite dimension does not see the difference between B and its truncation to some $A(N)$ with $N\gg 0$. Let $\mathcal{S}_B=\{R\mid \mathrm{Sq}(R)\in B\}$ and call it the set of "signatures" in B. We say that R and S have the same B-signature if $S_j\equiv R_j \bmod 2^{p(j)}$ for all j. We denote this by $\mathrm{Sq}(R)\simeq_B \mathrm{Sq}(S)$. For every S there is a unique $R\in\mathcal{S}_B$ such that $\mathrm{Sq}(S)\simeq_B \mathrm{Sq}(R)$; this is called the B-signature of $\mathrm{Sq}(S)$ and written as $\mathrm{sig}_B(\mathrm{Sq}(S))$. More simply put, the B-signature of $\mathrm{Sq}(S)$ just records the sequence of remainders $(s_j \bmod 2^{p(j)})_{j=1,2,\ldots}$.

Having the same signature defines the "signature decomposition"

$$A=\sum\nolimits^{\oplus}_{R\in\mathcal{S}_B}E_RA,\qquad E_RA=\mathbb{F}_2\left\{\mathrm{Sq}(S)\mid \mathrm{sig}_B(S)=R\right\}.$$

We will shortly put an ordering on the signatures $\mathcal{S}_B=\{R_0<R_1<\cdots<R_k\}$. This allows us to consider the "signature filtration"

$$F_{R_k}A\subset\cdots\subset F_{R_1}A\subset F_{R_0}A=A$$

with $F_RA=\sum_{S\ge R}E_S(A)$. We want every F_RA to be a right A-submodule of A because we can then extend the filtration to our resolution via $F_RC_*=F_RA\otimes_A C_*$. The following Lemma explains how to construct an ordering that achieves this. To state it recall that $P^s_t\in A$ denotes $\mathrm{Sq}(r_1,\ldots)$ with all $r_i=0$ except for $r_t=2^s$.

Lemma 2.5. *Let $B\subset A$ be the sub Hopf algebra associated to a profile function p with $p(i+j)\ge p(i)-j$ for every $i,j\ge 1$. Let $\mathcal{P}$ be the set of the $P^s_t\in B$ and choose an ordering $\mathcal{P}=\{P^{s_1}_{t_1}>\cdots>P^{s_n}_{t_n}\}$ with $P^s_t<P^{s'}_{t'}$ whenever $t<t'$. For $R\in\mathcal{S}_B$ write the binary decomposition of each r_j in the form[2] $r_j=\sum_{t_k=j}2^{s_k}\varepsilon_k$. Order the signatures via the lexicographic ordering of the bit vector $\tilde{R}=(\varepsilon_1,\ldots,\varepsilon_n)$. Then every F_RA is stable under right multiplication by A. Furthermore E_RA (which is a right A-module as a quotient of F_RA) is up to degree shift by $|R|$ isomorphic to $B\backslash\!\backslash A=k\otimes_B A$.*

[1] There is an interesting limiting case where B is just a sub algebra: this is discussed in Lemma 4.2 below.

[2] This can be done because $0\le r_j<2^{p(j)}$ and $\{2^s\,|\,P^s_j\in B\}=\{1,2,\ldots,2^{p(j)-1}\}$.

For the proof of the Lemma we should recall Milnor's multiplication algorithm (see [5] or [4, Ch. 15]). This expresses a multiplication

$$\mathrm{Sq}(R)\cdot\mathrm{Sq}(S)=\sum_X \beta_{R,S,X}\cdot Sq(T)$$

as a sum over certain matrices $X=(x_{i,j})$ such that

1. the weighted row sums decompose the first factor: $r_i=\sum_j 2^j x_{i,j}$
2. the column sums decompose the second factor: $s_j=\sum_i x_{i,j}$
3. the diagonal sums decompose the result: $t_k=\sum_{i+j=k} x_{i,j}$

The coefficient $\beta_{R,S,X}$ is nonzero if and only if the diagonal decomposition of each t_k is bitwise disjoint.

Lemma 2.6. *With the assumptions of Lemma 2.5, call a matrix $X=(x_{i,j})$ B-trivial if $x_{i,j}\equiv 0 \bmod 2^{p(i)-j}$ whenever $0<j\le p(i)$. Then*

$$\mathrm{Sq}(R)\cdot\mathrm{Sq}(S)=\sum_{B\text{-}trivial X}\beta_{R,S,X}\cdot Sq(T)+\textit{terms with signature} > R. \tag{4}$$

Proof. By design, a B-trivial X will have $\mathrm{sig}_B(R)\le\mathrm{sig}_B(T)$: from $0\equiv x_{i,j} \bmod 2^{p(i)-j}$ and $p(i)-j\ge p(i+j)$ one finds $t_k\equiv r_k+x_{0,k} \bmod 2^{p(k)}$ and this sum must be disjoint. Hence the multiplication with B-trivial X can only add nonzero bits to R which cannot lower the signature.

If X is not B-trivial one needs to chase the possible movements of a bit $2^k\in r_j$. This can only be removed from r_j by moving to the right in $x_{j,*}$, hence affecting a bit in t_k with $k>j$. Since we required $P_k^*>P_j^*$, such a bit is more significant than the original $2^k\in r_j$ and the signature is increased. □

Proof of Lemma 2.5. From (4) it is clear that every F_RA is a right A-submodule and that the A-action on E_RA is described by (4) with the terms of signature $>R$ omitted. It remains to show that the E_RA are all isomorphic to $B\backslash\backslash A$.

Let $R=R'+R''$ be the decomposition with $\mathrm{Sq}(R')\in B$ and $r''_j\equiv 0 \bmod 2^{p(j)}$. There is just a single B-trivial matrix X adapted to R' and it has $x_{i,j}=0$ for all $j>0$, so formula (4) shows that $\mathrm{Sq}(R')\,\mathrm{Sq}(R'')=\mathrm{Sq}(R'+R'')$ modulo terms of signature greater than $\mathrm{sig}_B(R')=\mathrm{sig}_B(R)$. It follows that left multipliation by $\mathrm{Sq}(R')$ induces an isomorphism $E_0A\to E_{\mathrm{Sq}(R')}A$. In particular, all E_RA are isomorphic.

For the largest signature $R_{\max}=(2^{p(1)}-1,2^{p(2)}-1,\dots)$ in B we find $E_{R_{\max}}=F_{R_{\max}}=\mathrm{Sq}(R_{\max})A$. Let $\tau_B=|\,\mathrm{Sq}(R_{\max})|$. The B-linear inclusion $k\{\mathrm{Sq}(R_{\max})\}\subset B$ realizes $\Sigma^{\tau_b}k\otimes_B A$ as a right A-submodule of $B\otimes_B A=A$ with generator $\mathrm{Sq}(R_{\max})$, which provides the identification $\mathrm{Sq}(R_{\max})A\cong\Sigma^{\tau_b}k\otimes_B A$. □

We will from now on only consider sub Hopf algebras B as in Lemma 2.5 with their compatible signature ordering; such B will be called admissible.

We now have a signature filtration $F_R C_*$ on the partial resolution. Note that $H(E_R C_*)_{p,q} \cong H(B\backslash\backslash A \otimes_A C_*)_{p,q}$ approximates $\mathrm{Tor}^A_{p,q-|\mathrm{Sq}(R)|}(B\backslash\backslash A)$ which is dual to $\mathrm{Ext}_B^{p,q-|R|}(k)$. Hence a vanishing result for $\mathrm{Ext}_B(k)$ will translate to a corresponding exactness assertion for $E_R C_*$. With these preparations the proposed new algorithm can then be formalized as in Algorithm 2 (see page 11).

As explained earlier, the algorithm is not automatically applicable everywhere: it only works and produces valid results when the bidegrees $(s,t-|R|)$, $(s-1,t-|R|)$ for the $R \in \mathcal{S}_B$ are contained in a known vanishing region for the cohomology of the subalgebra B. There are easily determined vanishing regions for the E_2-term of the May spectral sequence for Ext_B that we can use. To state them let $Q_s = P^0_{s+1}$ denote the usual Bockstein operation.

Lemma 2.7. *Let $B \subset A$ be a finite sub Hopf algebra and let s_{min}, s_{max} be the smallest, resp. largest s with $Q_s \in B$. Then $\mathrm{Ext}_B^{s,t}(k) = 0$ if either $t < s \cdot |Q_{s_{min}}|$ or $t > s \cdot |Q_{s_{max}}|$.*

One can thus choose between working above the vanishing line based on $s_{\min}$ or below the vanishing line for $s_{\max}$. We discuss the merits of these choices in the next sections.

3. Working below the vanishing line

Suppose $B \subset A(n)$ and let τ_B be the maxmimum of the dimensions of the $\mathrm{Sq}(R)$ in B. With $\rho_n = |Q_{n+1}| = 2^{n+1} - 1$ one has

Theorem 3.1. *Suppose $B \subset A(n)$ and $t > \rho_n \cdot (s+1) + \tau_B$. Then algorithm 2 is applicable.*

Proof. This is a straightforward diagram chase along the lines of Lemma 2.2 and 2.3. Details can be found in [6], Satz 2.2.15. □

For a fixed bidegree (s,t) this criterion yields a finite number of choices for applicable subalgebras B. Choosing the best one then amounts to finding that B for which the dimensions of the $E_R C_*$ over all $\mathcal{S}_B$ becomes smallest.

In practice we have just evaluated the size of the first piece $E_0 C_*$ to make the choice of B; experience shows that the initial homology calculation using $E_0 C_*$ is facing larger matrices than the subsequent lifting problems. In our actual implementation we have only implemented a simplified search for B using an

Input: A partial resolution below bidegree (s,t)
Input: An admissible subalgebra $B \subset A$ with its ordering of $\mathcal{S}_B$
Result: An extension of the resolution to (s,t)
Start by computing the homology of E_0C_*
$M \longleftarrow$ matrix of $d : E_0C_{s,t} \to E_0C_{s-1,t}$
$K \longleftarrow$ basis of kernel of M
$N \longleftarrow$ matrix of $d : E_0C_{s+1,t} \to E_0C_{s,t}$
$Q \longleftarrow$ basis of quotient $K/\operatorname{im} N$, i.e. of $H(E_0C_*)_{s,t}$
if *Q not empty* **then**
  Set up approximate boundaries for the new generators
  for $q_i \in Q$ **do**
    $x_i \longleftarrow$ a representative of q_i in $E_0C_{s,t}$ *(will become $d(g_i)$)*
    $d_i \longleftarrow d(x_i)$ *(represents $d^2(g_i)$, should be zero at the end)*
  end
  Extract error terms e_i from $d^2(g_i)$ and compute corrections to $d(g_i)$
  for $R \in \mathcal{S}_B$, $R \neq 0$ *(process these in order)* **do**
    $M \longleftarrow$ matrix of $d : E_RC_{s,t} \to E_RC_{s-1,t}$
    for $q_i \in Q$ **do**
      $e_i \longleftarrow$ extract the summands of d_i from $E_RC_{s-1,t}$
      $f_i \longleftarrow$ solution of $M \cdot f_i = e_i$
      $x_i \longleftarrow x_i - f_i$
      $d_i \longleftarrow d_i - d(f_i)$
    end
  end
  Introduce new generators
  for $q_i \in Q$ **do**
    Verify that $d_i = 0$
    Introduce new generator $g_i \in C_{s+1,t}$ with $dg_i = x_i$.
  end
end

Algorithm 2: The new algorithm

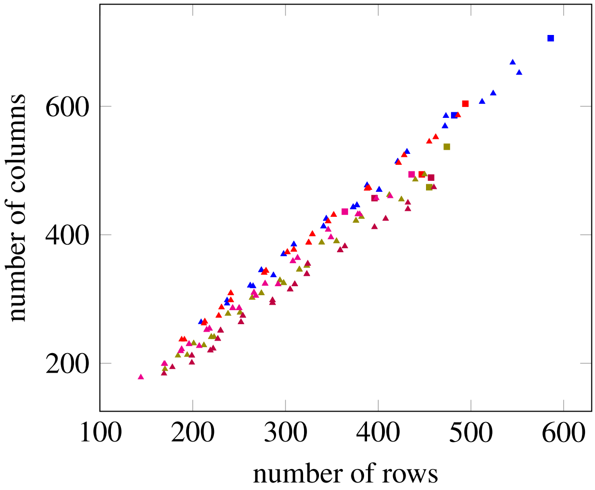

Figure 1: Application of Algorithm 2 to the computation of C_s for $s = 10, \ldots, 14$ and $t - s = 120$ with $B = A(2)$ (the corresponding colors are blue, red, olive, purple, magenta). The squares represent the matrices of the initial homology computation; the triangles correspond to the lifting problems.

ordering of the $P_t^s \in A$, first via $t + s$, then by s. We then considered only those B that are spanned by an initial segment of the P_t^s, i.e. $A(0)$, $E(\mathrm{Sq}^1, \mathrm{Sq}(0,1))$, $A(1)$, $A(1) \cdot E(\mathrm{Sq}(0,0,1))$, etc. In practice this seems to give a sufficiently good choice.

We illustrate the working of the algorithm with some statistics from the computation for $p = 2$ in topological dimension 120. Algorithm 2 is applicable there with $B = A(2)$. The dimensions of the vector spaces for $s = 10, \ldots, 14$ are given in the following table.

s	C_{s-1}	C_s	C_{s+1}	E_0C_{s+1}	E_0C_s	E_0C_{s-1}
10	29087	23997	19609	482	586	706
11	25029	20477	18385	447	494	604
12	21388	19213	18325	455	474	537
13	20070	19156	16601	396	457	489
14	19993	17350	14437	364	436	494

The dimensions of the matrices that are encountered in the subsequent lifting problems can be seen in Figure 1.

4. Working above the vanishing line

The subalgebras that were chosen in the last section become bigger as $(x,y) = (t-s,s)$ approaches the x-axis; conversely, when s gets bigger they tend to become smaller, hence less useful. For these cases a different choice of B presents itself: let $F(n) = \mathbb{F}_2\{\mathrm{Sq}(R) \mid r_1 = \cdots = r_n = 0\}$. The smallest Bockstein in $F(n)$ is Q_{n+1}, hence Lemma 2.7 gives

Theorem 4.1. *Suppose $B \subset F(n)$ and $t < (2^{n+1}-1)s$. Then algorithm 2 is applicable.*

Proof. This is again a straightforward diagram chase along the lines of Lemma 2.2 and 2.3. For details see [6], Satz 2.2.19. □

To see that this gives a powerful choice of B consider the problem of computing the zeroes above the Adams vanishing region, i.e. confirming mechanically Adams' theorem that $\mathrm{Ext}_A^{s,t} = 0$ if $0 < t-s < 2s-3$ (see [1]). The naive algorithm would have to verify the exactness of

$$Ah_0^{s-1} \xleftarrow{\cdot\mathrm{Sq}(1)} Ah_0^{s} \xleftarrow{\cdot\mathrm{Sq}(1)} Ah_0^{s+1}$$

in degree $t-s$; if $t-s = 200$ these vector spaces have dimension ≈ 15000 which makes the computation of kernels and images challenging. Theorem 4.1 allows to pick $B = F(1)$ in this region, so the homology calculation in Algorithm 2 will instead look at the sequence

$$F(1)\backslash\backslash Ah_0^{s-1} \xleftarrow{\cdot\mathrm{Sq}(1)} F(1)\backslash\backslash Ah_0^{s} \xleftarrow{\cdot\mathrm{Sq}(1)} F(1)\backslash\backslash Ah_0^{s+1} \tag{5}$$

Here $F(1)\backslash\backslash A \cong \mathbb{F}_2\left\{\mathrm{Sq}^k \mid k \geq 0\right\}$ is just one-dimensional in every degree so the computation is pretty trivial (and in fact independent of the topological dimension $t-s$).

We illustrate the effect of using $B = F(2)$ in the following table which lists the dimensions of the vector spaces for $s = 35$ and $t-s = 114,\ldots,118$.

$t-s$	C_{34}	C_{35}	C_{36}	E_0C_{36}	E_0C_{35}	E_0C_{34}
114	3187	2683	2471	235	255	322
115	3345	2817	2587	251	273	342
116	3501	2946	2712	261	283	356
117	3666	3075	2829	269	295	368
118	3844	3225	2961	286	314	390

The corresponding Figure 2 also shows the dimension of the matrices in the lifting problems. The figure shows that the decomposition of the C_* into the E_RC_* is not as uniform as in Figure 1.

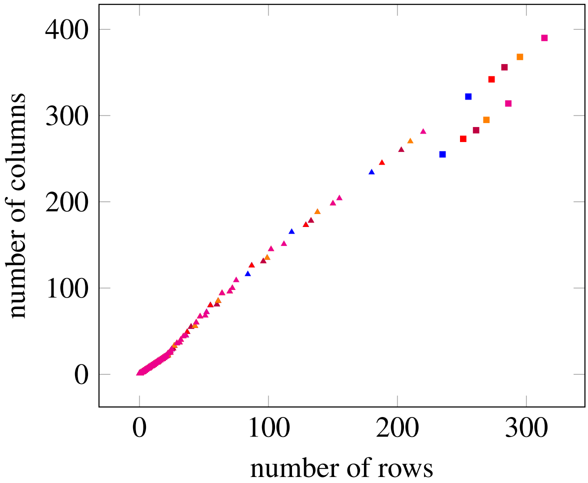

Figure 2: Application of Algorithm 2 to the computation of C_s for $s = 35$ and $t-s = 114,\dots,118$ with $B = F(2)$ (the corresponding colors are blue, red, purple, orange, magenta). The squares again represent the matrices of the initial homology computation, the triangles the lifting problems.

There is a small but interesting extension of this result for $p = 2$. Let

$$F'(n) = \mathbb{F}_2\{Sq(R) \mid r_1 = \cdots = r_{n-1} = 0,\, r_n \equiv 0 \bmod 2\} \subset F(n-1)$$

Although this is just a subalgebra of A, not a sub Hopf algebra, our theory is nonetheless applicable:

Theorem 4.2. *Suppose $B \subset F'(n)$ and $t < (2^{n+1}-2)s$. Then algorithm 2 is applicable.*

Proof. See [6], Satz 2.2.22. □

This theorem is best understood by comparison with the odd-primary situation. Recall that for $p > 2$ the Steenrod algebra has generators $P(R)$ that resemble the $Sq(2R)$, and separate Bockstein operators $Q(\varepsilon)$ where $\varepsilon = (\varepsilon_0, \varepsilon_1, \dots)$ with $\varepsilon_j \in \{0,1\}$. The analogues of $F(n)$ and $F'(n)$ are

$$F(n) = \mathbb{F}_p\{Q(\varepsilon)P(R) \mid r_1 = \cdots = r_n = 0,\, \varepsilon_0 = \cdots = \varepsilon_{n-1} = 0\},$$
$$F'(n) = \mathbb{F}_p\{Q(\varepsilon)P(R) \mid r_1 = \cdots = r_n = 0,\, \varepsilon_0 = \cdots = \varepsilon_n = 0\}.$$

For $p > 2$ both $F(n)$ and $F'(n)$ are sub Hopf algebras for which the analogue of Theorem 4.1 applies.

Using $F'(n)$ can give a considerable speedup. Consider again the reduction (5) that was applicable above the v_1-line of slope $1/2$. Theorem 4.2 allows to replace $F(1)$ by $F'(1)$ if the bidegree lies above the h_1-line of slope 1. Since $F'(1)\backslash\backslash A \cong A(0)$ this reduces the verification of $\mathrm{Ext}_A^{s,t} = 0$ in the region $1 < t-s < s$ to the empty computation!

Similarly, using $F'(2)$ is justified above a line of slope $1/5$ which eventually covers the entire v_1-periodic region. To verify the exactness of the resolution in that region the algorithm only looks at

$$F'(2)\backslash\backslash A \cong \mathbb{F}_2\{Sq(r,\varepsilon) \mid r \geq 0, \varepsilon = 0,1\}$$

which has at most 2 generators in every degree.

5. Lifting problems

It is important to realize that the signature filtration does not just allow the computation of a resolution; it also facilitates the computation *with* it. The central problem here is usually to solve lifting problems: a cycle $z \in C_{s,t}$ is given and the task is to find some $w \in C_{s+1,t}$ with $d(w) = z$. This process is the core, for example, of the computation of a chain map when the target is C_*. The signature filtration can be used to decompose this computation in exactly the same way as during the computation of the resolution (see Algorithm 3 for a formalization).

The author's experience seems to suggest that the computation of the matrices $E_0C_{s,t} \to E_0C_{s-1,t}$ takes considerably more time than the linear algebra routines. This suggests that it might be wise to already cache these matrices during the computation of the resolution.

6. Implementations

The author implemented the algorithm for $p = 2$ as part of his PhD thesis. That implementation was written in C. He was then able to compute the resolution up to $t-s = 210$ using a machine with a 300 MHz AMD K6-2 processor; the computation took 108 days. The running time per dimension seemed to double every 10 dimensions. In dimension 181 the author decided to rewrite part of the multiplication routine using the SSE2 instruction set; this essentially doubled the speed of the program. However, given the exponential growth of the computational challenge this was effectively only good enough to buy ten more stems. More information about running times, memory usage, etc. can be found in [6, Fig. 2.12-2.15].

Input: A resolution up to bidegree (s,t)
Input: An admissible subalgebra $B \subset A$ with its ordering of $\mathcal{S}_B$
Input: A cycle $z \in C_{s,t}$
Result: A preimage $w \in C_{s+1,t}$ with $d(w) = z$
$w \longleftarrow 0$
Extract error terms e from z and compute correction to w
for $R \in \mathcal{S}_B$ *(process these in order)* **do**
  $M \longleftarrow$ matrix of $d : E_R C_{s+1,t} \to E_R C_{s,t}$
  $e \longleftarrow$ extract the summands of z from $E_R C_{s,t}$
  $f \longleftarrow$ solution of $M \cdot f = e$
  $w \longleftarrow w + f$
  $z \longleftarrow z - d(f)$
end

Algorithm 3: Computing the lift of a cycle

In 2004 the author started a new project [7] which also works for (small) odd primes and comes equipped with an interface to the Tcl programming language. The tables in this paper were computed using that library. The library is the computational engine behind the author's Yacop/Sage project which strives to create an experimental Steenrod algebra cohomology package for the Sage computer algebra system.

7. Loose ends

We close this paper with a few remarks.

Firstly, our algorithm seems to be a strong argument in favour of the Milnor basis of the Steenrod algebra as the right basis for mechanical cohomology calculations. Our signature filtration seems to be difficult to handle in the Serre-Cartan basis of admissible monomials, for example. Furthermore, Lemma 2.6 shows how to compute the induced differential on the $E_R C_*$ directly. The naive approach, i.e. first computing the differential in $F_R C_*$ and then reducing modulo the $F_S C_*$ with $S > R$, would be a lot more wasteful.

Secondly, the algorithm can also be used to compute a minimal "complex motivic resolution" M_* of the Steenrod algebra (see [3] for an introduction to this topic). The reason is that such an M_* is just a resolution of the ordinary Steenrod algebra that is equipped with an extra "Bockstein filtration". One begins by computing a minimal resolution K_* of the trigraded algebra EA which is the "odd primary Steenrod algebra for $p = 2$". Our theory is directly applicable to this computation. In a second pass one then interprets EA as an associated graded of the ordinary Steenrod algebra. Using the same generators as in K_*

and lifting the terms of the differentials in K_* arbitrarily from EA to A defines an approximate M_* which however fails to satisfy $d^2(g) = 0$. One then computes successively correction terms to the $d(g)$ that remedy this. The correction process procedes along the third (Bockstein) grading of EA and requires at each step to solve a lifting problem in K_* for which our theory is again applicable.

Furthermore, the signature filtration can also be used to resolve modules other than the ground field. To find out which B is applicable at a given bidegree some external knowledge of $\mathrm{Ext}_B(M)$ is necessary. This might be interesting for modules that are free over some $A(n)$, for example. The author has not pursued this, though, since his preferred approach to the computation of $\mathrm{Ext}_A(M)$ uses the resolution $M \otimes_k C_*$ of M where C_* is the ground field resolution. At least for small M that makes the computation of a separate resolution for each M unnecessary.

Finally, a very interesting open question is the applicability of our shortcut to the computation of unstable cohomology charts.

REFERENCES

[1] J. F. Adams. A periodicity theorem in homological algebra. *Proc. Cambridge Philos. Soc.*, 62:365–377, 1966. ISSN 0008-1981. doi: 10.1017/s0305004100039955. URL `https://doi.org/10.1017/s0305004100039955`.

[2] Robert R. Bruner. Ext in the nineties. In *Algebraic topology (Oaxtepec, 1991)*, volume 146 of *Contemp. Math.*, pages 71–90. Amer. Math. Soc., Providence, RI, 1993. doi: 10.1090/conm/146/01216. URL `https://doi.org/10.1090/conm/146/01216`.

[3] Daniel Dugger and Daniel C. Isaksen. The motivic Adams spectral sequence. *Geom. Topol.*, 14(2):967–1014, 2010. ISSN 1465-3060. doi: 10.2140/gt.2010.14.967. URL `https://doi.org/10.2140/gt.2010.14.967`.

[4] H. R. Margolis. *Spectra and the Steenrod algebra*, volume 29 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, 1983. ISBN 0-444-86516-0. Modules over the Steenrod algebra and the stable homotopy category.

[5] John Milnor. The Steenrod algebra and its dual. *Ann. of Math. (2)*, 67:150–171, 1958. ISSN 0003-486X. URL `https://doi.org/10.2307/1969932`.

[6] Christian Nassau. *Ein neuer Algorithmus zur Untersuchung der Kohomologie der Steenrod-Algebra.* Berlin: Logos Verlag; Frankfurt am Main: Fachbereich Mathematik (Dissertation 2001), 2002. ISBN 3-89722-881-5/pbk. doi: 10.30819/881. URL `https://doi.org/10.30819/881`.

[7] Christian Nassau. The Steenrod Tcl library v2.1, October 2019. URL `https://doi.org/10.5281/zenodo.3473101`.

[8] Douglas C. Ravenel. *Complex cobordism and stable homotopy groups of spheres*, volume 121 of *Pure and Applied Mathematics*. Academic Press, Inc., Orlando, FL, 1986. ISBN 0-12-583430-6; 0-12-583431-4.

[9] Martin C. Tangora. Computing the homology of the lambda algebra. *Mem. Amer. Math. Soc.*, 58(337):v+163, 1985. ISSN 0065-9266. doi: 10.1090/memo/0337. URL `https://doi.org/10.1090/memo/0337`.

C. NASSAU
Jenaer Weg 31
65931 Frankfurt
Germany
e-mail: `nassau@nullhomotopie.de`