ELSEVIER

Topology and its Applications 65 (1995) 105–122

TOPOLOGY AND ITS APPLICATIONS

The annihilator ideal of the action of the Steenrod algebra on $H^*(RP^\infty)$

V. Giambalvo [a,*], F.P. Peterson [b]

[a] *Department of Mathematics, University of Connecticut, Storrs, CT 06268, USA*

[b] *Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 01239, USA*

Received 22 March 1993; revised 6 December 1993, 22 June 1994, 5 August 1994

Abstract

The mod 2 cohomology of real projective space RP^∞ has a simple, but rich structure as a module over the Steenrod algebra. In this paper we determine the annihilator ideal of $H^*(RP^\infty)$, and some other spaces of interest.

Keyword: Steenrod algebra

AMS classification: Primary 55S10, Secondary 08A35

1. Introduction and statement of results

The operation of the mod 2 Steenrod algebra on $H^*(P^q)$, the cohomology of a product of q copies of RP^∞, has been studied for about 40 years. Many results have been proven and many applications have been given. One problem that has not been solved is the following: what Steenrod operations annihilate every element in $H^*(P^q)$. This question is open even for $q = 1$ (see [3]).

Let $\mathcal{K}(X) \subset \mathcal{A}$, the mod 2 Steenrod algebra, be the ideal of elements which annihilate every element in $H^*(X)$, that is the kernel of the map $\mathcal{A} \to \mathcal{E} = \mathrm{End}(H^*(X))$, a two sided ideal in $\mathcal{A}$ of elements which annihilate every element of $H^*(X)$. Our first theorem computes $\mathcal{K}(P^1)$.

Theorem 1. *There exists elements $\phi_{r,s} \in \mathcal{A}$, in dimension $2^s(2^r + 2^{r-1} + 5)$, $s \geqslant 0$, $r \geqslant 4$, such that $\mathcal{K}(P^1)$ is the two sided ideal generated by $Sq^{2^r}Sq^{2^r}$, $r \geqslant 1$, and $\phi_{r,s}$. Furthermore these form a minimal set of generators for $\mathcal{K}(P^1)$.*

* Corresponding author.

SSDI 0166-8641(94)00109-X

It is easy to see that $Sq^{2^r}Sq^{2^r}$ is in $\mathcal{K}(P^1)$, but the other elements are more mysterious. $\phi_{r,s+1}$ is the double of $\phi_{r,s}$, so the important elements are $\phi_{r,0}$, and they will be described in detail in Section 5. The lowest dimensional new element is $\phi_{4,0}$ in dimension 29.

Although a closed form or generating function for the size of $\mathcal{A}/\mathcal{K}(P^1)$ remains elusive, the following theorem provides an efficient algorithm for determining $\rho_n = \operatorname{rank}_{Z/2}(\mathcal{A}/\mathcal{K}(P^1))_n$. We denote as usual by $\alpha(k)$ the number of 1's in the dyadic expansion of k.

Theorem 2. *For every integer k, $0 < k \leqslant n$, there is an equation with positive integer unknowns, $r_1, r_2, \ldots, r_\ell$, where $\ell = \alpha(k)$ given as follows: Let $k = \sum 2^{i_s}$ be the dyadic expansion of k. The equation is $\sum 2^{i_s+r_s} = n + k$. Then ρ_n is the number of k's for which the corresponding equation has at least one solution.*

We believe that a determination of a set of minimal generators for $\mathcal{K}(P^q)$ is hard. The following gives an algebraic "description" of $\mathcal{K}(X \times Y)$.

Theorem 3. $\mathcal{K}(X \times Y) = \{a \in \mathcal{A} \mid \psi(a) \in \mathcal{K}(X) \otimes \mathcal{A} + A \otimes \mathcal{K}(Y)\}$.

The lowest dimensional element in $\mathcal{K}(P^q)$ is $Sq^{2^{q+1}-1}Sq^{2^q-1}\cdots Sq^3Sq^1$, or in the Milnor basis $Sq(1,1,\ldots,1)$, with $q+1$ ones. The dimension of this element increases rapidly as q increases. Thus this may yield a method for verifying identities in $\mathcal{A}$.

We note the following easy theorem.

Theorem 4. $\mathcal{K}(BO_q) = \mathcal{K}(P^q)$.

This, together with Theorem 3 has the following consequence.

Corollary 5. $\mathcal{K}(BO) = 0$.

Our last main theorem is the determination of $\mathcal{K}(K(Z/2,n))$, $n > 1$. The result is somewhat surprising.

Theorem 6. $\mathcal{K}(K(Z/2,n)) = 0$ *for* $n > 1$.

The proofs will be given in Sections 2–6. A main technical tool will be a new additive basis for the Steenrod algebra discovered by Arnon [1]. This will be described in Section 2. Section 3 contains the proofs of Theorem 3 and Theorem 4. Section 4 contains the proof of Theorem 6. The final two sections are devoted to the proof of Theorems 1 and 2.

2. The Arnon basis for $\mathcal{A}$

We collect in this section a description of, and some facts about, a basis for the Steenrod algebra that was recently discovered by Arnon [1].

This basis consists of monomials in the indecomposable elements in the Steenrod algebra, i.e., Sq^{2^i}, $i \geqslant 0$. For any two integers i, j, $j \geqslant i$, we define a "string" s_i^j to be the product $Sq^{2^j} Sq^{2^{j-1}} \cdots Sq^{2^i}$. The basis elements consist of all finite products $s_{i_1}^{j_1} s_{i_2}^{j_2} \cdots s_{i_q}^{j_q}$, where $j_s \leqslant j_{s+1}$, and if $j_s = j_{s+1}$, then $i_s < i_{s+1}$. We call the sequence of j's the "tops" of the basis element, and the sequence of i's the "bottoms". We also write s_i for $s_i^i = Sq^{2^i}$.

In order to prove Theorem 6 we will need to order the elements of this basis in a particular way. We construct this ordering on the set of all basis elements in the following manner: Let $R = (r_0^0, r_0^1, r_1^1, r_0^2, r_1^2, r_2^2, \ldots)$ be a sequence of 0's and 1's, with finitely many 1's. Then a basis element is just the product $(s_0^0)^{r_0^0}(s_0^1)^{r_0^1} \cdots$. We order the sequences lexicographically from the left. This gives an ordering on the basis elements.

Denote by $\mathcal{I}_0$ the two-sided ideal in $\mathcal{A}$ generated by $\{Sq^{2^i} Sq^{2^i},\ i > 0\}$. Lemma 5.1 gives an alternate description of this ideal as the ideal generated by all elements of the form $s_i(\prod_{k_j > i} s_{k_j})s_i$. So an Arnon basis element for which the bottoms are not strictly increasing is in $\mathcal{I}_0$, but $\mathcal{I}_0$ is larger than the span of these. Let $\mathcal{V}$ be the vector subspace of $\mathcal{A}$ spanned by the Arnon basis elements with strictly increasing bottoms. We will refer to elements of this subspace as "not obviously in $\mathcal{I}_0$". The element of least dimension which is in $\mathcal{I}_0$ and also in $\mathcal{V}$ is $s_0^1 s_1^1 s_2^3 + s_0^1 s_1^1 s_2^2 s_3^3 + s_0^2 s_1^2 s_2^2$. We will call this element $\phi_{3,0}$, for reasons which will be apparent later.

3. The product theorem

In this section we will prove Theorems 3 and 4. We first consider Theorem 3. For fixed spaces X and Y, let $\mathcal{K}_\times = \{a \in \mathcal{A} \mid \psi(a) \in \mathcal{K}(X) \otimes \mathcal{A} + A \otimes \mathcal{K}(Y)\}$. Theorem 3 says that $\mathcal{K}(X \times Y) = \mathcal{K}_\times$. Consider the composition

$$\mathcal{A} \xrightarrow{\psi} \mathcal{A} \otimes \mathcal{A} \xrightarrow{\pi} \mathcal{A}/\mathcal{K}(X) \otimes \mathcal{A}/\mathcal{K}(Y) \xrightarrow{\alpha} \operatorname{End} H^*(X) \times \operatorname{End} H^*(Y)$$
$$\xrightarrow{\beta} \operatorname{End}\big(H^*(X) \otimes H^*(Y)\big) = \operatorname{End}\big(H^*(X \times Y)\big).$$

The kernel of this composite is $\mathcal{K}(X \times Y)$ by definition. α and β are monomorphisms, hence $\mathcal{K}(X \times Y) = Ker(\pi\psi)$. But $Ker(\pi\psi) = \mathcal{K}_\times$. This proves Theorem 3.

Theorem 4 says that if a Steenrod operation vanishes on all symmetric polynomials in the one dimensional generators $\{x_1, x_2, \ldots, x_q\}$ of $H^*(P^q)$, then it vanishes on all polynomials, or conversely if it is nonzero on some polynomial, then it is nonzero on a symmetric polynomial. So let $a \in \mathcal{A}$, and $w = x_1^{i_1} \cdots x_q^{i_q} \in H^*(P^q)$ be a monomial such that $a(w) \neq 0$. Let $k_1, \ldots, k_q$ be the largest exponents of $x_1, \ldots, x_q$ which appear in any monomial in $a(w)$. Choose an integer k such that $2^k > \max(|a|, k_1, \ldots, k_q)$ and let $w' = wx_q^{2^k}$. Then $a(w') = a(w)x_q^{2^k}$ and the largest exponent in any monomial in $a(w')$ is $k_q + 2^k$. Choose an integer j such that $2^j > i_q + 2^k$, and define $u = x_1^{2^{j+1}} \cdots x_q^{2^{j+q}}$. Then $a(uw') = ua(w') \neq 0$. Also all exponents in uw' are different, so the symmetric polynomial containing uw' is $\sum_{S_q} uw'$. The highest exponent of $a(\sum uw')$ is $k_q + 2^k + 2^{j+q}$, and it cannot be canceled by another term. Thus $a \notin \mathcal{K}(BO(q))$.

4. $K(K(Z/2,n)) = 0$, $n > 1$

This section contains the proof of Theorem 6. We first prove the theorem in the case $n = 2$, since this case provides the ideas, methods, and motivation for the general case.

We choose, for each basis element $a \in \mathcal{A}$, a class $u_a \in H^*(K(Z/2,2))$ such that if $\{a_k\}$ is the basis for $\mathcal{A}$ in a given dimension, then the matrix $\{a_k(u_{a_l})\}$ is nonsingular. The basis for $\mathcal{A}$ which we will use is the Arnon basis together with the order described in Section 2.

Recall that $H^*(K(Z/2,2))$ is a polynomial algebra with generators ι, $s_0^0\iota$, $s_0^1\iota$, $s_0^2\iota, \ldots$. If $R = s_l^k$, let $u_R = (s_0^{k-l+1}\iota)^{2^l}$. If $R = (r_0^0, r_0^1, r_0^2, \ldots)$, we let

$$u_R = \prod \left(\left(s_0^{k-l+1}\iota \right)^{2^l} \right)^{r_l^k}.$$

Define $\langle R', u_R \rangle$ to be the coefficient of $(Sq^1(\iota))^n$ which appears in $R'(u_R)$, where $n = (|R'| + |u_R|)/3$. We order the Arnon basis elements by ordering $R = (r_0^0, \ldots)$ lexicographically from the left. Consider all R of a given dimension and form the matrix $\langle R', u_R \rangle$. The theorem follows from the following proposition.

Proposition 4.1. *This matrix is lower triangular with ones on the diagonal, i.e., if $R' > R$ and R and R' have the same dimension, then $\langle R', u_R \rangle = 0$, and $\langle R, u_R \rangle = 1$.*

We first study how the Steenrod operations operate on the u_R's.

Lemma 4.2.

$$Sq^i\left(\left(s_0^{k-l+1}\iota \right)^{2^l} \right) = \begin{cases} (s_0^{k-l}\iota)^{2^{l+1}}, & \text{if } i = 2^l, \\ (s_0^{k-l+2}\iota)^{2^l}, & \text{if } i = 2^{k+1}, \\ (s_0^{k-l+1}\iota)^{2^{l+1}}, & \text{if } i = 2^{k+1} + 2^l, \\ 0, & \text{otherwise.} \end{cases}$$

This lemma is straightforward to prove. We note that the u_R are sent to other u_R's or 0. We also note that in the first case of this lemma k remains constant and l increases by 1, while in the other 2 cases k increases by 1, so $Sq^i((s_0^{k-l+1}\iota)^{2^l})$ is either 0 or u'_R, with $R' < r_l^k$, as long as $i > 0$.

Corollary 4.3. *Let Sq^I be an Adem basis element. Then $Sq^I((s_0^{k-l+1}\iota)^{2^l}) = (s_0^0\iota)^{2^{k+1}} +$ other terms in the monomial basis for $H^*(K(Z/2,2))$ if and only if $Sq^I = s_l^k$.*

Proof. The k for $(s_0^0\iota)^{2^{k+1}}$ has not increased and thus by the remark above, the only Adem basis element that can do this is $Sq^I = s_l^k$. □

Hold R fixed and consider all R' with $|R'| = |R|$. Note that

$$|u_R| = \sum_{r_l^k \neq 0} \left(2^{k+2} + 2^l\right).$$

To get $(Sq^1(\iota))^n = (s_0^0\iota)^n$, where $n = (|R'|+|u_R|)/3$, in $R'(u_R)$, each term $(s_0^{k-l+1}\iota)^{2^l}$ which appears in u_R must be sent to $(s_0^0)^{2^{k+l}}$ or a higher power of $s_0^0\iota$. By Corollary 4.3, an s_l^k must appear in the diagonal of R' and act on $(s_0^{k-l+1})^{2^l}$. Thus, if $s < k$, then $Sq^{2^s}(au_{k_1,l_l})$ cannot have the correct power of s_0^0 if $k_1 \geqslant k$. Here $au_{(k_1,l_1)}$ comes from a previous s_l^k.

Let (k,l) be the first term where $R' \neq R$, i.e., $r'^k_l = 1$, $r_l^k = 0$ as $R' > R$ and for smaller (k_2,l_2), $r'^{k_2}_{l_2} = r_{l_2}^{k_2}$. When s_l^k acts on the partially formed $R'(u_R)$, the terms $u_{(k_1,l_1)}$ with $k_1 > k$ must have already been sent to the appropriate power of $s_0^0\iota$. Hence s_l^k acts on terms of the form $au_{(k,l_1)}$, i.e., $k_1 = k$. Then $l_1 > l$, so $au_{(k,l_1)} = v^{2^{l_1}}$ and thus $Sq^{2^l}(v^{2^{l_1}}) = 0$. For dimensional reasons, s_l^k must act on such a term as the rest of the terms in u_R match up with R'. When $R' = R$, this argument gives $\langle R, u_R\rangle = 1$. This proves Proposition 4.1, and hence Theorem 6 for $n = 2$.

To complete the proof we now give the modifications needed for $n > 2$. Let $(a(\iota_2))^{2^r}$ be a 2^rth power of a polynomial generator in $H^*(Z/2,2)$. There is an Adem basis element acting on ι_2 which gives $(a(\iota_2))^{2^r}$. Denote this basis element by $\theta(a,r)$. For example $(\iota_2)^4 = Sq^4Sq^2\iota_2$, so $\theta(Sq^0,2) = Sq^4Sq^2 = s_1^2$.

We modify u_R as follows: Let $n = \sum 2^j$ be the dyadic expansion of n. Then

$$\big(Sq^1(\iota_2)\big)^n = \prod_j \big(Sq^1(\iota_2)\big)^{2^j} = \prod_j \theta\big(Sq^1,j\big)(\iota_2).$$

So we replace $(Sq^1(\iota_2))^n$ by $\prod_j \theta(Sq^1,j)(\iota_n)$.

If $R = s_l^k$ let $u_R = \theta(s_0{}^{k-l+1},l)\iota_n$, and for an arbitrary basis element R, we let

$$u_R = \prod \big(\theta\big(s_0{}^{k-l+1},l\big)(\iota_n)\big)^{r_l^k}.$$

In the definition of $\langle R', u_R\rangle$, replace $(Sq^1(\iota_2))^n$ as follows: $(Sq^1(\iota_2))^n$ = a product of terms of the form $(Sq^1(\iota_2))^{2^r} = \theta(Sq^1,r)\iota_2$, corresponding to the dyadic expansion of n. Replace $(Sq^1(\iota_2))^n$ by the corresponding product of $\theta(Sq^1,r)\iota_n$.

With these changes the above argument for $n = 2$ generalizes to prove Proposition 4.1 for $n > 2$, and hence Theorem 6.

5. Factoring the map

In this section we construct an algebra S and factor the map

$$\mathcal{A} \to \mathcal{E} = \mathrm{End}\big(H^*(RP^\infty, Z/2)\big)$$

through S, so that the map $S \to \mathcal{E}$ is a monomorphism. We construct some useful elements in the Steenrod algebra, and the ideal, which we call $\mathcal{I}_1 \subset \mathcal{K}$ that we are looking for and show that the set of generators described in Theorem 1 is minimal. The proof that $\mathcal{I}_1$ is the desired ideal requires some different techniques, and is completed in the last section, along with the proof of Theorem 2.

Let $\mathcal{I}_0$ be the ideal in the mod 2 Steenrod algebra $\mathcal{A}$ generated by $\{Sq^{2^j}Sq^{2^j},\ j \geqslant 0\}$. Then $\mathcal{I}_0 \subset \mathcal{K}$ since for any j, n, either $\binom{n}{2^j}$ or $\binom{n+2^j}{2^j}$ must be zero mod 2. There is

another description of $\mathcal{I}_0$ that will be useful. Let $s_i = Sq^{2^i} \in \mathcal{A}$. Then for the same reason as above, $s_i(\prod_{k_j>i} s_{k_j})s_i$ must be in $\mathcal{K}$. From Wall [2] one sees easily:

Lemma 5.1. *The ideal generated by all products of the form $s_i(\prod_{k_j>i} s_{k_j})s_i$ is equal to $\mathcal{I}_0$ and furthermore $\mathcal{A}/\mathcal{I}_0$ is the free graded algebra over $Z/2$ on generators $\{s_i,\ i \geqslant 0\}$ with degree $s_i = 2^i$, and relations*

(1) $s_i^2 = 0$,
(2) $s_i s_{i+1} s_i = 0$,
(3) $s_i s_j + s_j s_i + s_{i-1} s_j s_{i-1} = 0$ *if* $j < i - 1$.

We now construct an algebra S, modeled on $\mathcal{A}/\mathcal{I}_0$ with an additional generator t corresponding to the endomorphism which is multiplication by the generator $x \in H^1(RP^\infty)$.

Definition 5.2. Let S be the quotient of the free graded $Z/2$ algebra with generators s_i, $i \geqslant 0$, and t, $|s_i| = 2^i$, $|t| = 1$, with the relations:

(1) $s_i^2 = 0$,
(2) $s_i s_{i+1} s_i = 0$,
(3) $s_i s_j + s_j s_i + s_{i-1} s_j s_{i-1} = 0$, $j < i - 1$,
(4) $[s_j, s_{j-1}] = t^{2^j} s_{j-1}$,
(5) $[s_j, t] = t^2 s_0 s_1 \cdots s_{j-1}$, $j > 0$,
(6) $[s_0, t] = t^2$.

Some simple computations from these give the more familiar relations:

(7) $[t^{2^j}, s_j] = t^{2^{j+1}}$,
(8) $[t^{2^j}, s_k] = 0$, $k < j$,
(9) $[t^{2^j}, s_k] = t^{2^{j+1}} s_j s_{j+1} \cdots s_{k-1}$, $k > j$.

Before we proceed, we collect here a few additional relations in S that will be useful later.

Lemma 5.3. *The following relations hold in $\mathcal{A}/\mathcal{I}_0$, and consequently in S.*

(i) $s_i(\prod_{k_j>i} s_{k_j})s_i = 0$.
(ii) $s_c s_a s_b s_a = 0$ *if* $b < a$, $c < a$, *and* $b \leqslant c$.
(iii) $s_2 s_r s_0 s_1 = s_2 s_0 s_1 s_r$ *for* $r \geqslant 3$.

Proof. Relation (i) follows easily from relation (2) with the help of (3) and (1).

Relation (ii) follows from (i) if $b = c$, and if $b < c$, then $b < a - 1$ and (3) gives

$$s_c s_a s_b s_a = s_c s_b s_a^2 + s_c s_{a-1} s_b s_{a-1} s_a = s_c s_{a-1} s_b s_{a-1} s_a.$$

If $c = a - 1$ this is 0, and if not $c < a - 1$, so $b < a - 2$, and we can proceed with $s_c s_{a-1} s_b s_{a-1}$ as before.

Relation (iii) is obtained from (ii) as follows:

$$s_2 s_r s_0 s_1 = s_2 s_0 s_r s_1 + s_2 s_{r-1} s_0 s_{r-1} s_1 = s_2 s_0 s_r s_1,$$

by (ii), and continuing, $= s_2 s_0 s_1 s_r + s_2 s_0 s_{r-1} s_1 s_{r-1}$. Using $s_2 s_0 = s_0 s_2 + s_1 s_0 s_1$ followed by (ii) and (i) gives the desired result. □

Theorem 5.4. *The map $\mathcal{A} \to \mathcal{E}$ factors through S,*

$$\mathcal{A} \to \mathcal{A}/\mathcal{I}_0 \to S \to \mathcal{E}$$

and the last map in the sequence is a monomorphism.

Proof. The map $S \to \mathcal{E}$ just sends s_i to the endomorphism given by Sq^{2^i} and t to the map which is multiplication by the generator in $H^1(RP^\infty)$. We need to check of course that the relations go to 0, but that is a simple computation.

To show that the map $S \to \mathcal{E}$ is a monomorphism, we will show that there is a $Z/2$ basis for S consisting of monomials of the form $t^k s_{i_1} s_{i_2} \cdots s_{i_r}$, where $i_1 < i_2 < \cdots < i_r$. This is sufficient since the image in $\mathcal{E}$ of this monomial takes x^n to $\binom{n}{m} x^{n+m+k}$, where $m = \sum_j 2^{i_j}$. So the images of these monomials are independent.

Now we need to show that any element of S can be written as a sum of such monomials. We show this in two steps.

The first step is to show that any monomial can be written as a sum of monomials in which a power of t appears only once, at the front (or left edge). Relations (5)–(8) allow this to be done. If M is a monomial in S, we write $M = At^r B$, where B contains no powers of t, and A does not end with a power of t. If A is not 1, then one of the relations (5)–(8) allows M to be written as a sum of two monomials (one term if using relation (8)), such that for each monomial the degree of that part of the monomial preceding the rightmost power of t is less than the degree of A. So we can continue until we get a sum of monomials, each of which has nothing before the rightmost power of t, as desired.

The second step is to order the s_i's, while keeping the powers of t in the front. For any monomial $M = t^k s_{i_1} s_{i_2} \cdots s_{i_r}$ and any positive integer k let $q_k(M)$ be the number of s_k's in M which are followed in M by at least one s_ℓ with $\ell \leqslant k$, i.e., the number of s_k's which are out of order. Let $q(M)$ denote the sequence $\{q_0(M), q_1(M), \ldots\}$, and order the sequences lexicographically from the right. If $q_k(M) = 0$ for all q, then M is in the desired form. If not, let k be the largest integer for which $q_k(M)$ is not zero. We use downward induction on (q, p) (lexicographically ordered from the left), where $p(M)$ is the number of s's between the leftmost s_k and the nearest element on the right with a larger subscript, or to the end of the monomial if there is none with a larger subscript. Now this leftmost s_k is followed by one or more s_j with $j \leqslant k$. Since k is the largest integer with $q_k(M) \neq 0$, the element following s_k must have subscript less than or equal to k. If equal, then relation (1) shows that the monomial is zero in S. If the subscript is one less, apply relation (4). This gives $M = M_1 + M_2$, where M_1 has the s_k replaced by a t^{2^k}, which by relation (8) can be pulled to the front, (relation (8) applies since k was maximal) and hence $q(M_1) < q(M)$. We also have $p(M_2) = p(M) - 1$. Finally if the element following the leftmost s_k has subscript at least two smaller than k, relation (3) applies, giving two terms, one with smaller q and the other with smaller p. So in any case we can write M as a sum of two monomials one with smaller q, the other with smaller p. □

The reduction algorithm in the proof above gives a fast method for determining when an element of $\mathcal{A}$ is in $\mathcal{K}$. In fact it does quite a bit more, as the following two lemmas show.

For any $s \in S$, expand s in terms of the basis above and define the "leading term" of s to be the basis element with the highest power of t. Since a basis element in a given dimension is determined by its power of t, we will sometimes write $u_{n,n-k}$ for the basis element $t^{n-k}s_{i_1}\cdots s_{i_r}$, where $2^{i_1}+\cdots+2^{i_r}=k$, and if no confusion can occur, even u_{n-k}.

Lemma 5.5. *Let $b = s_{i_1}^{j_1}s_{i_2}^{j_2}\cdots s_{i_r}^{j_r}$ be an Arnon basis element with strictly increasing bottoms, and let $\tilde{b}$ be its image in S. Consider the expansion of $\tilde{b}$ in the basis for S that is given by Theorem* 5.4.

(i) *The leading term in this expansion is $u_{n,n-k}$, where n is of course the degree of b, and $k = 2^{i_1}+\cdots+2^{i_r}$ is the "sum of the bottoms of b".*

(ii) *The basis elements in the expansion of $\tilde{b}$ involve only those s_p for which $p \leqslant j_r$.*

Proof. First look at $s_i^{i+\ell} = s_{i+\ell}\cdots s_i$. In S we have $s_i^{i+\ell} = t^{2^{i+\ell}}s_i^{i+\ell-1} + s_i^{i+\ell-1}s_{i+\ell}$ by relation (4) followed by repeated applications of (3) and Lemma 5.3. This shows that

$$s_i^{i+\ell} = \sum_{j=0}^{2^\ell-1} u_{2^{i+\ell+1}-2^i,j2^{i+1}}.$$

Note that every possible multiple of 2^{i+1} occurs as a power of t, that each basis element contains s_i, and that each basis element contains no s_p for $p < i$. Hence the leading term of $s_i^{i+\ell}$ is $t^{2^{i+\ell+1}-2^{i+1}}s_i$.

Next note that part (ii) of the lemma is obvious from the commutation relations in S and the fact that j_r is at least as large as any of the other j's, since we started with an Arnon basis element. Part (ii) will be used explicitly in the inductive argument to be used below.

To proceed with the proof we consider only those with strictly increasing bottoms as the others are in $\mathcal{I}_0$ and therefore are zero in S. Let $b = s_{i_1}^{j_1}s_{i_2}^{j_2}\cdots s_{i_r}^{j_r}$. We need to show that the leading term of b is $u_{n,n-k}$ where n is of course the degree of b and $k = 2^{i_1}+\cdots+2^{i_r}$, which we call "the sum of the bottoms" of b. The proof is by induction on r. For $r = 1$ it was proved above. Let $b = c\,s_{i_r}^{j_r}$, and let $\tilde{b}$ and $\tilde{c}$ be the images in S of b and c, and expand $\tilde{c}$. Each term in the expansion of $\tilde{c}$ which will give a nonzero product when multiplied by $s_{i_r}^{j_r}$ must contain only s_p's, with $p < i_r$. To see this note that such a term can be written as $(t^?s_{p_1}\cdots s_{p_q})s_{j_r}s_{j_{r-1}}\cdots s_{i_r}$, where the part in parentheses comes from the expansion of $\tilde{c}$, and $p_1 < p_2 < \cdots < p_q$. From part (ii) we know that $p_a \leqslant j_r$, so if $p_a \geqslant i_r$ for some a, we have $i_r \leqslant p_a \leqslant j_r$, and by Lemma 5.3(i) the term must be zero. Thus the powers of t introduced in the expansion of $s_{i_r}^{j_r}$, namely multiples of 2^{i_r+1} will commute with c, and we get the leading term as claimed. □

Lemma 5.6. *Let b be any Arnon basis element, and a any element from the basis for S occurring in $\tilde{b}$ the expansion of b. Then there is an Arnon basis element c such that the leading term of $\tilde{c}$ is a.*

Proof. The key fact is that when expanding an Arnon basis element in S according to the method in the proof of Theorem 3.4, the only way that powers of t are introduced is from relation (4).

Start with $s_i^{i+\ell}$. From above, we know that all powers of $t^{2^{i+1}}$ will occur. Fix a basis element a in the expansion of $s_i^{i+\ell}$. Let n be the dimension of a, and choose k so that $a = u_{n,n-k} = t^{n-k}s_{j_1}\cdots s_{j_r}$. We need an Arnon basis element in degree n with bottoms $s_{j_1},\ldots,s_{j_r}$. Such a basis element is given by $c = s_{j_1}^{k_1}s_{j_2}^{k_2}\cdots s_{j_r}^{k_r}$, where $k_1 = j_2 - 1$, $k_2 = j_3 - 1$, $\ldots$, $k_{r-1} = j_r - 1$, $k_r = i + \ell$.

For the general Arnon basis element the techniques are essentially the same. Let $b = s_{i_1}^{i_1+\ell_1}\cdots s_{i_r}^{i_r+\ell_r}$, and let $a = t^{n-k}s_{j_1}\cdots s_{j_q}$ be a term in the expansion of b. Let n be the degree of a and of b. From the arguments above, the set $\{s_{i_1},\ldots s_{i_r}\}$ is contained in the set $\{s_{j_1},\ldots s_{j_q}\}$. We need to construct an Arnon basis element in degree n with bottoms $\{s_{j_1},\ldots s_{j_q}\}$. But all we are doing is adding additional bottoms. So for each new bottom, say s_{j_p}, find the first occurrence of it in b, and move it, and the numbers in the same decreasing sequence which lie above it as a new sequence in its proper position among the bottoms. This will give $s_{j_1}^{m_1}\cdots s_{j_q}^{m_q}$, decreasing sequences with the correct bottoms, but the tops may no longer be nondecreasing, as required for an Arnon basis element. If this occurs, let α be the smallest integer such that $m_\alpha > m_{\alpha+1}$. Then replace $s_{j_\alpha}^{m_\alpha}s_{j_{\alpha+1}}^{m_{\alpha+1}}$ by $s_{j_\alpha}^{m_{\alpha+1}}s_{j_{\alpha+1}}^{m_\alpha}$. Repeat this process, if needed, until the tops are nondecreasing. No new bottoms are created in this process, so we have constructed an Arnon basis element with the desired properties. □

Since this process is more complicated to describe than to do, we offer the following example in degree 59.

Let $b = s_0^3s_2^4s_4^4$. Then b expands in S to

$$t^{38}s_0s_2s_4 + t^{36}s_0s_1s_2s_4 + t^{30}s_0s_2s_3s_4 + t^{28}s_0s_1s_2s_3s_4.$$

We illustrate the procedure for $a = t^{28}s_0s_1s_2s_3s_4$. We are adding the bottoms s_1 and s_3, and these can both be taken from the s_0^3. So we obtain $s_0s_2s_1s_4s_3s_2s_3s_4$. Note that the s_3 from the front has moved to near the end, since we must have the bottoms increasing. Now this is not an Arnon basis element, since the tops are not nondecreasing, in fact it is that last s_3 that is causing the problem. But by moving the previous s_4 over, we get $s_0s_2s_1s_3s_2s_4s_3s_4 = s_0^0s_1^2s_2^3s_3^4s_4^4$, which has the correct bottoms.

The two lemmas above show that there is a basis for the image of $\mathcal{A}$ in S which is a subset of the basis for S constructed in Theorem 5.4. Except in some special degrees, we do not know the size of this subset.

Now we consider the kernel of the map $\mathcal{A}/\mathcal{I}_0 \to S$. Note that the map $D:\mathcal{A}/\mathcal{I}_0 \to \mathcal{A}/\mathcal{I}_0$ given on generators by $D(s_i) = s_{i+1}$ is an algebra homomorphism, since adding one to the subscripts in each relation still gives a relation. Since $\binom{n}{k} = \binom{2n}{2k} \bmod 2$, we have that if $a \in \mathcal{A}$ is in the kernel, then so is $D(a)$. We call D the doubling map.

Denote by $\mathcal{A}_r$ the subalgebra of $\mathcal{A}$ generated by s_i, $0 \leqslant i \leqslant r$.

Lemma 5.7. *For $r \geqslant 4$ there are elements c_r of dimension $2^r + 2^{r-1} + 5$ in $\mathcal{A}_{r-1}$ such that $\phi_{r,0} = [s_2, s_0][s_{r-1}, s_r] + c_r$ is in the kernel. Note that the first term is not in $\mathcal{A}_{r-1}$, but in $\mathcal{A}_r$. Define $\phi_{r,s}$, for $s > 0$ by $\phi_{r,s} = D(\phi_{r,s-1})$.*

Proof. We construct c_r, and show that has the desired properties. Let $w(i,r)$ be the iterated commutator $[s_i, [s_{i+1}, \ldots, [s_{r-3}, (s_{r-1}s_{r-2}s_{r-1})]\ldots]]$. Note that $w(i,r)$ lies in A_{r-1}. Let $c_r = s_1s_0s_2s_1w(2,r) + s_2s_1w(2,r)s_0s_1$. We need to show that the image of $\phi_{r,0} = [s_2, s_0][s_r, s_{r-1}] + c_r$ is zero in S.

First we show that the image of $w(i,r)$ in S is $t^{2^r-2^{i+1}}s_is_{r-1}$ by downward induction on i. To start the induction note that $w(r-2,r) = s_{r-1}s_{r-2}s_{r-1}$, and computing in S this is $t^{2^{r-1}}s_{r-2}s_{r-1}$ by relation (4) followed by relation (1). Then we have, inductively,

$$w(j-1,r) = [s_{j-1}, w(j,r)] = s_{j-1}t^{2^r-2^{j+1}}s_js_{r-1} + t^{2^r-2^{j+1}}s_js_{r-1}s_{j-1}.$$

Relation (8) puts the first term in the correct order, and the second term becomes

$$\begin{aligned} &t^{2^r-2^{j+1}}\left(s_js_{j-1}s_{r-1} + s_js_{r-2}s_{j-1}s_{r-2}\right)\\ &= t^{2^r-2^{j+1}}\left(s_{j-1}s_js_{r-1} + t^{2^j}s_{j-1}s_{r-1} + s_js_{r-2}s_{j-1}s_{r-2}\right). \end{aligned}$$

Adding the two pieces, the first terms cancel, the powers of t combine and we obtain $t^{2^r-2^j}s_{j-1}s_{r-1} + t^{2^r-2^{j+1}}s_js_{r-2}s_{j-1}s_{r-2}$. But since $j \leqslant r-2$ the last term is 0 in S by repeated application of relation (3). For if $j = r-2$ the term is clearly zero, and if $j < r-2$ it is equal to $s_js_{r-3}s_{j-1}s_{r-3}s_{r-2}$, which is zero if $j = r-3$, etc.

Now c_r then goes to

$$\begin{aligned} &s_1s_0s_2s_1t^{2^r-8}s_2s_{r-1} + s_2s_1t^{2^r-8}s_2s_{r-1}s_0s_1\\ &= t^{2^r-8}\left(s_1s_0s_2s_1s_2s_{r-1} + s_2s_1s_2s_{r-1}s_0s_1\right)\\ &= t^{2^r-8}\left(t^4s_1s_0s_1s_2s_{r-1} + s_2s_1s_2s_0s_1s_{r-1} + \text{terms which reduce to zero}\right)\\ &= t^{2^r-8}\left(t^6s_0s_1s_2s_{r-1} + t^4s_1s_2s_0s_1s_{r-1}\right)\\ &= t^{2^r-8}\left(t^6s_0s_1s_2s_{r-1} + t^8s_1s_0s_1s_{r-1} + t^4s_1s_0s_1s_2s_{r-1}\right)\\ &= t^{2^r-8}t^{10}s_0s_1s_{r-1}. \end{aligned}$$

Therefore the image of c_r in S is $t^{2^r+2}s_0s_1s_{r-1}$, which is the same as the image of $[s_2, s_0][s_{r-1}, s_r]$. Thus $\phi_{r,0} = [s_2, s_0][s_{r-1}, s_r] + c_r$ is in $\mathcal{K}$. The remark preceding this theorem then shows that $\phi_{r,s}$ is in $\mathcal{K}$ for all s. □

Without proof, we give a formula for a representative of c_r mod $\mathcal{I}_0$ in the Arnon basis. Let e_r be the sum of all Arnon basis elements in degree $2^r - 4$ which are made up of exactly one $s_2, s_3, \ldots, s_{r-1}$ with the condition that $s_{r-1}s_{r-2}$ always is in that order. Let f_r be the sum of all Arnon basis elements in degree $2^r - 2$ which are made up of exactly one $s_1, s_2, \ldots, s_{r-1}$ with the condition that s_2s_1 and $s_{r-1}s_{r-2}$ always are in that order. Then

$$c_r = s_1s_0s_2s_1e_rs_{r-1} + s_2s_1s_0f_rs_{r-1}.$$

For example $e_5 = s_2s_4s_3 + s_4s_3s_2$, $f_5 = s_2s_1s_4s_3 + s_4s_3s_2s_1$.

Let $\mathcal{I}_1$ be the ideal in $\mathcal{A}$ generated by $\mathcal{I}_0$ and the elements

$$\{\phi_{r,s} = D^s\phi_{r,s},\ r \geqslant 4,\ s \geqslant 0\}.$$

Lemma 5.8. *The elements $Sq^{2^i}Sq^{2^i}$, $i > 0$, and $\phi_{r,s}$, $r \geqslant 4$, $s \geqslant 0$, form a minimal set of generators for $\mathcal{I}_1$.*

Proof. This will be done by a leading term argument using the Milnor basis. We write $Sq(R)$ for a Milnor basis element, where $R = (i_1, i_2, \ldots)$ is a finite sequence of positive integers. Let $\mathcal{M}_3$ be the ideal in $\mathcal{A}$ having a basis consisting of $Sq(i_1, i_2, \ldots)$, with $i_j > 0$ for some $j > 2$. The algebra $\mathcal{A}/\mathcal{M}_3$ has a basis consisting of the image of all $Sq(R)$, where R is a sequence of length 2, and the multiplication simplifies to the formula

$$Sq(a,b)Sq(c,d) = \sum_{k=0}^{\min(c,\lfloor a/2\rfloor)} \binom{a+b-3k}{a-2k}\binom{b+d+k}{k}\binom{b+d}{b} \times Sq(a+c-3k, b+d+k). \tag{5.1}$$

We need the following easy consequences of this formula. Note that in this case the equality is in $\mathcal{A}$, since none of the products gives terms in $\mathcal{M}_3$.

(1) $Sq^{2^r}Sq^{2^r} = Sq(2^{r-1}, 2^{r-1}) +$ terms in $\mathcal{A}_{r-1}$.

(2) $[Sq^{2^r}, Sq^{2^{r-1}}] = Sq(0, 2^{r-1}) +$ terms in $\mathcal{A}_{r-1}$.

(3) $Sq^2Sq^1Sq^2[Sq^{2^r}, Sq^{2^{r-1}}] = Sq(2, 2^{r-1}+1) +$ terms in $\mathcal{A}_{r-1}$.

Somewhat more is true in the first case above. One can without difficulty show that $\{Sq(2^i, 2^i),\ i \geqslant 0\}$ form an alternate minimal set of generators for $\mathcal{I}_0$.

For the remainder of this proof, all computations will be done mod $\mathcal{M}_3$.

In order to prove this lemma, we need to show that $\phi_{r,s}$ is not in the ideal generated by $\mathcal{I}_0$ and $\phi_{k,t}$ where $(k,t) < (r,s)$. To avoid taxing the patience of the reader we only show here that $\phi_{r,s}$ is not in $\mathcal{I}_0$, for $r \geqslant 4$. The rest of the arguments are almost identical, with slightly different formulas.

From (3) above, we see that the leading term of $\phi_{r+1,0}$ is $Sq(2, 2^r+1)$, and it follows that the leading term of $\phi_{r+1,s-1}$ is $Sq(2^s, 2^{s+r}+2^{s-1})$. So it is sufficient to show that no element of $\mathcal{I}_0$ has a term of the form $Sq(2^s, 2^{s+r}+2^{s-1})$, at least if $r+1 \geqslant 4$. This is equivalent to showing that for each $j \geqslant 0$, and for all nonnegative integers a, b, c, and d the coefficient of $Sq(2^s, 2^{r+s}+2^{s-1})$ in the expansion of $Sq(a,b)Sq(2^j, 2^j)Sq(c,d)$ is zero.

Applying formula (5.1) twice, we obtain:

$$Sq(a,b)Sq(2^j,2^j)Sq(c,d) = \sum_k \sum_l C_1C_2C_3C_4C_5C_6\,Sq(a+c+2^j-3k-3l, b+d+2^j+k+l) \tag{5.2}$$

with

$$C_1 = \binom{c+2^j-3k}{2^j-2k}, \quad C_2 = \binom{d+k+2^j}{2^j},$$

$$C_3 = \binom{d+k}{k}, \quad C_4 = \binom{a+c+2^j-3k-3l}{a-2l},$$

$$C_5 = \binom{b+d+2^j+l+k}{l}, \quad \text{and} \quad C_6 = \binom{b+d+2^j+k}{b}.$$

We will show that the product $C = C_1 \cdots C_6$ is zero when $a+c+2^j-3k-3l = 2^s$, and $b+d+2^j+k+l = 2^{r+s}+s^{s-1}$.

First note that the numerator of C_5 is $2^{r+s}+2^{s-1}$, and the numerator of C_4 is 2^s. So if C_5 is to be nonzero, l must be either 0, 2^{s-1}, or 2^{r+s}. If $l = 2^{r+s}$ then $b+d+2^j+k = 2^{s-1}$, and so for C_6 to be nonzero we must have $b = 0$ or $b = 2^{2-1}$, but the latter would say $d+2^j+k = 0$, which can't happen, so b must be 0. Then $d+2^j+k = 2^{s-1}$, so $C_2 \neq 0$ gives $j = s-1$ and $d = k = 0$. Thus $a+c+2^{s-1}-3\cdot 2^{r+s} = 2^s$, so $a+c = 2^{s-1}+3\cdot 2^{r+s}$. Now C_4 says either $a = 2^{r+s}$ or $2^{r+s}+2^s$, and in either case $C_1 = 0$. So if $l = 2^{s+m}$, we have $C = 0$. A similar argument gives the same conclusion if $l = 2^{s-1}$. So if C is to be nonzero, l must be 0.

We next show that b must be 0. $C_6 \neq 0$ implies that $b = 0$, 2^{s-1}, or 2^{s+r}. If $b = 2^{s+r}$, then $d+2^j+k = 2^{s-1}$, so $j = s-1$, $k = 0$, and $d = 0$. Thus $a+c = 2^{s-1}$, and from $C_4 \neq 0$ we see that $a = 0$. But then $C_1 = 0$, so $b \neq 2^{r+s}$. Once again an almost identical argument shows that $b \neq 2^{s-1}$. Thus $b = 0$.

Since $b = l = 0$, we have $d+k+2^j = 2^{s-1}+2^{r+s}$. From C_2 we see that $j = s-1$ or $m+s$. We do the first case, the second being slightly simpler. Now $j = s-1$ gives $d+k = 2^{r+s}$, so C_3 says that $k = 0$ or 2^{r+s}. If the latter, then $d = 0$, $a+c = 2^{s-1}+3\cdot 2^{r+s}$. In this case C_4 says that $a = 0$ or $a = 2^s$, but both cases make $C_1 = 0$. Therefore we must have $k = 0$. But then $a+c+2^{s-1} = 2^s$, so $a+c = 2^{s-1}$. So C_4, which is now $\binom{a+c+2^{s-1}}{a}$ is 0, and the proof of of the lemma is complete. □

To complete the proof of Theorem 1, we need to show that $\mathcal{K}$ is not larger than $\mathcal{I}_1$. This will be proved in the next section.

6. Finding the kernel

In this section we will prove Theorem 2 and complete the proof of Theorem 1. To do this we look again at the Arnon basis in a slightly different way, using it to construct a set of equations which will help to describe the kernel of the map $\mathcal{A}/I_0 \to S$.

Each Arnon basis element can be described by two sequences, one listing the bottoms of the strings (which must be increasing, else obviously in I_0), and the other the length of the strings, which must be positive. Fix a dimension n. For each integer $k \leqslant n$ we construct an equation with $m = \alpha(k)$ unknowns. Let $R = (r_1, r_2, \ldots, r_m)$ be the unknowns, let $k = \sum 2^{i_j}$ be the dyadic expansion of k, with $i_1 < i_2 < \cdots < i_m$. The equation is $\sum 2^{i_j+r_j} = n+k$, and we call it the equation associated to (n,k). We require solutions $R = (r_1, r_2, \ldots, r_m)$ to be positive integers and to satisfy the additional condition that $i_j + r_j \leqslant i_{j+1} + r_{j+1}$ for all j.

How does this relate to the problem at hand? Given any such solution as above, $s_{i_1}^{i_1+r_1-1} \cdots s_{i_m}^{i_m+r_m-1}$ is an Arnon basis element $a \in \mathcal{A}$ with the i's being the bottoms and the r's being the lengths of the subsequences. We can map the solutions into S by sending any solution to the image of the corresponding Arnon basis element. It will be convenient to order the elements of S in a given dimension according to powers of t.

Lemma 6.1. *These equations have the following simple properties.*

(1) *The equation associated to (n,k) has zero or more solutions and each solution maps to an element of S whose highest power of t is $n-k$.*

(2) *If an element $a \in S$ is in the image of $\mathcal{A}$, then the equation associated to (n,k), where n is the dimension of a and $n-k$ is the highest power of t in a, must have a solution.*

(3) *Given any pair of solutions associated to (n,k), the sum of the two Arnon basis elements corresponding to the solutions may not be in the kernel, but there are basis elements corresponding to solutions with larger values of k (and hence smaller powers of t in S) such that the sum of all of them is in the kernel.*

(4) *Any pair of solutions to the same equation gives an element of the kernel of the map $\mathcal{I}_0 \to S$, and any element of the kernel corresponds to a linear combination of pairs of solutions.*

(5) *The solutions to the equation associated to (n,k) and $(2n,2k)$ are the same. The elements in the kernel in dimension $2n$ are obtained from those in dimension n via the doubling map D.*

Proof. (1) is just a restatement of Lemma 5.5 and (2) is a restatement of Lemma 5.6. To see (3), let a_1 and a_2 be Arnon basis elements corresponding to the same solution. Then by Lemma 5.5, the images of a_1 and a_2 have the same leading term. So if the image in S of $a_1 + a_2$ is not zero, then it must contain a term with a lower power of t than $n-k$. This term must also occur in the image of either a_1 or a_2, and Lemma 5.6 tells how to get an Arnon basis element which maps to this term. Now (4) follows from (3), and (5) is clear. One should not get the impression from (4) that a pair of solutions determines a unique element of the kernel. But the difference of any two such will correspond to a pair of solutions to an equation with a larger value of k, or smaller power of t. □

The rank of the image of the map to $\mathcal{E}$ in dimension n is the number of integers k for which the equation associated to (n,k) has a solution. This proves Theorem 2.

We are left with showing that $\mathcal{K} = \mathcal{I}_1$. Since Lemma 5.7 shows that $\mathcal{I}_1 \subset \mathcal{K}$, we need only show the reverse inclusion. We will use the equations to show this. For example, there are no elements of the kernel with equations corresponding to k with $\alpha(k) = 2$. Moreover, all of the ideal generators described in (1) and Lemma 5.7 correspond to equations with $\alpha(k) = 3$ and minimal n (for there to be multiple solutions with a given k). In particular $\phi_{r,0}$ corresponds to the pair of solutions $\{(2,1,2),(3,r-1,1)\}$ to the equation associated to (n,k), where $k = 2^{r-1}+3$, and $n = 2^r + 2^{r-1} + 5$. Hence $n + k = 2^{r+1} + 8$, and of course $\alpha(n+k) = 2$.

We pause here to construct $\phi_{4,0}$ from the appropriate equations. Let $n = 29$, and $k = 11$. Then $n + k = 40 = 4 + 4 + 32 = 8 + 16 + 16$. So $k = 1 + 2 + 8$. There are two solutions $R_1 = (2, 1, 2)$ and $R_2 = (3, 3, 1)$. Then the Arnon basis element corresponding to R_1 is $s_1 s_0 s_1 s_4 s_3$, which reduces in S to $t^{18} s_0 s_1 s_3 + t^2 s_0 s_1 s_3 s_4$, and the Arnon basis element corresponding to R_2 is $s_2 s_1 s_0 s_3 s_2 s_1 s_3$, which reduces to $t^{18} s_0 s_1 s_3 + t^{14} s_0 s_1 s_2 s_3$, so their sum has leading term containing a t^{14}. Now $29 - 14 = 15 = 1 + 2 + 4 + 8$, and the equation for $(29, 14)$ has the solution $(2, 2, 2, 1)$, which gives the Arnon basis element $s_1 s_0 s_2 s_1 s_3 s_2 s_3$, which reduces just to $t^{14} s_0 s_1 s_2 s_3$. So adding these three, we are left with $t^2 s_0 s_1 s_3 s_4$. Now $29 - 2 = 27$, and so $k = 27 = 1 + 2 + 8 + 16$, and $n + k = 56 = 4 + 4 + 16 + 32$, so we have the solution $(2, 1, 1, 1)$ which gives the Arnon basis element $s_1 s_0 s_1 s_3 s_4$, which reduces to its leading term. The sum of the four terms then gives an element in the kernel, and concludes the example.

We proceed by proving enough about the $\mathcal{A}$ action on $\mathcal{A}/I_0$ so that we can say that given any element in the kernel, its corresponding equation solution indicates that it is in the ideal generated by previous elements, unless it is minimal in the sense above.

Let us continue to let $m = \alpha(k)$. The following standard notation will be used. We will consider pairs of solutions $(r_1, r_2, \ldots, r_m)$ and $(r'_1, r'_2, \ldots, r'_m)$ to the equation with

$$k = \sum 2^{i_j}.$$

First note that we may assume that $i_1 = 0$. If not, we can reduce by just subtracting i_1 from each of the i's, and get the same solutions. This corresponds to recognizing the image of doubling.

We say that a pair of solutions is reducible if the elements a in the kernel that it determines are reducible, i.e., can be written as a sum of an $\mathcal{A}$-linear combination of lower dimensional elements of the kernel and possibly elements of the kernel of the same dimension corresponding to equations with larger values of k.

We will eventually show that the only pairs of solutions which are not reducible correspond to the elements $\{\phi_{r,s}\}$, $r \geqslant 3$, $s \geqslant 0$. The astute reader will note that we have detected the elements $\phi_{3,s}$ mentioned earlier, which are in $\mathcal{I}_0$, but not obviously so.

Let x be an element of the kernel corresponding to a pair of solutions to the equation corresponding to (n, k). The first step is to detect when $x = ya$ or $x = ay$, where $a \in \mathcal{A}$, and y is another element of the kernel. By Lemma 6.1 it is sufficient to find the pair of solutions to which y belongs, and check the action of a on the corresponding Arnon basis elements.

Now consider the action of $\mathcal{A}$ on the right.

Lemma 6.2 (Right action). *A pair of solutions is reducible if at least one of the following holds.*

(1) $r_m > 1$ *and* $r'_m > 1$.

(2) $r_m = 1 = r'_m$.

(3) *For any* j, $1 \leqslant j < m - 1$, *we have* $i_j < i_{j+1} - 1$ *and both* r_j *and* r'_j *are larger than* 1.

Proof. For case (1), just obtain the new solution by subtracting 1 from both r_m and r'_m. For case (2), get a new set of solutions by dropping both, as well as i_m. In both of these cases this corresponds to dropping the final $Sq^{2^{i_m}}$ from the Arnon basis elements. In the third case we factor out a $Sq^{2^{i_j}}$. The reduced equations have the new i_j increased by 1, and the r_j and r'_j decreased by 1. □

The left action is somewhat more complicated. But the easy part is

Lemma 6.3 (Left action). *A pair of solutions is reducible if one of the following holds.*
(1) $r_1 = r'_1$.
(2) $r_1 > r'_1$ *and for some* $j > 2$, $r_1 = r'_j + i_j$, $r'_j > 1$.

Proof. For (1) just factor out the leading $Sq^{2^{r_1-1}}$ from each, leaving solutions with r_1 and r'_1 decreased by 1, unless they were both 1 to start with. In this case delete them both, and also delete i_1. In the second case, we still want to factor out a $Sq^{2^{r_1-1}}$ on the left. Since r'_j is larger than 1, the reduced solutions are obtained by subtracting 1 from r_1, and also from r'_j. □

Now the lemmas above simply look at right or left action, but they do not deal with sums, which is essential. Given a solution pair R, R' which is not reducible by the above lemmas, we find solutions $R_1, \ldots, R_p$ such that the pairs R, R_1, R_p, R', and R_i, R_{i+1}, for $1 \leqslant i \leqslant p-1$ are all reducible by the above lemmas.

The minimal solutions that we seek all have $\alpha(k) = 3$ and $\alpha(n+k) = 2 = \alpha(k) - 1$. So we first look at the case where $\alpha(n+k) < \alpha(k) - 1$.

Proposition 6.4. *Any pair of solutions corresponding to* (n, k) *with* $\alpha(n+k) < \alpha(k) - 1$ *is reducible.*

Proof. Let $(r_1, \ldots, r_m)$ and $(r'_1, \ldots, r'_m)$ be a pair of solutions corresponding to (n, k). For convenience, let $d_j = r_j + i_j$, and $d'_j = r'_j + i_j$, and note that the condition on solutions requires both the d_j's and the d'_j's to be nondecreasing. Assume that $d_m > d'_m$ (if they are equal, then $r_m = r'_m$ and the pair is reducible by Lemma 6.2). Assume also that $i_1 = 0$. Let the dyadic expansion of $n + k = \sum_1^\gamma 2^q$.

Lemma 6.5. *With the above notation, if* $d_m = q_\gamma$, *then there is a third solution* $(r''_1, \ldots, r''_m)$, *with* $d''_j = r''_j + i_j$ *such that* $d''_1 = d'_1$, *and the difference between* d''_m *and* d_m *is less than the difference between* d'_m *and* d_m.

Proof. Let $d''_m = d_m - 1 \geqslant d'_m$, and $d''_{m-1} = d_m - 1 \geqslant d'_m \geqslant d'_{m-1}$. If $d_{m-1} = q_{\gamma-1}$, let $d''_{m-2} = d_{m-1} \geqslant d_{m-2}$. Continue until $d_{m-\ell} < q_{\gamma-\ell}$. Note here we have chosen $d''_m, d''_{m-1}, \ldots, d''_{m-\ell}$, and we want $d''_{m-\ell-1}$. If $d_{m-\ell-1} = d_{m-\ell}$, let $d''_{m-\ell-1} = d_{m-\ell} + 1$, and continue with $d''_{m-\ell-2} = d_{m-\ell-2}$, i.e., copying the first solution down to the end. This gives a solution satisfying the required properties. If $d_{m-\ell-1} < d_{m-\ell}$, then it must be exactly one less. So continue choosing $d''_\beta = d_{\beta+1}$ until you get equality, then proceed

as above. This will work to give a new solution with $d_1'' = d_1$, unless the duplicates occur at positions 1 and 2. Should this happen, we must have $q_1 = d_{m-\ell} + 1$. Thus the only 2-power in $n+k$ which is subdivided for the first solution is q_1. If $d_1' < d_1$, then q_1 must have been subdivided more for the second solution, but there is no room for this. If $d_1 > d_1'$, then every 2-power between d_1 and $q_{m-\ell-1}$ must appear, in particular d_1', so the original pair was reducible by the second part of the left lemma, unless the corresponding i is so large that the appropriate r is 1. First note that $r_1 = 2$, and $1 = r_2 = \cdots = r_{\ell-1} = 1$. If $r_{\ell-1}'$ were not greater than 1, then the second solution would have to start out the same as the first, and the pair would be reducible. So we can now construct a new solution, $d_1'' = d_1 + 1 = d_2 + 1$, $d_\nu'' = d_{\nu+1}$ for $2 \leqslant \nu \leqslant \ell - 2$, $d_{\ell-1}'' = d_\ell'' = d_\ell - 1$, and $d_\nu'' = d_\nu$ for $\nu > \ell$. This agrees with the first solution at the end, and the pair it forms with the second solution is reducible by the left lemma part (2). □

There is a similar result if $d_m < q_\gamma$, but the statement is more complicated.

Lemma 6.6. *Suppose $d_m < q_\gamma$, and the rest of the hypotheses of Lemma* 6.5 *hold. Let p be the smallest integer such that $d_{m-p} < d_m$. Then there is a solution $(r_1'', \ldots, r_m'')$, with $d_j'' = r_j'' + i_j$ such that $d_1'' = d_1'$, and $d_{m-p+1}'' < d_{m-p+1}$. Note that in the previous case p was forced to be* 1.

Proof. The proof is almost identical to the proof of Lemma 6.5. In fact the only difference is when $p > 1$. Then instead of subdividing d_m subdivide d_{m-p+1}. □

We now return to the proof of the proposition. Given a pair of solutions R, R' satisfying the hypotheses, the two lemmas above guarantee that we can find a solution R'' such that the pair R, R'' are reducible by Lemma 6.3, and the right end of R'' is either the same as that of R', or closer. Hence by repeatedly applying the lemmas we get a chain of solutions, decreasing d_m, until $d_m'' = d_m'$, and the pair R'', R' is reducible by Lemma 6.2. □

If $\alpha(n + k) + 1 = \alpha(k)$, only one 2-power can be subdivided. So the only way to find a pair which is not reducible is for only the solutions corresponding to splitting q_1 and q_γ to exist. We show that in this case one of the solutions must be $(2, 1, \ldots, 1, 2)$. If there is to be no third solution, then for each j, $1 < j < m - 1$, we must have either $q_j - 1 - i_j \leqslant 0$ or $q_j - 1 - i_{j+1} \leqslant 0$. But the second quantity is less than the first, and the fact that we already have two solutions says that $q_j \geqslant i_j + 1$, and $q_j \geqslant i_{j+1} + 1$. So $q_j = i_{j+1} + 1$. This says that one solution is $(q_1 - i_1, q_1 - i_2 - 1, 1, 1, \ldots, 1, 2)$ and the other is $(q_1, i_3 - i_2 + 1, i_4 - i_3 + 1, \ldots, 1)$. But now Lemma 6.2(3), and the fact that $\alpha(n + k) + 1 = \alpha(k)$ give that $q_1 - i_1 = 2$.

So all that is left is to show that if $m > 3$ the single pair of solutions above is reducible. We do this by direct construction.

Lemma 6.7. *For any sequence $I = (i_1, i_2, \ldots, i_m)$, with $m > 3$, $i_2 = i_1 + 1$, $i_3 > i_2 + 1$, and solutions $(2, 1, \ldots, 1, 2)$ and $(3 - i_1, i_3 + 1 - i_2, \ldots, i_m + 1 - i_{m-1}, 1)$, the element in the kernel corresponding to this pair of solutions is reducible.*

Proof. First note that $i_2 = i_1 + 1$, since 2^{i_1+2} must be the same 2-power as 2^{i_2+1}. Also $i_3 > i_2 + 1$, for if not, $2^{i_1+2} + 2^{i_2+1} + 2^{i_3+1} = 2^{i_3+2}$, and hence $\alpha(n+k) < \alpha(k) - 1$. As above it is sufficient to compute when $i_1 = 0$ since everything else is in the image of the doubling map D.

So let $I = (0, 1, i_3, \ldots, i_m)$, with $m \geqslant 3$. Define $g_I = s_1 s_0 s_1 s_{i_3} \cdots s_{i_{m-1}}[s_{i_m}, s_{i_m+1}] + c_I$, where $c_I = s_1 s_0 s_2 s_1 s_{i_3} \cdots s_{i_{m-1}} w(2, i_m + 1) + s_2 s_1 s_{i_3} \cdots s_{i_{m-1}} w(2, i_m + 1) s_0 s_1$.

We need to show that g_I is in $\mathcal{K}$, is reducible, and comes from the pair of solutions in the lemma.

To prove the first two assertions, we first compute g_I in terms of $g_{I'}$ and $g_{I''}$, where the lengths of I' and I'' are one less than the length of I. This will only work if $m > 3$ but that is all we need. So we set $I = (0, 1, i_3, i_4, \ldots, i_m)$, with $m > 3$ and $i_3 > 2$. Then let $I' = (0, 1, i_4, \ldots, i_m)$, and $I'' = (1, 2, i_4, \ldots, i_m)$. Let $H_r = s_{r-1} s_{r-2} \cdots s_3$, if $r > 3$, and 1 if $r = 3$. Then a straightforward computation shows that $g_I = s_{i_3} g_{I'} + s_1 s_0 H_{i_3} g_I'' + H_{i_3} g_I'' s_0 s_1$. This shows that g_I is reducible if the length of I is greater than 3. Now $g_{(0,1,r)} = \phi_{r+1,0}$, and $g_{(s,s+1,r+s)} = \phi_{r+1,s}$. which are both in $\mathcal{K}$, and therefore all the g_I with length of I greater than 3 are also in $\mathcal{K}$.

To complete the proof of the lemma, and hence the entire Theorem 1 we need verify that g_I comes from the pair of solutions in the lemma, i.e., we need to show that this element is the sum of terms in the Arnon basis consisting of the two terms coming from the pair of solutions plus terms which reduce in S to terms with lower powers of t. The Arnon basis element corresponding to the solution $(2, 1, \ldots, 1, 2)$ is $s_1 s_0 s_1 s_{i_3} \cdots s_{i_{m-1}} s_{i_m+1} s_{i_m}$ which reduces in S to $t^{2^{i_m+1}+2} s_0 s_1 s_{i_3} \cdots s_{i_m} + t^2 s_0 s_1 s_{i_3} \cdots s_{i_m} s_{i_m+1}$. So we need to show that c_I reduces to $t^{2^{i_m+1}+2} s_0 s_1 s_{i_3} \cdots s_{i_m}$ + terms with lower powers of t. To do this we need a refinement of the formula from the proof of Lemma 5.7. There we showed that $w(2, i_m + 1)$ reduces in S to $t^{2^{i_m+1}-8} s_2 s_{i_m}$. We claim that $s_{i_3} \cdots s_{i_m} w(2, i_m + 1)$ reduces to $t^{2^{i_m+1}-8} s_2 s_{i_3} \cdots s_{i_m}$. In fact we have the following lemma.

Lemma 6.8. *If $3 \leqslant j_1 < j_2 < \cdots < j_m < r$ then $s_{j_1} \cdots s_{j_m} w(2, r + 1)$ reduces to $t^{2^{r+1}-8} s_2 s_{j_1} \cdots s_{j_m} s_r$ in S.*

Proof. The argument is by induction on m and j_1. Note that the lemma is true if $m = 0$. We will verify the formula for $s_{j_1} \cdots s_{j_m} w(2, r+1)$, given that it is true for all terms with smaller m, and for those with the same m, but smaller j_1. To simplify the notation, let $j = j_1$, $z = s_{j_2} \cdots s_{j_m}$ and $z' = s_{j_2-1} \cdots s_{j_m-1}$, so that $z = D(z')$. There are two cases. The first case is if $j = 3$. Then $s_j z w(2, r + 1) = s_3 t^{2^{r+1}-8} s_2 z s_r = t^{2^{r+1}-16}(s_3 t^8 s_2) z s_r$. Now the term in parentheses is $t^{16} s_2 + t^8 s_3 s_2 = t^{16} s_2 + t^8 s_2 s_3 + t^{16} s_2 = t^8 s_2 s_3$, so the lemma is true in this case.

If $j > 3$, then

$$s_j z w(2, r + 1) = s_j z s_2 w(3, r + 1) + s_j z w(3, r + 1) s_2$$

$$= s_2 s_j zw(3, r+1) + s_j zw(3, r+1) s_2$$
$$= D\big(s_1 s_{j-1} z' w(2, r) + s_{j-1} z' w(2, r) s_1\big).$$

Now inductively this is

$$D\big(s_1 t^{2^r-8} s_2 s_{j-1} z' s_{r-1} + t^{2^r-8} s_2 s_{j-1} z' s_{r-1} s_1\big)$$
$$= s_2 t^{2^{r+1}-16} s_3 z s_r + t^{2^{r+1}-16} s_3 z s_r s_2$$
$$= t^{2^{r+1}-8} s_2 s_j z s_r. \qquad \square$$

To finish the proof of Lemma 6.7 we reduce c_I in S. Let $z = s_{i_1} \cdots s_{i_{m_1}}$. We reduce the two terms in c_I separately. First

$$s_1 s_0 s_2 s_1 zw(2, i_m + 1) = s_1 s_0 s_2 s_1 t^{2^{i_m+1}-8} s_2 z s_{i_m} = t^{2^{i_m+1}-2} s_0 s_1 s_2 z s_{i_m},$$

and

$$s_2 s_1 zw(2, i_m + 1) s_0 s_1 = s_2 s_1 t^{2^{i_m+1}-8} s_2 z s_{i_m} s_0 s_1 = t^{2^{i_m+1}-8} s_2 s_1 s_2 s_0 s_1 z s_{i_m}$$
$$= t^{2^{i_m+1}+2} s_0 s_1 z s_{i_m} + t^{2^{i_m+1}-2} s_0 s_1 s_2 z s_{i_m}.$$

Thus there are no higher powers of t than $2^{i_m+1} + 2$, and so g_I is associated with the desired equation. $\square$

The authors would like to thank the referee for his many helpful suggestions.

References

[1] D. Arnon, Monomial bases in the Steenrod algebra, J. Pure Appl. Algebra, to appear.
[2] C.T.C. Wall, Generators and relations for the Steenrod algebra, Ann. of Math. (2) 72 (1960) 429–444.
[3] D. Carlisle and R. Wood, Facts and fancies about relations in the Steenrod algebra, Preprint.