THE NILPOTENCE HEIGHT OF P_t^s FOR ODD PRIMES

ISMET KARACA

ABSTRACT. K. G. Monks has recently shown that the element P_t^s has nilpotence height $2\left[\frac{s}{t}\right] + 2$ in the mod 2 Steenrod algebra. Here the method and result are generalized to show that for an odd prime p the element P_t^s has nilpotence height $p\left[\frac{s}{t}\right] + p$ in the mod p Steenrod algebra.

1. INTRODUCTION AND MAIN RESULTS

Using Monks' method [14] and some new results, we prove the following theorem. Recall that P_t^s is the Milnor basis element $P(r_1, r_2, \dots, r_t)$ with $r_t = p^s$ and $r_i = 0$ for $i < t$.

Theorem 1. *For all $s \geq 0$, $t \geq 1$,*

- (i) $(P_t^s)^{p\left[\frac{s}{t}\right]+p} = 0,$
- (ii) $(P_t^s)^{p\left[\frac{s}{t}\right]+p-1} \neq 0.$

Thus the nilpotence height of P_t^s is exactly $p\left[\frac{s}{t}\right] + p$. The upper bound (i) on the nilpotence order was proved in [14] for the case $p = 2$. The lower bound (ii) was proved in [13] for the case $p = 2$. Here we generalize these arguments.

Let $P_t(r_1, r_2, \dots, r_m)$ be the Milnor basis element $P(s_1, s_2, \dots, s_{tm})$, where $s_{ti} = r_i$ and $s_j = 0$ if t does not divide j . In particular, $P_t(p^s) = P_t^s$ and $P_1(n) = P(n)$.

If $R = (r_1, r_2, \dots, r_m)$ is a sequence of nonnegative integers, we will write $P_t(R)$ for the corresponding Milnor basis element. The degree of $P_t(R)$ is $2|R|_t$, where $|R|_t = \sum_{i=1}^{\infty} (p^{it} - 1)r_i$, and the excess of $P_t(R)$ is $2e(R)$, where $e(R) = \sum_{i=1}^{\infty} r_i$. For a fixed t let B_t be the vector subspace of A with basis the set of all $P_t(R)$. For $P_t^s \in B_t$ write $\widehat{P}_t^s$ for $(-1)^s \chi(P_t^s)$, where χ denotes the canonical antiautomorphism of B_t .

We introduce some notation. Each natural number a has a unique expansion

$$(1) \quad a = \sum_{i=0}^{\infty} \alpha_i(a) p^i$$

with $0 \leq \alpha_i(a) < p$. Let $0 \leq b < p^t$, and $i < t$. Then the following are obvious:

$$(2) \quad \alpha_i(a) = \alpha_{i+t}(p^t a + b),$$

$$(3) \quad \alpha_i(b) = \alpha_i(p^t a + b).$$

Received by the editors May 16, 1996.

1991 *Mathematics Subject Classification.* Primary 55S10, 55S05; Secondary 57T05.

I would like to thank sincerely my PhD. adviser Professor Donald M. Davis for every piece of advice and guidance. This paper would not exist without his help.

Definition. We say that m and n have no carries if $\alpha_i(m) + \alpha_i(n) \leq p - 1$ for all i . This is equivalent to the condition that the binomial coefficient $\binom{m+n}{m}$ is nonzero mod p . If m and n have no carries, we will write $m \asymp n$.

Define $\gamma_t(m) = \sum_{i=0}^{m-1} p^{it}$ for any integer $m \geq 0$ and $t \geq 1$, where $\gamma_t(0) = 0$. The following fact is immediate.

Fact 2. $\gamma_t(m+1) = p^t \gamma_t(m) + 1$.

Proposition 3. For any $t \geq 1$, $m \geq 0$, and $i < t$,

$$(4) \quad P_t((p-1)p^i \gamma_t(m+1)) \cdot P_t^{mt+i} = 0.$$

Proof. By Milnor's product formula, $P_t(a) \cdot P_t(b) = \sum u_j \cdot P_t(a+b-(p^t+1)j, j)$, where the sum is taken over all j such that $(a-p^t j) \asymp (b-j)$, and u_j is a unit mod p . So it is sufficient to show that $(p-1)p^i \gamma_t(m+1) - p^t j$ and $p^{mt+i} - j$ have at least one carry for any $0 \leq j \leq p^i(p-1)\gamma_t(m)$. This is the content of the following lemma. $\square$

Lemma 4. For all $t \geq 1$, $m \geq 0$, $i < t$ and $0 \leq j \leq p^i(p-1)\gamma_t(m)$, there exists a nonnegative integer k such that $\alpha_{kt+i}(p^i(p-1)\gamma_t(m+1)-p^t j) + \alpha_{kt+i}(p^{mt+i}-j) \geq p$.

Proof. We will proceed by induction on m . Let

$$(5) \quad X = (p-1)p^i \gamma_t(m+1) - p^t j$$

$$(6) \quad Y = p^{mt+i} - j.$$

If $m = 0$, then $j = 0$, $X = (p-1)p^i$, and $Y = p^i$. So we have $\alpha_i(X) + \alpha_i(Y) = p$.

Assume that for all $t \geq 1$, $0 \leq i < t$ and $0 \leq j \leq p^i(p-1)\gamma_t(m-1)$, there exists a nonnegative integer k such that $\alpha_{kt+i}(p^i(p-1)\gamma_t(m)-p^t j) + \alpha_{kt+i}(p^{(m-1)t+i}-j) \geq p$.

Choose $t \geq 1$, $i < t$ and $0 \leq j \leq p^i(p-1)\gamma_t(m)$. If $j = 0$, then

$$\begin{aligned} X &= (p-1)p^i \gamma_t(m+1) \\ &= (p-1) \left(p^{mt+i} + p^{(m-1)t+i} + p^{(m-2)t+i} + \dots + p^{t+i} + p^i \right) \\ Y &= p^{mt+i} \end{aligned}$$

Hence $\alpha_{mt+i}(X) + \alpha_{mt+i}(Y) = p$.

Suppose $j \neq 0$.

Case 1 : $\alpha_i(j-1) \neq p-1$.

$$X = (p-1)p^i(p^t \gamma_t(m) + 1) - p^t j = p^t[(p-1)p^i \gamma_t(m) - j] + (p-1)p^i.$$

Since $\alpha_i(j-1) \neq p-1$, $j-1 = p^{i+1}q + p^i h + r$, where $0 \leq r < p^i$ and $0 \leq h < p-1$. Then

$$\begin{aligned} Y &= p^{mt+i} - j = p^{mt+i} - (p^{i+1}q + p^i h + r + 1) \\ &= p^{i+1}[p^{mt-1} - (q+1)] + (p-1-h)p^i + (p^i - (r+1)). \end{aligned}$$

Since $r < p^i$, the term $(p^i - (r+1))$ is nonnegative and less than p^i . So $\alpha_i(X) + \alpha_i(Y) = 2p - h - 2 \geq p$.

Case 2 : $\alpha_i(j-1) = p-1$.

Let $j - 1 = p^t q + r$, where $0 \leq r < p^t$. Since $\alpha_i(j - 1) = p - 1$, $p^i(p - 1) \leq r < p^t$ by (3). In the assumption we have $j \leq p^i(p - 1)\gamma_t(m)$. Then $p^t q + r + 1 \leq p^i(p - 1)(p^t \gamma_t(m - 1) + 1)$. Solving for $q + 1$ shows that

$$q + 1 \leq p^i(p - 1)\gamma_t(m - 1) + \frac{p^i(p - 1) - r - 1 + p^t}{p^t}.$$

Since $p^i(p - 1) \leq r$, $\frac{p^i(p - 1) - r - 1 + p^t}{p^t} < 1$. Thus $q + 1 \leq p^i(p - 1)\gamma_t(m - 1)$, and so by the inductive hypothesis there exists a nonnegative integer k such that

$$\alpha_{kt+i}((p - 1)p^i\gamma_t(m) - p^t(q + 1)) + \alpha_{kt+i}(p^{(m-1)t+i} - (q + 1)) \geq p.$$

Let k be any such value. We will show that $\alpha_{(k+1)t+i}(X) + \alpha_{(k+1)t+i}(Y) \geq p$, which will complete the induction and hence the proof.

Now since $\alpha_i(j - 1) = p - 1$, $\alpha_i(r) = p - 1$. Hence $\alpha_i(p^t - 1 - r) = 0$. Therefore $p^t - 1 - r + (p - 1)p^i < p^t$. Then we have

$$\begin{aligned} \alpha_{kt+i}((p - 1)p^i\gamma_t(m) - p^t(q + 1)) \\ &= \alpha_{kt+i}((p - 1)p^i\gamma_t(m) - p^t(q + 1) + p^t - 1 - r) \\ &= \alpha_{(k+1)t+i}(p^t[(p - 1)p^i\gamma_t(m) - p^t(q + 1) + p^t - 1 - r] + (p - 1)p^i) \\ &= \alpha_{(k+1)t+i}(X) \end{aligned}$$

by (2) and (3). Also,

$$Y = p^{mt+i} - (p^t q + r + 1) = p^t(p^{(m-1)t+i} - (q + 1)) + (p^t - (1 + r)).$$

Thus

$$\begin{aligned} \alpha_{kt+i}(p^{(m-1)t+i} - (q + 1)) &= \alpha_{(k+1)t+i}(p^t(p^{(m-1)t+i} - (q + 1)) + (p^t - (1 + r))) \\ &= \alpha_{(k+1)t+i}(Y) \end{aligned}$$

by (2). By the induction hypothesis, $\alpha_{(k+1)t+i}(X) + \alpha_{(k+1)t+i}(Y) \geq p$. $\square$

Using Davis' method [6], we can derive

Proposition 5.

$$(8) \quad P_t(u) \cdot \widehat{P}_t(v) = \sum_R \binom{|R|_t + e(R)}{p^t u} P_t(R),$$

$$(9) \quad \widehat{P}_t(u) \cdot P_t(v) = \sum_R \binom{e(R)}{v} P_t(R),$$

where the sum is taken over all R for which $|R|_t = (p^t - 1)(u + v)$.

Proof. The formula (8) is exactly Corollary 1a in [8]. So we will prove formula (9). Using Gallant's Proposition 1 that $\chi(P_t^s)$ is $(-1)^s$ times the sum of all $P_t(R)$ in the appropriate dimension, we see that the product $\widehat{P}_t(u) \cdot P_t(v)$ contains a term

$$\prod_i \binom{r_i}{s_i} P_t(r_1, r_2, \dots)$$

for each Milnor matrix,

$$\begin{pmatrix} * & 0 & \dots & 0 & s_1 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 \\ r_1 - s_1 & 0 & \dots & 0 & s_2 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 \\ r_2 - s_2 & 0 & \dots & 0 & s_3 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \end{pmatrix}$$

such that $v = \sum_i s_i$. Thus

$$\hat{P}_t(u) \cdot P_t(v) = \sum_R \sum_S \prod_i \binom{r_i}{s_i} P_t(R)$$

where S ranges over sequences $(s_1, s_2, \dots)$ having $\sum_i s_i = v$. The equation

$$\sum_S \prod_i \binom{r_i}{s_i} = \binom{\sum_i r_i}{v}$$

follows immediately from considering the coefficient of x^v in the expansion of

$$(1+x)^{r_1} \cdot (1+x)^{r_2} \cdots (1+x)^{r_n}.$$

Hence we have

$$\hat{P}_t(u) \cdot P_t(v) = \sum_R \binom{\sum_i r_i}{v} P_t(R) = \sum_R \binom{e(R)}{v} P_t(R).$$

□

Using these formulae, we can prove the following proposition.

Proposition 6. *If a, b and t are positive integers with $a \geq t$, then*

$$\hat{P}_t(p^a(p-1)) \cdot P_t(p^{a+b} - p^a(p-1)) = P_t(p^{a+b} - p^{a-t}(p-1)) \cdot \hat{P}_t(p^{a-t}(p-1)).$$

Proof. Using (8) and (9), we have

$$P_t(p^{a+b} - p^{a-t}(p-1)) \cdot \hat{P}_t(p^{a-t}(p-1)) = \sum_R \binom{|R|_t + e(R)}{p^{a+b+t} - p^a(p-1)} P_t(R)$$

and

$$\hat{P}_t(p^a(p-1)) \cdot P_t(p^{a+b} - p^a(p-1)) = \sum_R \binom{e(R)}{p^{a+b} - p^a(p-1)} P_t(R)$$

where $1 \leq e(R) \leq p^{a+b}$ and $|R|_t = (p^t - 1)p^{a+b}$.

In order to prove these sums are equal, we need to show that their binomial coefficients are equivalent mod p . Note that

$$\binom{e(R)}{p^{a+b} - p^a(p-1)} = \binom{e(R)}{e(R) - p^{a+b} + p^a(p-1)},$$

$$\binom{|R|_t + e(R)}{p^{a+b+t} - p^a(p-1)} = \binom{|R|_t + e(R)}{e(R) - p^{a+b} + p^a(p-1)}.$$

Case 1 : If $1 \leq e(R) < p^{a+b} - p^a(p-1)$, then both binomial coefficients are zero because $e(R) - p^{a+b} + p^a(p-1)$ is a negative integer.

Case 2 : If $p^{a+b} - p^a(p-1) \leq e(R) < p^{a+b}$, then

$$\begin{aligned} \binom{|R|_t + e(R)}{e(R) - p^{a+b} + p^a(p-1)} &= \binom{\sum_{i=a+b}^{a+b+t-1} \alpha_i(|R|_t) p^i + \sum_{i=0}^{a+b-1} \alpha_i(e(R)) p^i}{\sum_{i=0}^{a+b-1} \alpha_i(e(R) - p^{a+b} + p^a(p-1)) p^i} \\ &\equiv \prod_{i=a+b}^{a+b+t-1} \binom{\alpha_i(|R|_t)}{0} \prod_{i=0}^{a+b-1} \binom{\alpha_i(e(R))}{\alpha_i(e(R) - p^{a+b} + p^a(p-1))} \pmod{p} \\ &\equiv \binom{e(R)}{e(R) - p^{a+b} + p^a(p-1)} \pmod{p}. \end{aligned}$$

Hence

$$\binom{|R|_t + e(R)}{p^{a+b+t} - p^a(p-1)} \equiv \binom{e(R)}{p^{a+b} - p^a(p-1)} \pmod{p}.$$

Case 3 : If $e(R) = p^{a+b}$, then

$$\binom{e(R)}{p^{a+b} - p^a(p-1)} = \binom{p^{a+b}}{p^a(p-1)} \equiv 0 \pmod{p}$$

and

$$\binom{|R|_t + e(R)}{p^{a+b+t} - p^a(p-1)} = \binom{p^{a+b+t}}{p^a(p-1)} \equiv 0 \pmod{p}.$$

So the result holds. $\square$

If n, k and t are positive integers with $n = k + mt$ for some m , we define

$$(X_t)_k^n = P_t(p^n(p-1)) \cdot P_t(p^{n-t}(p-1)) \cdots P_t(p^k(p-1)).$$

The following corollary is immediate from Proposition 5.

Corollary 7. *Let $m \geq 1$, $c \geq 0$, and $a = c + mt$. Then*

$$\chi((X_t)_{c+mt}^a) \cdot P_t(p^{a+b} - p^a(p-1)) = P_t(p^{a+b} - p^c(p-1)) \cdot \chi((X_t)_c^{a-t}).$$

For any Milnor basis element θ , define $\kappa_\theta : A \longrightarrow A$ by

$$(10) \quad \phi(x) = \sum \kappa_\theta(x) \otimes \theta$$

where ϕ is the diagonal map in A . These operations were first defined by Kristensen [10]. We will call it “stripping by θ ”. It follows from (10) that stripping a Milnor basis element by $\theta = P(t_1, t_2, \dots)$ is given by

$$\kappa_\theta(P(r_1, r_2, \dots)) = P(r_1 - t_1, r_2 - t_2, \dots)$$

where the right hand side is taken to be 0 if $r_i < t_i$ for any i (see [18] and [19] for more details).

For any $x, y \in A$,

$$\begin{aligned} \sum \kappa_{P(R)}(x \cdot y) \otimes P(R) &= (\sum \kappa_{P(I)}(x) \otimes P(I))(\sum \kappa_{P(J)}(y) \otimes P(J)) \\ &= \sum \kappa_{P(I)}(x) \kappa_{P(J)}(y) \otimes P(I)P(J) = \sum \lambda_R^{I,J} \kappa_{P(I)}(x) \kappa_{P(J)}(y) \otimes P(R) \end{aligned}$$

where $\lambda_R^{I,J} = \langle P(I)P(J), \xi^R \rangle$ and the sums are taken over all I, J, R such that $R = I + J$. So

$$\kappa_{P(R)}(x \cdot y) = \sum_{I, J, R} \lambda_R^{I,J} \kappa_{P(I)}(x) \kappa_{P(J)}(y).$$

In particular, if $\kappa_t^s = \kappa_{P_t^s}$, then $\kappa_t^s(x \cdot y) = \sum_{j=0}^t \kappa_{t-j}^{s+j}(x) \kappa_j^s(y)$ follows from the formula $\phi(\xi_k) = \sum_{i=0}^k \xi_{k-i}^{p^i} \otimes \xi_i$.

Lemma 8. *If x and y belong to B_t then stripping by P_t^s is a derivation, i.e.*

$$\kappa_t^s(x \cdot y) = \kappa_t^s(x) \cdot y + x \cdot \kappa_t^s(y).$$

Proof. The proof follows from the formula above, since all of the other terms in the sum correspond to stripping by Milnor basis elements which are not in B_t and therefore give zero. $\square$

A sequence $R = (r_1, r_2, \dots)$ is called a t -representation of a positive integer m if $m = \sum_i \gamma_t(i) r_i$. We define $\mu_t(m) = \min\{\sum_i r_i : (r_1, r_2, \dots) \text{ is a } t\text{-representation of } m\}$.

Lemma 9. *For $P_t(R) \in B_t$ and $m \geq 0$,*

$$\mu_t(m) = \min\{e(P_t(R)) : |R|_t = (p^t - 1)m\}.$$

Proof. There is a $1 - 1$ correspondence between Milnor basis elements $P_t(R)$ satisfying $|R|_t = (p^t - 1)m$ and t -representations of m given by

$$P_t(R) \longleftrightarrow m = \sum_i r_i \gamma_t(i).$$

Under this correspondence, $e(P_t(R))$ corresponds to the number $\sum_i r_i$ which is used in determining $\mu_t(m)$. The lemma follows immediately from this observation. $\square$

Thus we have following lemma which is analogous to Davis' formula [6, Theorem 1].

Lemma 10. *For all $m \geq 0$ and $t \geq 1$,*

$$\widehat{P}_t((p-1)p^{t-1}\gamma_t(m)) = (X_t)_{t-1}^{mt-1}.$$

Proof. We will prove it by induction on m . If $m = 1$ then the result holds since $P_t(p^{t-1}(p-1))$ is the only $P_t(R)$ in this dimension. Assume that the result holds for $m-1$. By (8),

$$\begin{aligned} (X_t)_{t-1}^{mt-1} &= P_t((p-1)p^{mt-1}) \cdot (X_t)_{t-1}^{(m-1)t-1} \\ &= P_t((p-1)p^{mt-1}) \cdot \widehat{P}_t((p-1)p^{t-1}\gamma_t(m-1)) \\ &= \sum_R \binom{|R|_t + e(R)}{(p-1)p^{(m+1)t-1}} P_t(R) \end{aligned}$$

where the sum is over all R such that $|R|_t = \sum_i (p^{it} - 1)r_i = (p-1)p^{t-1}(p^{mt} - 1)$. By Lemma 9,

$$\mu_t((p-1)p^{t-1}\gamma_t(m)) \leq \sum_i r_i \leq (p-1)p^{t-1}\gamma_t(m).$$

By [8, Proposition 2], the t -representation of $(p-1)p^{t-1}\gamma_t(m)$ with $r_m = (p-1)p^{t-1}$ and all other $r_i = 0$ has minimal $\sum_i r_i$. Hence $\mu_t((p-1)p^{t-1}\gamma_t(m)) = (p-1)p^{t-1}$. So we have

$$(p-1)p^{t-1}(p^{mt} - 1) + (p-1)p^{t-1} \leq \sum_i p^{it}r_i \leq (p-1)p^{t-1}\gamma_t(m+1);$$

that is,

$$(p-1)p^{(m+1)t-1} \leq \sum_i p^{it}r_i \leq (p-1)p^{t-1}\gamma_t(m+1).$$

Hence $(\sum_i p^{it}r_i)_{(p-1)p^{(m+1)t-1}} \equiv 1 \pmod{p}$. By [8, Proposition 1],

$$(11) \quad \hat{P}_t((p-1)p^{t-1}\gamma_t(m)) = \sum_R P_t(R)$$

where the sum is taken over all R such that $|R|_t = (p-1)p^{t-1}(p^{mt} - 1)$. Therefore we have $(X_t)_{t-1}^{mt-1} = \hat{P}_t((p-1)p^{t-1}\gamma_t(m))$. $\square$

The following lemma is analogous to [19, Lemma 1.4].

Lemma 11. (i) For $s \geq 0$ and $t \geq 1$ let κ_t^s denote the operation of stripping by P_t^s . Then

$$\kappa_t^s(\hat{P}_t(k)) = \hat{P}_t(k - p^s)$$

where $\hat{P}_t(k - p^s) = 0$ for $k < p^s$.

(ii) Let Θ be an element in B_t which gives zero when stripped by P_t^s , and assume $\Theta \cdot \hat{P}_t(ip^s) \cdot (P_t^s)^m = 0$. Then $\Theta \cdot \hat{P}_t((i-1)p^s) \cdot (P_t^s)^{m+1} = 0$.

Proof. (i) We will prove it by induction on k . Note that $\sum_{n \in \mathbb{Z}} P_t(n) \cdot \chi(P_t(k-n)) = 0$. Hence we have

$$(12) \quad \sum_{n \in \mathbb{Z}} (-1)^{k-n} P_t(n) \cdot \hat{P}_t(k-n) = 0$$

with the convention that $P_t(i) = 0$ and $\hat{P}_t(i) = 0$ if $i < 0$. Applying the derivation κ_t^s to (12), we have

$$\kappa_t^s(\hat{P}_t(k)) + \sum_{n>0} (-1)^n \{ \kappa_t^s(P_t(n)) \cdot \hat{P}_t(k-n) + P_t(n) \cdot \kappa_t^s(\hat{P}_t(k-n)) \} = 0.$$

By the induction hypothesis, we obtain

$$\begin{aligned} \kappa_t^s(\hat{P}_t(k)) + \sum_{n \neq 0} (-1)^n P_t(n - p^s) \cdot \hat{P}_t(k-n) \\ + \sum_{m \neq p^s} (-1)^{m-p^s} P_t(m - p^s) \cdot \hat{P}_t(k-m) = 0. \end{aligned}$$

All terms cancel except the term with $n = p^s$ in the first sum. Hence

$$\kappa_t^s(\hat{P}_t(k)) = \hat{P}_t(k - p^s).$$

This completes the induction.

(ii) If $\Theta \cdot \widehat{P}_t(ip^s) \cdot (P_t^s)^m = 0$ then

$$\kappa_t^s(\Theta) \cdot \widehat{P}_t(ip^s) \cdot (P_t^s)^m + \Theta \cdot \kappa_t^s(\widehat{P}_t(ip^s)) \cdot (P_t^s)^m + \Theta \cdot \widehat{P}_t(ip^s) \cdot \kappa_t^s(P_t^s)^m = 0.$$

By part (i),

$$\Theta \cdot \widehat{P}_t((i-1)p^s) \cdot (P_t^s)^m + m\Theta \cdot \widehat{P}_t(ip^s) \cdot (P_t^s)^{m-1} = 0.$$

So

$$\Theta \cdot \widehat{P}_t((i-1)p^s) \cdot (P_t^s)^{m+1} = -m\Theta \cdot \widehat{P}_t(ip^s) \cdot (P_t^s)^m = 0.$$

□

Let E be the exterior subalgebra of A generated by $\{P_t^0 | t \geq 1\}$. There is an algebra isomorphism between A and $A//E$. This isomorphism $F : A \longrightarrow A//E$ is given by

$$F(P(t_1, t_2, t_3 \dots)) = [P(pt_1, pt_2, pt_3 \dots)]$$

where $[x]$ is equivalence class in $A//E$ of $x \in A$ (see [11, Chapter 15]). Let $(P_t^s)^n = 0$. Then $[0] = [P_t^s]^n = F((P_t^{s-1})^n)$. Since F is an algebra isomorphism, $(P_t^{s-1})^n = 0$. So by iterating we see that if $(P_t^s)^n = 0$ then $(P_t^i)^n = 0$ for all $i \leq s$. This proves the following lemma.

Lemma 12. *Let $t > 1$.*

- (i) *If Theorem 1(i) holds for all $s \equiv -1 \pmod{t}$, then it holds for all s .*
- (ii) *If Theorem 1(ii) holds for all $s \equiv 0 \pmod{t}$, then it holds for all s .*

2. THE PROOF OF THE MAIN RESULT

The proof of Theorem 1(i) now follows by imitating the proof of [14] for the case $p = 2$. We proceed by proving the following two equations by induction on k for $1 \leq k \leq m$:

$$(13) \quad \chi((X_t)_{kt-1}^{mt-1}) \cdot (P_t^{mt-1})^{p(k-1)+1} = 0,$$

$$(14) \quad \chi((X_t)_{kt-1}^{(m-1)t-1}) \cdot (P_t^{mt-1})^{pk} = 0.$$

If $k = 1$ then

$$\chi((X_t)_{t-1}^{mt-1}) \cdot P_t^{mt-1} = P_t((p-1)p^{t-1}\gamma_t(m)) \cdot P_t^{mt-1} = 0$$

by Lemma 10 and Proposition 3.

Next we show that equation (13) for k implies equation (14) for k . The assumption says that

$$\chi((X_t)_{kt-1}^{(m-1)t-1})\chi(P_t(p^{mt-1}(p-1))) (P_t^{mt-1})^{p(k-1)+1} = 0.$$

On applying Lemma 11 $(p-1)$ times with $\Theta = \chi((X_t)_{kt-1}^{(m-1)t-1})$, we obtain

$$\chi((X_t)_{kt-1}^{(m-1)t-1}) \cdot (P_t^{mt-1})^{pk} = 0,$$

as desired.

Now we show that equation (14) for k implies equation (13) for $k+1$. Indeed we have the following equations with $z = p^{mt} - p^{kt-1}(p-1)$. At the second step we

use Corollary 7 with $a = mt - 1$, $b = 1$, and $c = kt - 1$. The induction hypothesis is used at the third step. This gives us

$$\begin{aligned}\chi((X_t)_{(k+1)t-1}^{mt-1}) \cdot (P_t^{mt-1})^{pk+1} &= \chi((X_t)_{kt-1+t}^{mt-1}) \cdot (P_t^{mt-1}) \cdot (P_t^{mt-1})^{pk} \\ &= P_t(z) \cdot \chi((X_t)_{kt-1}^{mt-1-t}) \cdot (P_t^{mt-1})^{pk} \\ &= P_t(z) \cdot 0 = 0.\end{aligned}$$

Thus by induction on k we see that both equations (13) and (14) hold for $1 \leq k \leq m$. Equation (14) for $k = m$ proves the theorem for all $s \equiv -1 \pmod{t}$. By Lemma 12(i) this proves Theorem 1(i). $\square$

Proof of Theorem 1(ii). We follow the method of Davis, using properties of the coproduct ϕ in A to find elements $\xi^{R_{m,t}(i)}$ in the dual algebra A^* for $i < pm$ such that

$$(15) \quad \langle (P_t^{(m-1)t})^i, \xi^{R_{m,t}(i)} \rangle \neq 0.$$

If $i = kp + w$ with $0 \leq k \leq m-1$ and $0 \leq w \leq p-1$, then let

$$(16) \quad \xi^{R_{m,t}(i)} = \xi_t^{r_1(i)} \xi_{2t}^{r_2(i)} \cdots \xi_{(k+1)t}^{r_{k+1}(i)}$$

where $r_l(i) = a_l(i) + b_l(i)$, with

$$a_l(i) = \begin{cases} (w-p+1)p^{(m-1)t} & \text{if } l = 1, \\ 0 & \text{if } l > 1 \end{cases}$$

and

$$b_l(i) = \begin{cases} (p-1)p^{(m-k-1)t} & \text{if } l = k+1, \\ (p^{t+1} - p + 1)p^{(m-k-1)t} & \text{if } l = k, \\ (p^t - 1)p^{(m-l-1)t+1} & \text{if } 1 \leq l < k. \end{cases}$$

For example,

1. for $k = 0$, $R_{m,t}(i) = (wp^{(m-1)t})$,
2. for $k = 1$, $R_{m,t}(i) = ((w+1)p^{(m-1)t} - (p-1)p^{(m-2)t}, (p-1)p^{(m-2)t})$,
3. for $k = 2$, $R_{m,t}(i) = ((w+1)p^{(m-1)t} - p^{(m-2)t+1}, p^{(m-2)t+1} - (p-1)p^{(m-3)t}, (p-1)p^{(m-3)t})$,
4. for $k = 3$, $R_{m,t}(i) = ((w+1)p^{(m-1)t} - p^{(m-2)t+1}, (p^t - 1)p^{(m-3)t+1}, p^{(m-3)t+1} - (p-1)p^{(m-4)t}, (p-1)p^{(m-4)t})$.

The proof of (15) depends on the following calculation.

Lemma 13.

$$\phi(\xi^{R_{m,t}(i)}) = (z\xi^{R_{m,t}(i-1)} + \xi') \otimes \xi_t^{p^{(m-1)t}} + \sum_j a_j \otimes b_j$$

where $b_j \neq \xi_t^{p^{(m-1)t}}$ for all j , ξ' is divisible by $\xi_t^{p^{(m-1)t+1}}$, and $z = w$ if $w > 0$, $z = 1$ if $w = 0$.

This implies (15), since it follows by induction on i that

$$\langle (P_t^{(m-1)t})^i, \xi^{R_{m,t}(i)} \rangle = \langle (P_t^{(m-1)t})^{i-1}, w\xi^{R_{m,t}(i-1)} \rangle \langle P_t^{(m-1)t}, \xi_t^{p^{(m-1)t}} \rangle \neq 0,$$

since the evaluation of ξ' on all elements of the subalgebra $A(mt-1)$ is zero. By Lemma 12(ii), this implies Theorem 1(ii).

Proof of Lemma 13. Let $R_{m,t}(i)$ be as in (16) above. Since we are only interested in terms of the form $A \otimes \xi_t^{p^{(m-1)t}}$, we will work mod terms involving ξ_{jt} for $j \leq 1$ in the second factor. So we have

$$(17) \quad \phi(\xi^{R_{m,t}(i)}) = \phi\left(\prod_{l=1}^{k+1} \xi_{lt}^{r_l(i)}\right) = \prod_{l=1}^{k+1} \phi(\xi_{lt}^{r_l(i)}) \equiv \prod_{l=1}^{k+1} (\xi_{lt} \otimes 1 + \xi_{(l-1)t}^{p^t} \otimes \xi_t)^{r_l(i)}.$$

Note that

$$\sum_{l=1}^{k+1} r_l(i) = (w+1)p^{(m-1)t}.$$

We only want terms of the form $A \otimes \xi_t^{p^{(m-1)t}}$. When $w = 0$, the only such term is obtained from the product $\prod_{l=1}^{k+1} (\xi_{(l-1)t}^{p^t} \otimes \xi_t)^{r_l(i)}$, and hence

$$A = \prod_{l=1}^{k+1} \xi_{(l-1)t}^{p^t r_l(i)} = \prod_{l=1}^k \xi_{lt}^{p^t b_{l+1}(i)} = \prod_{l=1}^k \xi_{lt}^{b_l(i-1)} = \xi^{R_{m,t}(i-1)}$$

since $i-1 = (k-1)p + p-1$. Suppose $w > 0$. The l -th factor of (17) can be written as

$$\begin{cases} (\xi_{(k+1)t}^{p^{(m-k-1)t}} \otimes 1 + \xi_{kt}^{p^{(m-k)t}} \otimes \xi_t^{p^{(m-k-1)t}})^{p-1} & \text{if } l = k+1, \\ (\xi_{kt}^{p^{(m-k-1)t}} \otimes 1 + \xi_{(k-1)t}^{p^{(m-k)t}} \otimes \xi_t^{p^{(m-k-1)t}})^{p^{t+1}-p+1} & \text{if } l = k, \\ (\xi_{lt}^{p^{(m-l-1)t+1}} \otimes 1 + \xi_{(l-1)t}^{p^{(m-l)t+1}} \otimes \xi_t^{p^{(m-l-1)t+1}})^{p^t-1} & \text{if } 1 < l < k, \\ (\xi_t^{p^{(m-2)t+1}} \otimes 1 + 1 \otimes \xi_t^{p^{(m-2)t+1}})^{(w+1)p^{t-1}-1} & \text{if } l = 1, 1 < k, \\ (\xi_t^{p^{(m-2)t}} \otimes 1 + 1 \otimes \xi_t^{p^{(m-2)t}})^{(w+1)p^t-p+1} & \text{if } l = 1, k = 1. \end{cases}$$

We expand each of these factors, and if we choose for each l the term with the j_l -th power of the second term, then we must have ($k \geq 2$)

$$(18) \quad j_1 p^{(m-2)t+1} + \sum_{l=2}^{k-1} j_l p^{(m-l-1)t+1} + j_k p^{(m-k-1)t} + j_{k+1} p^{(m-k-1)t} = p^{(m-1)t}$$

and $(\frac{(w+1)p^{t-1}-1}{j_1})$ is a unit, $0 \leq j_l \leq p^t - 1$ for $2 \leq l \leq k-1$, $(\frac{p^{t+1}-p+1}{j_k})$ is a unit, and $0 \leq j_{k+1} \leq p-1$.

To satisfy (18) we must have $j_{k+1} + j_k \equiv 0 \pmod{p^{t+1}}$. Since $(\frac{p^{t+1}-p+1}{j_k})$ is a unit, either $j_k \equiv 0 \pmod{p}$ or $j_k \equiv 1 \pmod{p}$. Therefore either $j_{k+1} = 0$ or $p-1$ since $j_{k+1} \leq p-1$.

If $j_{k+1} = 0$, then $j_k = 0$. So we have the following equation:

$$(19) \quad j_1 p^{(m-2)t+1} + \sum_{l=2}^{k-1} j_l p^{(m-l-1)t+1} = p^{(m-1)t}.$$

j_{k-1} is multiple of p^t because $j_{k-1} p^{(m-k)t+1} \equiv 0 \pmod{p^{(m-k+1)t+1}}$. Therefore $j_{k-1} = 0$ since $j_{k-1} \leq p^t - 1$. By a similar argument, $j_{k-2} = j_{k-3} = \dots = j_2 = 0$. So we have $j_1 p^{(m-2)t+1} = p^{(m-1)t}$, which implies $j_1 = p^{t-1}$. Therefore we obtain a

term of the form $A \otimes \xi_t^{p^{(m-1)t}}$ with $A = A_1 A_2 \cdots A_k A_{k+1}$, where

$$\begin{aligned} A_1 &= w \xi_t^{wp^{(m-1)t} - p^{(m-2)t+1}} \\ A_2 &= \xi_{2t}^{(p^t-1)p^{(m-3)t+1}} \\ &\dots \\ A_{k-1} &= \xi_{(k-1)t}^{(p^t-1)p^{(m-k)t+1}} \\ A_k &= \xi_{kt}^{(p^{t+1}-p+1)p^{(m-k-1)t}} \\ A_{k+1} &= \xi_{(k+1)t}^{(p-1)p^{(m-k-1)t}}. \end{aligned}$$

Hence $A = \xi^{R_{m,t}(i-1)}$.

If $j_{k+1} = p - 1$, then we have $j_k = p^{t+1} - p + 1$. From (18),

$$j_1 p^{(m-2)t+1} + \sum_{l=2}^{k-2} j_l p^{(m-l-1)t+1} + j_{k-1} p^{(m-k)t+1} + p^{(m-k)t+1} = p^{(m-1)t}.$$

So $j_{k-1} \equiv -1 \pmod{p^t}$. Hence $j_{k-1} = p^t - 1$, since $j_{k-1} \leq p^t - 1$. By a similar argument, $j_{k-2} = j_{k-3} = \cdots = j_2 = p^t - 1$. If we put these j_l in the equation (18) for $2 \leq l \leq k-2$, we will have $(j_1 + 1)p^{(m-2)t+1} = p^{(m-1)t}$. This implies that $j_1 = p^{t-1} - 1$. Therefore we obtain the other term of the form $B \otimes \xi_t^{p^{(m-1)t}}$ with $B = B_1 \cdot B_2 \cdots B_{k+1}$, where

$$\begin{aligned} B_1 &= \xi_t^{wp^{(m-1)t}} \\ B_2 &= \xi_t^{(p^t-1)p^{(m-2)t+1}} \\ &\dots \\ B_{k-1} &= \xi_{(k-2)t}^{(p^t-1)p^{(m-k+1)t+1}} \\ B_k &= \xi_{(k-1)t}^{(p^{t+1}-p+1)p^{(m-k)t}} \\ B_{k+1} &= \xi_{kt}^{(p-1)p^{(m-k)t}}. \end{aligned}$$

So we have

$$\phi(\xi^{R_{m,t}(i)}) = (A + B) \otimes \xi_t^{p^{(m-1)t}}$$

where $A = w \xi^{R_{m,t}(i-1)}$ and $B = \xi'$ is divisible by $\xi_t^{p^{(m-1)t+1}}$, as claimed. $\square$

REFERENCES

- [1] J.F. Adams and H.R. Margolis, *Modules Over the Steenrod Algebra*, Topology **10** (1971), 271–282. MR **45**:3520
- [2] J.F. Adams and H.R. Margolis, *Sub-Hopf-Algebra of the Steenrod Algebra*, Proc. Camb. Phil. Soc. **76** (1974), 45–52. MR **49**:6238
- [3] D.W. Anderson and D.M. Davis, *A Vanishing Theorem in Homological Algebra*, Comment. Math. Helvet. **48** (1973), 318–327. MR **48**:12526
- [4] D. Arnon, *Monomial Bases in the Steenrod Algebra*, J. Pure and Applied Algebra **96** (1994), 215–223. MR **95i**:55015
- [5] D.P. Carlisle and R.M.W. Wood, *On an Ideal Conjecture in the Steenrod Algebra*, preprint (1994).
- [6] D.M. Davis, *The Antiautomorphism of the Steenrod Algebra*, Proc. Amer. Math. Soc. **44** (1974), 235–236. MR **48**:7276

- [7] D.M. Davis, *On the height of Sq^{2^n}* , preprint (1985).
- [8] A.M. Gallant, *Excess and Conjugation in the Steenrod Algebra*, Proc. Amer. Math. Soc. **76** (1979), 161–166. MR **81a**:55029
- [9] B. Gray, *Homotopy Theory*, Academic Press (1975). MR **53**:6528
- [10] L. Kristensen, *On a Cartan Formula for Secondary Cohomology Operations*, Math. Scand. **16** (1965), 97–115. MR **33**:4926
- [11] H.R. Margolis, *Spectra and the Steenrod Algebra*, vol 29 North Holland Math.Library (1983). MR **86j**:55001
- [12] J. Milnor, *The Steenrod Algebra and Its Dual*, Ann. of Math. **67** (1958), 150–171. MR **20**:6092
- [13] K.G. Monks, *Nilpotence in the Steenrod Algebra*, Bol.Soc.Mat.Mexicana **37** (1992), 401–416. MR **95j**:55032
- [14] K.G. Monks, *The Nilpotence Height of P_t^s* , Proc. Amer. Math. Soc. **124** (1966), 1297–1303. MR **96g**:55023
- [15] J.H. Silverman, *Conjugation and Excess in the Steenrod Algebra*, Proc. Amer. Math. Soc. **119** (1993), 657–661. MR **93k**:55020
- [16] J.H. Silverman, *Hit Monomials and the Canonical Antiautomorphism of the Steenrod Algebra*, Proc. Amer. Math. Soc. **123** (1995), 627–637. MR **95c**:55023
- [17] P. D. Straffin, Jr., *Identities for Conjugation in the Steenrod Algebra*, Proc. Amer. Math. Soc. **49** (1975), 253–255. MR **52**:1693
- [18] G.Walker and R.M.W. Wood, *The Nilpotence Height of Sq^{2^n}* , Proc. Amer. Math. Soc. **124** (1966), 1291–1295. MR **96g**:55024
- [19] G.Walker and R.M.W. Wood, *The Nilpotence Height of P^{p^n}* , preprint (1995).
- [20] R.M.W. Wood, *A Note on Bases and Relations in the Steenrod Algebra*, Bull. London Math. Soc. **27** (1995), 380–386. MR **96e**:55013
- [21] R.M.W. Wood, *Differential Operators and the Steenrod Algebra*, preprint (1995).

DEPARTMENT OF MATHEMATICS, LEHIGH UNIVERSITY, BETHLEHEM, PENNSYLVANIA 18015
Current address: Department of Mathematics, Ege University, Bornova, Izmir 35100, Turkey
E-mail address: karaca@fenfak.ege.edu.tr