ELSEVIER

Journal of Pure and Applied Algebra 128 (1998) 1–10

JOURNAL OF
PURE AND
APPLIED ALGEBRA

The intersection of the admissible basis and the Milnor basis of the Steenrod algebra

D.P. Carlisle, G. Walker*, R.M.W. Wood

Department of Mathematics, University of Manchester, Oxford Road, Manchester M13 9PL, UK

Communicated by J. Huebschmann; received 29 April 1996; revised 10 September 1996

Abstract

We prove a conjecture of Monks [4] on the relation between the admissible basis and the Milnor basis of the mod 2 Steenrod algebra A_2, and generalise the result to the mod p Steenrod algebra A_p where p is prime. This establishes a necessary and sufficient condition for the Milnor basis element $P(r_1,r_2,\dots,r_k)$ and the admissible basis element $P^{t_1}P^{t_2}\dots P^{t_k}$ to coincide. The main technique used is the 'stripping' method which utilises the action of the dual algebra A_p^* on A_p. © 1998 Elsevier Science B.V. All rights reserved.

1991 Math. Subj. Class.: 55S10

1. The main result

We shall prove the following result relating the Milnor basis and the admissible basis of the mod p Steenrod algebra A_p. Here $\omega(n)$ is the smallest integer such that $p^{\omega(n)} > n$.

Theorem 1.1. *The Milnor basis element $P(r_1,r_2,\dots,r_m)$ is a scalar multiple of an admissible monomial if and only if $r_i \equiv -1 \bmod p^{\omega(r_{i+1})}$ for all $1 \le i < m$. In this case,*

$$P(r_1,r_2,\dots,r_m) = P^{t_1}P^{t_2}\dots P^{t_m}, \tag{1}$$

where $t_m = r_m$ and $t_i = r_i + pt_{i+1}$ for $1 \le i < m$.

It was shown by Milnor [3, Lemma 8] that the admissible basis is related to the Milnor basis by a triangular matrix for all p, using the right lexicographic ordering on both bases. The stated correspondence between the indexing sequences

* Corresponding author. Tel.: +44 0 1625 583402; fax: +44 0 1612 755819; e-mail: grant@ma.man.ac.uk.

0022-4049/98/$19.00 © 1998 Elsevier Science B.V. All rights reserved
PII S0022-4049(97)00035-2

$R=(r_1,r_2,\ldots,r_m)$ for Milnor basis elements and $T=(t_1,t_2,\ldots,t_m)$ for admissible monomials, and the fact that the diagonal entries of the matrix are equal to ± 1, can also be read off from [3].

For $p=2$, the 'if' part of Theorem 1.1 was proved by Ken Monks [4, Theorem 2.3], who also conjectured the 'only if' part in [4, Section 2]. As pointed out in [4, Section 9], the condition $r_i \equiv -1 \bmod 2^{\omega(r_{i+1})}$ is easily checked by writing the binary representations of $r_1,r_2,\ldots,r_m$ horizontally above one another (with r_1 on top) and checking that no digit ever appears below a 0. (Note that the condition implies that $r_i \geq r_{i+1}$ for all $1 \leq i < m$.) For brevity, we shall say that the sequence $(r_1,r_2,\ldots,r_m)$ is an *M-sequence* if it satisfies the condition $r_i \equiv -1 \bmod p^{\omega(r_{i+1})}$ for $1 \leq i < m$. Thus Theorem 1.1 states that the Milnor basis element $P(r_1,r_2,\ldots,r_m)$ is an admissible monomial if and only if $(r_1,r_2,\ldots,r_m)$ is an M-sequence.

As an example, the highest degree class T_n in the finite subalgebra $A(n)$ of A generated by P^t for $t < p^{n+1}$ is the Milnor basis element $P(R_n)$, where R_n is the M-sequence $(p^{n+1}-1, p^n-1, \ldots, p-1)$ [2, Ch. 15]. In Section 4 we prove that T_n is an admissible monomial.

The method of proof of Theorem 1.1 uses the stripping technique which has proved successful in a number of problems [1, 5–8]. This technique is explained in Section 2. The necessity of Monks's criterion will be proved in Section 3, and in Section 4 we give an alternative proof of sufficiency of the criterion.

2. The stripping method in the Steenrod algebra

In order to explain the stripping method as it applies to the present problem, we give a brief resumé of the structure of the Steenrod algebra A and its dual A^*. Since Bocksteins play no part in our work, we shall write $A=A_2$ if $p=2$, while for an odd prime p we use A to denote the subalgebra of A_p generated by the Steenrod pth powers. Thus, A and A^* are connected graded Hopf algebras over the field $\boldsymbol{F}_p$ of p elements. As an associative algebra, A is generated by the Steenrod powers P^i, to which we assign the grading $i(p-1)$, with P^0 equal to the identity element. These generators are subject to the Adem relations

$$P^iP^j = \sum_{0 \leq k \leq [i/p]} (-1)^{i+k} \binom{(j-k)(p-1)-1}{i-pk} P^{i+j-k}P^k, \quad 0 < i < pj, \tag{2}$$

where $[i/p]$ denotes the greatest integer $\leq i/p$, and the binomial coefficients are taken modulo p.

We begin by making the conventions that a finite sequence of integers is to be identified with the infinite sequence obtained from it by adding final zeros, and that a sequence whose terms are named by lower-case Roman letters is denoted by the corresponding capital Roman letter. This applies to the sequence $R=(r_1,r_2,\ldots,r_m)$ which indexes the Milnor basis element $P(R)$, and to the sequence $T=(t_1,t_2,\ldots,t_m)$ which indexes the string of Steenrod powers (or *monomial*) $P^T=P^{t_1}P^{t_2}\cdots P^{t_m}$. The sequence T

and the monomial P^T are called *admissible* if $t_j \geq pt_{j+1}$ for $j \geq 1$. The set of admissible monomials, taken in (left) lexicographic order of the corresponding sequences T, is a vector space basis of A. We write $U < V$ to mean that U precedes V in the left lexicographic order, whether U and V are admissible or not. For any element $X \in A$, we say that the admissible monomial P^T *occurs* in X if the coefficient of P^T in the expression for X in the admissible basis is nonzero.

The coproduct ψ in A is defined on generators by

$$\psi(P^k) = \sum_{i=0}^{k} P^i \otimes P^{k-i},$$

and the dual algebra A^* is the polynomial algebra $\boldsymbol{F}_p[\xi_1, \xi_2, \ldots]$, where ξ_n is the dual of $P^{p^{n-1}} P^{p^{n-2}} \cdots P^p P^1$ with respect to the admissible basis [3]. The element in A dual to $\xi_1^{r_1} \xi_2^{r_2} \cdots \xi_m^{r_m}$ with respect to the monomial basis of A^* is denoted by $P(R) = P(r_1, r_2, \ldots, r_m)$. As R ranges over all finite sequences of nonnegative integers, the elements $P(R)$ form the Milnor basis of A. For each $n \geq 0$, the subalgebra $A(n)$ has an additive basis consisting of the Milnor basis elements $P(R)$ with $r_i < p^{n+2-i}$ for all i [2, p. 240].

We now come to the stripping technique [1, 5, 7, 10]. The process works in any Hopf algebra, and may be regarded as a representation of the dual algebra on the original algebra. The term 'stripping' refers to the way in which this general structure is implemented in terms of strings of Steenrod powers. Using the map

$$A^* \otimes A \xrightarrow{1 \otimes \psi} A^* \otimes A \otimes A \xrightarrow{\kappa \otimes 1} A, \tag{3}$$

where κ is evaluation of a vector space on its dual, we associate with an element $\xi \in A^*$ the vector space endomorphism of A which maps $X \in A$ to $\sum \langle \xi, X' \rangle X''$, where $\psi(X) = \sum X' \otimes X''$. This construction is analogous to the construction of the cap product of a cohomology class ξ and a homology class X, so we shall write

$$\xi \cap X = \sum \langle \xi, X' \rangle X''.$$

In [5] the endomorphism $X \mapsto \xi \cap X$ of A is denoted by $D(\xi)$. Writing X, Y for elements of A, and ξ, η for elements of A^*, we may rewrite some of the formulae of [5, Section 2] as follows. The formula $D(\xi\eta) = D(\xi)D(\eta)$ becomes the associative law

$$\xi\eta \cap X = \xi \cap (\eta \cap X), \tag{4}$$

the formula $D(\xi)(X_1 X_2) = \sum D(\xi')X_1 \cdot D(\xi'')X_2$ becomes

$$\xi \cap X_1 X_2 = \sum (\xi' \cap X_1)(\xi'' \cap X_2), \tag{5}$$

and the formula $\chi \circ D(\xi) = D(\chi(\xi)) \circ \chi$, where χ denotes conjugation in A or A^*, is equivalent to

$$\chi(\xi \cap X) = \chi(\xi) \cap \chi(X). \tag{6}$$

In addition, duality of the product in A^* with the coproduct in A gives

$$\langle \xi\eta, X\rangle = \langle \xi, \eta \cap X\rangle. \tag{7}$$

The interesting question is how the cap product action of A^* on A is implemented in terms of specific bases. To handle this in the case of the admissible basis, we shall carry out algebraic manipulations with multisets of sequences which index elements of A. For example, when $p=2$ the set consisting of distinct sequences U and V, each with multiplicity 1, will index $Sq^U + Sq^V$. When $U=V$, the multiset consists of the sequence U with multiplier 2, and this will index $Sq^U + Sq^U = 0$. We shall reserve the notation $U+U=2U$ for this purpose. For this reason, we write the termwise sum of the sequences U and V as $U \cdot V$, and the termwise difference of U and V as U/V.

Recalling that the Milnor basis is dual to the basis of monomials $\xi^S = \xi_1^{s_1}\xi_2^{s_2}\dots\xi_n^{s_n}$ of A^*, (7) yields the following rule:

$$\xi^S \cap P(R) = P(R/S), \tag{8}$$

where $P(R/S)$ is interpreted as zero if any term of the sequence R/S is negative. In particular, the action maps each Milnor basis element to a Milnor basis element or to zero.

The cap product action can be described in terms of monomials P^T by a combinatorial process which we call *stripping*. Note first that it is sufficient in principle, using (4), to consider the action of the generators ξ_k of A^* on A. The action of a general element of A^* may then be considered as a sum of composites of the actions of these generators. In practice, however, it is more convenient to take the cap products with elements of the form $\xi_k^{p^a}$ as the basic family of operations on A.

Thus we consider $\xi_k^{p^a} \cap P^T$, which is evaluated in the case $p=2$ in [10, Lemma 5.1], [6, Proposition 3.1]. If $k \le m$, it is the sum of $\binom{m}{k}$ strings P^U, where each sequence U is formed by subtracting the sequence $C=(p^{a+k-1},\dots,p^{a+1},p^a)$ from some k-term subsequence of the sequence $T=(t_1,t_2,\dots,t_m)$, and where $P^U=0$ if any term of U is negative. If $k>m$, then $\xi_k^{p^a} \cap P^T = 0$. We refer to the element $\sum_U P^U \in A$ as the monomial P^T *stripped* by C. Here C is restricted to be a sequence of descending adjacent powers of p.

We may reformulate this result as follows. Given a sequence C, we write $\imath(C)$ for the (infinite) set of sequences I whose nonzero terms make up the given sequence C. Given a finite sequence of nonnegative integers T, we write $T/\imath(C)$ for the (infinite) set of all sequences T/I, where $I \in \imath(C)$. We may now define an element of the Steenrod algebra A by

$$P^{T/\imath(C)} = \sum_{I \in \imath(C)} P^{T/I}, \tag{9}$$

where $P^{T/I}=0$ if any term of T/I is negative. Then

$$\xi_k^{p^a} \cap P^T = P^{T/\imath(C)}, \quad \text{where } C=(p^{a+k-1},\dots,p^{a+1},p^a). \tag{10}$$

This formula may be verified as follows, using induction on a. (An alternative approach, based on (5), is given in [5, Proposition 4.1].) For the case $a=0$, we follow through the map (3) on the element $\xi_k \otimes T$. Thus let $\psi(T) = \sum T' \otimes T''$, where T' and T'' are monomials. Now $\langle \xi_k, T' \rangle$ is nonzero only when $T' = P^{p^{k-1}} \cdots P^p P^1$. To see this, recall that ξ_k is defined as the dual of $P^{p^{k-1}} \cdots P^p P^1$ with respect to the admissible basis. Since $P^{p^{k-1}} \cdots P^p P^1$ has excess 1, it occurs in the monomial $P^{T'}$ if and only if $T' \in \imath(C)$, where $C = (p^k, \dots, p, 1)$. This gives the result for $a = 0$.

For the inductive step, we use the identity (4). Writing $\xi_k^{p^a}$ as $(\xi_k^{p^{a-1}})^p$, the operation we require is the pth iterate of the stripping process for $a-1$. All the terms in this iterated stripping process, except those in which the subtractions occur in the same places in all p iterations, will appear with a multinomial coefficient which is $\equiv 0 \bmod p$. Thus these terms cancel, leaving the terms given by formula (10).

If U and V are integer sequences, we say that U *dominates* V if $u_i \ge v_i$ for all i. The purpose of this definition is shown by the lemma which follows. The point is that although P^U and P^V have different gradings, when U is admissible P^U is an upper bound (in the left lexicographic order) for all admissibles which can arise by applying Adem relations to P^V.

Lemma 2.1. *Let U be an admissible sequence which strictly dominates the sequence V, and suppose that U and V first differ at the rth term. Let P^W be any admissible monomial occurring in P^V. Then U and W first differ at the rth term, and $u_r > w_r$.*

Proof. We may assume that V is not admissible and that $v_r < w_r$, otherwise there is nothing to prove. The Adem relations can be used to express P^V as a sum of admissible monomials. Suppose that Eq. (2) is applied to two consecutive terms $P^i P^j$ of P^V, where $0 < i < pj$. Thus $v_s = i$, $v_{s+1} = j$, where $s \ge r$. Let $c_s = i + j - k$, $c_{s+1} = k$ be a corresponding pair of terms produced by the relation, so that

$$\binom{(j-k)(p-1)-1}{i-pk} \not\equiv 0 \bmod p.$$

Then $(j-k)(p-1) - 1 \ge i - pk$, that is $i - k \le j(p-1) - 1$, and so $c_s \le pj - 1$. Since U dominates V and U is admissible, $pj = pv_{s+1} \le pu_{s+1} \le u_s$, and hence $c_s < u_s$. Also $c_{s+1} = k \le [i/p] < j = v_{s+1} \le u_{s+1}$, so $c_{s+1} < u_{s+1}$. Iterating this argument, it follows that if P^W is an admissible monomial which occurs in P^V, and if the term v_s of V is affected by the Adem relations used, then the corresponding term w_s of W satisfies $w_s < u_s$. Since by hypothesis $v_r < w_r$, this applies in particular when $s = r$. □

The corollary which follows provides a crucial argument for our proof of Monks's conjecture. By identifying the maximal admissible monomial (in the left lexicographic order) that occurs in the result of applying a stripping operation to an given admissible monomial, we show in particular that the value of the operation is nonzero.

Corollary 2.2. *Let $T=(t_1,t_2,\dots,t_m)$ be an admissible sequence and let $C=(p^{a+n-1},\dots,p^{a+1},p^a)$, where $m \geq n$ and $t_m \geq p^a$. Then the maximum admissible monomial which occurs in $P^{T/\iota(C)}$ is $P^{T/(0,C)}$, where $(0,C)$ is the sequence obtained by prefixing $m-n$ zeros to C.*

Proof. Since T is admissible and C consists of consecutive descending powers of p, $T/(0,C)$ is admissible. Suppose that P^W occurs in $P^{T/J}$, where $J \in \iota(C)$ and $J \neq I$. Then T/J has no negative entries, so if j_r is the first nonzero entry of J, we have $r < m-n$. Then T strictly dominates T/J, the two sequences differing first at the rth term. By Lemma 2.1 it follows that T and W first differ at the rth term, and $w_r < t_r$. Hence $W < T/(0,C)$. □

3. Proof of Monks's conjecture

In this section, we prove the necessity of Monks's criterion for an element to lie in the intersection of the Milnor and the admissible bases. That is to say, we shall assume that for some $\alpha \in \boldsymbol{F}_p$

$$P(r_1,r_2,\dots,r_m)=\alpha P^{t_1}P^{t_2}\dots P^{t_m}$$

for sequences $R=(r_1,r_2,\dots,r_m)$ and $T=(t_1,t_2,\dots,t_m)$ with $t_m=r_m$ and $t_i=r_i+pt_{i+1}$ for $1 \leq i < m$, and we shall prove that R is an M-sequence (see Section 1). Recall that by [3, Lemma 8] we may assume that the indexing sequences R and T are related in this way.

The proof is in two steps. The first step is an induction argument which reduces the search for a counterexample of minimal grading to a special case, namely the case where r_m is a power of p, $r_{m-1}=\lambda r_m - 1$ with $1 \leq \lambda < p$ and $(r_1,r_2,\dots,r_{m-1})$ is an M-sequence. The second step shows that no sequence of this type is a counterexample.

Step 1: We assume, as induction hypothesis, that Eq. (1) holds for an admissible sequence T, where the corresponding sequence R is not an M-sequence, and that this counterexample is minimal in the sense that, for every similar relation in A in strictly lower grading, the sequence specifying the Milnor basis element is an M-sequence.

Taking the cap product of Eq. (1) with ξ_m, and using (8) and (10) we obtain

$$P(r_1,r_2,\dots,r_m-1)=\alpha P^{t_1-p^{m-1}}\dots P^{t_{m-1}-p}P^{t_m-1},$$

where the grading has been reduced by p^m-1. Since $(t_1-p^{m-1},\dots,t_{m-1}-p,t_m-1)$ is admissible, the induction hypothesis implies that $(r_1,r_2,\dots,r_m-1)$ is an M-sequence. Hence $(r_1,r_2,\dots,r_{m-1})$ is an M-sequence, and in addition $r_{m-1} \equiv -1 \bmod p^{\omega(r_m-1)}$. If $r_{m-1} \equiv -1 \bmod p^{\omega(r_m)}$, then $R=(r_1,r_2,\dots,r_m)$ is an M-sequence, contrary to hypothesis. Hence $\omega(r_m) \neq \omega(r_m-1)$, which implies that $r_m=p^a$ for some integer a. Thus, $r_{m-1}=\lambda p^a - 1$ for some integer λ prime to p.

If $\lambda > p$, we take the cap product of Eq. (1) with $\xi_{m-1}^{p^{a+1}}$. On the right-hand side, this corresponds to stripping P^T with $C=(p^{a+m-1},\dots,p^{a+2},p^{a+1})$. Since $t_m=p^a$, T/I has a negative term for all $I \in \iota(C)$ except for $I = C$ itself. Using (8) and (10), this gives the relation

$$P(r_1,\ldots,r_{m-1} - p^{a+1}, p^a) = \alpha P^{t_1 - p^{a+m-1}} \ldots P^{t_{m-1} - p^{a+1}} P^{p^a}.$$

Since $\lambda > p$, the Milnor basis element on the left is nonzero, and since $(r_1,\ldots,r_{m-1}, p^a)$ is not an M-sequence, $(r_1,\ldots,r_{m-1} - p^{a+1}, p^a)$ is not an M-sequence either. Recalling that $t_{m-1} = r_{m-1} + p^{a+1}$, the string on the right is still admissible, and so we have constructed an example which contradicts the induction hypothesis. This contradiction implies that we may assume $\lambda < p$. This completes Step 1.

Step 2: We may now assume that $r_m = p^a$ for some $a \geq 0$, that $r_{m-1} = \lambda p^a - 1$, where $1 \leq \lambda < p$, and that $(r_1, r_2, \ldots, r_{m-1})$ is an M-sequence. The argument is simplest in the case $\lambda = 1$, so we begin with this case.

We take the cap product of Eq. (1) with $\xi_{m-1}^{p^a}$. By (8), this operation maps the Milnor basis element $P(R)$ to zero. However, the result of stripping P^T by the corresponding sequence $C = (p^{a+m-2},\ldots, p^{a+1}, p^a)$ is nonzero, because by Corollary 2.2 the maximal admissible monomial which occurs in $P^{T/\iota(C)}$ is identified as $P^{T/(0,C)}$, where $(0,C) = (0, p^{a+m-2},\ldots, p^{a+1}, p^a)$. This completes Step 2 in the case $\lambda = 1$.

In the general case, we take the cap product of Eq. (1) with $\xi_{m-1}^{\lambda p^a}$. Again, this operation maps the Milnor basis element $P(R)$ to zero, by (8). To complete the proof, we shall show that the result of stripping P^T λ times by the corresponding sequence $C = (p^{a+m-2},\ldots, p^{a+1}, p^a)$ is nonzero.

Note that we cannot strip more than once by p^a in the last position, so we may assume that the sequence C itself (i.e. $(C, 0)$) is subtracted at least $\lambda - 1$ times in the total of λ steps. Since λ is prime to p, we may assume that the *first* $\lambda - 1$ steps consist of subtraction of the sequence C, at the cost of ignoring the scalar multiple λ. However, the effect of these first $\lambda - 1$ steps is to reduce r_{m-1} to $p^a - 1$ and to make the corresponding changes to the sequence T. This argument in effect reduces the general case to the case $\lambda = 1$ already considered, and so the proof is complete. □

4. Another proof of Monks's theorem

In this section we shall give a new proof of [4, Theorem 9.1], that is to say, of the statement that Eq. (1) holds when R is an M-sequence. The method is to prove the result first for the case of the top class T_n of $A(n)$ for all n, and then to argue by a downward induction using a stripping operator.

For the first step, we give two arguments in the case $p = 2$. The first argument is that of Monks, and the second is taken from [1]. Recall that $T_n = P(R_n)$, where $R_n = (p^{n+1} - 1, p^n - 1, \ldots, p - 1)$.

Lemma 4.1. *For all* $n \geq 0$, $T_n = P^{a_n} T_{n-1}$ *where* $T_{-1} = 1$ *and* $a_n = (n+1)p^{n+1} - (1 + p + \cdots + p^n)$.

Proof. (1) We use induction on n. Consider $P^{a_n}T_{n-1}$ as the product of the Milnor basis elements $P(a_n)$ and $P(R_{n-1})$. Using Milnor's multiplication formula [3], T_n arises from the Milnor matrix

$$\begin{array}{cccccc} * & 0 & 0 & \dots & 0 & 0 \\ p^{n+1}-1 & p^n-1 & p^{n-1}-1 & \dots & p^2-1 & p-1 \end{array}.$$

Thus it suffices to show that if the Milnor matrix

$$\begin{array}{llllll} * & x_2 & x_3 & \dots & x_n & x_{n+1} \\ y_1 & y_2 & y_3 & \dots & y_n & y_{n+1} \end{array}$$

gives a nonzero term in the product, then $x_i = 0$ for all i, so that the matrix must be the one given above.

To do this, we show by finite induction on k for $1 \le k \le n$ that all the x_i are $\equiv 0 \bmod p^k$. To start the induction, we observe that $y_1 \equiv a_n \equiv -1 \bmod p$. Since $\binom{x_2+y_1}{y_1} \not\equiv 0 \bmod p$, it follows that $x_2 \equiv 0 \bmod p$. Since $x_2 + y_2 = p^n - 1$, $y_2 \equiv -1 \bmod p$. Since $\binom{x_3+y_2}{y_2} \not\equiv 0 \bmod p$, it follows that $x_3 \equiv 0 \bmod p$. Continuing in this way, we see that all the x_i are $\equiv 0 \bmod p$.

For the inductive step, let $k < n$ and assume that $x_i \equiv 0 \bmod p^k$ for all i. Since $x_i + y_i = p^{n-i+2} - 1$ for all $i > 1$, this implies that $y_i \equiv -1 \bmod p^k$ for $2 \le i \le n+2-k$ and $y_i = p^{n+2-i} - 1$ for $i \ge n + 2 - k$. We thus have $p^{i-1}y_i \equiv -p^{i-1} \bmod p^{k+1}$ for all i. Since $a_n \equiv 1 \bmod p^{k+1}$, it follows that $y_1 \equiv 1 + p + \cdots + p^k \equiv -1 \bmod p^{k+1}$.

From this point, we may proceed as in the case $k = 1$. Since $\binom{x_2+y_1}{y_1} \not\equiv 0 \bmod p$, $x_2 \equiv 0 \bmod p^{k+1}$. Since $x_2 + y_2 = p^n - 1$, this gives $y_2 \equiv -1 \bmod p^{k+1}$. Continuing in this way, we obtain $x_i \equiv 0 \bmod p^{k+1}$ for all i. This completes the induction on k and the first proof of Lemma 4.1.

(2) For $p = 2$, we use the Z-basis theorem of [9], which states in particular that $T_n = Z_n$, where Z_n is the product of all Sq^i of the form $i = 2^a(2^b - 1)$ with $i < 2^{n+1}$, taken in the order in which $2^a(2^b - 1)$ precedes $2^c(2^d - 1)$ if $a + b > c + d$ or if $a + b = c + d$ and $a > c$. For example,

$$Z_3 = Sq^8 Sq^{12} Sq^{14} Sq^{15} Sq^4 Sq^6 Sq^7 Sq^2 Sq^3 Sq^1.$$

Thus $Z_n = X_n Z_{n-1}$, where

$$X_n = Sq^{2^n} Sq^{3 \cdot 2^{n-1}} Sq^{7 \cdot 2^{n-2}} \cdots Sq^{2^{n+1}-1}.$$

Thus, we shall prove by induction on n that $Z_n = Sq^{a_n} Z_{n-1}$. For the inductive step, it follows from the Adem relations (2) that

$$X_n = Sq^{a_n} + Y_n,$$

where Y_n lies in the left ideal $A.A(n-1)^+$ of A generated by $Sq^1, Sq^2, \dots, Sq^{2^{n-1}}$. To see this, we multiply the factors in X_n from the right and observe that the leading coefficient in each Adem relation is 1, while the other terms in the relation all lie in $A.A(n-1)^+$. The inductive step is now completed by observing that $YT_{n-1} = 0$ for any element $Y \in A.A(n-1)^+$. (In fact, it is shown in [1, Fact 1.2] that the converse is also true, i.e. $A.A(n-1)^+$ is precisely the set of elements of A which are annihilated by right multiplication by T_{n-1}.)

This completes our second proof of Lemma 4.1. □

Theorem 4.2. *If $(r_1, r_2, \ldots, r_n)$ is an M-sequence, then*

$$P(r_1, r_2, \ldots, r_n) = P^{t_1} P^{t_2} \ldots P^{t_n}, \tag{11}$$

where $t_i - pt_{i+1} = r_i$ for $1 \le i < n$ and $t_n = r_n$.

Proof. By Lemma 4.1 the result holds when $P(R) = T_{n-1}$, *i.e.* for the M-sequence $R = (p^n - 1, p^{n-1} - 1, \ldots, p - 1)$. Now let R be an M-sequence such that $P(R) \in A(n-1)$, and assume, as induction hypothesis, that the result is true for every M-sequence R^+ which corresponds either to an element of $A(n-2)$ or to an element of $A(n-1)$ in grading higher than that of $P(R)$.

Since $P(R) \in A(n-1)$, we have $r_i < p^{n+1-i}$, and so the base p expansions of $r_1, r_2, \ldots, r_n$ can be regarded as the nonzero rows of an upper triangular $n \times n$ matrix $M = (m_{i,j})$ with entries in $\{0, 1, \ldots, p-1\}$. Since R is an M-sequence, M has the property that if $m_{i,j} = p-1$ then $m_{i',j'} = p-1$ for all $i' < i$ and $j' \ge j$. We order the upper triangular entries of M downwards on each column and from right to left. If $P(R) \ne T_{n-1}$, then $m_{i,j} < p-1$ for some (i,j) with $i \le j$. Let M^+ be the matrix obtained from M by increasing the first such entry which occurs in M, in the given order, by 1. Then the sequence R^+ which corresponds to M^+ is clearly an M-sequence, and $P(R^+) \in A(n-1)$ has grading higher than that of R, so that the induction hypothesis applies to R^+. For example, if $p = 2$ and $R = (15, 11, 3, 3, 1)$, then $n = 5$ and $R^+ = (15, 15, 3, 3, 1)$, and if $R = (15, 11, 3)$, then $n = 5$ and $R^+ = (15, 11, 3, 1)$.

By repeating this construction, we obtain a preferred sequence of Milnor basis elements in increasing grading which joins a given element $P(R)$ to the top class T_{n-1} of the smallest subalgebra $A(n-1)$ in which it lies. By the induction hypothesis, $P(R^+) = P^{T^+}$, where T^+ is related to R^+ as T to R. Now if M^+ is obtained from M by increasing the (i,j)th entry by 1, then R^+ is obtained from R by replacing r_i by $r_i + p^{n-j}$, and $(r_{i+1}, \ldots, r_n)$ is a monotonic decreasing sequence of integers of the form $p^b - 1$, where $b \le n - j$.

By (8), $P(R)$ can be recovered from $P(R^+)$ by stripping with $\xi_i^{p^{n-j}}$. Using (10), to complete the induction we must show that the result of stripping the admissible monomial P^{T^+} by the sequence $C = (p^{n-j+i-1}, \ldots, p^{n-j+1}, p^{n-j})$ is P^T, where $T = T^+/C$. Note that the monomial P^T is admissible, and that it is this admissible monomial that we wish to prove equal to $P(R)$.

It therefore suffices to show that for any $U \in \iota(C)$ with $U \ne C$, $P^{T^+/U} = 0$. Since there are no such sequences U to consider if $i \ge n$, we may assume $i < n$. Let $C = (C', C'')$ where $C' = (p^{n-j+i-1}, \ldots, p^{n-j+1})$ and $C'' = (p^{n-j})$. Any string $T^+/U \in T^+/\iota(C)$ can then be broken into two substrings $(T'/U', T''/U'')$, where $U' \in \iota(C')$ and

$U'' \in \imath(C'')$. Thus, it suffices to show that $P^{T''/\imath(C'')} = 0$, where $T'' = (t_{k+1}, t_{k+2}, \ldots, t_n)$ for some $k \geq i$.

Let $S = (r_{k+1}, r_{k+2}, \ldots, r_n)$. Then S is an M-sequence, so the induction hypothesis on n gives $P^{T''} = P(S)$. Using (10), $P^{T''/\imath(C'')} = \xi_1^{p^{n-j}} \cap P^{T''} = \xi_1^{p^{n-j}} \cap P(S)$. Now, as remarked above, the construction of R^+ implies that $r_{k+1} < p^{n-j}$. It follows from (8) that $\xi_1^{p^{n-j}} \cap P(S) = 0$.

This completes the inductive step, and the proof. □

References

[1] D.P. Carlisle, R.M.W. Wood, On an ideal conjecture in the Steenrod algebra, preprint, University of Manchester, 1994.

[2] H.R. Margolis, Spectra and the Steenrod Algebra, Elsevier, Amsterdam, 1983.

[3] J. Milnor, The Steenrod algebra and its dual, Ann. Math. 67 (2) (1958) 150–171.

[4] K.G. Monks, Change of basis, monomial relations, and P_t^S bases for the Steenrod algebra, J. Pure Appl. Algebra 125 (1998) 235–260.

[5] J.H. Silverman, Stripping and conjugation in the Steenrod algebra, J. Pure Appl. Algebra 121 (1997) 95–106.

[6] J.H. Silverman, Hit polynomials and conjugation in the dual Steenrod algebra, Math. Proc. Cambridge Philos. Soc., to appear.

[7] G. Walker, R.M.W. Wood, The nilpotence height of Sq^{2^n}, Proc. Amer. Math. Soc. 124 (1996) 1291–1295.

[8] G. Walker, R.M.W. Wood, The nilpotence height of P^{p^n}, Math. Proc. Cambridge Philos. Soc., to appear.

[9] R.M.W. Wood, A note on bases and relations in the Steenrod algebra, Bull. London Math. Soc. 27 (1995) 380–386.

[10] R.M.W. Wood, An introduction to the Steenrod algebra through differential operators, preprint, University of Manchester, 1995.