Czechoslovak Mathematical Journal

Ismet Karaca

Monomial bases in the mod-p Steenrod algebra

Czechoslovak Mathematical Journal, Vol. 55 (2005), No. 3, 699–707

Persistent URL: http://dml.cz/dmlcz/128014

Czechoslovak Mathematical Journal, 55 (130) (2005), 699–707

MONOMIAL BASES IN THE MOD-p STEENROD ALGEBRA

Ismet Karaca, Izmir

(Received October 22, 2002)

Abstract. In this paper we study sets of some special monomials which form bases for the mod-p Steenrod algebra $\mathscr{A}$.

Keywords: Steenrod algebra

MSC 2000: 55S10, 55S05, 57T05

1. Introduction and main results

Let $\mathscr{A}_p$ be the mod-p Steenrod algebra where p is an odd prime number. We use $\mathscr{A}$ to denote $\mathscr{A}_p$ generated by the Steenrod pth powers because Bocksteins play no part in our work. Thus $\mathscr{A}$ is a connected graded Hopf algebra over the field $\mathbb{F}_p$ of p elements. As an associative algebra, $\mathscr{A}$ 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

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

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

There are many descriptions of bases for the mod-2 Steenrod algebra in literature. There are bases developed by Milnor [3], Wall [4], D. Arnon [1], and R. Wood [6]. In this paper we generalize results of Arnon [1] to odd primes.

We begin by making the convention 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 $T = (t_1, t_2, \ldots, t_m)$ which indexes the string of Steenrod powers (the monomial) $P^T = P^{t_1} P^{t_2} \ldots P^{t_m}$. The sequence T and the monomial P^T are called admissible if $t_j \geqslant pt_{j+1}$ for $j \geqslant 1$. The set of admissible monomials is a vector space basis of $\mathscr{A}$. The admissible monomial can be defined in the following equivalent manner. Define a monomial $P^{t_1} P^{t_2} \ldots P^{t_m}$ to be smaller than $P^{s_1} P^{s_2} \ldots, P^{s_n}$ if the sequence $T = (t_1, t_2, \ldots, t_m)$ is smaller than $S = (s_1, s_2, \ldots, s_n)$ when read from left to right. Then the admissible monomials are those which cannot be expressed as a combination of larger monomials. This point of view naturally leads to the following definition.

Definition 1.1. Let F be the free (non-commutative) graded algebra over a field k generated by the set of symbols $\{x_i\}_{i \in I}$ and assume that for any integer N only a finite number of symbols have degrees smaller than N. Let $\leqslant$ be any linear ordering on the monomials in F, and let U be a two sided homogeneous ideal in F. A monomial M is called maximal (minimal) with respect to $(U, \leqslant)$ if M is not equivalent, mod U, to a linear combination of monomials larger (smaller) than M under $\leqslant$.

Then following corollary is immediate.

Corollary 1.2. *Given F, U and $\leqslant$ as above, the set of maximal (minimal) monic monomials forms a vector space basis for F/U.*

Definition 1.3. Let $S = (s_1, s_2, \ldots, s_n)$ and $T = (t_1, t_2, \ldots, t_m)$ be finite sequences of integers. Write $T \leqslant_R S$ if T is less than S in lexicographic order from the right, i.e. if either $m < n$ or else $m = n$ and there exists i such that $t_i < s_i$ and $t_j = s_j$ for all $j > i$. If $T \leqslant_R S$, we say T is right lexicographic less than S. We introduce a similar definition for left lexicographic order, i.e. $T \leqslant_L S$ if there exists i such that $t_i < s_i$ and $t_j = s_j$ for all $j < i$ (where we take $t_k = 0$ for $k > m$ and $s_k = 0$ for $k > n$). If $T \leqslant_L S$, we will say T is left lexicographic less than S.

Similarly, for two sequences of positive integers T, S, define

$$P^T \leqslant_R P^S \quad \text{if } T \leqslant_R S$$

and

$$P^T \leqslant_L P^S \quad \text{if } T \leqslant_L S.$$

For two polynomials $G = \sum M_i$ and $H = \sum N_j$, define $G \leqslant_L H$ if $M_i \leqslant_L N_j$ for all i, j.

Remark. Notice that the order relation was defined on formal monomials and polynomials. To avoid confusion, monomials and polynomials will be always considered as elements of the free algebra generated by $\{P^i\}_{i=0}^{\infty}$. Identity in $\mathscr{A}$ will be denoted by $\equiv$. However, a basis of monomials will always mean a basis in $\mathscr{A}$.

The standard basis is the basis of maximal monomials with respect to the ideal generated by the Adem relations and the left hand lexicographic ordering.

Definition 1.4.

(1) The basis the ξ-monomials has the form

$$X_k^n = P^{p^n} P^{p^{n-1}} \dots P^{p^k}.$$

(2) The basis the ζ-monomials has the form

$$Z_k^n = P^{p^k} P^{p^{k+1}} \dots P^{p^n}.$$

(3) A monomial of the form $P^{t_m} P^{t_{m-1}} \dots P^{t_1}$ is said to be C-admissible if $t_{i+1} \leqslant p t_i$ for $1 \leqslant i < m$ and t_i is divisible by p^{i-1}.

Now we can state our results which are mod-p analogues of Arnon [1].

Theorem 1.5.

(i) *The set of all monomials of the form* $X_{k_0}^{n_0} X_{k_1}^{n_1} \dots X_{k_r}^{n_r}$ *such that* $(n_0, k_0) <_L \dots <_L (n_r, k_r)$ *forms a basis for* $\mathscr{A}$.

(ii) *The set of all monomials of the form* $Z_{k_0}^{n_0} Z_{k_1}^{n_1} \dots Z_{k_r}^{n_r}$ *such that* $(n_r, k_r) <_L \dots <_L (n_0, k_0)$ *forms a basis for* $\mathscr{A}$.

(iii) *The set of all* C*-admissible monomials forms a basis for* $\mathscr{A}$.

2. Preliminaries

In this section the details, notation, and background will be presented.

We introduce useful notation: each natural number a has a unique p-adic expansion

$$a = \sum_{i=0}^{\infty} \alpha_i(a) p^i$$

with $0 \leqslant \alpha_i(a) < p$. It is a fact that

$$\binom{a}{b} \equiv \prod_{i=0}^{\infty} \binom{\alpha_i(a)}{\alpha_i(b)} \bmod p. \tag{2.1}$$

Definition 2.1. Let $\mathscr{S}$ be the set of finite sequences of nonnegative integers, $\mathscr{T} \subset \mathscr{S}$ the subset of admissible sequences and $\mathscr{T}' \subset \mathscr{S}$ the subset of C-admissible sequences. Define

$$\alpha\colon\ \mathscr{T} \longrightarrow \mathscr{T}', \quad (t_m, t_{m-1}, \dots, t_1) \longmapsto \alpha(t_m, t_{m-1}, \dots, t_1) = (s_m, s_{m-1}, \dots, s_1)$$

where $s_k = p^{k-1}\left[t_{m-k+1} - (p-1)\sum\limits_{l=1}^{m-k} t_l\right]$.

Note that $\sum s_k = \sum t_k$, so α is degree preserving. We need to check if the new sequence is in $\mathscr{T}'$:

$$\begin{aligned} p \cdot s_k - s_{k+1} &= p^k\left(t_{m-k+1} - (p-1)\sum_{l=1}^{m-k} t_l\right) - p^k\left(t_{m-k} - (p-1)\sum_{l=1}^{m-k-1} t_l\right) \\ &= p^k(t_{m-k+1} - pt_{m-k}) \geqslant 0. \end{aligned}$$

Hence $s_{k+1} \leqslant ps_k$. It is clear that p^{k-1} divides s_k. So the map α is well defined. The inverse β of α is defined as

$$\beta\colon\ \mathscr{T}' \longrightarrow \mathscr{T}, \quad (s_m, s_{m-1}, \dots, s_1) \longmapsto \alpha(s_m, s_{m-1}, \dots, s_1) = (t_m, t_{m-1}, \dots, t_1)$$

where $t_k = p^{-m+k-1}\Big(p \cdot s_{m-k+1} + (p-1)\sum\limits_{l=m-k+2}^{m} s_l\Big)$. This proves the following result.

Lemma 2.2. *There is a bijection between the standard basis monomials and the C-monomials.*

Proposition 2.3. *Assume that $t_k = p^{s_k}$ for $1 \leqslant k \leqslant m$. A monomial $M = P^{t_1}P^{t_2}\dots P^{t_m}$ is not of the form required in part* (ii) *of Theorem* 1.5 *if and only if at least one of the following holds:*

(1) *For some k, $s_{k+1} > s_k + 1$.*
(2) *The sequence $P^{p^m}Z_k^n$ with $k < m < n$ appears in M.*
(3) *The sequence $Z_k^n Z_k^n$ appears in M.*

P r o o f. To handle the first case, use the following relation, which holds when $t > s + 1$:

$$P^{p^s}P^{p^t} \equiv P^{p^t}P^{p^s} + P^{p^{s+1}}P^{p^t-(p-1)p^s} + \sum_{i=0}^{s-1}\binom{(p-1)(p^t-p^i)-1}{p^s-p^{i+1}}P^{p^t+p^s-p^i}P^{p^i}.$$

To resolve the second case, we need more effort. Without loss of generality we can assume $n = m + 1$. We now reduce the monomial $P^{p^m} Z_k^{m+1}$ in several steps. One can prove by descending induction on k that

$$Z_k^m \equiv P^{p^{m+1}-p^k} + L$$

where $L <_R P^{p^m}$. This yields

$$P^{p^m} Z_k^{m+1} \equiv P^{p^m} Z_k^m P^{p^{m+1}} \equiv P^{p^m} P^{p^{m+1}-p^k} P^{p^{m+1}} + P^{p^m} L P^{p^{m+1}}.$$

The-right hand summand is already lexicographically lower than $P^{p^m} Z_k^{m+1}$, so we have to deal with the left-hand summand. Now we use the Adem relation

$$P^{p^m} P^{p^{m+1}-p^k} \equiv P^{p^{m+1}+p^m-p^k} + L'$$

where $L' <_R P^{p^m}$. Again using the Adem relation, we get

$$P^{p^m+p^{m+1}-p^k} P^{p^{m+1}} \equiv \binom{p^{m+1}-1}{p^{m+1}+p^m-p^k} P^{p^{m+2}+p^m-p^k} + L''$$

where $L'' \leqslant_R P^{p^m+p^{m-1}-p^{k-1}} <_R P^{p^{m+1}}$. By equation (2.1), we have

$$\binom{p^{m+1}-1}{p^{m+1}+p^m-p^k} \equiv \prod_{i=0}^{m+1} \binom{\alpha_i(p^{m+1}-1)}{\alpha_i(p^{m+1}+p^m-p^k)}.$$

Since $\alpha_{m+1}(p^{m+1}-1) = 0$ and $\alpha_{m+1}(p^{m+1}+p^m-p^k) = 1$, we conclude that

$$\binom{p^{m+1}-1}{p^{m+1}+p^m-p^k} \equiv 0 \bmod p.$$

So we are done.

Resolving the third case we use the identity

$$Z_k^n \equiv P^{p^{n+1}-p^k} + L.$$

From this identity we obtain

$$(Z_k^n)^2 \equiv L Z_k^n + (P^{p^{n+1}-p^k})^2 + P^{p^{n+1}-p^k} L.$$

The first and second summands are lexicographically lower than $(Z_k^n)^2$. For the right-hand summand we use the Adem relation

$$(P^{p^{n+1}-p^k})^2 = \sum_{i=0}^{p^n-p^{k-1}} c_i P^{p^{n+2}-p^{k+1}-i} P^i$$

where the c_i's are some binomial coefficients. Since i is bounded above by $p^n - 1$, we are done in this case as well. This completes the proof. □

Now let us define a set isomorphism

$$\begin{aligned}\gamma\colon\ \mathscr{T} &\longrightarrow \mathscr{S},\\ (t_m, t_{m-1}, \ldots, t_1) &\longmapsto \gamma((t_m, t_{m-1}, \ldots, t_1))\\ &= (t_m - pt_{m-1}, t_{m-1} - pt_{m-2}, \ldots, t_2 - pt_1, t_1).\end{aligned}$$

Lemma 2.4. *Let $T \in \mathscr{S}$ and $S \in \mathscr{T}$ be sequences of length k. Then*

$$\langle \xi^{\gamma(S)}, P^T\rangle = \begin{cases} 0 & \text{if } T <_R S,\\ 1 & \text{if } T = S.\end{cases}$$

P r o o f. We will prove this by induction. It is trivial for $S = (0, \ldots)$. Let $S = (s_m, \ldots, s_1)$ and $T = (t_m, t_{m-1}, \ldots, t_1)$ where, assuming $T \leqslant_R S$, we have $s_1 \geqslant b_1 > 0$, $a_1 \geqslant 1$. Put $S' = (s_m - p^{m-1}, s_{m-1} - p^{m-2}, \ldots, s_1 - 1)$. Since $\gamma(S) = \gamma(S')$ except in the mth place, $\xi^{\gamma(S)} = \xi^{\gamma(S')}\xi_m$ where ξ_m is the dual of $P^{p^{m-1}}P^{p^{m-2}}\ldots P^pP^1$. Calculating, we obtain

$$\langle \xi^{\gamma(S)}, P^T\rangle = \langle \xi^{\gamma(S')}\xi_m, P^T\rangle = \langle \psi^*(\xi^{\gamma(S')} \otimes \xi_m), P^T\rangle = \langle \xi^{\gamma(S')} \otimes \xi_m, \psi(P^T)\rangle.$$

Using the definition of the diagonal map ψ in $\mathscr{A}$, we infer that

$$\langle \xi^{\gamma(S)}, P^T\rangle = \Big\langle \xi^{\gamma(S')} \otimes \xi_m, \sum P^{T_1} \otimes P^{T_2}\Big\rangle = \sum \langle \xi^{\gamma(S')}, P^{T_1}\rangle\langle \xi_m, P^{T_2}\rangle$$

where the summation is over sequences T_1, T_2 (not necessarily admissible) such that $T_1 + T_2 = T$ (in the sense of termwise addition).

Now if $t_1 = 0$, then T_2 has 0 at the mth place and hence $\langle \xi_m, P^{T_2}\rangle = 0$. If $t_1 \neq 0$, we see that the only nonzero term in the above summation occurs for $T_2 = (p^{m-1}, \ldots, p, 1)$. Thus $\langle \xi^{\gamma(S)}, P^T\rangle = \langle \xi^{\gamma(S')}, P^{T'}\rangle$ where $T' = (t_m - p^{m-1}, \ldots, t_2 - p, t_1 - 1)$; for this is the only nonzero term in the above summation.

Descending on t_1 and m we complete the proof. □

Definition 2.5. The halving endomorphism D on the free algebra generated by the Steenrod powers is defined by setting $D(P^{pn}) = P^n$ and $D(P^{pn+r}) = 0$ for $n \geqslant 0$ where r is a unit in mod-p. In fact it induces an endomorphism of $\mathscr{A}$. The two properties of D which we will need are

(1) for any cohomology class x and $\Theta \in \mathscr{A}$, $\Theta(x^p) = (D(\Theta)x)^p$,

(2) for any basis C-monomial $P^TP^{t_1}$, $D(P^T)$ is also a basis C-monomial.

The following result is stated as a theorem in [2, p. 518].

Proposition 2.6. *For each odd prime p, $H^*(K(\mathbb{Z}_p, n); \mathbb{Z}_p)$ is the free commutative algebra on the generators $\Theta(i_n)$ where $i_n \in H^n(K(\mathbb{Z}_p, n); \mathbb{Z}_p)$ is a generator and Θ ranges over all admissible monomials of excess less than n.*

Here 'free commutative algebra' means 'polynomial algebra on even-dimensional generators tensored exterior algebra on odd-dimensional generators'.

The proposition says in particular that the admissible monomials in $\mathscr{A}$ are linearly independent, hence form a basis. For if some linear combination of admissible monomials were zero, then it would be zero when applied to the class i_n, but if we choose n larger than the excess of each monomial in the linear combination, this would contradict the freeness of the algebra $H^*(K(\mathbb{Z}_p, n); \mathbb{Z}_p)$. Even though the multiplicative structure of the Steenrod algebra is rather complicated, the Adem relations provide a way of performing calculations algorithmically by systematically reducing all products to sums of admissible monomials.

3. Proof of main results

P r o o f of Theorem 1.5. In order to prove the theorem we need to show that

(1) any monomial which is not of the required form is not maximal (or minimal);

(2) the number of the monomials of degree k having the required form is equal to the dimension of $\mathscr{A}$ at that degree.

First let's prove case (2) in each part of the theorem. It is clear that we have the same number of monomials at each degree in Parts (i) and (ii) so we can handle them as one part. Notice that the basic ξ-monomial X_k^n has the same degree as the dual algebra element $(\xi_{n-k})^{p^k}$. Each element in the dual algebra can be uniquely written as a Steenrod-free polynomial in $(\xi_{n-k})^{p^k}$. Since the dual algebra has the same dimension in each degree, the result follows. By Lemma 2.2, case (2) holds for part (iii).

We now show case (1) for part (ii) of Theorem 1.5. Let $M = P^{t_1} P^{t_2} \dots P^{t_m}$. If for some k, t_k is not a power of p, then P^{t_k} is decomposable, and so can be expressed as a polynomial in lower Steenrod powers. Substituting this polynomial for P^{t_k} in M will reduce it with respect to both the left and right lexicographic ordering. Then by Proposition 2.3, part (ii) of the theorem is proved.

We now prove case (1) for part (i) of Theorem 1.5. Notice that by the same argument we used for part (ii), the maximal monomials for part (i) must be comprised of Steenrod p-powers only. Part (i) now easily follows from part (ii). Notice that the monomials of part (i) are mirror images of the monomials of part (ii). Recall that the Steenrod algebra admits an antiautomorphism $\chi\colon \mathscr{A} \longrightarrow \mathscr{A}$. We use the

following property of χ:

$$\chi(P^{p^n}) \equiv P^{p^n} + L$$

where L is a polynomial in lower Steenrod powers. In particular, substituting L for P^{p^n} in any monomial reduces it lexicographically with respect to both the left and right orders. Given any monomial which is comprised of Steenrod p-powers and which is not of the form (i), use part (ii) and two applications of χ to get an expression of that monomial in terms of lower ones.

We are ready to prove case (1) for part (iii) of Theorem 1.5. Let $M = P^{n_r} \dots P^{n_1} P^n$ be any monomial, and let its expansion in the basis of part (iii) be

$$M \equiv L + \sum_{t \geqslant 0} W_t P^{np^{t-1}} P^{np^{t-2}} P^n$$

where L, W_t are polynomials such that $L \geqslant_R P^{n+1}$ and $W_t <_R P^{np^t}$. Notice that W_0 gives all the monomials in the expansion which are lower than P^n.

Let $M' = P^{n_r} \dots P^{n_1}$. Then

$$Mi_n = M'P^n i_n = M'(i_n)^n = (D(M')i_n)^n,$$
$$Mi_n = Li_n + \sum_{t \geqslant 0} W_t P^{np^{t-1}} P^{np^{t-2}} P^n i_n = \sum_{t \geqslant 0} ((D^t W_t) i_n)^{p^t}.$$

We need to consider two cases. The first case is that M' contains Steenrod powers P^n where n is a unit in mod-p. The second case is that $n_1 > pn$. In the first case we have $D(M') = 0$ and hence Mi_n. In the second case we also have $Mi_n = 0$. Therefore

$$\sum_{t \geqslant 0} ((D^t W_t) i_n)^{p^t} = 0.$$

Notice that $D^t W_t$ is a sum of basis C-elements, all of which are lexicographically smaller than P^n. Since those elements form a free polynomial basis when acting on i_n, the above polynomial equation gives $D^t(W_t) = 0$ for all t, and since all Steenrod powers in W_t have degrees divisible by p^t, we have $W_t = 0$ for all t. So $M \equiv L$ in this case, where $L \geqslant_R P^{n+r}$, r is a unit in mod-p, and therefore $L >_R M$.

In case M' contains no Steenrod powers P^n where n is a unit in mod-p, we can assume by induction that $D(M') \equiv L'$ where $L' \geqslant_R D(M')$. Lifting this equation we get $M \equiv L'' + N$ where $D(L'') = L'$ and all monomials of N contain the Steenrod powers P^n where n is a unit in mod-p. Then

$$M = M'P^n \equiv L''P^n + NP^n$$

where $L''P^n \geqslant_R M$ and NP^n can be made bigger than M by the previous argument. Therefore the above equation provides an expression of M as a sum of bigger monomials unless $L'' = M$ and $N = 0$. In this case $D(M')$ must be a basis C-monomial, and therefore M would be a basis C-monomial unless $n_1 > pn$. But that case has already been dealt with, and so M is a basis C-monomial □

Acknowledgements. I would like to thank D. M. Davis for introducing to me the Steenrod algebra and for every piece of advice and guidance during my work on my PhD degree.

References

[1] *D. Arnon*: Monomial basis in the Steenrod algebra. J. Pure Appl. Algebra *96* (1994), 215–223.
[2] *A. Hatcher*: Algebraic Topology I. http://math.cornell.edu/~hatcher.
[3] *J. Milnor*: The Steenrod algebra and its dual. Ann. of Math. *67* (1958), 150–171.
[4] *N. E. Steenrod and D. B. A. Epstein*: Cohomology operations. Ann. of Math. Stud. *50* (1962).
[5] *C. T. C. Wall*: Generators and relations for the Steenrod algebra. Ann. of Math. *72* (1960), 429–444.
[6] *R. M. W. Wood*: A note on bases and relations in the Steenrod algebra. Bull. London Math. Soc. *27* (1995), 380–386.

Author's address: Department of Mathematics Ege University, Izmir 351 00, Turkey, e-mail: karaca@sci.ege.edu.tr, karaca@bornova.ege.edu.tr.