New York Journal of Mathematics

New York J. Math. **19** (2013) 23–37.

Commutators in the Steenrod algebra

John H. Palmieri and James J. Zhang

Abstract. A family of bases for the mod p Steenrod algebra is constructed from iterated commutators of algebra generators.

Contents

1. Introduction

Fix a prime p and let $\mathscr{A} = \mathscr{A}_p$ denote the mod p Steenrod algebra. In this paper, we construct a new basis for $\mathscr{A}$; its elements are products of iterated commutators of the algebra generators for $\mathscr{A}$. We state our results at an odd prime, then indicate the changes necessary when $p = 2$.

Recall that $\mathscr{A}$ is a graded Hopf algebra over the field $\mathbf{F}_p$, and from Milnor's work [Mil58] the graded dual $\mathscr{A}^*$ of $\mathscr{A}$ has the form

$$\mathscr{A}^* \cong \Lambda(\tau_0, \tau_1, \dots) \otimes \mathbf{F}_p[\xi_1, \xi_2, \dots].$$

This is graded by setting $\deg \tau_i = 2p^i - 1$, $\deg \xi_i = 2(p^i - 1)$. The *Milnor basis* for the Steenrod algebra is the dual to the monomial basis for $\mathscr{A}^*$: its elements have the form

$$Q_{i_1} Q_{i_2} \dots \mathscr{P}(r_1, r_2, \dots),$$

dual to

$$\tau_{i_1} \tau_{i_2} \dots \xi_1^{r_1} \xi_2^{r_2} \dots .$$

Received January 10, 2013.
2010 *Mathematics Subject Classification.* 55S10, 16T05, 16S30.
Key words and phrases. Steenrod algebra, commutators.

ISSN 1076-9803/2013

It is well known that a minimal set of algebra generators for $\mathscr{A}$ is

$$\{Q_0, \mathscr{P}^1, \mathscr{P}^p, \mathscr{P}^{p^2}, \dots, \mathscr{P}^{p^i}, \dots\}.$$

For any positive integer s, the element $\mathscr{P}^s$ is equal to the Milnor basis element $\mathscr{P}(s)$, and we recall from [Mil58, p. 151] that Q_{i+1} may be defined inductively, starting from Q_0, by

$$Q_{i+1} = [\mathscr{P}^{p^i}, Q_i] = \mathscr{P}^{p^i} Q_i - Q_i \mathscr{P}^{p^i}. \tag{1.1}$$

We define elements $c_{s,t}$ of $\mathscr{A}$ as follows: for each integer $s \geq 0$, let $c_{s,1} = \mathscr{P}^{p^s}$, and for $t \geq 2$, inductively define $c_{s,t} = [\mathscr{P}^{p^{s+t-1}}, c_{s,t-1}]$. For example,

$$c_{0,3} = [\mathscr{P}^{p^2}, [\mathscr{P}^p, \mathscr{P}^1]], \quad c_{1,4} = [\mathscr{P}^{p^4}, [\mathscr{P}^{p^3}, [\mathscr{P}^{p^2}, \mathscr{P}^p]]].$$

The degree of $c_{s,t}$ is

$$\deg c_{s,t} = 2p^s(p^t - 1).$$

We refer to each element $c_{s,t}$ as an *iterated commutator* of *length* t. (We also note that by Milnor's calculation (1.1), the Q_i's can also be viewed as iterated commutators of length $i+1$ — for example, $Q_2 = [\mathscr{P}^p, [\mathscr{P}^1, Q_0]]$.)

For elements in low degrees, alternate notation is sometimes helpful: let $s_i = \mathscr{P}^i$, let $s_{ij} = [s_i, s_j]$, and inductively let $s_{i_1,i_2,\dots,i_n} = [s_{i_1}, s_{i_2,\dots,i_n}]$. Thus when $p = 5$,

$$c_{0,3} = s_{25,5,1} = [\mathscr{P}^{25}, [\mathscr{P}^5, \mathscr{P}^1]].$$

The 's' notation is easier to read: it is easy to read off the elements which form the commutator, and the degree of $s_{i_1,\dots,i_n}$ is just $2(p-1)(i_1 + \cdots + i_n)$. On the other hand, $c_{0,5}$ is more compact than $s_{p^4,p^3,p^2,p,1}$.

Theorem 1.2 (p odd)**.** *Choose a linear ordering on the set*

$$\{c_{s,t} \,:\, s \geq 0,\, t \geq 1\}$$

of iterated commutators. Then the products

$$Q_{i_1} \dots Q_{i_m} c_{s_1,t_1}^{j_1} \cdots c_{s_n,t_n}^{j_n}$$

where $i_1 < \cdots < i_m$, $c_{s_1,t_1} < \cdots < c_{s_n,t_n}$, and $1 \leq j_k \leq p-1$ for each k, form a basis for the Steenrod algebra.

We refer to these bases as "commutator bases". See Theorem 1.3 for the $p = 2$ case, and see Remarks 2.5 and 3.2 for generalizations.

For example, consider the degree 52 part of the mod 3 Steenrod algebra. Note that this degree is divisible by 4. The elements $\mathscr{P}^{3^i}$ have degrees divisible by 4, while the Q_i's have degrees congruent to 1 mod 4. There are only three Q_i's with degree less than 52, so they will not be involved in the basis in this degree. The iterated commutators in degree 52 and below are

$$\begin{aligned} s_1 &= \mathscr{P}^1, \ \deg = 4, & s_3 &= \mathscr{P}^3, \ \deg = 12, \\ s_9 &= \mathscr{P}^9, \ \deg = 36, & s_{31} &= [\mathscr{P}^3, \mathscr{P}^1], \ \deg = 16, \\ s_{93} &= [\mathscr{P}^9, \mathscr{P}^3], \ \deg = 48, & s_{931} &= [\mathscr{P}^9, [\mathscr{P}^3, \mathscr{P}^1]], \ \deg = 52. \end{aligned}$$

Two different commutator bases in this degree are

$$\{s_{931}, s_1 s_{93}, s_9 s_{31}, s_1^2 s_3 s_{31}^2, s_1 s_3 s_9\},$$
$$\{s_{931}, s_{93} s_1, s_{31} s_9, s_{31}^2 s_3 s_1^2, s_9 s_3 s_1\}.$$

There are six iterated commutators involved here, and thus 6! different ways of ordering them, producing 24 different commutator bases in this degree: there are 6 permutations of s_1, s_3, and s_9 for the last entry, the choice between $s_1 s_{93}$ and $s_{93} s_1$ doubles this, and the choice between $s_9 s_{31}$ and $s_{31} s_9$ doubles it again. (The element s_{31} commutes with s_1 and s_3, so its ordering relative to those two elements plays no role.)

1.1. The $p = 2$ case. When $p = 2$, the picture is very similar. The dual of the mod 2 Steenrod algebra has the form

$$\mathscr{A}^* \cong \mathbf{F}_2[\xi_1, \xi_2, \dots],$$

graded by $\deg \xi_i = 2^i - 1$. As in the odd prime case, the Milnor basis is the dual to the monomial basis, with

$$\mathrm{Sq}(r_1, r_2, \dots) \quad \text{dual to} \quad \xi_1^{r_1} \xi_2^{r_2} \dots .$$

A minimal generating set for $\mathscr{A}$ is $\{\mathrm{Sq}^{2^i} : i \geq 0\}$. The iterated commutators $c_{s,t}$ and the s notation are defined exactly as above, with Sq^- in place of $\mathscr{P}^-$; for example,

$$c_{0,3} = s_{421} = [\mathrm{Sq}^4, [\mathrm{Sq}^2, \mathrm{Sq}^1]].$$

The degrees of these commutators are as follows:

$$\deg c_{s,t} = 2^s(2^t - 1), \quad \deg s_{i_1, \dots i_n} = i_1 + \dots + i_n.$$

We have the following result.

Theorem 1.3 ($p = 2$)**.** *Choose a linear ordering on the set*

$$\{c_{s,t} : s \geq 0, t \geq 1\}$$

of iterated commutators. Then the products

$$c_{s_1,t_1} \cdots c_{s_n,t_n},$$

where $c_{s_1,t_1} < \dots < c_{s_n,t_n}$, form a basis for the Steenrod algebra.

1.2. Other results, organization. Many other bases for the Steenrod algebra have been constructed, at least when $p = 2$ — see the papers of Monks [Mon98] and Wood [Woo98] for more information. Wood points out that many of the bases are comprised of products of distinct elements from degrees of the form $2^s(2^t-1)$, and the commutator bases fit into this pattern.

One good feature of the commutator bases is that they are expressed in terms of the algebra generators Q_0 and $\mathscr{P}^{p^n}$. A consequence of this is that the elements of the commutator bases may be explicitly written as polynomials in these generators. Another consequence is that the commutator bases restrict to give bases for the sub-Hopf algebras $\mathscr{A}(n)$ of $\mathscr{A}$. (Unfortunately, they don't restrict to give bases for every sub-Hopf algebra of $\mathscr{A}$

— this is discussed in Section 3.) Fix $n \geq 0$ and recall that $\mathscr{A}(n)$ is the subalgebra of $\mathscr{A}$ generated by Q_0 and $\{\mathscr{P}^{p^i} : 0 \leq i \leq n-1\}$ (or when $p = 2$, the subalgebra generated by $\{\mathrm{Sq}^{2^i} : 0 \leq i \leq n\}$). This turns out to be closed under the coproduct, and hence is actually a sub-Hopf algebra.

Corollary 1.4. *Fix an integer $n \geq 0$.*

(a) *When $p = 2$, an iterated commutator $c_{s,t}$ is in $\mathscr{A}(n)$ if and only if $s+t \leq n+1$. Given a linear ordering on the set $\{c_{s,t} : s+t \leq n+1\}$ of commutators in $\mathscr{A}(n)$, the set of products*

$$c_{s_1,t_1} \cdots c_{s_k,t_k}$$

such that $c_{s_1,t_1} < \cdots < c_{s_k,t_k}$ and $s_i + t_i \leq n+1$ for each i, forms a basis for $\mathscr{A}(n)$.

(b) *When $p > 2$, an iterated commutator $c_{s,t}$ is in $\mathscr{A}(n)$ if and only if $s + t \leq n$. Also, Q_i is in $\mathscr{A}(n)$ if and only if $i \leq n$. Given a linear ordering on the set $\{c_{s,t} : s + t \leq n\}$ of commutators in $\mathscr{A}(n)$, the set of products*

$$Q_{i_1} \ldots Q_{i_m} c_{s_1,t_1}^{j_1} \cdots c_{s_k,t_k}^{j_k}$$

where $i_1 < \cdots < i_m \leq n$, $c_{s_1,t_1} < \cdots < c_{s_n,t_n}$, $s_i + t_i \leq n$, and $1 \leq j_k \leq p-1$, forms a basis for $\mathscr{A}(n)$.

At the prime 2, for example, the ordering $s_1 < s_2 < s_{21}$ determines the following basis for $\mathscr{A}(1)$:

$$\{1, s_1, s_2, s_1 s_2, s_{21}, s_1 s_{21}, s_2 s_{21}, s_1 s_2 s_{21}\}.$$

(For most of these elements, the ordering has no effect; for instance, the six permutations of the elements s_1, s_2, and s_{21} all yield the same product $s_1 s_2 s_{21}$. Changing the ordering can only affect the basis in degree 3, in which the two commutator bases are $\{s_1 s_2, s_{21}\}$ and $\{s_2 s_1, s_{21}\}$.)

Organization: In the next section, we prove Theorems 1.2 and 1.3; the main tools are the May filtration and the Poincaré-Birkhoff-Witt (PBW) theorem. In Section 3, we discuss the relationship between the iterated commutator $c_{s,t}$ and the element P_t^s, and in Section 4, we discuss several ways in which Wall's 1960 paper laid the seeds for the ideas here. Finally, in Section 5, we discuss some questions which motivated this work about relationships between Artin–Schelter regular algebras and finite-dimensional sub-Hopf algebras of the Steenrod algebra.

Acknowledgments. During the writing of this paper, a number of computations were done using the computer software Sage [Sage]. These were of two sorts: checking of results like Lemma 2.3 before we had a proof, and getting Milnor basis expressions for elements like $[\mathrm{Sq}^1, [\mathrm{Sq}^2, [\mathrm{Sq}^4, [\mathrm{Sq}^8, \mathrm{Sq}^{16}]]]]$ — see Section 3. None of the proofs in the paper depend on these calculations.

2. Proof of the main theorem

In this section we prove Theorems 1.2 and 1.3, using the May filtration and the Poincaré–Birkhoff–Witt theorem. Along the way, we compare the iterated commutators to the more familiar Margolis P^s_t elements, and we show that modulo terms of higher filtration, $c_{s,t}$ is congruent to P^s_t. This allows us to prove our main result, and also to reprove a theorem of Monks about P^s_t-bases. For more about how $c_{s,t}$ and P^s_t compare, see Section 3 below.

We can filter any augmented algebra by powers of the augmentation ideal; when applied to the Steenrod algebra $\mathscr{A}$, this is also called the *May filtration*. May first described this in his thesis [May64], and Ravenel has a nice exposition [Rav86].

We let I denote the augmentation ideal of $\mathscr{A}$, and then we define $F^0\mathscr{A} = \mathscr{A}$ and $F^n\mathscr{A} = I^n$ for any $n \geq 1$. One of May's main results [May64, May66] is that the associated graded algebra $\operatorname{gr}\mathscr{A}$ is a primitively generated Hopf algebra, and so is isomorphic to the restricted enveloping algebra of a restricted Lie algebra. In the case of the Steenrod algebra, he identifies the Lie algebra; see Ravenel [Rav86] also. We state what we need of his results below.

For any element $x \in \mathscr{A}$, we write $\overline{x}$ for its image in the associated graded algebra $\operatorname{gr}\mathscr{A}$. We let P^s_t be the Milnor basis element dual to $\xi_t^{p^s}$: that is, $P^s_t = \mathscr{P}(\underbrace{0, \ldots, 0}_{t-1}, p^s)$.

Theorem 2.1 (May). (a) *When $p = 2$, the associated graded algebra $\operatorname{gr}\mathscr{A}$ is isomorphic to the restricted enveloping algebra of the graded restricted Lie algebra with basis $\{\overline{P^s_t} : s \geq 0, t \geq 1\}$. The restriction is trivial.*

(b) *When $p > 2$, the associated graded algebra $\operatorname{gr}\mathscr{A}$ is isomorphic to the restricted enveloping algebra of the graded restricted Lie algebra with basis*

$$\{\overline{Q_i} : i \geq 0\} \cup \{\overline{P^s_t} : s \geq 0, t \geq 1\}.$$

The restriction is trivial.

There is also a description of the Lie bracket, but we do not need it.

We recall another result of May's. Following May [May64], the *weight* of a nonzero element a of $\mathscr{A}$ is the integer n so that $a \in F^n\mathscr{A}$ and $a \notin F^{n+1}\mathscr{A}$. For example, if $a = \mathrm{Sq}^2\,\mathrm{Sq}^2 = \mathrm{Sq}^1\,\mathrm{Sq}^2\,\mathrm{Sq}^1$, then a is in F^2 because it is a product of two indecomposables, and it is also in F^3 since it is a product of three indecomposables. One can see that it may not be written involving nontrivial products of four indecomposables, so the weight of this element is 3. The element $\mathrm{Sq}^4 + \mathrm{Sq}^2\,\mathrm{Sq}^2$ has weight 1, because every expression for it in terms of indecomposables involves the singleton Sq^4.

Lemma 2.2 (Theorem 2.6 in [May64])**.** *Given a finite sequence* $(r_1, r_2, \dots)$ *of non-negative integers, write each* r_i *in base* p*:* $r_i = \sum_j p^j r_{ij}$ *with* $0 \leq r_{ij} \leq p-1$*. Then the weight of the Milnor basis element* $\mathscr{P}(r_1, r_2, \dots)$ *is* $\sum_{i,j} i r_{ij}$*. Also, the weight of* Q_i *is* $i+1$*. Therefore the weight of the Milnor basis element*

$$Q_{i_1} Q_{i_2} \dots \mathscr{P}(r_1, r_2, \dots)$$

is $\sum (i_k + 1) + \sum_{i,j} i r_{ij}$*.*

The weight of a sum of Milnor basis elements is the minimum of the weights of the summands.

For example, the weight of P^s_t is t.

Lemma 2.3.

(a) *Let* x *be an element of* $\mathscr{A}$ *and fix an integer* $k \geq 0$*. The weights of* $\mathscr{P}^{p^k} x$ *and* $x \mathscr{P}^{p^k}$ *are at least one more than the weight of* x*.*

(b) *For any* $s \geq 0$ *and* $t \geq 1$*, the weight of* $c_{s,t}$ *is* t*, and the weight of* $c_{s,t} - P^s_t$ *is at least* $t+1$*.*

Proof. (a) Saying that x has weight at least w means x is in $F^w \mathscr{A} = I^w$; i.e., there is an expression E for x in terms of the indecomposables of $\mathscr{A}$ such that every summand has at least w factors. In this case, each summand in both $\mathscr{P}^{p^k} E$ and $E \mathscr{P}^{p^k}$ has at least $w+1$ factors.

(b) We use induction on t. When $t = 1$, $c_{s,1} = \mathscr{P}^{p^s} = P^s_1$; this starts the induction.

Now suppose that $t \geq 1$ and $c_{st} = P^s_t + (\text{other terms})$, where each of the other terms has weight at least $t+1$. Then

$$\begin{aligned} c_{s,t+1} &= [\mathscr{P}^{p^{s+t}}, c_{st}] \\ &= [\mathscr{P}^{p^{s+t}}, P^s_t] + [\mathscr{P}^{p^{s+t}}, (\text{other terms})]. \end{aligned}$$

The terms in the second commutator are of one of the two forms $x \mathscr{P}^{p^{s+t}}$ or $\mathscr{P}^{p^{s+t}} x$, where x has weight at least $t+1$. By part (a), each of these terms has weight at least $t+2$.

Using Milnor multiplication, one sees that the first commutator equals

$$\begin{aligned} \mathscr{P}^{p^{s+t}} P^s_t - P^s_t \mathscr{P}^{p^{s+t}} = P^s_{t+1} &+ \left(\sum_{j=1}^{p^s - 1} b_j \mathscr{P}(p^{s+t} - p^t j, 0, \dots, 0, p^s - j, j) \right) \\ &- \left(\sum_{j=1}^{p^{s-1}} c_j \mathscr{P}(p^{s+t} - j, 0, \dots, 0, p^s - pj, j) \right) \end{aligned}$$

for some coefficients b_j and c_j, where the entries in each basis element are in positions 1, t, and $t+1$. If $t \geq 2$, then May's lemma 2.2 says that the weight of each such basis element is at least $t+2$. If $t = 1$, then the entries are in positions 1 and 2; both are nonzero, and hence each summand has weight at least 3, as desired.

This finishes the inductive step, and hence the proof. □

Proof of Theorems 1.2 and 1.3. Suppose that p is odd and $\mathfrak{g}$ is a graded restricted Lie algebra over a field of characteristic p. Then one version of the Poincaré–Birkhoff–Witt theorem says that the associated graded algebra of its restricted enveloping algebra $u(\mathfrak{g})$ is isomorphic to a tensor product of an exterior algebra on the odd-degree classes in $\mathfrak{g}$ with a truncated polynomial algebra on the even-degree classes in $\mathfrak{g}$: see Proposition 6.12 and Theorem 7.11 in [MM65], for example. That is, if we choose bases (x_α) for $\mathfrak{g}_{\text{odd}}$ and (y_β) for $\mathfrak{g}_{\text{even}}$, then

$$\operatorname{gr} u(\mathfrak{g}) \cong \Lambda(\overline{x}_\alpha) \otimes k[\overline{y}_\beta]/(\overline{y}_\beta^p).$$

Any choice of basis for $\operatorname{gr} u(\mathfrak{g})$ lifts to give one for $u(\mathfrak{g})$. As a consequence, a basis for $u(\mathfrak{g})$ may be obtained as follows: if we choose orderings on the bases (x_α) and (y_β), then the set of monomials

$$x_1 \dots x_m y_1^{j_1} \dots y_n^{j_n}$$

where $x_1 < \cdots < x_m$, $y_1 < \cdots < y_m$, and $1 \leq j_k \leq p-1$, forms a basis for $u(\mathfrak{g})$.

In the case of interest here, $(\operatorname{gr} \mathscr{A})_{\text{odd}}$ is the restricted enveloping algebra on the graded restricted Lie algebra with basis $(\overline{Q_0}, \overline{Q_1}, \dots)$, while the restricted Lie algebra underlying $(\operatorname{gr} \mathscr{A})_{\text{even}}$ has basis $(\overline{P^s_t} \,:\, s \geq 0, t \geq 1)$. From Lemma 2.3, we see that in $\operatorname{gr} \mathscr{A}$, we have $\overline{c_{s,t}} = \overline{P^s_t}$. Since any lift of a vector space basis for $\operatorname{gr} \mathscr{A}$ gives one for $\mathscr{A}$, we have the desired result.

The case when $p = 2$ is simpler: then the associated graded of a restricted Lie algebra $\mathfrak{g}$ over a field of characteristic 2 is isomorphic to a truncated polynomial algebra $k[y_1, y_2, \dots]/(y_i^2)$, with one generator for each basis element of $\mathfrak{g}$, and the proof proceeds as above. □

This also gives a proof of the following theorem, due to Monks when $p = 2$; the bases constructed here are called P^s_t*-bases*.

Theorem 2.4.

(a) [Mon98] *Let* $p = 2$. *Choose a linear ordering on the set*

$$\{P^s_t \,:\, s \geq 0,\ t \geq 1\}.$$

Then the set of products

$$P^{s_1}_{t_1} \cdots P^{s_n}_{t_n}$$

where $P^{s_1}_{t_1} < \cdots < P^{s_n}_{t_n}$ *forms a basis for the Steenrod algebra.*

(b) *Suppose* $p > 2$. *Choose a linear ordering on the set*

$$\{P^s_t \,:\, s \geq 0,\ t \geq 1\}.$$

Then the set of products

$$Q_{i_1} \dots Q_{i_m} (P^{s_1}_{t_1})^{j_1} \cdots (P^{s_n}_{t_n})^{j_n}$$

where $i_i < \cdots < i_m$, $P^{s_1}_{t_1} < \cdots < P^{s_n}_{t_n}$, and $1 \leq j_k \leq p-1$, forms a basis for the Steenrod algebra.

These restrict, in the obvious way, to bases for any sub-Hopf algebra of the Steenrod algebra.

Remark 2.5. The proof of Theorems 1.2 and 1.3 actually produces more bases than described in the statements of those results. First, one can certainly change the ordering on the Q_i's, although they anticommute, so this only changes the signs of the resulting monomials. One can also intermingle the Q_i's and the $c_{s,t}$'s. Finally, rather than choosing a "global" ordering on, say, the $c_{s,t}$'s, one can choose a different ordering for each monomial. As stated in the proof, any lift of a basis for $\operatorname{gr} u(\mathfrak{g})$ is a basis for $\mathscr{A}$, so one may choose $c_{0,1}c_{0,2}$ as the lift of $\overline{P^0_1 P^0_2}$, while choosing $c_{0,2}c_{0,1}c_{0,3}$ as the lift of $\overline{P^0_1 P^0_2 P^0_3}$. Stating the theorems in this generality is a bit unwieldy and not very motivated, though.

3. Comparing $c_{s,t}$ to P^s_t

Readers familiar with the Steenrod algebra may be curious about the relationship between a given iterated commutator and the element P^s_t in the same degree. Note first that $\deg c_{s,t} = \deg P^s_t$. Also, for any integer $s \geq 0$, by definition we have $c_{s,1} = P^s_1 = \mathscr{P}^{p^s}$.

Lemma 3.1. *Fix an integer $t \geq 1$. Then $c_{0,t} = P^0_t$.*

Proof. This is proved by induction on t: an easy Milnor multiplication computation shows that $[\mathscr{P}^{p^{t-1}}, P^0_{t-1}] = P^0_t$. □

It is easy to see that when $p = 2$, $c_{1,2} = P^1_2$. However, hand and computer calculations [Sage] suggest that for all other combinations of p, s, and t, the elements $c_{s,t}$ and P^s_t differ. One can prove that $c_{s,2} \neq P^s_2$ if $s \geq 2$ at the prime 2: in the Milnor basis, the commutator $[\mathrm{Sq}(2^s), \mathrm{Sq}(2^{s+1})]$ has a term $\mathrm{Sq}(2^{s-1} + 2^s, 2^{s-1})$, arising from the Milnor matrix

$$\left\| \begin{matrix} * & 2^{s-1} \\ 2^s & 2^{s-1} \end{matrix} \right\|$$

in the product $\mathrm{Sq}(2^{s+1})\,\mathrm{Sq}(2^s)$.

By theorems of Anderson and Davis [AD73] and Adams and Margolis [AM74], any sub-Hopf algebra of $\mathscr{A}$ is determined by which P^s_t's (and when p is odd, which Q_n's) it contains, and as a consequence, any P^s_t-basis for the Steenrod algebra restricts to a basis for any sub-Hopf algebra of $\mathscr{A}$. This is not true for commutator bases. For example, when $p = 2$, the sub-Hopf algebra B generated by P^0_3 and P^1_3 is four-dimensional with basis

$$\{1, P^0_3, P^1_3, P^0_3 P^1_3\}.$$

However, the intersection of B with any commutator basis has only three elements:

$$1, c_{03}, c_{03}c_{13}.$$

(The elements c_{03} and c_{13} commute.) Thus commutator bases for $\mathscr{A}$ are not well-suited for studying arbitrary sub-Hopf algebras B of the Steenrod algebra; instead, one should use the Milnor basis or P^s_t-bases, or one should construct new commutator bases, built from algebra generators for B and their iterated commutators.

By the way, there are several ways to define an iterated commutator of consecutive $\mathscr{P}^{p^n}$s. At the prime 2, for example, with the elements Sq^1, Sq^2, and Sq^4, either $c_{0,3} = [[\mathrm{Sq}^1, \mathrm{Sq}^2], \mathrm{Sq}^4]$ or $[\mathrm{Sq}^1, [\mathrm{Sq}^2, \mathrm{Sq}^4]]$ seem like natural choices. These happen to be equal, because $[\mathrm{Sq}^2, [\mathrm{Sq}^1, \mathrm{Sq}^4]] = 0$. Similarly,

$$[[[\mathrm{Sq}^1, \mathrm{Sq}^2], \mathrm{Sq}^4], \mathrm{Sq}^8] = [\mathrm{Sq}^1, [\mathrm{Sq}^2, [\mathrm{Sq}^4, \mathrm{Sq}^8]]].$$

However,

$$[[[[\mathrm{Sq}^1, \mathrm{Sq}^2], \mathrm{Sq}^4], \mathrm{Sq}^8], \mathrm{Sq}^{16}] \neq [\mathrm{Sq}^1, [\mathrm{Sq}^2, [\mathrm{Sq}^4, [\mathrm{Sq}^8, \mathrm{Sq}^{16}]]]].$$

Thus one needs to choose one of these to be the iterated commutator $c_{0,5}$. According to Lemma 3.1, the left side is equal to P^0_5, and this led to the choice made in this paper. This is not entirely arbitrary: the element P^0_n commutes with Sq^{2^i} for $i \leq n-1$, while the element obtained as on the right side does not have such good centrality properties: if we let $b = [\mathrm{Sq}^1, [\mathrm{Sq}^2, [\mathrm{Sq}^4, [\mathrm{Sq}^8, \mathrm{Sq}^{16}]]]]$, then in the Milnor basis, we have

$$b = \mathrm{Sq}(0,0,0,0,1) + \mathrm{Sq}(0,3,1,1) + \mathrm{Sq}(1,3,3) + \mathrm{Sq}(1,5,0,1) + \mathrm{Sq}(6,1,1,1)$$

and

$$[b, \mathrm{Sq}^2] = \mathrm{Sq}(1,1,2,1) + \mathrm{Sq}(2,3,1,1).$$

This element b does not commute with Sq^4, Sq^8, or Sq^{16}, either.

At odd primes, one has the same considerations, as well as sign issues; these determined our choice of $c_{s,t} = [\mathscr{P}^{p^{s+t-1}}, c_{s,t-1}]$. Using $[c_{s,t-1}, \mathscr{P}^{p^{s+t-1}}]$ instead just introduces a sign, of course, but it seems pleasant to have $c_{0,t} = P^0_t$ instead of $c_{0,t} = \pm P^0_t$.

Remark 3.2. Note that if we replace $c_{s,t}$ with iterated commutators defined like b — that is, if we define $c'_{s,1} = \mathscr{P}^{p^s}$ and $c'_{s,t} = [\mathscr{P}^{p^s}, c'_{s+1,t-1}]$ — then Lemma 2.3 still holds, and hence so do Theorems 1.2 and 1.3. This gives yet another family of bases for $\mathscr{A}$.

4. Wall's relations

In a 1960 paper [Wal60], Wall described generators and relations for the mod 2 Steenrod algebra; the generators are the Sq^{2^n}'s, and the relations are of the two forms

$$[\mathrm{Sq}^{2^n}, \mathrm{Sq}^{2^{n+i}}] = (\text{terms}) \quad \text{for } i \geq 2, \tag{4.1}$$

$$(\mathrm{Sq}^{2^n})^2 = (\text{other terms}). \tag{4.2}$$

One could imagine that, given an appropriate ordering of the Sq^{2^n}'s and the other iterated commutators, one could use these relations to prove a PBW type of theorem, thus establishing Theorem 1.3, or at least some cases of it (depending on what properties the ordering might have to satisfy).

Wall proceeded along these lines to produce a basis, the elements of which are *monomials* in the Sq^{2^n}'s — see the end of this section. He also used a precursor of the May filtration, which he called *height* [Wal60, p. 432]: the height of a monomial in the Sq^{2^n}'s is the vector $(i_0, i_1, \dots)$, where i_n is the number of times Sq^{2^n} appears. These are ordered right-lexicographically; then the height of a sum of such monomials is the greatest of the heights of the summands, and the height of an element of the Steenrod algebra is the minimum of the heights of any expression for it as a polynomial in the Sq^{2^n}s. For example, since $\mathrm{Sq}^2 \mathrm{Sq}^2 = \mathrm{Sq}^1 \mathrm{Sq}^2 \mathrm{Sq}^1$, there are two possible height vectors for this element: $(0, 2)$ and $(2, 1)$. Since $(2, 1)$ is smaller in the right lex ordering, it is the height of $\mathrm{Sq}^2 \mathrm{Sq}^2$. From [Wal60, Theorem 3] and Lemma 2.2, it follows that if $(i_0, i_1, \dots)$ is the height of a Milnor basis element $\mathrm{Sq}(r_1, r_2, \dots)$, then its May weight is $\sum i_n$.

We also note that Wall actually used the iterated commutators we are discussing; he wrote T^t_s for what we call $c_{s,t}$ [Wal60, p. 436].

Thus the ideas in this paper are descended from those of Wall's, even though we have not explicitly used any of his results, and we only discovered some of the connections (such as Wall's use of the iterated commutators) after we had proved our main results.

Now we describe Wall's basis for the mod 2 Steenrod algebra, the closely related "Arnon A basis," and a possible connection with commutator bases. Wall's basis first appeared in [Wal60], and Arnon's A basis first appeared in [Arn94]. Both are discussed in [Mon98].

For integers $m \geq k$, let

$$Q^m_k = \mathscr{P}^{2^k} \mathscr{P}^{2^{k+1}} \cdots \mathscr{P}^{2^{m-1}} \mathscr{P}^{2^m},$$
$$X^m_k = \mathscr{P}^{2^m} \mathscr{P}^{2^{m-1}} \cdots \mathscr{P}^{2^{k+1}} \mathscr{P}^{2^k}.$$

At the prime 2, the set of words in the Q^m_k's, ordered in decreasing left lexicographic order on the pairs (m, k), is a basis for $\mathscr{A}$ — this is the *Wall basis* — as is the set of words in the X^m_k's, ordered in increasing left lexicographic order on the pairs (m, k) — this is *Arnon's A basis.*

(Karaca [Kar02] has claimed the existence of similar bases at odd primes, although the statements of his results are problematic.)

We refer to these as *monomial* bases, since their elements are monomials in the algebra generators Sq^{2^n}, $n \geq 0$. For example, in degree 5, we have

$$\text{Wall basis} : \{Q_1^1 Q_0^1, Q_2^2 Q_0^0\} = \{(\mathrm{Sq}^2)(\mathrm{Sq}^1 \mathrm{Sq}^2), (\mathrm{Sq}^4)(\mathrm{Sq}^1)\},$$
$$\text{Arnon's A basis} : \{X_0^1 X_1^1, X_0^0 X_2^2\} = \{(\mathrm{Sq}^2 \mathrm{Sq}^1)(\mathrm{Sq}^2), (\mathrm{Sq}^1)(\mathrm{Sq}^4)\}.$$

Now we put the commutators $c_{s,t}$ in decreasing left lexicographic ordering on the pairs $(s+t, s)$:

$$c_{0,1} < c_{0,2} < c_{1,1} < c_{0,3} < c_{1,2} < c_{2,1} < c_{0,4} < \cdots .$$

In the 's' notation, this is the ordering

$$s_1 < s_{21} < s_2 < s_{421} < s_{42} < s_4 < s_{8421} < \cdots .$$

This ordering gives a commutator basis. If we make the assignment

$$c_{s,t} \mapsto X_s^{s+t-1},$$

then the elements of this commutator basis produce the elements of Arnon's A basis. More precisely, for each pair (s,t), the Arnon monomial X_s^{s+t-1} is a summand of $c_{s,t}$, and may be considered the "leading" summand. Indeed, given a commutator basis element $c_{s_1,t_1} \cdots c_{s_n,t_n}$, expand each c_{s_i,t_i} in terms of the generators Sq^{2^m} and then sort the resulting summands left lexicographically; for example,

$$\begin{aligned} s_{21} s_{42} &= (\mathrm{Sq}^1 \mathrm{Sq}^2 + \mathrm{Sq}^2 \mathrm{Sq}^1)(\mathrm{Sq}^2 \mathrm{Sq}^4 + \mathrm{Sq}^4 \mathrm{Sq}^2) \\ &= \mathrm{Sq}^1 \mathrm{Sq}^2 \mathrm{Sq}^2 \mathrm{Sq}^4 + \mathrm{Sq}^1 \mathrm{Sq}^2 \mathrm{Sq}^4 \mathrm{Sq}^2 \\ &\quad + \mathrm{Sq}^2 \mathrm{Sq}^1 \mathrm{Sq}^2 \mathrm{Sq}^4 + \mathrm{Sq}^2 \mathrm{Sq}^1 \mathrm{Sq}^4 \mathrm{Sq}^2, \end{aligned}$$

with the summands going from smallest to largest. Then the Arnon basis element $X_{s_1}^{s_1+t_1-1} \cdots X_{s_n}^{s_n+t_n-1}$ is the largest term in this expansion. This is a step toward reproving that Arnon's A basis is in fact a basis.

Similarly, if we reverse the ordering on the commutators, we get a different basis, and the assignment $c_{s,t} \mapsto Q_s^{s+t-1}$ converts this commutator basis to the Wall basis.

Problem 4.3. Make these arguments precise; produce alternate proofs of Wall's and Arnon's results, as well as odd primary analogues.

Problem 4.4. Generalize these arguments and use them to find more monomial bases for the Steenrod algebra.

5. Artin–Schelter regular algebras

The results in this paper were discovered while investigating questions about sub-Hopf algebras of the Steenrod algebra and Artin–Schelter regular algebras. For example:

Question 5.1. Let $p = 2$. For any $n \geq 0$, what is the smallest possible global dimension of an Artin–Schelter regular algebra mapping onto $\mathscr{A}(n)$?

This has been resolved for $n = 0$ and $n = 1$, but not for $n \geq 2$. See below.

We should recall the following definition; see [AS87], [Ste96], and others.

Definition 5.2. A graded connected algebra R over a field k is called *Artin–Schelter regular* (or *AS regular*) if the following three conditions hold.

(AS1) R has finite global dimension d.

(AS2) R is *Gorenstein*, i.e., for some integer l,

$$\operatorname{Ext}^i_R(k, R) \cong \begin{cases} k(l) & \text{if } i = d \\ 0 & \text{if } i \neq d \end{cases}$$

where k is the trivial module $R/R_{\geq 1}$ and $k(l)$ is a shift of it.

(AS3) R has finite polynomial growth; i.e., there is positive number c such that $\dim R_n < c\, n^c$ for all $n \geq 0$.

Artin–Schelter regular algebras form an important class of algebras. As suggested in the introduction of [LPWZ07], for example, the noncommutative noetherian AS regular algebras can be viewed as good analogues of finitely generated polynomial algebras. The analogy is not fully developed though: the following is unresolved.

Problem 5.3. Classify the homomorphic images of the noetherian AS regular algebras. If an algebra is the homomorphic image of a noetherian AS regular algebra, find the smallest global dimension among the AS regular algebras mapping onto it.

Of course, if we replace "AS regular" by "finitely generated polynomial," we get precisely the finitely generated commutative algebras, and the smallest possible global dimension is just the size of a minimal generating set. With the problem as stated, though, finite generation is not sufficient: the free algebra $k\langle x, y\rangle$ is finitely generated, but from (AS3) one can see that there is no AS regular algebra mapping onto it.

If $\mathfrak{g}$ is a finite-dimensional positively graded Lie algebra, then its enveloping algebra $U(\mathfrak{g})$ is AS regular with global dimension equal to the vector space dimension of $\mathfrak{g}$. From this, one can show that any finite-dimensional graded connected algebra B is the image of an AS regular algebra: via the adjointness between $U(-)$ and the forgetful functor from algebras to Lie algebras, there is a surjective algebra map $U(B) \twoheadrightarrow B$. This leads to questions like 5.1 above.

Regarding Question 5.1, when $n = 0$, $\mathscr{A}(0) = \mathbf{F}_2[s_1]/(s_1^2)$, so let $R(0) = \mathbf{F}_2[s_1]$. This has global dimension 1, which is clearly as small as possible. When $n = 1$, let

$$R(1) = \mathbf{F}_2\langle s_1, s_2\rangle/([s_1, s_{21}], [s_2, s_{21}]),$$

where as usual, $s_{21} = [s_1, s_2]$. This algebra is AS regular since it is an enveloping algebra, and it maps onto $\mathscr{A}(1)$. The kernel is the ideal

$$(s_1^2,\ s_2^2 + s_1 s_{21},\ s_{21}^2).$$

The algebra $R(1)$ has global dimension 3, and one can show that there is no AS regular algebra of smaller dimension mapping onto $\mathscr{A}(1)$ (for example using a classification of AS regular algebras of dimension at most 2). When $n = 2$, we found an AS regular algebra $R(2)$ of dimension 6 mapping onto $\mathscr{A}(2)$:

$$R(2) = \mathbf{F}_2\langle s_1, s_2, s_4\rangle / I$$

where I is the ideal generated by the relations

$$[s_1, s_{21}], \quad [s_2, s_{21}], \quad [s_2, s_{421}], \quad [s_1, s_4] + s_2 s_{21},$$
$$[s_2, s_{42}] + s_1 s_{421}, \quad [s_4, s_{42}] + s_2 s_1 s_{421}$$

(where s_{21}, etc., are commutators, as above). One can show that $R(2)$ is AS regular by constructing it as an iterated Ore extension: start with the polynomial algebra on s_1 and s_{12}, then adjoin s_2, s_{124}, s_{24}, and s_4, in that order. The kernel of the map $R(2) \twoheadrightarrow \mathscr{A}(2)$ is the ideal

$$(s_1^2,\ s_2^2 + s_1 s_{21},\ s_{21}^2,\ s_4^2 + s_2 s_{42},\ s_{42}^2,\ s_{421}^2).$$

$R(2)$ has dimension 6, and we believe this to be smallest possible, but we were unable to prove it. We note that in each of these cases, the global dimension of $R(n)$ equals the number of iterated commutators $c_{s,t}$ (which equals the number of P^s_t elements) in the Hopf algebra $\mathscr{A}(n)$. We were unable to extend this to the $n = 3$ case, but it leads to a possible answer to Question 5.1.

Guess 5.4. Let $p = 2$. For any $n \geq 0$, the algebra $\mathscr{A}(n)$ is the homomorphic image of an Artin–Schelter regular algebra of global dimension $\binom{n+2}{2}$. Any AS regular algebra mapping onto $\mathscr{A}(n)$ has global dimension at least $\binom{n+2}{2}$. Indeed, if B is any finite-dimensional sub-Hopf algebra of $\mathscr{A}$, then there is an AS regular algebra of global dimension $\log_2 \dim_{\mathbf{F}_2} B$ mapping onto B, and this global dimension is as small as possible.

One viewpoint is this: any such Hopf algebra B may be filtered so that its associated graded algebra is a restricted enveloping algebra $u(\mathfrak{g})$ for a restricted Lie algebra $\mathfrak{g}$ (with trivial restriction) of dimension $d = \log_2 \dim_{\mathbf{F}_2} B$. Thus the (full) enveloping algebra $U(\mathfrak{g})$ is an AS regular algebra of global dimension d. Perhaps the filtration can be "unwound" to get an algebra R mapping onto B, so that there is a filtration on R with associated graded $U(\mathfrak{g})$. This would give R the structure of an AS regular algebra of dimension d. That is, we hope for an AS regular algebra R, filtered compatibly with B, fitting into this diagram:

$$\begin{array}{ccc} R & \overset{\mathrm{gr}}{\dashmapsto} & U(\mathfrak{g}) \\ \vdots\downarrow\!\downarrow & & \downarrow\!\downarrow \\ B & \overset{\mathrm{gr}}{\longmapsto} & u(\mathfrak{g}) \end{array}$$

In other words, especially in light of how $R(0)$, $R(1)$ and $R(2)$ are defined above: one should view the Hopf algebra B as some sort of deformation of the restricted enveloping algebra $u(\mathfrak{g})$, and so it has relations of two types: if its generators and their iterated commutators are denoted $\{x_i\}$, then there will be "commutator relations" $[x_i, x_j] = \cdots$ and "restriction relations" $x_i^p = \cdots$. (For example, in addition to the relations for $\mathscr{A}(n)$ and $R(n)$ above, see also Wall's relations (4.1)–(4.2).) Ideally, R should be defined just by using the commutator relations.

In any case, given a sub-Hopf algebra B of $\mathscr{A}$, understanding its generators, their iterated commutators, and the resulting commutator and restriction relations should provide insight into the structure of B and the AS regular algebras mapping onto it.

References

[AD73] Anderson, Donald W.; Davis, Donald M. A vanishing theorem in homological algebra. *Comment. Math. Helv.* **48** (1973), 318–327. MR0334207 (48 #12526), Zbl 0267.55022, doi: 10.1007/BF02566125.

[AM74] Adams, J. F.; Margolis, H. R. Sub-Hopf-algebras of the Steenrod algebra. *Proc. Cambridge Philos. Soc.* **76** (1974), 45–52. MR0341487 (49 #6238), Zbl 0283.55012.

[Arn94] Arnon, Dan. Monomial bases in the Steenrod algebra. *J. Pure Appl. Algebra* **96** (1994), no. 3, 215–223. MR1303282 (95i:55015), Zbl 0840.55012.

[AS87] Artin, Michael; Schelter, William F. Graded algebras of global dimension 3. *Adv. in Math.* **66** (1987), no. 2, 171–216. MR0917738 (88k:16003), Zbl 0633.16001, doi: 10.1016/0001-8708(87)90034-X.

[Kar02] Karaca, Ismet. Nilpotence relations in the mod-p Steenrod algebra. *J. Pure Appl. Algebra* **171** (2002), no. 2–3, 257–264. MR1904482 (2003d:55019), Zbl 1034.55008, doi: 10.1016/S0022-4049(01)00158-X.

[LPWZ07] Lu, D.-M.; Palmieri, J. H.; Wu, Q.-S.; Zhang, J. J. Regular algebras of dimension 4 and their A_∞-Ext-algebras. *Duke Math. J.* **137** (2007), no. 3, 537–584. MR2309153 (2008d:16022), Zbl 1193.16014, arXiv:math/0411497, doi: 10.1215/S0012-7094-07-13734-7.

[May64] May, J. P. The cohomology of restricted Lie algebras and of Hopf algebras; application to the Steenrod algebra. Thesis (Ph.D.) - Princeton University. *ProQuest LLC, Ann Arbor, MI*, 1964. 171 pp. MR2614527.

[May66] May, J. P. The cohomology of restricted Lie algebras and of Hopf algebras. *J. Algebra* **3** (1966), 123–146. MR0193126 (33 #1347), Zbl 0163.03102, doi: 10.1016/0021-8693(66)90009-3.

[Mil58] Milnor, John. The Steenrod algebra and its dual. *Ann. of Math.* (2) **67** (1958), 150–171. MR0099653 (20 #6092), Zbl 0080.38003.

[MM65] Milnor, John W.; Moore, John C. On the structure of Hopf algebras. *Ann. of Math.* (2) **81** (1965), 211–264. MR0174052 (30 #4259), Zbl 0163.28202.

[Mon98] Monks, Kenneth G. Change of basis, monomial relations, and P_t^s bases for the Steenrod algebra. *J. Pure Appl. Algebra* **125** (1998), no. 1–3, 235–260. MR1600025 (98i:55020), Zbl 0889.55009, doi: 10.1016/S0022-4049(96)00140-5.

[Rav86] Ravenel, Douglas C. Complex cobordism and stable homotopy groups of spheres. Pure and Applied Mathematics, 121. *Academic Press Inc., Orlando, FL*, 1986. xx+413 pp. ISBN: 0-12-583430-6; 0-12-583431-4. MR0860042 (87j:55003), Zbl 0608.55001.

[Sage] Stein, William; et al. Sage Mathematics Software (version 5.4.1), The Sage Development Team, 2012, http://www.sagemath.org.

[Ste96] Stephenson, D. R. Artin-Schelter regular algebras of global dimension three. *J. Algebra* **183** (1996), no. 1, 55–73. MR1397387 (97h:16053), Zbl 0868.16027, doi: 10.1006/jabr.1996.0207.

[Wal60] Wall, C. T. C. Generators and relations for the Steenrod algebra. *Ann. of Math.* (2) **72** (1960), 429–444. MR0116326 (22 #7117), Zbl 0137.16603.

[Woo98] Wood, R. M. W. Problems in the Steenrod algebra. *Bull. London Math. Soc.* **30** (1998), no. 5, 449–517. MR1643834 (99h:55028), Zbl 0924.55015, doi: 10.1112/S002460939800486X.

Department of Mathematics, Box 354350, University of Washington, Seattle, WA 98195, USA
palmieri@math.washington.edu
zhang@math.washington.edu

This paper is available via http://nyjm.albany.edu/j/2013/19-3.html.