PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 2, February 1995

HIT POLYNOMIALS AND THE CANONICAL ANTIAUTOMORPHISM OF THE STEENROD ALGEBRA

JUDITH H. SILVERMAN

(Communicated by Thomas Goodwillie)

ABSTRACT. In this paper, we generalize a formula of Davis (Proc. Amer. Math. Soc. **44** (1974), 235–236) for the antiautomorphism of the mod-2 Steenrod algebra $\mathscr{A}(2)$, in the process formulating the analogue of the Adem relations for products $Sq(\overbrace{0, \dots, 0}^{t-1}, a) \cdot Sq(\overbrace{0, \dots, 0}^{t-1}, b)$. We also state a generalization of a conjecture by the author and Singer (*On the action of Steenrod squares on polynomial algebras* II, J. Pure Appl. Algebra (to appear)) concerning the $\mathscr{A}(2)$-action on $\mathbb{F}_2[x_1, \dots, x_s]$ and use the antiautomorphism formula to prove several cases of the generalized conjecture. We discuss the relationship between the two conjectures and make explicit a sufficient condition for Monks's work to prove a special case of the original conjecture. Finally, we illustrate in a table the relative strengths of the special cases of the conjectures known to be true.

1. STATEMENT OF RESULTS

The mod-2 Steenrod algebra $\mathscr{A}(2)$ of cohomology operations is a connected Hopf algebra, and as such admits a unique antiautomorphism χ [Mil58]. In this paper we generalize an antiautomorphism formula of Davis [Dav74] and use the result to study the action of $\mathscr{A}(2)$ on $\mathbb{F}_2[x_1, \dots, x_s]$, the mod-2 cohomology algebra of the s-fold copy of $\mathbb{RP}^\infty$ with itself.

The Milnor basis of $\mathscr{A}(2)$ is indexed by the set of sequences of non-negative integers almost all of which are 0. Let $\mathscr{S}$ be the set of such sequences. If $S \in \mathscr{S}$ with $s_i = 0$ for $i > N$, the corresponding basis element is denoted $Sq(S) = Sq(s_1, \dots, s_N)$; its dimension is $|Sq(S)| = \sum_{j=1}^{\infty}(2^j - 1)s_j$.

For $t \geq 1$, define $\iota_t : \mathscr{S} \longrightarrow \mathscr{S}$ by $(s_1, \dots, s_N) \mapsto (r_1, \dots, r_{tN})$ with

$$r_i = \begin{cases} s_j, & i = jt, \\ 0, & t \text{ does not divide } i. \end{cases}$$

Let $Sq_t(S) \stackrel{\text{def}}{=} Sq(\iota_t(S))$. Then $|Sq_t(S)| = \sum(2^{jt} - 1)s_j$; in particular, $|Sq_t(s)| = (2^t - 1)s$. The elements $\{Sq_t(S) : S \in \mathscr{S}\}$ form a basis for a Hopf

Received by the editors May 19, 1993.
1991 *Mathematics Subject Classification*. Primary 55S05, 55S10; Secondary 20J05.
Key words and phrases. Steenrod algebra, antiautomorphism, hit polynomials.

0002-9939/94 \$1.00 + \$.25 per page

subalgebra $\mathscr{B}_t \subset \mathscr{A}(2)$ [AM74]. Given $t \geq 1$ and $k, f \geq 0$, define the element $T_t(k; f) \in \mathscr{B}_t$ by

$$T_t(k; f) = Sq_t\left(2^{kt}f\right) \cdot Sq_t\left(2^{(k-1)t}f\right) \cdot \cdots \cdot Sq_t\left(2^t f\right) \cdot Sq_t(f).$$

Note that $|T_t(k; f)| = (2^{(k+1)t} - 1)f$.

The canonical antiautomorphism χ of $\mathscr{A}(2)$ has the property that for all $t \geq 1$ and $n \geq 0$, $\chi Sq_t(n)$ is the sum of all Milnor basis elements $Sq_t(S)$ of appropriate dimension:

$$\chi Sq_t(n) = \sum_{|Sq_t(S)|=(2^t-1)n} Sq_t(S). \tag{1}$$

The Hopf subalgebras $\mathscr{B}_t$ are invariant under χ [Gal79].

For integers $t \geq 1$ and $m \geq 1$, define $\gamma_t(m) = \sum_{i=0}^{m-1} 2^{it}$ as in [Mon]. Note that $\gamma_1(m) = 2^m - 1$ for all m and that

$$\gamma_1(t)\gamma_t(m) = (2^t - 1)\sum_{i=0}^{m-1} 2^{it} = 2^{mt} - 1 = \gamma_1(mt) \tag{2}$$

for all $t \geq 1$, $m \geq 1$.

We prove the following antiautomorphism formulas, generalizing results of [Dav74], [Sil], and [Mon]:

Theorem 1.1. *Fix $t \geq 1$.*

(1) *If $1 \leq f \leq 2^t$, then $\chi Sq_t(f\gamma_t(k+1)) = T_t(k; f)$ for all $k \geq 0$.*
(2) *If $0 \leq \phi < t$, then $\chi T_t(j; 2^\phi\gamma_t(k+1)) = T_t(k; 2^\phi\gamma_t(j+1))$ for all $j, k \geq 0$.*

The Steenrod algebra acts on $\mathbb{P}_s \stackrel{\text{def}}{=} \mathbb{F}_2[x_1, \ldots, x_s]$ according to well-known rules. A (homogeneous) polynomial F is said to be *hit* if it is in the image of the action $\overline{\mathscr{A}(2)} \otimes \mathbb{P}_s \longrightarrow \mathbb{P}_s$, where $\overline{\mathscr{A}(2)}$ is the augmentation ideal of $\mathscr{A}(2)$. For example, since $Sq(f)F = F^2$ for all (homogeneous) polynomials F of degree f, it follows that all squares in $\mathbb{P}_s$ are hit. One is led to ask for conditions under which polynomials of the form EF^2 — or more generally EF^{2^k} — are also hit. Theorems 1.2 and 1.4 below give conditions of this type.

Given the positive integers t and f, we define the function $\mu_t(f)$ to be the minimum possible number of summands in an expression of the form $f = \sum_{i=1}^{p} \gamma_t(k_i)$ [Mon].

Theorem 1.2. *Fix integers $t, f \geq 1$ such that either*

(1) *$1 \leq f \leq 2^t$, or*
(2) *$f = 2^\phi\gamma_t(k)$ for some $0 \leq \phi < t$ and $k \geq 1$.*

Fix also $n \geq 1$. Then for any $e < \gamma_t(n)\mu_t(f)$ and any homogeneous polynomials E and F of degrees e and f respectively, the polynomial $EF^{2^{nt}}$ is hit.

Theorem 1.2 may be regarded as a special case of the following conjecture:

Conjecture 1.3. *Fix integers $t, n, f \geq 1$. Then for any $e < \gamma_t(n)\mu_t(f)$ and any homogeneous polynomials E and F of degrees e and f respectively, the polynomial $EF^{2^{nt}}$ is hit.*

Conjecture 1.3 generalizes Conjecture 1.2 of [SS] (reproduced below as Conjecture 5.1), which requires that $t = 1$. The reader is referred to [SS] for motivation.

The cases $(t, n, f) = (t', n', f')$ and $(t, n, f) = (1, n't', f')$ of Conjecture 1.3 both concern polynomials of the form $EF^{2^{n't'}}$. In general, taking $(t, n, f) = (1, n't', f')$ as in Conjecture 1.2 of [SS] yields a stronger statement, but by studying the function $\mu_t(f)$ we arrive at sufficient conditions for the statements in the two cases to be equivalent. In particular, Theorem 1.1 of [Mon] and Theorem 5.2 of this paper, which confirm Conjecture 1.3 in the cases $(1, t, f)$ and $(2, t, f)$ (t and f arbitrary) respectively, imply the following:

Theorem 1.4. *Let $t \geq 1$ and $f \geq 1$ be integers, and suppose that $f = \sum_{i=1}^{m}(2^{j_i} - 1)$ for some sequence $t+1 \leq j_1 < j_2 < \cdots < j_m$ such that $j_{i+1} - j_i \geq 2t$ for $1 \leq i \leq m-1$. Then Conjecture 1.3 is true for the triplets $(1, t, f)$ and $(1, 2t, f)$.*

The paper concludes with a table comparing the various cases in which Conjecture 1.3 is known to be true.

I thank Ken Monks for sending me an early version of [Mon], by which this paper was inspired.

2. Preliminaries

2.1. **Multiplication in $\mathscr{B}_t$.** The elegant formulation of the Adem relations given in [BM82] generalizes readily to give a formula for the multiplication in $\mathscr{B}_t$. Here the binomial coefficient $\binom{p}{q}$ is defined by $\binom{p}{q} = \frac{p(p-1)\cdots(p-q+1)}{q!}$ for $q \in \mathbb{Z}_{\geq 0}$ and all $p \in \mathbb{Z}$.

Proposition 2.1 (cf. [BM82]). *For $t \geq 1$, define the power series $P_t(z) = \sum_{j\geq 0} Sq_t(j)\, z^j$. Then there is a power series identity*

$$P_t(r^{2^t} + rs)P_t(s^{2^t}) = P_t(s^{2^t} + rs)P_t(r^{2^t}),$$

and it follows that for all a and b,

$$Sq_t(a) \cdot Sq_t(b) = \sum_{j=0}^{[\frac{a}{2^t}]} \binom{(2^t-1)(b-j)-1}{a-2^t j} Sq_t(a+b-j) \cdot Sq_t(j).$$

Accordingly $\mathscr{B}_t$ has an additive basis of "t-admissible" elements $Sq_t(a_1) \cdot Sq_t(a_2) \cdot \cdots \cdot Sq_t(a_n)$ satisfying $a_i \geq 2^t a_{i+1}$ for $1 \leq i \leq n-1$ and $a_n \neq 0$ if $n > 1$.

2.2. **The $\mathscr{A}(2)$-action on $\mathbb{P}_s$.** The action of $\mathscr{A}(2)$ on $\mathbb{P}_s$ has the property [Mon] that for $n \geq 0$ and $F \in \mathbb{P}_s$,

$$Sq_t(n)F = \begin{cases} 0, & \deg F < n, \\ F^{2^t}, & \deg F = n. \end{cases} \tag{3}$$

The *excess* of an element $\theta \in \mathscr{A}(2)$ is given by

$$\operatorname{ex}(\theta) = \min\{ s : \theta(x_1 x_2 \cdots x_s) \neq 0 \in \mathbb{P}_s \}.$$

Since linear maps commute with the action of $\mathscr{A}(2)$, it follows that whatever s might be, $\theta(F) = 0$ for any polynomial in $\mathbb{P}_s$ of degree $< \mathrm{ex}(\theta)$. In [Kra71], Kraines proves that $\mathrm{ex}(Sq_t(S)) = \sum_{j=1}^{\infty} s_j$ and that the excess of a sum of Milnor basis elements is the minimum of the excesses of the summands.

2.3. ***t*-representations.** If $\sum_{j=1}^{\infty} \gamma_t(j) r_j = f$, the sequence $R = (r_1, r_2, \dots) \in \&$ is called a *t-representation of f* (cf. [Mon]). The *length* $l(R)$ is defined to be $l(R) = \sum_{j=1}^{\infty} r_j = \mathrm{ex}(Sq_t(R))$. Since $|Sq_t(R)| = \sum_{j=1}^{\infty}(2^{jt} - 1) r_j = (2^t - 1)\sum_{j=1}^{\infty} r_j \gamma_t(j)$, the sequence R is a t-representation of $f \iff$ the Milnor basis element $Sq_t(R)$ has dimension $(2^t - 1)f$. The set of all t-representations of f is denoted $\mathscr{R}_{t,f}$. When no confusion is possible, we may refer to the sum $\sum_{j=1}^{\infty} \gamma_t(j) r_j$ itself as a t-representation of f.

As mentioned in Section 1, Monks defines the minimum excess function $\mu_t(f)$ to be the minimal length of all t–representations of f [Mon], so that

$$\mu_t(f) \le l(R) \quad \text{for all } R \in \mathscr{R}_{t,f}. \tag{4}$$

In view of (1) and Kraines's theorem concerning excess, we have

$$\mathrm{ex}(\chi Sq_t(f)) = \mu_t(f). \tag{5}$$

3. Canonical t–representations

In [Mon], Monks shows that

$$\mu_t(f) \le (2^t - 1)\mu_1(f) = \gamma_1(t)\mu_1(f) \quad \text{for all } t, f \ge 1. \tag{6}$$

For pairs (t, f) such that equality holds in (6), he observes, an antiautomorphism formula of his proves a special case of the conjecture of [SS] concerning hit polynomials, mentioned in Section 1 and stated below as Conjecture 5.1. In this section we study the function $\mu_t(f)$ and the inequality (6) by singling out t–representations of f of a particular form.

Definition. Let $t, f \ge 1$. A t–representation R of f is said to be *in canonical form* if $r_j \le 2^t$ provided $r_{j'} = 0$ for $j' < j$, and $r_j \le 2^t - 1$ otherwise.

Proposition 2 of [Gal79] states that for fixed $t \ge 1$, each f has a unique t–representation $\tilde{R}(f) = (\tilde{r}_1, \tilde{r}_2, \dots)$ in canonical form, and moreover that $\tilde{R}(f)$ is of minimal length, i.e., $\sum_{j=1}^{\infty} \tilde{r}_j = \mu_t(f)$. We list below two cases of interest (cf. [Gal79], [Mon]).

Example. Let $1 \le f \le 2^t$. Then for all $m \ge 1$, the canonical t–representation of $f\gamma_t(m)$ is simply $\sum_{i=1}^{f} \gamma_t(m)$, so that

$$\mu_t(f\gamma_t(m)) = f. \tag{7}$$

Example. Now let $j \ge 1$ and write $j = tq + r$ where $0 \le r \le t - 1$. The canonical t–representation of $2^j - 1 = \gamma_1(j)$ is

$$2^j - 1 = \begin{cases} 2^j - 1, & j \le t, \\ (2^t - 2^r)\gamma_t(q) + (2^r - 1)\gamma_t(q+1), & j > t, \end{cases} \tag{8}$$

so that

$$(9) \qquad \mu_t(2^j - 1) = \begin{cases} 2^j - 1, & j \le t, \\ 2^t - 1, & j > t. \end{cases}$$

Equations (8) and (9) suggest sufficient conditions to ensure that equality and strict inequality respectively hold in (6); these conditions are stated in Proposition 3.1.

Proposition 3.1. *Suppose that f has canonical 1-representation $\sum_{i=1}^{\mu_1(f)} \gamma_1(j_i) = \sum_{i=1}^{\mu_1(f)} (2^{j_i} - 1)$, where w.l.o.g. $j_1 \le j_2 < j_3 < \cdots < j_{\mu_1(f)}$. For $1 \le i \le \mu_1(f)$, write $j_i = tq_i + r_i$ where $0 \le r_i < t$.*

(1) *Suppose that $q_1 \ge 1$ and $q_{i+1} - q_i \ge 2$ for all i. Then $\mu_t(f) = (2^t - 1)\mu_1(f)$.*

(2) *Suppose that either*

(a) *$q_1 = 1$ and $q_{i+1} = q_i \ge 1$ for some $i \ge 1$;*

(b) *$q_1 = 1$, and $q_{i+1} = q_i + 1$ and $r_{i+1} < r_i$ for some $i \ge 1$; or*

(c) *$q_1 = 0$.*

Then $\mu_t(f) < (2^t - 1)\mu_1(f)$.

Proof. If $q_1 \ge 1$, (8) implies that

$$(10) \qquad f = \sum_{i=1}^{\mu_1(f)} (2^{j_i} - 1) = \sum_{i=1}^{\mu_1(f)} (2^t - 2^{r_i})\gamma_t(q_i) + \sum_{i=1}^{\mu_1(f)} (2^{r_i} - 1)\gamma_t(q_i + 1).$$

In case (1), the sets $\{q_i\}$ and $\{q_i + 1\}$ are disjoint. Therefore (10) is the canonical t-representation of f, and $\mu_t(f) = (2^t - 1)\mu_1(f)$ as claimed. In cases (2a) and (2b), the t-representation R in (10) fails to be in canonical form, and one may generate a representation R' of shorter length by consolidating 2^t of the summands $\gamma_t(q_i)$ with one summand $\gamma_t(q_1) = \gamma_t(1) = 1$ in (10) to form a single summand $\gamma_t(q_{i+1})$. Consequently $\mu_t(f) \le l(R') < l(R) = (2^t - 1)\mu_1(f)$.

If $q_1 = 0$ as in case (2c),then in view of (9) we have

$$\mu_t(f) \le \sum_{i=1}^{\mu_1(f)} \mu_t(2^{j_i} - 1) \le 2^{j_1} - 1 + (\mu_1(f) - 1)(2^t - 1) < (2^t - 1)\mu_1(f).$$

This proves the proposition. □

4. Antiautomorphism formulas

Recall from Section 1 that $T_t(k; f) = Sq_t(2^{kt}f) \cdot Sq_t(2^{(k-1)t}f) \cdot \cdots \cdot Sq_t(2^t f) \cdot Sq_t(f)$. In this section we compute $\chi T_t(k; f)$ for special values of j and f.

Theorem 1.1. *Fix $t \ge 1$.*

(1) *If $1 \le f \le 2^t$, then $\chi Sq_t(f\gamma_t(k + 1)) = T_t(k; f)$ for all $k \ge 0$.*

(2) *If $0 \le \phi < t$, then $\chi T_t(j; 2^\phi \gamma_t(k + 1)) = T_t(k; 2^\phi \gamma_t(j + 1))$ for all $j, k \ge 0$.*

Note. Part (1) of the theorem in the case $t = 1$ is proven in [Dav74], and part (2) for $t = 1$ is proven in [Sil]. Monks proves a different generalization of

Davis's theorem to $t > 1$ in [Mon]. The generalizations in Theorem 1.1 lend themselves readily to the study of hit polynomials; this application is discussed in Section 5.

Proof of Theorem 1.1. The proof of part (1) is based on Davis's proof in the case $t = 1$, but the bookkeeping is more complicated and we give the inductive argument in full. The case $k = 0$ is Theorem 1.2 of [Mon] with $s = k + 1$. Assume then that the result is true for $k - 1$, and write

$$T_t(k; f) = Sq_t\left(2^{kt}f\right) \cdot T_t(k-1; f) \stackrel{\text{ind}}{=} Sq_t\left(2^{kt}f\right) \cdot \chi Sq_t\left(f\gamma_t(k)\right). \tag{11}$$

In order to evaluate the product in (11), we make use of Corollary 1a of [Gal79], which generalizes the proposition of [Dav74]:

Proposition 4.1 ([Gal79]). *For all integers m and l, the product*

$$Sq_t(m) \cdot \chi Sq_t(l) = \sum \binom{\sum 2^{jt} r_j}{2^t m} Sq_t(R), \tag{12}$$

where the sum is taken over all R for which $|Sq_t(R)| = (2^t - 1)(m + l)$; that is, over all $R \in \mathscr{R}_{t, m+l}$, the set of t-representations of $m + l$.

Note. Recall that the binomial coefficient $\binom{a}{b}$ is odd $\Longleftrightarrow$ the binary representations $\sum 2^i a_i$ and $\sum 2^i b_i$ of a and b respectively satisfy $a_i \geq b_i$ for all i [Luc78]. In this case we say a *dominates* b.

Take $l = 2^{kt} f$ and $m = f\gamma_t(k)$, so that $m + l = f\gamma_t(k+1)$ and the sum in (12) is over $R \in \mathscr{R}_{t, \gamma_t(k+1)f} \stackrel{\text{def}}{=} \mathscr{R}$. We claim now that the binomial coefficient $\binom{\sum 2^{tj} r_j}{2^t \cdot f\gamma_t(k)}$ is non–zero for all $R \in \mathscr{R}$; the theorem will then follow immediately from (1).

Observe that the top line in the binomial coefficient is

$$\begin{aligned} \sum_{j=1}^{\infty} 2^{jt} r_j &= \sum_{j=1}^{\infty} (2^{jt} - 1) r_j + \sum_{j=1}^{\infty} r_j = |Sq_t(R)| + l(R) \\ &= f(2^{t(k+1)} - 1) + l(R). \end{aligned} \tag{13}$$

Recall from (4) that

$$\mu_t(f\gamma_t(k+1)) \leq l(R) \leq f\gamma_t(k+1) \tag{14}$$

for all $R \in \mathscr{R}$. Since by hypothesis $f \leq 2^t$, it follows that the t–representation $\sum_{k=1}^{f} \gamma_t(k+1)$ of $f\gamma_t(k+1)$ is in canonical form, and so

$$\mu_t(f\gamma_t(k+1)) = f. \tag{15}$$

From (13), (14), and (15), we find that the top line of the binomial coefficient in (12) satisfies

$$f(2^{(k+1)t} - 1) + f \leq \sum_{j=1}^{\infty} 2^{jt} r_j \leq f(2^{(k+1)t} - 1) + f\gamma_t(k+1);$$

that is,

$$f2^{(k+1)t} \leq \textstyle\sum_{j=1}^{\infty} 2^{jt} r_j \leq f2^t\gamma_t(k+1) = f2^{(k+1)t} + f2^t\gamma_t(k) \tag{16}$$

for all $R \in \mathscr{R}$.

In order to show that the binomial coefficient in (12) is non–zero for all $R \in \mathscr{R}$, one must distinguish between the cases $f \leq 2^t - 1$ and $f = 2^t$. If $f \leq 2^t - 1$, then $f2^t\gamma_t(k) < 2^{(k+1)t}$. For each $R \in \mathscr{R}$, therefore, (16) implies that $\sum_{j=1}^{\infty} 2^{jt} r_j = f2^{(k+1)t} + \epsilon$ for some ϵ with $0 \leq \epsilon < 2^{(k+1)t}$. From this we see that $\sum_{j=1}^{\infty} 2^{jt} r_j$ dominates $f2^{(k+1)t}$ as in the note following Proposition 4.1. Accordingly, the binomial coefficient associated to R is indeed non–zero. If on the other hand $f = 2^t$, then (16) becomes

$$2^{(k+2)t} \leq \sum_{j=1}^{\infty} 2^{jt} r_j \leq 2^{(k+2)t} + 2^{2t}\gamma_t k < 2^{(k+2)t+1},$$

and all numbers in this range evidently dominate $2^{(k+2)t}$. Hence once again the binomial coefficients are all non–zero.

Thus for $f \leq 2^t$ we find that the binomial coefficient in (12) is odd for all $R \in \mathscr{R} = \mathscr{R}_{t,\gamma_t(k+1)f}$, so that

$$Sq_t\left(f2^{kt}\right) \cdot \chi Sq_t\left(f\gamma_t(k)\right) = \sum_{R \in \mathscr{R}_{t,\gamma_t(k+1)f}} Sq_t(R) = \chi Sq_t\left(f\gamma_t(k+1)\right)$$

by Proposition 4.1 and (1). From equality (11) we find that $T_t(k; f) = \chi Sq_t\left(f\gamma_t(k+1)\right)$, thus completing the inductive step and proving part (1) of the theorem.

Part (1) implies the case $j = 0$ of part (2). Inductively assuming that the result is known for $j - 1$, write

$$\begin{aligned} \chi T_t(j; 2^\phi\gamma_t(k+1)) &= \chi(T_t(j-1; 2^\phi\gamma_t(k+1))) \cdot \chi Sq_t\left(2^{jt+\phi}\gamma_t(k+1)\right) \\ &\overset{\text{ind}}{=} (T_t(k; 2^\phi\gamma_t(j))) \cdot \chi Sq_t\left(2^{jt+\phi}\gamma_t(k+1)\right). \end{aligned} \tag{17}$$

Exactly as in the proof given in [Sil] for the case $t = 1$, we proceed by multiplying $\chi Sq_t\left(2^{jt+\phi}\gamma_t(k+1)\right)$ by the successive terms $Sq_t\left(2^{lt+\phi}\gamma_t(j)\right)$, $0 \leq l \leq k$, of $T_t(k; 2^\phi\gamma_t(j))$. The main ingredients of the argument, straightforward generalizations of their analogues for $t = 1$, are given below; the reader is referred to [Sil] for details. The first of these is a consequence of Proposition 4.1 and an analogous formula for $\chi Sq_t(l) \cdot Sq_t(m)$:

Lemma 4.2. *With notation as above, we have*

$$\begin{aligned} &Sq_t\left(2^{lt+\phi}\gamma_t(j)\right) \cdot \chi Sq_t\left(2^{(j+l)t+\phi}\gamma_t(k+1-l)\right) \\ &= \chi Sq_t\left(2^{(j+l+1)t+\phi}\gamma_t(k-l)\right) \cdot Sq_t\left(2^{lt+\phi}\gamma_t(j+1)\right) \\ &+ Sq_t\left(2^{(j+k)t+\phi} + 2^{(l-1)t+\phi}\gamma_t(j+1)\right) \cdot \chi Sq_t\left(2^{(l-1)t+\phi}(2^t\gamma_t(j+k-l) - \gamma_t(j+1))\right) &(18)\\ &+ Sq_t\left(2^{(j+k)t+\phi} - 2^{(l-1)t+\phi}\right) \cdot \chi Sq_t\left(2^{(l-1)t+\phi}\gamma_t(j+k-l+1)\right), &(19) \end{aligned}$$

with the understanding that the rightmost two terms vanish when $l = 0$.

The second major ingredient of the argument is a consequence of the inductive assumption and the generalized Adem relations of Proposition 2.1:

Lemma 4.3. *Let j, k, l, t, and ϕ be as above, and suppose that $h \equiv 1 \mod 2$. Then*

$$\chi Sq_t\left(2^{(l-1)t+\phi}h\right) \cdot T_t(l-1; 2^{\phi}\gamma_t(j+1)) = 0.$$

Proof. The deduction of the inductive step for part (2) from Lemmas 4.2 and 4.3 is identical to the analogous deduction in the case $t = 1$ [Sil]. Roughly speaking, the idea is as follows. At the cost of the two error terms (18) and (19), Lemma 4.2 allows us to push the factor involving χ in (17) past the lth term to its left, leaving behind the lth term $Sq_t\left(2^{lt+\phi}\gamma_t(j+1)\right)$ of the desired product $T_t(k; 2^{\phi}\gamma_t(j+1))$. Furthermore, Lemma 4.3 ensures that these error terms vanish upon multiplication by the $(l-1)$ terms already to their right. After performing the k multiplications, we therefore find that $\chi T_t(j; 2^{\phi}\gamma_t(k+1)) = T_t(k; 2^{\phi}\gamma_t(j+1))$, proving the inductive step and with it part (2) of the theorem. □

5. Hit elements

5.1. **Proof of Theorem 1.2.** Recall that a polynomial $F \in \mathbb{P}_s$ is *hit* if it is in the image of the action $\overline{\mathscr{A}(2)} \otimes \mathbb{P}_s \longrightarrow \mathbb{P}_s$. The following conjecture is discussed in [SS] and [Sil]:

Conjecture 5.1. *Fix integers $n, f \geq 1$. Then for any $e < (2^n - 1)\mu_1(f) = \gamma_1(n)\mu_1(f)$ and any homogeneous polynomials E and F of degrees e and f respectively, the polynomial EF^{2^n} is hit.*

Several special cases of the conjecture have already been proved. The case $n = 1$, f arbitrary is proved in [Woo89]; the cases $n = 2$, f arbitrary and n arbitrary, f of the form $2^j - 1$ are proved in [SS] and [Sil] respectively. The proofs of these partial results all depend on the following observation of Wood: for any polynomials $E, F \in \mathbb{P}_s$ and any $\theta \in \mathscr{A}(2)$, we have the congruence $E \cdot \theta F \equiv (\chi\theta)E \cdot F$ modulo hit elements [Woo89].

Recent work of Monks [Mon] suggests a generalization of this conjecture:

Conjecture 1.3. *Fix integers $t, n, f \geq 1$. Then for any $e < \gamma_t(n)\mu_t(f)$ and any homogeneous polynomials E and F of degrees e and f respectively, the polynomial $EF^{2^{nt}}$ is hit.*

The arguments used to prove special cases of Conjecture 5.1 generalize readily to prove the analogous cases of Conjecture 1.3. The case $n = 1$, t and f arbitrary, for example, is Theorem 1.1 of [Mon]. The argument of [SS] yields the following:

Theorem 5.2. *Conjecture* 1.3 *is true for* $(2, t, f)$ *for all* $t, f \geq 1$.

The above-mentioned result of [Sil] generalizes to $t > 1$ in two ways, corresponding to the two generalizations given in Theorem 1.1 of the antiautomorphism formula used in its proof. We outline the argument to illustrate the use of these formulas.

Theorem 1.2. *Fix integers* $t, f \geq 1$ *such that either*

(1) $1 \leq f \leq 2^t$, *or*

(2) $f = 2^\phi \gamma_t(k)$ *for some* $0 \leq \phi < t$ *and* $k \geq 1$.

Then Conjecture 1.3 *is true for the triple* (t, n, f) *regardless of the choice of* $n \geq 1$.

Proof. Observe that $\mu_t(f) = f$ in part (1) and $\mu_t(f) = 2^\phi$ in part (2) by (7). We prove only part (1); the proof of part (2) is virtually identical. Suppose that $1 \leq f \leq 2^t$, so that the hypothesis of Conjecture 1.3 is that $e < \gamma_t(n)\mu_t(f) = f\gamma_t(n)$. Let E and F be as in Conjecture 1.3. In view of (3), we have $F^{2^{nt}} = T_t(n-1; f)F$ for all t, n, and f. Accordingly

$$\begin{aligned} EF^{2^{nt}} &= E \cdot T_t(n-1; f)F \\ &\equiv \chi T_t(n-1; f)E \cdot F && \text{modulo hit elements} \\ &= Sq_t(f\gamma_t(n))\, E \cdot F && \text{by Theorem 1.1} \\ &= 0, \end{aligned}$$

the last equality holding because by hypothesis $e < f\gamma_t(n) = \mathrm{ex}(Sq_t(f\gamma_t(n)))$. So $EF^{2^{nt}}$ is hit, as claimed. □

5.2. **Comparison of Conjectures 1.3 and 5.1.** The cases $(t, n, f) = (t', n', f')$ of Conjecture 1.3 and $(n, f) = (n't', f')$ of Conjecture 5.1 both concern polynomials of the form $EF^{2^{n't'}}$. In order to compare the corresponding statements, observe from (2) and (6) that

$$\gamma_t(n)\mu_t(f) \leq \gamma_t(n)\gamma_1(t)\mu_1(f) = \gamma_1(nt)\mu_1(f)$$

for all $t, n, f \geq 1$, with equality holding $\Longleftrightarrow$ equality holds in (6). Consequently the assertion of Conjecture 1.3 concerning polynomials of the form $EF^{2^{n't'}}$ agrees with that of Conjecture 5.1 $\Longleftrightarrow$ equality holds in (6), and is otherwise weaker. Criteria such as those in part (2) of Proposition 3.1 point to pairs (t', f') for which Conjecture 5.1 makes a stronger statement about $EF^{2^{n't'}}$ than does Conjecture 1.3 regardless of the choice of n'. Part (1) of Proposition 3.1, on the other hand, describes a condition under which equality does hold in (6). Combining this condition with Theorem 1.1 of [Mon] (mentioned above) and Theorem 5.2, we arrive at the following:

Theorem 1.4. *Let* $t', f' \geq 1$ *be integers, and suppose that* $f' = \sum_{i=1}^{m} 2^{j_i} - 1$ *for some sequence* $t' + 1 \leq j_1 < j_2 < \cdots < j_m$ *such that* $j_{i+1} - j_i \geq 2t'$ *for* $1 \leq i \leq m-1$. *Then Conjecture* 5.1 *is true for the pairs* $(n, f) = (t', f')$ *and* $(n, f) = (2t', f')$.

The conditions given in part (1) of Proposition 3.1 are incompatible with the hypotheses of Theorem 1.2, so the latter sheds no further light on Conjecture 5.1.

5.3. **Comparison of partial results.** As an illustration of the relative strengths of the partial results of Sections 5.1 and 5.2, we fix integers $t, n, f \geq 1$ and use each result in turn to estimate the minimum value $\epsilon(t, n, f)$ of e such that $EF^{2^{nt}}$ fails to be hit for some polynomials E and F of degrees e and f respectively. For example, to use Wood's theorem for the case $n = 1$ and f

TABLE 1

Version of conjecture	Suitable expression for $EF^{2^{nt}}$	Estimated value of $\epsilon(t, n, f)$	Estimated value of $E_{t,n,2^\rho}$, $1 \leq \rho \leq t$
THE CONJECTURES THEMSELVES			
Conjecture 5.1 n, f arbitrary	$EF^{2^{(nt)}}$	$(2^{nt}-1)\mu_1(f)$	$2(2^{nt}-1)$
Conjecture 1.3 t, n, f arbitrary	$EF^{2^{nt}}$	$\gamma_t(n)\mu_t(f)$	$2^\rho\gamma_t(n)$
PARTIAL RESULTS			
Conjecture 5.1 with $n=1$, f arbitrary [Woo89]	$E\cdot(F^{2^{(nt)-1}})^2$	$\mu_1(2^{nt-1}f)$	2
Conjecture 5.1 with $n=2$, f arbitrary [SS]	$E\cdot(F^{2^{(nt)-2}})^{2^2}$	$3\mu_1(2^{nt-2}f)$	6
Conjecture 1.3 with $n=1$, f & t arbitrary [Mon]	$E\cdot(F^{2^{(n-1)t}})^{2^t}$	$\mu_t(2^{(n-1)t}f)$	2^ρ, $n=1$; 2^t, $n\geq 2$
Conjecture 1.3 with $n=2$, f & t arbitrary (Theorem 5.2)	$E\cdot(F^{2^{(n-2)t}})^{2^{2t}}$	$3\mu_t(2^{(n-2)t}f)$	$3\cdot 2^\rho$, $n=2$; $3\cdot 2^t$, $n\geq 3$
Conjecture 1.3 with $1\leq f\leq 2^t$, n arbitrary (Theorem 1.2)	$EF^{2^{nt}}$ (f of correct form)	$f\gamma_t(n)$ (f of correct form)	$2^\rho\gamma_t(n)$
Conjecture 1.3 with $f=2^\phi\gamma_t(k)$ for some $0\leq\phi<t$ and $k\geq 1$, n arbitrary (Theorem 1.2)	$EF^{2^{nt}}$ (f of correct form)	$2^\phi\gamma_t(n)$ (f of correct form)	$2^\rho\gamma_t(n)$
Conjecture 5.1 with either $2^{(n-1)t}f=\sum(2^{j_i}-1)$ or $2^{(n-2)t}f=\sum(2^{j_i}-1)$ as in Theorem 1.4	$E\cdot(F^{2^{(n-1)t}})^{2^t}$; $E\cdot(F^{2^{(n-2)t}})^{2^{2t}}$ (f of correct form)	$(2^t-1)\mu_1(2^{(n-1)t}f)$; $(2^{2t}-1)\mu_1(2^{(n-2)t}f)$ (f of correct form)	not applicable; not applicable
Conjecture 5.1 with n arbitrary, $f=2^j-1$ [Sil]	$EF^{2^{(nt)}}$ (f of correct form)	$(2^{nt}-1)\mu_1(f)$ $=2^{nt}-1$ (f of correct form)	not applicable

arbitrary, we write

$$EF^{2^{nt}} = E\cdot(F^{2^{nt-1}})^2$$

to find that $\epsilon(t, n, f) \geq \mu_1(2^{nt-1}f)$. Of course, there are few choices of (t, f, n) for which all the results work well or even apply. We show in Table 1 the general estimates and those for t, n arbitrary, $f = 2^\rho < 2^t$.

REFERENCES

[AM74] J. F. Adams and H. R. Margolis, *Sub-Hopf-algebras of the Steenrod algebra*, Proc. Amer. Math. Soc. **76** (1974), 45–52.

[BM82] S. R. Bullett and I. G. Macdonald, *On the Adem relations*, Topology **21** (1982), 329–332.

[Dav74] D. Davis, *The antiautomorphism of the Steenrod algebra*, Proc. Amer. Math. Soc. **44** (1974), 235–236.

[Gal79] A. Gallant, *Excess and conjugation in the Steenrod algebra*, Proc. Amer. Math. Soc. **76** (1979), 161–166.

[Kra71] D. Kraines, *On excess in the Milnor basis*, Bull. London Math. Soc. **3** (1971), 363–365.

[Luc78] E. Lucas, *Théorie des functions numériques simplement periodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321.

[Mil58] J. Milnor, *The Steenrod algebra and its dual*, Ann. of Math. (2) **67** (1958), 150–171.

[Mon] K. G. Monks, *Polynomial modules over the Steenrod algebra and conjugation in the Milnor basis*, Proc. Amer. Math. Soc. (to appear).

[Sil] J. H. Silverman, *Conjugation and excess in the Steenrod algebra*, Proc. Amer. Math. Soc. **119** (1993), 657–661.

[SS] J. H. Silverman and W. Singer, *On the action of Steenrod squares on polynomial algebras* II, J. Pure Appl. Algebra (to appear).

[Woo89] R. M. W. Wood, *Steenrod squares of polynomials and the Peterson conjecture*, Math. Proc. Cambridge Philos. Soc. **105** (1989), 307–309.

Department of Mathematics, University of Michigan, 317 W. Engineering Building, Ann Arbor, Michigan 48109-1092

Current address: Department of Mathematics, Indiana University–Purdue University Columbus, 4601 Central Avenue, Columbus, Indiana 47203

E-mail address: `jsilverm@silver.ucs.indiana.edu`