Comment. Math. Helvetici **66** (1991) 322–331

0010–2571/91/020322–10$1.50 + 0.20/0

On the ring of invariants of $\mathbf{F}_{2^n}^*$

H. E. A. CAMPBELL*, I. HUGHES, F. PAPPALARDI AND P. S. SELICK*

Abstract. In [1] the first and last authors studied a decomposition of $H^*(\mathbf{R}P^\infty \times \cdots \times \mathbf{R}P^\infty; \mathbf{F}_2)$ into modules over the Steenrod algebra obtained from an action of the cyclic group $\mathbf{F}_{2^n}^*$. Here a minimal set of generators for the ring of invariants is characterized and counted by analyzing the associated ring of Laurent polynomials. A structure theorem for the ring of invariant Laurent polynomials is given and a 'destabilisation cancels localisation' theorem is obtained.

Introduction

This paper is intended as a sequel to [1], although it is self-contained. First of all the title should be explained since the group $\mathbf{F}_{2^n}^*$ never makes an appearance in the body of this paper. Choose a primitive $2^n - 1$-st root of unity ω in $\mathbf{F}_{2^n}$ so that $\{\omega^0 = 1, \omega, \ldots, \omega^{n-1}\}$ is a basis for $\mathbf{F}_{2^n}$. Multiplication by ω determines an invertible $\mathbf{F}_2$-linear transformation of $\mathbf{F}_{2^n}$ to itself and so generates a subgroup, G, of order $2^n - 1$ in $Gl_n(\mathbf{F}_2)$ – think of G as $\mathbf{F}_{2^n}^*$. G acts as a group of algebra automorphisms of the symmetric algebra of $\mathbf{F}_{2^n}$ over $\mathbf{F}_2$ (the former thought of as a vector space of dimension n over the latter). This algebra may be identified with the mod 2 cohomology of a product of n copies of $\mathbf{R}P^\infty$ with the usual action of Steenrod's algebra. On the other hand, a non-modular abelian group such as $\mathbf{F}_{2^n}^*$ may be diagonalized usually by extending the scalars (in this case to $\mathbf{F}_{2^n}$) and taking a basis of eigenvectors. This is made explicit in [1, Section 1]. Here the diagonalized group is taken as the point of departure.

This paper studies the ring of polynomials left invariant under the action of this diagonal group. The invariants of diagonal groups are particularly simple to describe since such groups map monomials to monomials. Consequently they act also on the associated ring of Laurent polynomials. A structure theorem for the ring of invariant Laurent polynomials is obtained – it is again a ring of Laurent polynomials on generators of degree 1 (see theorem 1.2). A careful study of this ring leads to a minimal set of generators for the original ring of invariants which

* The authors gratefully acknowledge the support of NSERC. 1980 Mathematics Subject classification, 13F20, 55. Keywords: Invariant theory, Steenrod algebra.

can then be counted. This is of interest to commutative algebraists, for the number of such generators minus the Krull dimension (here the Krull dimension is n) is the homological dimension of the ring of invariants – the length of a resolution of the ring of invariants by syzygies. Perhaps it is worthwhile to note the rapid growth of these generating sets with n. For example, if $n = 8$, the ring of invariants of the group in question of order 255 is minimally generated by 5,095,775 elements. These questions are addressed in Section two.

The behaviour of these rings with respect to the action of Steenrod's algebra A is interesting. This was first noted by G. Carlsson in [3], and was independently rediscovered by W. Singer (private communication). They point out that the process of extending the scalars and taking a basis of eigenvectors involves twisting the action of A. Such twisted actions play an important role in H. Miller's proof of the Sullivan conjecture [13], and in G. Carlsson's proof of the Segal conjecture [2], especially as explained by J. Lannes and his collaborators, see [10], [11], and [12], and also by D. Davis [6]. The connections are more fully discussed in [1, Section 2]. In this paper we prove a 'destabilization cancels localisation' theorem (theorem 3.3), that is, the subalgebra of unstable elements in the ring of Laurent polynomials is the original ring.

There is a well understood representation theoretic technology for decomposing the classifying spaces of various groups (or rather their associated suspension spectra) as a wedge of (perhaps indecomposable) spectra. These decompositions begin with a decomposition of the cohomology as an A-module into a sum of sub-A-modules. On the other hand, such decompositions are also provided by the relative invariants (the graded eigenspaces) of the group $\mathbf{F}_{2^n}^*$. Relations existing between the invariant theoretic approach of [1] and the representation theoretic approach of, say, [7] or [14], are explored by J. Harris in [8] and by J. Harris, T. Hunter and J. Shank in [9]. In particular, [8] identifies the relative invariants of the group $\mathbf{F}_{2^n}^*$ with the summands constructed by M. Witten in her thesis [15].

Recall the following discussion from [1]. Let $\mathbf{F}_{2^n}^*$ be the group generated by ω so that $\mathbf{F}_{2^n}^*$ acts on the additive group $\mathbf{F}_{2^n}$ by multiplication. Form the semidirect product $\mathbf{F}_{2^n}^* \times \mathbf{F}_{2^n}$. In general, if N is a normal subgroup of a group Q with $|Q/N|$ relatively prime to 2, then $H^*(Q; F_2) \cong H^*(N; F_2)^{Q/N}$ (c.f. [4, pages 257–258]). Applying this to the inclusion $\mathbf{F}_{2^n} \to \mathbf{F}_{2^n}^* \ltimes \mathbf{F}_{2^n}$ gives $H^*(\mathbf{F}_{2^n} \ltimes \mathbf{F}_{2^n}; \mathbf{F}_2) \cong H^*(\mathbf{F}_{2^n}; \mathbf{F}_2)^{\mathbf{F}_{2^n}^*}$. This last is the ring of invariants studied here at least as an A-module, see theorem 1 of [1] (which requires that ω be chosen to provide a normal basis for $\mathbf{F}_{2^n}$ – such an ω exists by Davenport's primitive normal basis theorem [5]).

All of the results of this paper apply to the case of odd primes in a straightforward way. Some of the minor changes required are indicated in Section four.

Section One

Let V be a vector space with basis $\{x_{n-1}, \ldots, x_0\}$ over $\mathbf{F}_2$. Let $W = \mathbf{F}_{2^n} \otimes_{\mathbf{F}_2} V$ be the corresponding vector space of dimension n over $\mathbf{F}_{2^n}$ with the same basis. Let ω be a primitive $2^n - 1$ root of unity in $\mathbf{F}_{2^n}$ and let $g \in Gl(W)$ be the diagonal matrix with entries $(\omega^{2^{n-1}}, \ldots, \omega)$. Then g has order $2^n - 1$ and generates a cyclic group, G, of the same order.

Consider the polynomial algebras $P_n = \mathbf{F}_2[x_{n-1}, \ldots, x_0]$ and $Q_n = \mathbf{F}_{2^n} \otimes_{\mathbf{F}_2} P_n = \mathbf{F}_{2^n}[x_{n-1}, \ldots, x_0]$. These are the symmetric algebras $Sym_{\mathbf{F}_2}(V)$ and $Sym_{\mathbf{F}_{2^n}}(W)$ respectively. Each is graded by defining the degree of x_i, denoted $|x_i|$, to be 1. Elements g^i of G act on Q_n by extending the given action on W multiplicatively. The ring of invariants is denoted Q_n^G. Let $I = (i_{n-1}, \ldots, i_0)$ be any sequence of non-negative integers, and let $x^I = x_{n-1}^{i_{n-1}} \cdots x_0^{i_0}$ denote the corresponding monomial of degree $|x^I| = \Sigma\, i_j$. Let Θ be the sequence $(2^{n-1}, \ldots, 2, 1)$ and define $w(I) = \Theta \cdot I = \Sigma\, i_j 2^j$; we call $w(I)$ the weight of I or x^I. Note that $g(x^I) = \omega^{w(I)} x^I$ so that g maps monomials to scalar multiples of themselves. Further note that x^I is left fixed by all elements of G if and only if

$$\Theta \cdot I \equiv 0 \bmod (2^n - 1).$$

I will be called an x-exponent sequence. By abuse of notation I is often said to be invariant if x^I is invariant.

View this equation as defining a 'hyperplane' in $(\mathbf{Z}/(2^n - 1)\mathbf{Z})^n$. Then every invariant x-exponent sequence can be uniquely written 'modulo $2^n - 1$' in terms of the $n - 1$ fixed invariant x-exponent sequences

$$I = a_{n-1}(1, \ldots, 1) + a_{n-2}(0, 3, 1, \ldots, 1) + \cdots + a_1(0, \ldots, 0, 2^{n-1} - 1, 1),$$

for $a_l \in \mathbf{Z}/(2^n - 1)\mathbf{Z}$. In the language of commutative algebra, there are $(2^n - 1)^{n-1}$ such invariants and these are free module generators for the ring of invariants over the homogeneous system of parameters $\{x_{n-1}^{2^n-1}, \ldots, x_0^{2^n-1}\}$. In other words, the x-exponent sequences of the free module generators can be written as

$$(a_{n-1}, a_{n-1} + 3a_{n-2}, \ldots, a_{n-1} + \cdots + a_2 + (2^{n-1} - 1)a_1, a_{n-1} + \cdots + a_1);$$

taken modulo $2^n - 1$. This qualifies as a description of the ring of invariants perhaps, but this is unsatisfactory; for example, the authors have been unable to determine in general the number of module generators in any given degree using this description.

If I is invariant, write $\Theta \cdot I = m(I)(2^n - 1)$; $m(I)$ is called the *multiplier* of I. For non-trivial I, $m(I) \geq 1$. Furthermore, $m(I + J) = m(I) + m(J)$.

For $I = (i_{n-1}, \ldots, i_0)$ define $\sigma(I) = (i_{n-2}, \ldots, i_0, i_{n-1})$.

LEMMA 1.1. *If I is invariant, then $\sigma(I)$ is invariant and $m(\sigma(I)) = 2m(I) - i_{n-1}$. Hence $m(\sigma^j(I)) = 2^j m(I) - 2^{j-1} i_{n-1} - \cdots - i_{n-j}, j \leq n$.*

Proof. Since I is invariant, $\Theta \cdot I = m(I)(2^n - 1)$. Consequently,

$$\begin{aligned}\Theta \cdot \sigma(I) &= 2^{n-1} i_{n-2} + \cdots + 2i_0 + i_{n-1} \\ &= 2(2^{n-2} i_{n-2} + \cdots + i_0) + i_{n-1} \\ &= 2(m(I)(2^n - 1) - 2^{n-1} i_{n-1}) + i_{n-1} \\ &= (2m(I) - i_{n-1})(2^n - 1).\end{aligned}$$

The second statement is an easy induction. □

Let $P_n^G = Q_n^G \cap P_n$. The notation is misleading – the group G does not act on P_n.

Let K_n respectively L_n denote the multiplicative subsets of P_n respectively Q_n generated by $\{x_{n-1}, \ldots, x_0\}$. Let $R_n = \mathbf{F}_2[x_{n-1}^{\pm 1}, \ldots, x_0^{\pm 1}]$ respectively $S_n = \mathbf{F}_{2^n} \otimes_{\mathbf{F}_2} R_n = \mathbf{F}_{2^n}[x_{n-1}^{\pm 1}, \ldots, x_0^{\pm 1}]$ denote the corresponding localisations. The rings R_n and S_n are called the rings of Laurent polynomials associated to P_n and Q_n respectively. The action of G extends to S_n and the ring of invariants is denoted S_n^G. The monomials x^I form a basis for S_n but now negative exponents are allowed. Furthermore, the notions of invariance, weight and multiplier admit the obvious extensions to S_n. Lemma 1.1 is still true when applied to monomials of S_n. Let $R_n^G = S_n^G \cap R_n$. Again, the notation is misleading – the group G does not act on R_n.

Define $\Omega_0 = (2, 0, \ldots, 0, -1)$ and $\Omega_i = \sigma^i(\Omega_0)$ for $1 \leq i \leq n-1$. Define $y_i = x^{\Omega_i} = x_i^{-1} x_{i-1}^2$ for $i = n-1, \ldots, 0$ (the indices are read modulo n as usual). Then $y_i \in S_n^G$ and $|y_i| = 1$. Given a monomial y^M, M is said to be a y-exponent sequence.

Given $M = (m_{n-1}, \ldots, m_0)$ with integer entries m_i define $I(M) = (i_{n-1}, \ldots, i_0)$ by $i_{n-1} = 2m_0 - m_{n-1}, \ldots, i_0 = 2m_1 - m_0$. An easy computation shows $\Theta \cdot I(M) = m_0(2^n - 1)$, so $I(M)$ is invariant. Hence $I(\sigma^j(M)) = \sigma^j(I(M))$ is invariant, with $m(\sigma^j(I(M))) = m_j$. Moreover $I(M + N) = I(M) + I(N)$.

On the other hand, given an invariant sequence $I = (i_{n-1}, \ldots, i_0)$ define $M(I) = (m_{n-1}, \ldots, m_0)$ by the rule $m_j = m(\sigma^j(I))$. It is clear that $M(I + J) = M(I) + M(J)$.

Define

$$\phi : \mathbf{F}_{2^n}[y_{n-1}^{\pm 1}, \ldots, y_0^{\pm 1}] \to \mathbf{F}_{2^n}[x_{n-1}^{\pm 1}, \ldots, x_0^{\pm 1}]^G$$

by the rule $\phi(y^M) = x^{I(M)}$ and

$$\rho : \mathbf{F}_{2^n}[x_{n-1}^{\pm 1}, \ldots, x_0^{\pm 1}]^G \to \mathbf{F}_{2^n}[y_{n-1}^{\pm 1}, \ldots, y_0^{\pm 1}]$$

by the rule $\rho(x^I) = y^{M(I)}$. Then ϕ is the algebra map defined on generators by the rule $\phi(y_i) = x_i^{-1}x_{i-1}^2$. It is easy to check that ϕ and ρ are inverse to each other. Consequently

THEOREM 1.2. $S_n^G \cong \mathbf{F}_{2^n}[y_{n-1}^{\pm 1}, \ldots, y_0^{\pm 1}]$, *and* $R_n^G \cong \mathbf{F}_2[y_{n-1}^{\pm 1}, \ldots, y_0^{\pm 1}]$, *as algebras.* □

Section Two – Algebra generators for P_n^G and Q_n^G

A non-negative invariant non-trivial x-exponent sequence I is said to be decomposable if $I = J + K$ where J and K are non-negative invariant non-trivial x-exponent sequences. Otherwise, I is said to be indecomposable. Note that I decomposable implies $\sigma^j(I)$ is decomposable. Finally, if I is decomposable then $m(I) \geq 2$ since $m(J), m(K) \geq 1$. Simple examples show this necessary condition on the multiplier of an indecomposable is far from sufficient.

The indecomposable sequences in P_n^G and R_n^R can be analyzed using theorem 1.2. A y-exponent sequence $M = (m_{n-1}, \ldots, m_0)$ is said to be admissible if $2m_j \geq m_{j-1}$; otherwise M is said to be inadmissible. The admissible sequences are the y-exponent sequences which map onto the non-negative invariant x-exponent sequences under the map ϕ. The analogous definitions of decomposable and indecomposable sequences apply also to admissible y-exponent sequences. Furthermore, $M(I)$ is indecomposable if and only if $I(M)$ is indecomposable (since ϕ and ρ are multiplicative and map monomials to monomials). Finally, note that if $m_l = 0$ for some l then M is inadmissible, or trivial $M = (0, \ldots, 0)$.

LEMMA 2.1. *Suppose I is a non-negative invariant indecomposable x-exponent sequence. If $I - \Omega_l$ is non-negative, it is also indecomposable, $0 \leq l \leq n-1$.*

Proof. Suppose not, then $I - \Omega_l = J + K$ for some l and J, K non-negative invariant non-trivial x-exponent sequences. In particular, $i_{l+1} + 1 = j_{l+1} + k_{l+1}$ and $i_l - 2 = j_l + k_l$. It follows that one of j_{l+1} or k_{l+1} is greater than or equal to 1,

say $j_{l+1} \geq 1$. Then $\Omega_l + J$ is a non-negative invariant non-trivial x-exponent sequence and $I = (J + \Omega_l) + K$, contradicting the indecomposability of I. □

PROPOSITION 2.2. *Let I be a non-negative invariant x-exponent sequence, and let $M = M(I)$ be the associated admissible y-exponent sequence. Then I is decomposable if and only if $m_l \geq 2$ for all l, $0 \leq l \leq n-1$.*

Proof. If I is decomposable then $I = J + K$ for non-trivial non-negative invariant x-exponent sequences J and K. But then $m_l = m(\sigma^l(I)) = m(\sigma^l(J)) + m(\sigma^l(K)) \geq 2$.

On the other hand, suppose there exists an indecomposable I with $m(\sigma^l(I)) \geq 2$ for all l. Choose such an indecomposable of lowest degree. If all the m_l's are equal then so are all the i_l's and I would be decomposable. Suppose $\alpha \geq 2$ is the smallest integer occurring as an entry of M. Not all entries of M are equal so there is an l with $m_l = \alpha$ and $m_{l+1} = \alpha + \beta$ for some $\alpha \geq 2$ and $\beta \geq 1$. Thus $i_l = 2(\alpha + \beta) - \alpha = \alpha + 2\beta \geq 2$. Consequently, $L = I - \Omega_l$ is a non-negative indecomposable invariant x-exponent sequence of degree $|I| - 1$. Furthermore $M(L) = (m_{n-1}, \ldots, m_{l+2}, \alpha + \beta - 1, \alpha, m_{l-1}, \ldots, m_0)$. Hence each entry in $M(L)$ is greater than or equal to 2. This contradicts the definition of I, so no such I exists. □

THEOREM 2.3. *The number, $G(n)$, of non-negative indecomposable invariant x-exponent sequences is given by the formula*

$$G(n) = \sum_{l=0}^{n-1} \sum_{m_{n-2}=2}^{2} \sum_{m_{n-3}=2}^{2m_{n-2}} \cdots \sum_{m_l=2}^{2m_{l+1}} \sum_{m_{l-1}=1}^{2m_l} \cdots \sum_{m_0=1}^{2m_l} 1$$

Define

$$\mathscr{F}_k(n) = \{M \mid m_{n-1} = k, \quad \text{and } 2m_{n-1} \geq m_{n-2}, \ldots, 2m_1 \geq m_0, m_i \geq 1\},$$

and let $F_k(n) = |\mathscr{F}_k(n)|$. A sequence, $M \in \mathscr{F}_k(n)$ need not be admissible since such an M need not satisfy $2m_0 \geq m_{n-1}$. However if $M \in \mathscr{F}_1(n)$ then M is admissible. David Horrocks, a graduate student at the University of Waterloo, observed that $M \in \mathscr{F}_1(n)$ implies that $I(M)$ is a partition of $2^n - 1$ using only powers of 2. In other words, $F_1(n)$ is the coefficient d_{2^n-1} of t^{2^n-1} in the power series expansion of

$$\prod_{j=0}^{j=\infty} (1 - t^{2^j})^{-1} = \sum_{0}^{\infty} d_i t^i.$$

This helps to explain the phenomenal rate of growth of $G(n)$ with n. It is not hard to see that $d_{2i+1} = d_{2i}$ and $d_{2i} = d_{2i-2} + d_i$. This gives a crude estimate

$$(n-1)(n-2)/2 \leq \log_2(d_{2^n-1}) = \log_2(F_1(n)) \leq \log_2(G(n))$$

by induction on n.

LEMMA 2.4. *$F_k(n) = \Sigma_{l=1}^{2k} F_l(n-1)$ and $F_k(1) = 1$.* □

It follows that

LEMMA 2.5. $F_k(n) = \Sigma_{m_{n-2}=1}^{2k} \cdots \Sigma_{m_0=1}^{2m_1} 1$. □

Define $\mathcal{G}_i(n) = \{M = (m_{n-1} \ldots, m_0) | M$ admissible and $m_i = 1$, $m_{i-1} \neq 1, \ldots, m_0 \neq 1\}$. Set $G_i(n) = |\mathcal{G}_i(n)|$. Then $M \in \mathcal{G}_0(n) = \mathcal{F}_1(n)$ if and only if $m_0 = 1$. Note that $M \in \mathcal{G}_i(n)$ implies $m_{i-1} = 2$. The collection $\mathcal{G}_i(n)$ partitions the set of indecomposable admissible sequences of length n. Hence $\Sigma\, G_i(n) = G(n)$.

LEMMA 2.6.

$$G_i(n) = \sum_{m_{n-2}=2}^{2} \sum_{m_{n-3}=2}^{2m_{n-2}} \cdots \sum_{m_{n-i-1}=2}^{2m_{n-i}} \sum_{m_{n-i-2}=1}^{2m_{n-i-1}} \cdots \sum_{m_0=1}^{2m_1} 1$$

Proof. $G_i(n)$ counts

$$\{M | M \text{ admissible and } m_{n-1} = 1, m_{n-2} \neq 1, \ldots m_{n-i-1} \neq 1\}$$

{by cyclicly permuting the entries of each sequence $M \in \mathcal{G}_i(n)$). Let $a = (a_0, \ldots, a_{n-1})$ and $\alpha = (\alpha_0, \ldots, \alpha_{n-2})$ be two sequences of non-negative integers. Consider the set of sequences $b = (b_0, \ldots, b_{n-1})$ satisfying $b_0 = a_0$, $a_1 \leq b_1 \leq \alpha_0 b_0, \ldots, a_{n-1} \leq b_{n-1} \leq \alpha_{n-2} a_{n-2}$. If G denotes the number of such sequences then

$$G = \sum_{b_1=a_1}^{\alpha_0 a_0} \cdots \sum_{b_{n-1}=a_{n-1}}^{\alpha_{n-2} a_{n-2}} 1$$

for each term in the sum determines a sequence and vice versa. Lemma 2.6 is the case $\alpha = (1, 2, \ldots, 2, 1, \ldots, 1)$ (i 2's) and $\alpha = (2, \ldots, 2)$. □

Theorem 2.3 now follows.

PROPOSITION 2.7. *Let $R = \oplus R_i$ be a connected finitely generated graded algebra over a field $R_0 = k$. Then any two minimal homogeneous generating sets for R as an algebra have the same number of elements.*

COROLLARY 2.8. *The set $\{x^I | I$ indecomposable$\}$ is a minimal generating set for P_n^G and Q_n^G.* □

COROLLARY 2.9. *P_n^G is minimally generated by $G(n)$ elements. So also is Q_n^G.* □

For example, $G(2) = 3$, $G(3) = 13$, $G(4) = 79$, $G(5) = 681$, $G(6) = 8{,}595$, $G(7) = 165{,}677$ and $G(8) = 5{,}095{,}775$.

Proof of 2.7. This is well-known but here is a proof anyway. Let $\mathscr{U}$ and $\mathscr{V}$ be two minimal generating sets for R. Both $\mathscr{U}$ and $\mathscr{V}$ are graded by degree $\mathscr{U} = \oplus \mathscr{U}_i$ and $\mathscr{V} = \oplus \mathscr{V}_i$ where, for example, $\mathscr{U}_i = \mathscr{U} \cap R_i$. It is easy to see that if $R_i \neq 0$ and $R_j = 0$ for $0 < j < i$ then $\mathscr{U}_i$ and $\mathscr{V}_i$ are bases for R_i.

Let $k[\mathscr{U}_{<i}]$ respectively $k[\mathscr{V}_{<i}]$ denote the subalgebras generated by $\mathscr{U}_j$ respectively $\mathscr{V}_j$ for $j < i$. Let $\langle \mathscr{U}_i \rangle$ respectively $\langle \mathscr{V}_i \rangle$ denote the subspaces of R_i spanned by the respective subsets $\mathscr{U}_i$ and $\mathscr{V}_i$. Suppose by induction that $|\mathscr{U}_i| = |\mathscr{V}_j|$ for $j < i$, and that $k[\mathscr{U}_{<i}] = k[\mathscr{V}_{<i}]$. Since $\mathscr{U}$ and $\mathscr{V}$ are minimal generating sets $R_i = \langle \mathscr{U}_i \rangle \oplus (k[\mathscr{U}_{<i}])_i = \langle \mathscr{V}_i \rangle \oplus (k[\mathscr{V}_{<i}])_i$ (the sum is direct by minimality). The result follows. □

Section Three – Destabilization cancels localisation

Let A denote Steenrod's algebra acting on P_n and Q_n by the rule $Sq^1(x_i) = x_{i-1}^2$, $Sq^j(x_i) = 0$ if $j > 1$ and by the requirement that each element of A be $\mathbf{F}_{2^n}$-linear. In fact these rules determine an action of A on P_n and Q_n in a purely formal manner according to an argument of Thomas Hunter (unpublished). That is, this action respects the Adem relations – this may be verified monomial by monomial. Thus both P_n and Q_n receive the structure of unstable modules over A. On the other hand, it is shown in [1, theorem 1] that this A-module structure on P_n is isomorphic to the more usual A-module structure on such a polynomial algebra obtained by identifying it as the cohomology of a product of $\mathbf{R}P^\infty$'s.

The action of Steenrod's algebra is extended to the localised algebras R_n and S_n requiring that the total Steenrod operation $Sq = \Sigma_{i=0} Sq^i$ be a ring homomorphism. Consequently both S_n and R_n receive the structure of A-modules although, of course, they are no longer unstable.

LEMMA 3.1. $Sq^j(x_i^{-1}) = x_i^{-j-1}x_{i-1}^{2j} = x_i^{-1}y_i^j$.

Proof. $Sq(x_i^{-1}) = (Sq(x_i))^{-1} = (x_i + x_{i-1}^2)^{-1} = x_i^{-1}(1+y_i)^{-1}) = x_i^{-1}\sum_{j=0}^{\infty} y_i^j$. Now compare terms of degree $j-1$ to obtain the formula above. □

This A-action commutes with the action of G on P_n so that P_n^G becomes an A-module. Hence so also is S_n^G. The subalgebras Q_n^G and R_n^G are closed under the A-action, so they too receive the structure of A-modules.

LEMMA 3.2. $Sq^0(y_i) = y_i$, $Sq^1(y_i) = y_i^2$, *and, for* $j > 1$, $Sq^j(y_i) = y_i^{j-1}(y_i^2 + y_{i-1}^2)$. □

Suppose M is a module over A which is also an algebra. Let $Uns(M)$ denote the A-submodule of M consisting of the unstable elements of M. That is, $Uns(M) = \{f \in M \mid Sq^J(f) = 0, \text{ if excess}(J) > |f|\}$. $Uns(M)$ is a subalgebra of M.

THEOREM 3.3. $Uns(S_n) = Q_n$ *and* $Uns(R_n) = P_n$.

COROLLARY 3.4. $Uns(S_n^G) = Q_n^G$ *and* $Uns(R_n^G) = P_n^G$.

Proof 3.3. Note $Q_n \subset Uns(S_n)$. If $f \in Uns(S_n)$ then $f = \Sigma \alpha_j x^{I_j}$ for $\alpha_j \in \mathbf{F}_{2^n}$. Assume without loss of generality that f is homogeneous. Let r be the least exponent occurring in any of the monomials x^{I_j}, say, $x^{I_1} = x_{n-1}^{i_n} \cdots x_l^r \cdots x_0^{i_0}$. That is, $i_l = r$ and $i_j \geq r$ for $j \neq l$. Suppose $r < 0$ and consider $x = x_{n-1}^{-r} \cdots x_l^{-r-1} \cdots x_0^{-r} \in Q_n$. Since $Uns(S_n)$ is an algebra $xf \in Uns(S_n)$. By construction

$$xf = x_l^{-1}f' + f'',$$

where $f', f'' \in Q_n$ and no monomials in f' are divisible by x_l.

But no element of the form $x_l^{-1}f'$ can be unstable since $Sq^j(x_l^{-1}f') = x_l^{-j-1}x_{l-1}^{2j}f - + \hat{f} \in Uns(S_n)$ and where $\hat{f}$ has degree bigger than $-j-1$ in x_l. Hence no cancellation occurs, so $Sq^j(x_l^{-1}f') \neq 0$, for all j. This contradicts $xf \in Uns(S_n)$. Consequently $r \geq 0$, so that $f \in Q_n$ as required.

The second statement follows from the first. □

Section Four – Extension to odd primes

All of the results of the previous three sections admit straightforward extensions to odd primes p. Some of the minor changes required are indicated here. Proceed

as above with ω a primitive $p^n - 1$-st root of unity in $\mathbf{F}_{p^n}$, $g = diag(\omega^{p^{n-1}}, \ldots, \omega)$ and $\Theta = (p^{n-1}, \ldots, 1)$. Topologists will want to take $|x_i| = 2$. Define $\Omega_0 = (p, 0, \ldots, 0, -1)$ to obtain y_i with $|y_i| = 2(p-1)$.

Theorem 2.3 now reads

$$G(n) = \sum_{l=0}^{n-1} \sum_{m_{n-2}=2}^{p} \sum_{m_{n-3}=2}^{pm_{n-2}} \cdots \sum_{m_l=2}^{pm_{l+1}} \sum_{m_{l-1}=1}^{pm_l} \cdots \sum_{m_0=1}^{pm_1} 1$$

In Section three the twisted action is $P^1(x_i) = x_{i-1}^p$.

REFERENCES

[1] H. E. A. CAMPBELL and P. S. SELICK, *Polynomial algebras over the Steenrod algebra*, Comment. Math. Helv. *65* (1990) 171–180.

[2] G. CARLSSON, *G. B. Segal's Burnside ring conjecture for* $(\mathbf{Z}/2)^k$, Top. *22* (1983) 83–103.

[3] G. CARLSSON, *Some restrictions on finite groups acting freely on* $(S^n)^k$, Trans. Amer. Math. Soc. *264* (1981) 449–457.

[4] H. CARTAN and S. EILENBERG, Homological algebra, Princeton Math. Series 19, Princeton Univ. Press, 1956.

[5] H. DAVENPORT, *Bases for finite fields*, J. London Math. Soc. *43* (1968) 21–39.

[6] DON DAVIS, *A family of unstable Steenrod modules which includes those of G. Carlsson*, J. Pure and Appl. Alg. *35* (1985) 253–267.

[7] J. HARRIS and N. KUHN, *Stable decompositions of classifying spaces of finite abelian p-groups*, Math. Proc. Camb. Phil. Soc. *103* (1988) 427–449.

[8] J. HARRIS, *On certain stable wedge summands of* $B(\mathbf{Z}/p\mathbf{Z})^z_+$, preprint (1989).

[9] J. HARRIS, T. HUNTER and J. SHANK, *The A-module maps from* $(\mathbf{R}P^\infty)^n$ *to* $(\mathbf{R}p^\infty)^m$, preprint (1989).

[10] W. HENN and L. SCHWARTZ, *Summands of* H^*V *which are unstable algebras*, to appear.

[11] J. LANNES and L. SCHWARTZ, *Sur la structure des A-modules instable injectifs*, to appear.

[12] J. LANNES and S. ZARATI, *Sur les* $\mathcal{U}$*-injectifs*, Ann. Scient. Ec. Norm. Sup. *19* (1986) 303–333.

[13] H. R. MILLER, *The Sullivan conjecture on maps from classifying spaces*, Ann. of Math. *120* (1984) 39–87.

[14] S. A. MITCHELL and S. B. PRIDDY, *Stable splittings derived from the Steinberg module*, Topology *22* (1983) 285–298.

[15] C. M. WITTEN, Self-maps of classifying spaces of finite groups and classification of low-dimensional poincaré duality spaces, Thesis, Stanford University, 1978.

Mathematics and Statistics Department
Queen's University Kingston
Ontario, Canada K7L 3N6 (Campbell, Hughes)

Department of Mathematics and Statistics
McGill University, Montreal
Quebec, Canada H3A 2K6 (Pappalardi)

Mathematics Department
University of Toronto
Toronto, Ontario, Canada M5S 1A1 (Selick)

Received November 5, 1990