Homology, Homotopy and Applications, vol.2, No.1, 2000, pp.1–16 ISSN 1512–0139

STRIPPING AND CONJUGATION IN THE MOD p STEENROD ALGEBRA AND ITS DUAL

DAGMAR M. MEYER

(*communicated by Hvedri Inassaridze*)

Abstract

Let p be an odd prime and $\mathcal{A}^*$ the mod p Steenrod algebra. We study the technique known as "stripping" applied to $\mathcal{A}^*$ and derive certain conjugation formulas both for $\mathcal{A}^*$ and its dual, generalising work of J. H. Silverman for $p = 2$ ("Conjugation and excess in the Steenrod algebra", *Proc. Am. Math. Soc.* **119** (1993), no.2, 657 – 661; "Hit polynomials and conjugation in the dual Steenrod algebra", *Math. Proc. Camb. Philos. Soc.* **123** (1998), no.3, 531 – 547) to the case of an odd prime.

1. Introduction and statement of results

In this note we study the technique known as "stripping" applied to the mod p Steenrod algebra $\mathcal{A}^*$, where p is an *odd* prime, and use the results obtained to prove certain conjugation formulas both in $\mathcal{A}^*$ and its dual. This generalises work of Judith Silverman carried out in [**S1**] and [**S3**] for $p = 2$ to the case of an odd prime. More precisely, our results concern Steenrod operations which lie in the sub-Hopf algebra $\mathcal{P}^*$ of $\mathcal{A}^*$ which is generated by the reduced power operations $\mathrm{P}(i)$, $i \geqslant 1$, in dimensions $|\mathrm{P}(i)| = 2i(p-1)$. We use the convention $\mathrm{P}(0) := 1$.

Of particular interest are the Steenrod operations in $\mathcal{P}^*$ which are of the form

$$\mathrm{P}[k; f] := \mathrm{P}(p^{k-1}f) \cdot \mathrm{P}(p^{k-2}f) \cdot \ldots \cdot \mathrm{P}(pf) \cdot \mathrm{P}(f)$$

where $k \geqslant 1$ and $f \geqslant 0$. Note that $\mathrm{P}[1; f]$ is just $\mathrm{P}(f)$. Being a sub-Hopf algebra, $\mathcal{P}^*$ inherits the canonical anti-automorphism χ of $\mathcal{A}^*$; following notation introduced in [**WW**], we write $\hat{\theta}$ instead of $\chi(\theta)$. In particular, $\hat{\mathrm{P}}(a) = \chi(\mathrm{P}(a))$ and $\hat{\mathrm{P}}[k; f] = \chi(\mathrm{P}[k; f])$.

For $m \geqslant 0$ we define

$$\gamma(m) := \sum_{i=0}^{m-1} p^i.$$

Our first main result is an explicit conjugation formula for $\mathrm{P}[k; f]$ in certain special cases. It generalises Thm. 3.1 in [**S1**] to odd primes:

Theorem 4.6 *For all positive integers s, t and c with $1 \leqslant c \leqslant p$ the following conjugation formula holds:*

$$\hat{\mathrm{P}}[s; c\gamma(t)] = (-1)^{stc}\mathrm{P}[t; c\gamma(s)]$$

The main result concerning conjugation in the dual $\mathcal{P}_*$ is a conjugation formula for certain elements $\mathcal{X}_I(k)$, which are defined in Section 5. This formula is the mod p analogue of

---

During the preparation of this article the author was supported by a "bourse post-doctorale Alfred Kastler" of the French Ministry of Foreign Affairs.
Received 11 October 1999; published on 24 January 2000.
1991 Mathematics Subject Classification: 55S10
Key words and phrases: stripping, conjugation, Steenrod algebra, antiautomorphism

Prop. 5.5 in [**S3**]. A special case states that modulo monomials of length strictly greater than k the operations $\hat{\xi}_i^{\gamma(k)}$ and $(-1)^{ik}\xi_k^{\gamma(i)}$ coincide up to a certain error term; the conjugate of the error term is a sum of monomials of length strictly greater than i:

Theorem 5.6 *Let $i, k > 0$. Modulo monomials of length $> k$ we have*

$$\hat{\xi}_i^{\gamma(k)} \equiv (-1)^{ik}\xi_k^{\gamma(i)} - \sum_{\mathrm{Id}_k \neq \tau \in \mathfrak{S}(k)} \operatorname{sign}(\tau) \prod_{j=0}^{k-1} \hat{\xi}_{i+\tau(j)-j}^{p^j}.$$

Here $\mathfrak{S}(k)$ denotes the symmetric group acting on $\{0, 1, 2, \ldots, k-1\}$ and $\hat{\xi}_r := 0$ for $r < 0$.

In particular, if $f < \gamma(k+1)$ is a non-negative integer then

$$\hat{\xi}_k^{\gamma(i)} \cap \mathrm{P}[i; f] = (-1)^{ik}\xi_i^{\gamma(k)} \cap \mathrm{P}[i; f] \;=\; (-1)^{ik}\mathrm{P}[i; f - \gamma(k)],$$

where we use the notation $y \cap \_$ for the stripping operation $D(y)$.

The ideas underlying the proofs of the results in this paper are similar to those of their mod 2 counterparts in [**S1**] and [**S3**]. However, getting down to the details we note two major differences that appear in the odd-primary case: first of all, in just about every formula we prove there are some signs involved, and secondly (in Section 4) we have to deal with mod p binomial coefficients which appear as non-trivial coefficients in our formulas. These difficulties cause the generalisation of the mod 2 results to be not quite as straightforward as it may seem at first glance.

Both Thm. 4.6 and Thm. 5.6 are essential ingredients for the work carried out in [**M**]. There the Steenrod operations $\hat{\mathrm{P}}[k; f]$ are studied further; in particular the excess of these operations is determined. In fact, that project was one of the main motivations for the work on the problems discussed in the present paper.

Acknowledgements: I would like to thank Judith Silverman for many helpful comments on the subject of this paper, in particular for supplying the elegant proof of Lemma 4.4 which is reproduced here. I also thank Ken Monks for pointing out to me the work of Ismet Karaca on related problems and for sending me copies of [**Ka2**], [**Ka3**].

2. Preliminaries

Let $\mathcal{S}$ denote the additive monoid of sequences of non-negative integers almost all of which are 0, with componentwise addition. We write $0_{\mathcal{S}}$ for the trivial element. Throughout we shall use capital letters to denote sequences in $\mathcal{S}$ and small letters for their coordinates; e.g. $S = (s_1, s_2, \ldots)$. If S has $s_i = 0$ for $i > L$, we write S as $(s_1, s_2, \ldots, s_L)$. The *degree* of an element $S \in \mathcal{S}$ is defined to be $|S| = \sum_{i \geqslant 1} s_i(p^i - 1)$, its *length* as $\operatorname{len}(S) = \min\{i \geqslant 0 \mid s_j = 0 \ \forall j > i\}$, and its *excess* as $\operatorname{ex}(S) = \sum_{i \geqslant 1} s_i$. It will be convenient to adjoin an extra element $*$ to $\mathcal{S}$ with the property that $* + x = x + * = *$ for all $x \in \mathcal{S} \cup \{*\} =: \mathcal{S}^*$. We also define sequences $B(j)$ for any $j \in \mathbb{Z}$: if $j \geqslant 0$ then $B(j)$ is the sequence with $b(j)_i := \delta_{ij}$, if $j < 0$ we set $B(j) := *$.

There are many interesting bases for $\mathcal{A}^*$ and hence for $\mathcal{P}^*$; the most important and most commonly used are the basis of admissible monomials ("admissible basis") and the Milnor basis. Recall that the monomial $\mathrm{P}(a_1) \cdot \ldots \cdot \mathrm{P}(a_n)$ with $a_n > 0$ is *admissible* if $a_r \geqslant pa_{r+1}$ for all $1 \leqslant r < n$; we also define $P(0) = 1$ to be admissible. The admissible basis of $\mathcal{P}^*$ can be parameterised in terms of the numbers $s_i = a_i - pa_{i+1}$; that is, given a sequence $S \in \mathcal{S}$ of length $n > 0$, we define the admissible element $E[S] := \mathrm{P}(a_1) \cdot \ldots \cdot \mathrm{P}(a_n)$ by setting $a_n = s_n$ and $a_i = pa_{i+1} + s_i$ for $1 \leqslant i \leqslant n-1$. We also set $E[0_{\mathcal{S}}] := P(0) = 1$. For example, if $S = (0, \ldots, 0, f)$ has length k then $E[S] = \mathrm{P}(p^{k-1}f) \cdot \ldots \cdot \mathrm{P}(f) = \mathrm{P}[k; f]$.

For the Milnor basis of $\mathcal{P}^*$ consider the dual Hopf algebra $\mathcal{P}_*$. This is a polynomial algebra over $\mathbb{F}_p$ on generators ξ_i $(i \geqslant 1)$ in dimension $2(p^i - 1)$; we use the convention $\xi_0 := 1$. For

$S \in \mathcal{S}$ we write $\xi[S]$ for the monomial $\prod_{i \geqslant 1} \xi_i^{s_i}$. In particular, $\xi[B_j] = \xi_j$ for any $j \geqslant 0$. The Milnor basis of $\mathcal{P}^*$ itself is the basis dual to the basis of $\mathcal{P}_*$ consisting of all the monomials $\xi[S]$ with $S \in \mathcal{S}$; the element dual to $\xi[S]$ will be denoted by $M[S]$.

We further set $M[*] = 0 = E[*]$ and $\xi[*] = 0$, and we adopt the convention that $M[S] = 0 = E[S]$ and $\xi[S] = 0$ if S is a finite sequence of integers which does *not* belong to $\mathcal{S}$, i.e. with at least one negative entry. In particular, $\xi_i := 0$ if $i < 0$.

For any $S \in \mathcal{S}$ we define length and excess of the monomial $\xi[S]$ as $\mathrm{len}(S)$ and $2\mathrm{ex}(S)$ respectively. Likewise, for the admissible and the Milnor basis we define

$$\mathrm{len}_E(E[S]) := \mathrm{len}(S) =: \mathrm{len}_M(M[S])\,,$$
$$\mathrm{ex}_E(E[S]) := 2\mathrm{ex}(S) =: \mathrm{ex}_M(M[S])\,.$$

More generally, suppose θ is any homogeneous element of $\mathcal{P}^*$ with a basis representation given by $\theta = \sum_{i=1}^n \alpha_i B[S_i]$, where B stands for either E or M. Then we set

$$\mathrm{len}_B(\theta) := \max_i\{\mathrm{len}_B(B[S_i])\} = \max_i\{\mathrm{len}(S_i)\}$$
$$\mathrm{ex}_B(\theta) := \min_i\{\mathrm{ex}_B(B[S_i])\} = 2\min_i\{\mathrm{ex}(S_i)\}\,.$$

The excess of any operation θ in $\mathcal{P}^*$ can also be defined as $\mathrm{ex}(\theta) := \min\{n \,|\, \theta(\iota_n) \neq 0 \in H^*(K(\mathbb{Z}/p,n);\mathbb{F}_p)\}$, where $\iota_n \in H^*(K(\mathbb{Z}/p,n);\mathbb{F}_p)$ is the fundamental class. In fact, all the different definitions of excess that we have given coincide (cf. [**Kr**]); in particular $\mathrm{ex}_E(\theta) = \mathrm{ex}(\theta) = \mathrm{ex}_M(\theta)$.

By [**Mi**], the change-of-basis matrix in each dimension between the admissible and the Milnor basis is upper triangular with diagonal entry ± 1, if for both bases we use the order induced by the right-lexicographical order on $\mathcal{S}$. From this it follows that for any $S \in \mathcal{S}$ we have $\mathrm{len}_E(M[S]) = \mathrm{len}_E(E[S]) = \mathrm{len}(S)$ and $\mathrm{len}_M(E[S]) = \mathrm{len}_M(M[S]) = \mathrm{len}(S)$, and one easily sees that this implies $\mathrm{len}_M(\theta) = \mathrm{len}_E(\theta)$ for any $\theta \in \mathcal{P}^*$. Henceforth we denote this common value simply by $\mathrm{len}(\theta)$.

3. Stripping in $\mathcal{P}^*$

3.1. Recollections about the stripping technique

Much recent progress on problems related to the structure of the Steenrod algebra has been made by applying a tool that has become known as "stripping technique" (for a detailed account see [**W**]). This technique applies to any Hopf algebra, so in particular to the cocommutative, connected Hopf algebra $\mathcal{P}^*$.

Let Δ^* denote the diagonal map of $\mathcal{P}^*$ and $\langle\,,\,\rangle$ the inner product. We consider the natural action of the dual Hopf algebra $\mathcal{P}_*$ on $\mathcal{P}^*$ which is given for each $\xi \in \mathcal{P}_*$ by

$$D(\xi) : \mathcal{P}^* \xrightarrow{\Delta^*} \mathcal{P}^* \otimes \mathcal{P}^* \xrightarrow{\mathrm{id}\otimes\langle \xi,\,\rangle} \mathcal{P}^*\,;$$

this action satisfies

$$\langle \xi \cdot \psi, \theta\,\rangle = \langle \psi, D(\xi)\theta\,\rangle \tag{1}$$

for all $\psi \in \mathcal{P}_*$, $\theta \in \mathcal{P}^*$. The operation $D(\xi) : \mathcal{P}^* \longrightarrow \mathcal{P}^*$ is called "stripping by ξ" and can be considered as a kind of cap-product. For this reason the notation

$$D(\xi)\theta =: \xi \cap \theta$$

has become customary.

For the reader's convenience we now recall some important properties of the stripping operation (cf. [**S2**]):

Let Δ_* denote the product of $\mathcal{P}_*$ and ϕ_* the comultiplication; the canonical anti-automorphism of $\mathcal{P}_*$ will again be denoted by χ, with $\chi(y) =: \hat{y}$. In what follows let $\phi_*(y) =: \sum y' \otimes y''$ and $\Delta^*(\theta) =: \sum \theta' \otimes \theta''$. We write $\mathcal{D}$ for the $\mathbb{F}_p$-vector space with basis $\{D(\xi[S]) \,|\, S \in \mathcal{S}\}$.

The maps $\chi : \mathcal{P}_* \longrightarrow \mathcal{P}_*$, $\Delta_* : \mathcal{P}_* \otimes \mathcal{P}_* \longrightarrow \mathcal{P}_*$ and $\phi_* : \mathcal{P}_* \longrightarrow \mathcal{P}_* \otimes \mathcal{P}_*$ induce maps

$$\begin{aligned} \chi : \mathcal{D} \longrightarrow \mathcal{D}, &\quad D(y) \mapsto D(\hat{y}) \\ \Delta_* : \mathcal{D} \otimes \mathcal{D} \longrightarrow \mathcal{D}, &\quad D(y_1) \otimes D(y_2) \mapsto D(y_1 \cdot y_2) \\ \phi_* : \mathcal{D} \longrightarrow \mathcal{D} \otimes \mathcal{D}, &\quad D(y) \mapsto \sum D(y') \otimes D(y''). \end{aligned}$$

Proposition 3.1. *The following formulas hold:*

1. $(y_1 + y_2) \cap \theta = y_1 \cap \theta + y_2 \cap \theta$
2. $(y_1 \cdot y_2) \cap \theta = (y_2 \cdot y_1) \cap \theta = y_1 \cap (y_2 \cap \theta) = y_2 \cap (y_1 \cap \theta)$
3. $y \cap (\theta_1 \cdot \theta_2) = \sum (y' \cap \theta_1) \cdot (y'' \cap \theta_2)$
4. $\hat{y} \cap (\theta_1 \cdot \theta_2) = \sum (\widehat{y''} \cap \theta_1) \cdot (\widehat{y'} \cap \theta_2)$
5. $\hat{y} \cap \hat{\theta} = \widehat{y \cap \theta}$

□

3.2. Stripping in the Milnor basis and in the admissible basis

The effect of stripping by an element $y \in \mathcal{P}_*$ on a Milnor basis element can easily be described by writing y as a sum of basis elements $\xi[R]$. In fact, recall that the comultiplication Δ^* of $\mathcal{P}^*$ is determined by the formula

$$\Delta^*\big(M[S]\big) = \sum_{S'+S''=S} M[S] \otimes M[S'']$$

([**Mi**]). From this and the definition of stripping one easily sees that

$$\xi[R] \cap M[S] = M[S-R].$$

In particular, stripping does not increase length.

Determining the effect of $D(\xi[R])$ on a given admissible monomial is more involved. More generally, let $\mathrm{P}(a_1) \cdots \mathrm{P}(a_n)$ be any (not necessarily admissible) monomial in $\mathcal{P}^*$. For $n \geqslant k$, we define $\mathcal{V}_{n,k}$ to be the set of all sequences $(v_1, \ldots, v_n)$ in which the non-zero elements form exactly the subsequence $(p^{k-1}, \ldots, p, 1)$. For example, $\mathcal{V}_{3,2}$ consists of $(0, p, 1)$, $(p, 0, 1)$, and $(p, 1, 0)$. For $n < k$, we define $\mathcal{V}_{n,k} := \emptyset$.

Proposition 3.2. *With this notation*

$$\xi_k \cap \big(\mathrm{P}(a_1) \cdot \ldots \cdot \mathrm{P}(a_n)\big) = \sum_{V \in \mathcal{V}_{n,k}} \mathrm{P}(a_1 - v_1) \cdot \ldots \cdot \mathrm{P}(a_n - v_n).$$

Proof. The proof is analogous to that of Prop. 3.1 in [**S3**]. Alternatively, see [**CWW**, Section 2]. □

We note the following consequences:

Corollary 3.3.

1. *If $\theta \in \mathcal{P}^*$ has length n, then $\xi[S] \cap \theta = 0$ for any $S \in \mathcal{S}$ of length greater than n; in particular $\xi_k \cap \theta = 0$ for any $k > n$.*
2. *If $\mathrm{P}(a_1) \cdot \ldots \cdot \mathrm{P}(a_k)$ is admissible of excess $2e$, then*
$$\xi_k \cap \big(\mathrm{P}(a_1) \cdot \ldots \cdot \mathrm{P}(a_k)\big) = \mathrm{P}(a_1 - p^{k-1}) \cdot \mathrm{P}(a_2 - p^{k-2}) \cdot \ldots \cdot \mathrm{P}(a_k - 1),$$
which is again admissible and has excess $2e - 2$. Consequently, if $R = (r_1, \ldots, r_k) \in \mathcal{S}$, then $\xi_k \cap E[R] = E[(r_1, \ldots, r_{k-1}, r_k - 1)]$.
3. *In particular,*
$$\xi_k \cap \mathrm{P}[k; f] = \mathrm{P}[k; f-1] \quad \text{and} \quad \hat{\xi}_k \cap \hat{\mathrm{P}}[k; f] = \hat{\mathrm{P}}[k; f-1],$$

where the second equation follows from Prop. 3.1(5).

□

The next thing we determine is the action of $D(\widehat{\xi[R]})$ on a given element $\theta \in \mathcal{P}^*$. By [**Mi**], conjugation in $\mathcal{P}_*$ is determined by

$$\hat{\xi}_k = \sum_{\alpha \in \mathrm{Part}(k)} (-1)^{l(\alpha)} \prod_{i=1}^{l(\alpha)} \xi_{\alpha_i}^{p^{\sigma_i(\alpha)}} \tag{2}$$

where α runs through all ordered partitions $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_{l(\alpha)})$ of k, $l(\alpha)$ is the length of the partition α, and $\sigma_i(\alpha)$ is the partial sum $\sum_{j=1}^{i-1} \alpha_j$.

Consequences 3.4. *1. The excess of $\xi_k = \xi[B_k]$ is 2 for any k, so the summand with the largest excess in formula (2) is the monomial corresponding to the partition α of length $l(\alpha) = k$ with $\alpha_i = 1$ for $1 \leqslant i \leqslant k$, i.e. the summand*

$$(-1)^k \prod_{i=1}^{k} \xi_1^{p^{i-1}} = (-1)^k \xi_1^{\gamma(k)}$$

which has excess $2\gamma(k)$. Hence stripping by $\hat{\xi}_k$ reduces excess by no more than $2\gamma(k)$.

2. Since $\xi_l \cap \mathrm{P}(f) = 0$ for all $l > 1$, we have

$$\begin{aligned} \hat{\xi}_k \cap \mathrm{P}(f) &= (-1)^k \xi_1^{\gamma(k)} \cap \mathrm{P}(f) \\ &= \begin{cases} (-1)^k \mathrm{P}(f - \gamma(k)) & \textit{if } f \geqslant \gamma(k) \\ 0 & \textit{otherwise.} \end{cases} \end{aligned}$$

3.3. Stripping $\mathrm{P}[\Lambda; f]$ by $\hat{\xi}_k^j$

We will be mostly concerned with the special Steenrod operations $\mathrm{P}[\Lambda; f]$. Therefore we take a closer look at the action of the stripping operations $D(\hat{\xi}_k^j)$ on these elements.

Lemma 3.5. *For any θ in $\mathcal{P}^*$ we have*

$$\hat{\xi}_k \cap \left(\mathrm{P}[2; f] \cdot \theta\right) = \mathrm{P}(pf) \cdot \left(\hat{\xi}_k \cap \left(\mathrm{P}(f) \cdot \theta\right)\right).$$

Proof. The proof is analogous to the proof of Lemma 4.4 in [**S2**]: recall that the comultiplication in $\mathcal{P}_*$ is given by

$$\phi_*(\xi_k) = \sum_{j=0}^{k} \xi_{k-j}^{p^j} \otimes \xi_j \tag{3}$$

([**Mi**]). Hence by Prop. 3.1(3) we obtain

$$\hat{\xi}_k \cap (\mathrm{P}[2; f] \cdot \theta) = \mathrm{P}(pf) \cdot \left(\hat{\xi}_k \cap (\mathrm{P}(f) \cdot \theta)\right) + \sum_{j=1}^{k} \left(\hat{\xi}_j \cap \mathrm{P}(pf)\right) \cdot \left(\hat{\xi}_{k-j}^{p^j} \cap (\mathrm{P}(f) \cdot \theta)\right).$$

Cons. 3.4(2) implies that $\hat{\xi}_j \cap \mathrm{P}(pf) = -\hat{\xi}_{j-1}^p \cap \mathrm{P}(pf - 1)$, thus

$$\begin{aligned} &\sum_{j=1}^{k} \left(\hat{\xi}_j \cap \mathrm{P}(pf)\right) \cdot \left(\hat{\xi}_{k-j}^{p^j} \cap (\mathrm{P}(f) \cdot \theta)\right) \\ &\qquad = -\sum_{j=1}^{k} \left(\hat{\xi}_{j-1}^p \cap \mathrm{P}(pf - 1)\right) \cdot \left((\hat{\xi}_{(k-1)-(j-1)}^p)^{p^{j-1}} \cap (\mathrm{P}(f) \cdot \theta)\right) \\ &\qquad = -\hat{\xi}_{k-1}^p \cap \left(\mathrm{P}(pf - 1) \cdot \mathrm{P}(f) \cdot \theta\right). \end{aligned}$$

But by the Adem relations $\mathrm{P}(pf-1)\cdot\mathrm{P}(f)=0$, which proves the claim. □

The following more general result is now easily proved by induction on Λ, the case $\Lambda=2$ being given by Lemma 3.5:

Proposition 3.6. *For $\Lambda \geqslant 2$ and any θ in $\mathcal{P}^*$ we have*

$$\hat{\xi}_k \cap \left(\mathrm{P}[\Lambda; f]\cdot\theta\right) = \mathrm{P}[\Lambda-1; pf]\cdot\left(\hat{\xi}_k \cap (\mathrm{P}(f)\cdot\theta)\right).$$

□

Finally, we investigate what happens if we strip $\mathrm{P}[\Lambda; f]$ by $\hat{\xi}_k$ a total of j times. We note that only the right-most j places are affected:

Proposition 3.7. *Suppose $\Lambda > j \geqslant 1$. Then*

$$\hat{\xi}_k^j \cap \mathrm{P}[\Lambda; f] = \mathrm{P}[\Lambda-j; p^j f]\cdot(\hat{\xi}_k^j \cap \mathrm{P}[j; f]).$$

Proof. The proof is by induction on j, starting with $j=1$ where the result is provided by Prop. 3.6. □

4. Conjugation formulas for $\mathcal{P}^*$

In this section we establish some useful formulas involving conjugation of elements in $\mathcal{P}^*$. In particular, we determine the simple formula for $\hat{\mathrm{P}}[s; c\gamma(t)]$ with $1 \leqslant c \leqslant p$ that was announced in the introduction.

Suppose that y is a non-negative integer. We use the notation $\alpha_i(y)$ for the coefficient of p^i in the p-adic expansion of y, i.e. $y =: \sum_{i\geqslant 0}\alpha_i(y)p^i$.

The following lemma will be needed for the proof of Prop. 4.3.

Lemma 4.1. *Suppose that k, l, c, m and e are non-negative integers with*

1. $k > l$,
2. $1 \leqslant c \leqslant p-1$,
3. $m < p^{k-1}$,
4. $m \equiv 0 \mod p^l$.

Then the following relation mod p holds:

$$\binom{c(p^k-p^l)+e}{pm} \equiv -\sum_{i=1}^{c}\binom{c}{i}\binom{c(p^k-p^l)+e}{pm+ip^l} + \binom{e}{pm+cp^l} \tag{4}$$

Proof. The proof relies on the fact that mod p we have the relation $\binom{x}{y} \equiv \prod_{i\geqslant 0}\binom{\alpha_i(x)}{\alpha_i(y)}$. There are three cases: (I) $\alpha_l(e)=c$, (II) $0 \leqslant \alpha_l(e) \leqslant c-1$, and (III) $c+1 \leqslant \alpha_l(e) \leqslant p-1$. If we are in case (I) then the first term on the right of (4) is 0 and

$$\binom{c(p^k-p^l)+e}{pm} \equiv \binom{e}{pm+cp^l}$$

as required.

If we are in case (II) then the second term on the right of (4) is zero and so we have to show that

$$\binom{c(p^k-p^l)+e}{pm} \equiv -\sum_{i=1}^{c}\binom{c}{i}\binom{c(p^k-p^l)+e}{pm+ip^l},$$

i.e. that

$$1 \equiv -\sum_{i=1}^{c} \binom{c}{i} \binom{p-c+\alpha_l(e)}{i}$$

for $0 \leqslant \alpha_l(e) \leqslant c-1$. Setting $a := p-c+\alpha_l(e)$ this amounts to showing that

$$\sum_{i=0}^{c} \binom{c}{i} \binom{a}{i} \equiv 0$$

for all $p-c \leqslant a \leqslant p-1$. In order to show this equivalence, note that

$$\sum_{i=0}^{c} \binom{c}{i} \binom{a}{i} \equiv \sum_{i=0}^{c} \binom{c}{i} \binom{a}{a-i} \equiv \binom{c+a}{c} \tag{5}$$

as one sees by considering the coefficient of x^c in the binomial expansion of $(x+1)^{c+a} = (x+1)^c(x+1)^a$. Now the claim follows since $\binom{c+a}{c} \equiv 0$ for $p-c \leqslant a \leqslant p-1$.

Case (III) is similar. □

We will need the following multiplication formulas:

Lemma 4.2. *Let u and v be non-negative integers. Then*

$$\mathrm{P}(u) \cdot \hat{\mathrm{P}}(v) = (-1)^v \sum_R \binom{|R| + \mathrm{ex}(R)}{pu}_p M[R] \tag{6}$$

and

$$\hat{\mathrm{P}}(u) \cdot \mathrm{P}(v) = (-1)^u \sum_R \binom{\mathrm{ex}(R)}{v}_p M[R] \tag{7}$$

where the sum ranges over all sequences R in $\mathcal{S}$ with $|R| = (p-1)(u+v)$ and $(\ )_p$ denotes mod p binomial coefficients.

Proof. The proof of (6) can be found in [**G**]. The other equality, (7), can be extracted from [**Ka1**]. □

Remark. In [**Ka1**], our Lemma 4.2 is stated (wrongly) without any minus signs. Unfortunately, Karaca does not explicitly say what his definition of $\hat{\mathrm{P}}(u)$ is. Instead, for the special Milnor basis elements $M[(0,\dots,0,r_t = p^s)] =: \mathrm{P}^s_t$ he defines $\widehat{\mathrm{P}^s_t}$ as $(-1)^s\chi(\mathrm{P}^s_t)$. Since there exists a basis of $\mathcal{P}^*$ which consists of certain monomials in elements of the form P^s_t, it is possible to figure out what the expression $\hat{\mathrm{P}}(u)$ should mean according to Karaca's definition, assuming that $\widehat{\mathrm{P}^s_t \cdot \mathrm{P}^v_u} := \widehat{\mathrm{P}^v_u} \cdot \widehat{\mathrm{P}^s_t}$. However, doing this translation one easily sees that there should be some non-trivial coefficients in his formula. The correct result can nevertheless easily be deduced from the argument given in [**Ka1**].

After these preparations we are in a position to prove the following "hat-passing formula", which is a slightly generalised odd prime version of the formula given in [**S1**, Lemma 2.3]:

Proposition 4.3. *Suppose that k, l, c, m and n are non-negative integers with*

1. $k > l$,
2. $1 \leqslant c \leqslant p-1$,
3. $m + n = cp^l\gamma(k-l)$,
4. $m < p^{k-1}$,
5. $m \equiv 0 \mod p^l$.

We use the convention $\hat{\mathrm{P}}(s) := 0$ *if* $s < 0$. *Then for* $l = 0$ *we have*

$$\mathrm{P}(m) \cdot \hat{\mathrm{P}}(n) = (-1)^c \hat{\mathrm{P}}(m + n - pm - c) \cdot \mathrm{P}(pm + c)$$

and for $l > 0$ *we have*

$$\mathrm{P}(m) \cdot \hat{\mathrm{P}}(n) = \sum_{i=1}^{c} (-1)^{i+1} \binom{c}{i}_p \mathrm{P}(m + ip^{l-1}) \cdot \hat{\mathrm{P}}(n - ip^{l-1}) + (-1)^c \hat{\mathrm{P}}(m + n - pm - cp^l) \cdot \mathrm{P}(pm + cp^l)\,.$$

Proof. In order to see that for $l = 0$ only one term in the expression for $\mathrm{P}(m) \cdot \hat{\mathrm{P}}(n)$ appears, note that $|R| = (p-1)c\gamma(k) = c(p^k - 1)$, so that by applying Equation (6) in Lemma 4.2 we obtain

$$\mathrm{P}(m) \cdot \hat{\mathrm{P}}(n) = (-1)^n \sum_{|R| = c(p^k - 1)} \binom{c(p^k - 1) + \mathrm{ex}(R)}{pm}_p M[R]\,.$$

Now recall that $\mathrm{ex}(R) = \sum_{i \geqslant 1} r_i$. Dividing $|R|$ by $(p-1)$ and substituting $\mathrm{ex}(R) - \sum_{i \geqslant 2} r_i$ for r_1 we have

$$c\gamma(k) = \frac{|R|}{p-1} = \sum_{i \geqslant 1} r_i \gamma(i) = \mathrm{ex}(R) + \sum_{i \geqslant 2} r_i p \gamma(i-1)\,.$$

Thus we see that $\mathrm{ex}(R) \equiv c \bmod p$. Now we apply Lemma 4.1 with $e = \mathrm{ex}(R)$; we have just seen that we are always in case (I) so that

$$\binom{c(p^k - 1) + \mathrm{ex}(R)}{pm} \equiv \binom{\mathrm{ex}(R)}{pm + c}\,.$$

Equation (7) in Lemma 4.2 now implies that

$$\begin{aligned} \mathrm{P}(m) \cdot \hat{\mathrm{P}}(n) &= (-1)^n \sum_{|R| = c(p^k - 1)} \binom{c(p^k - 1) + \mathrm{ex}(R)}{pm}_p M[R] \\ &= (-1)^c (-1)^{m+n-pm-c} \sum_{|R| = c(p^k - 1)} \binom{\mathrm{ex}(R)}{pm + c}_p M[R] \\ &= (-1)^c \hat{\mathrm{P}}(m + n - pm - c) \cdot \mathrm{P}(pm + c)\,. \end{aligned}$$

The formula for $l > 0$ easily follows from Lemma 4.1, carefully keeping track of any minus signs that enter into the formula. □

In order to arrive at the simple description of $\hat{\mathrm{P}}[s; c\gamma(t)]$ that will be obtained in Theorem 4.6 we need yet another lemma. The elegant proof given here, due to Judith Silverman, is a nice application of the "stripping technique" discussed in Section 3 and replaces the original, more complicated proof which didn't use stripping at all.

Lemma 4.4. *Let* c *and* l *be positive integers with* $1 \leqslant c \leqslant p - 1$. *Then* $\mathrm{P}(c\gamma(l)) \cdot \mathrm{P}(ap^{l-1}) = 0$ *for any* a *which satisfies* $p - c \leqslant \alpha_0(a) \leqslant p - 1$.

Proof. The lemma is proved by downward induction on c. We start with the case $c = p - 1$ so that $1 \leqslant \alpha_0(a) \leqslant p - 1$. Then by the Adem relations we have

$$\begin{aligned} &\mathrm{P}(p^l - 1) \cdot \mathrm{P}(ap^{l-1}) \\ &= \sum_{z=0}^{p^{l-1}} (-1)^{p^l - 1 + z} \binom{(p-1)(ap^{l-1} - z) - 1}{p^l - 1 - pz}_p \mathrm{P}(p^l - 1 + ap^{l-1} - z) \cdot \mathrm{P}(z)\,. \end{aligned}$$

We show that the mod p binomial coefficients appearing in this formula are all 0. First consider the case $z=0$: since $1 \leqslant \alpha_0(a) \leqslant p-1$ we have $0 \leqslant \alpha_{l-1}((p-1)ap^{l-1}-1) \leqslant p-2$, but $\alpha_{l-1}(p^l-1) = p-1$ and so $\binom{(p-1)ap^{l-1}-1}{p^l-1} \equiv 0$. On the other hand, if $z \neq 0$ then there exists some index j_0 with $0 \leqslant j_0 \leqslant l-2$ such that $1 \leqslant z_{j_0} \leqslant p-1$ but $z_j = 0$ for all $0 \leqslant j < j_0$. Hence $1 \leqslant \alpha_{j_0}((p-1)z) = p - z_{j_0} \leqslant p-1$ and so $0 \leqslant \alpha_{j_0}((p-1)(ap^{l-1}-z)-1) \leqslant p-2$. But $\alpha_{j_0}(p^l-1-pz) = p-1$ and so again $\binom{(p-1)(ap^{l-1}-z)-1}{p^l-1-pz} \equiv 0$.

Now let $1 \leqslant c < p-1$ and suppose that the lemma has been shown to be true for all $\hat{c}$ with $c < \hat{c} \leqslant p-1$. Choose a with $p-c \leqslant \alpha_0(a) \leqslant p-1$ (which implies $p-(c+1) \leqslant \alpha_0(a-1) \leqslant p-1$ and $p-(c+1) \leqslant \alpha_0(a) \leqslant p-1$). The lemma for $c+1$ guarantees that

$$\mathrm{P}\big((c+1)\gamma(l)\big) \cdot \mathrm{P}(ap^{l-1}) = 0 \tag{8}$$

and

$$\mathrm{P}\big((c+1)\gamma(l)\big) \cdot \mathrm{P}\big((a-1)p^{l-1}\big) = 0\,. \tag{9}$$

Using Equation (3), Prop. 3.1(4) and Cons. 3.4(2) we strip Equation (8) by $\hat{\xi}_l$ to obtain

$$\begin{aligned} 0 &= \hat{\xi}_l \cap \big[\mathrm{P}((c+1)\gamma(l)) \cdot \mathrm{P}(ap^{l-1})\big] \\ &= \big[\hat{\xi}_l \cap \mathrm{P}((c+1)\gamma(l))\big] \cdot \mathrm{P}(ap^{l-1}) \\ &\qquad\qquad + \sum_{i=0}^{l-1} \big[\hat{\xi}_i \cap \mathrm{P}((c+1)\gamma(l))\big] \cdot \big[\hat{\xi}_{l-i}^{p^i} \cap \mathrm{P}(ap^{l-1})\big] \qquad (10) \\ &= (-1)^l \mathrm{P}(c\gamma(l)) \cdot \mathrm{P}(ap^{l-1}) + E, \end{aligned}$$

where E is defined to be the big sum in (10). It remains to show that $E=0$. We fix i with $1 \leqslant i \leqslant l-1$ and observe that for any $b \geqslant 0$ we have

$$\hat{\xi}_{l-i}^{p^i} \cap \mathrm{P}(b) \;=\; (-1)^{l-i}\mathrm{P}(b - p^i\gamma(l-i)) \;=\; -\hat{\xi}_{l-i-1}^{p^i} \cap \mathrm{P}(b - p^{l-1})\,.$$

Setting $b = ap^{l-1}$, we find that E can be rewritten as

$$\begin{aligned} E &= -\sum_{i=0}^{l-1} \big[\hat{\xi}_i \cap \mathrm{P}((c+1)\gamma(l))\big] \cdot \big[\hat{\xi}_{l-i-1}^{p^i} \cap \mathrm{P}((a-1)p^{l-1})\big] \\ &= -\hat{\xi}_{l-1} \cap \big[\mathrm{P}((c+1)\gamma(l)) \cdot \mathrm{P}((a-1)p^{l-1})\big]\,. \qquad (11) \end{aligned}$$

But by (9), the product in (11) is 0. Consequently $E=0$ as desired. □

The next lemma establishes the basis of induction for Theorem 4.6.

Lemma 4.5. *Let c be an integer with $1 \leqslant c \leqslant p-1$. Then*

$$\hat{\mathrm{P}}(c\gamma(s)) = (-1)^{sc}\mathrm{P}[s;c]\,.$$

Proof. The case $s=1$ is clear: by [**Mi**] we have

$$\hat{\mathrm{P}}(c) \;=\; (-1)^c \sum_{|Q|=c(p-1)} M[Q] \;=\; (-1)^c\mathrm{P}(c)\,,$$

and in general

$$\hat{\mathrm{P}}(c\gamma(s)) = (-1)^{c\gamma(s)} \sum_{|Q|=c(p^s-1)} M[Q]\,. \tag{12}$$

By induction and Equation (6) we obtain

$$\begin{aligned}(-1)^{sc}\mathrm{P}[s;c] &= (-1)^{sc}\mathrm{P}(p^{s-1}c)\cdot \mathrm{P}[s-1;c]\\ &= (-1)^{c}\mathrm{P}(p^{s-1}c)\cdot \hat{\mathrm{P}}(c\gamma(s-1))\\ &= (-1)^{c\gamma(s)}\sum_{|R|=c(p^s-1)}\binom{|R|+\mathrm{ex}(R)}{cp^s}_p M[R]\,,\end{aligned}$$

so that by (12) it only remains to show that $\binom{|R|+\mathrm{ex}(R)}{cp^s}\equiv 1$ for all R with $|R|=c(p^s-1)$. It follows directly from the definitions that $0\leqslant \mathrm{ex}(R)\leqslant \frac{|R|}{p-1}=c\gamma(s)$. On the other hand it is easy to see that the sequence $(0,\cdots,0,r_s=c)$ is of excess c and that this is the minimal excess of any sequence in $\mathcal{S}$ of degree $c(p^s-1)$. The inequality $c\leqslant \mathrm{ex}(R)\leqslant c\gamma(s)$ now implies that

$$cp^s \;\leqslant\; |R|+\mathrm{ex}(R)\;\leqslant\; cp\gamma(s)\;=\;cp^s+cp^{s-1}+\ldots+cp$$

so that indeed $\binom{|R|+\mathrm{ex}(R)}{cp^s}\equiv 1$ for all R with $|R|=c(p^s-1)$. □

Finally we can prove the conjugation formula announced earlier on, which is a slightly generalised mod p version of [**S1**, Theorem 3.1]. The proof is similar to the one in the mod 2 case.

Theorem 4.6. *For all positive integers s, t and c with $1\leqslant c\leqslant p$ the following conjugation formula holds:*

$$\hat{\mathrm{P}}[s;c\gamma(t)]=(-1)^{stc}\mathrm{P}[t;c\gamma(s)]$$

Proof. We first prove the theorem for $1\leqslant c\leqslant p-1$. The case $c=p$ will follow from the case $c=1$ by a stripping argument.

The proof for $1\leqslant c\leqslant p-1$ is by induction on t. The basis of induction (i.e. the case $t=1$ or equivalently $s=1$) has been established in Lemma 4.5. So let us assume that $t>1$, $s>1$ and that the theorem has been shown to be true for all $1\leqslant \hat{t}\leqslant t-1$, all s and also for $\hat{t}=t$, all $1\leqslant \hat{s}\leqslant s-1$. We begin with the following remark:

Remark. *Under the above assumptions the following is true:*
For all non-negative integers a with $p-c\leqslant \alpha_0(a)\leqslant p-1$ and for all $1\leqslant l<s$ we have

$$\hat{\mathrm{P}}(ap^{l-1})\cdot \mathrm{P}[l;c\gamma(t)]=0\,.$$

We prove this result as follows: we have

$$\hat{\mathrm{P}}(ap^{l-1})\cdot \mathrm{P}[l;c\gamma(t)]=\chi\big[\hat{\mathrm{P}}[l;c\gamma(t)]\cdot \mathrm{P}(ap^{l-1})\big]\,,$$

which by induction equals

$$(-1)^{tlc}\chi\big[\mathrm{P}[t;c\gamma(l)]\cdot \mathrm{P}(ap^{l-1})\big]=(-1)^{tlc}\chi\big[\mathrm{P}[t-1;pc\gamma(l))]\cdot \mathrm{P}(c\gamma(l))\cdot \mathrm{P}(ap^{l-1})\big]\,.$$

But by Lemma 4.4 the expression $\mathrm{P}(c\gamma(l))\cdot \mathrm{P}(ap^{l-1})$ vanishes. This proves the remark.

Now we get back to the proof of the theorem: by induction we obtain

$$\begin{aligned}\hat{\mathrm{P}}[t;c\gamma(s)] &= \chi(\mathrm{P}[t-1;c\gamma(s)])\cdot\chi(\mathrm{P}(p^{t-1}c\gamma(s)))\\ &= (-1)^{(t-1)sc}\mathrm{P}[s;c\gamma(t-1)]\cdot \hat{\mathrm{P}}(p^{t-1}c\gamma(s))\,. \end{aligned}\tag{13}$$

We claim that for $1\leqslant d\leqslant s$ the following formula holds:

$$\mathrm{P}[d;c\gamma(t-1)]\cdot\hat{\mathrm{P}}(p^{t-1}c\gamma(s))=(-1)^{dc}\hat{\mathrm{P}}(p^{t+d-1}c\gamma(s-d))\cdot \mathrm{P}[d;c\gamma(t)]$$

Proof of the claim: for $d=1$ we have to show that

$$\mathrm{P}(c\gamma(t-1))\cdot\hat{\mathrm{P}}(p^{t-1}c\gamma(s))=(-1)^{c}\hat{\mathrm{P}}(p^{t}c\gamma(s-1))\cdot \mathrm{P}(c\gamma(t))\,.$$

This follows immediately from Prop. 4.3 with $m = c\gamma(t-1)$, $n = p^{t-1}c\gamma(s)$, $k = t+s-1$ and $l = 0$. So suppose that $2 \leqslant d \leqslant s$, assuming that the claim has been proved for all $1 \leqslant \hat{d} < d$. Then using induction we obtain

$$\begin{aligned}
&\mathrm{P}[d; c\gamma(t-1)] \cdot \hat{\mathrm{P}}(p^{t-1}c\gamma(s)) \\
&\qquad = \mathrm{P}(p^{d-1}c\gamma(t-1)) \cdot \mathrm{P}[d-1; c\gamma(t-1)] \cdot \hat{\mathrm{P}}(p^{t-1}c\gamma(s)) \\
&\qquad = (-1)^{(d-1)c}\mathrm{P}(p^{d-1}c\gamma(t-1)) \cdot \hat{\mathrm{P}}(p^{t+d-2}c\gamma(s-d+1)) \cdot P[d-1; c\gamma(t)]\,.
\end{aligned}$$

Again, we apply Prop. 4.3, this time to the first two terms, with the parameters $m = p^{d-1}c\gamma(t-1)$, $n = p^{t+d-2}c\gamma(s-d+1)$, $k = t+s-1$ and $l = d-1$. We deduce that

$$\begin{aligned}
&\mathrm{P}(p^{d-1}c\gamma(t-1)) \cdot \hat{\mathrm{P}}(p^{t+d-2}c\gamma(s-d+1)) \\
&\quad = \sum_{i=1}^{c}(-1)^{i+1}\binom{c}{i}_p \mathrm{P}(p^{d-1}c\gamma(t-1) + ip^{d-2}) \cdot \hat{\mathrm{P}}((p^{t+d-2}c\gamma(s-d+1) - ip^{d-2}) \\
&\qquad + (-1)^c\hat{\mathrm{P}}(p^{t+d-1}c\gamma(s-d)) \cdot \mathrm{P}(p^{d-1}c\gamma(t))\,.
\end{aligned}$$

By the remark, the terms in the big sum vanish upon multiplication with $\mathrm{P}[d-1; c\gamma(t)]$ from the right, and so we arrive at

$$\begin{aligned}
&\mathrm{P}[d; c\gamma(t-1)] \cdot \hat{\mathrm{P}}(p^{t-1}c\gamma(s)) \\
&\qquad = (-1)^{dc}\hat{\mathrm{P}}(p^{t+d-1}c\gamma(s-d)) \cdot \mathrm{P}(p^{d-1}c\gamma(t)) \cdot \mathrm{P}[d-1; c\gamma(t)] \\
&\qquad = (-1)^{dc}\hat{\mathrm{P}}(p^{t+d-1}c\gamma(s-d)) \cdot \mathrm{P}[d; c\gamma(t)]
\end{aligned}$$

which proves the claim.

Setting $d = s$ and substituting back into expression (13) yields

$$\begin{aligned}
\hat{\mathrm{P}}[t; c\gamma(s)] &= (-1)^{(t-1)sc}\mathrm{P}[s; c\gamma(t-1)] \cdot \hat{\mathrm{P}}(p^{t-1}c\gamma(s)) \\
&= (-1)^{tsc}\mathrm{P}[s; c\gamma(t)]
\end{aligned}$$

which finishes the proof of the theorem for $1 \leqslant c \leqslant p-1$.

There remains the case $c = p$. We strip the formula

$$\hat{\mathrm{P}}[s; \gamma(t+1)] = (-1)^{s(t+1)}\mathrm{P}[t+1; \gamma(s)]$$

(this is the case $c = 1$ with $t+1$ instead of t) by $\hat{\xi}_s$, and by Cor. 3.3(3) we obtain

$$\begin{aligned}
\hat{\mathrm{P}}[s; p\gamma(t)] &= \hat{\xi}_s \cap \hat{\mathrm{P}}[s; \gamma(t+1)] \\
&= (-1)^{s(t+1)}\hat{\xi}_s \cap \mathrm{P}[t+1; \gamma(s)]
\end{aligned}$$

which by Cons. 3.4(2) and Prop. 3.6 equals

$$\begin{aligned}
(-1)^{s(t+1)}\mathrm{P}[t; p\gamma(s)] \cdot \big(\hat{\xi}_s \cap \mathrm{P}(\gamma(s))\big) &= (-1)^{s(t+1)}\mathrm{P}[t; p\gamma(s)] \cdot (-1)^s\mathrm{P}(0) \\
&= (-1)^{st}\mathrm{P}[t; p\gamma(s)]\,.
\end{aligned}$$

This completes the proof of the theorem. □

We observe the following:

Corollary 4.7. *Let s, t and c be non-negative integers with $s \geqslant 1$ and $1 \leqslant c \leqslant p$. Then the operations $\hat{\mathrm{P}}[s; c\gamma(t)]$ have length exactly t independently of s and c. More generally, if $\gamma(t) \leqslant f < \gamma(t+1)$ then the operations $\hat{\mathrm{P}}[s; f]$ are all of length exactly t, independently of s.*

Proof. For $t \geqslant 1$ the first statement is an immediate consequence of Theorem 4.6; for $t = 0$ the statement is trivial. The second statement follows since stripping operations cannot increase length (cf. Section 3.2). □

5. Conjugation formulas for $\mathcal{P}_*$

We now turn to conjugation in the dual Steenrod algebra. Let $\mathfrak{S}(k)$ be the symmetric group with identity Id_k acting on $\{0,1,2,\ldots,k-1\}$. For $\tau \in \mathfrak{S}(k)$ and $i \geqslant 0$ we define

$$Z_i(k;\tau) := \sum_{j=0}^{k-1} p^j B(i+\tau(j)-j)\,,$$

$$X_i(k;\tau) := \xi[Z_i(k;\tau)] \;=\; \prod_{j=0}^{k-1} \xi_{i+\tau(j)-j}^{p^j}\,,$$

and

$$\mathcal{X}_i(k) := \sum_{\tau\in\mathfrak{S}(k)} \mathrm{sign}(\tau)\, X_i(k;\tau)\,.$$

Observation 5.1. *$Z_i(k;\mathrm{Id}_k) = \gamma(k)B(i)$ and $X_i(k;\mathrm{Id}_k) = \xi_i^{\gamma(k)}$.*

We will need the following lemma:

Lemma 5.2. *For $k \geqslant 1$ we have $\mathcal{X}_1(k) = (-1)^k\hat{\xi}_k$.*

Proof. The proof is by induction on k. Let $k=1$, then $\mathcal{X}_1(1) = \xi_1 = -\hat{\xi}_1$, so the assertion is true in this case. Now suppose the statement has been shown to be true for all $1 \leqslant \hat{k} < k$. Note that if $X_1(k;\tau) \neq 0$ then necessarily $\tau(j) \geqslant j-1$ for all j. So if $X_1(k;\tau)\neq 0$ then define l by $l = \tau^{-1}k-1$. If $l = k-1$ then we obtain a cycle decomposition of τ as $(k-1)\sigma$ for some $\sigma\in\mathfrak{S}(k-1)$. If $l\neq k-1$ then we obtain $\tau(k-1)=k-2$, $\tau(k-2)=k-3$, $\ldots$, $\tau(l+1)=l$, so that τ has a cycle decomposition as $(k-1,k-2,\ldots,l)\sigma$ for some $\sigma\in\mathfrak{S}(l)$. In any case we have

$$X_1(k;\tau) = X_1(l;\sigma)\cdot \xi_{k-l}^{p^l}\,.$$

So for $0\leqslant l\leqslant k-1$ let $\mathfrak{S}_l(k) = \{\tau\in\mathfrak{S}(k)\,|\,\tau(l)=k-1\}$; obviously $\mathfrak{S}(k) = \bigcup \mathfrak{S}_l(k)$. Then by induction

$$\begin{aligned}
\mathcal{X}_1(k) &= \sum_{l=0}^{k-1}\sum_{\tau\in\mathfrak{S}_l(k)} \mathrm{sign}(\tau)\,X_1(k;\tau)\\
&= \sum_{l=0}^{k-1} \xi_{k-l}^{p^l}\cdot\sum_{\sigma\in\mathfrak{S}(l)} (-1)^{k-1-l}\mathrm{sign}(\sigma)\,X_1(l;\sigma)\\
&= (-1)^{k-1}\sum_{l=0}^{k-1}\xi_{k-l}^{p^l}\cdot\hat{\xi}_l \;=\; (-1)^k\hat{\xi}_k\,,
\end{aligned}$$

where in the last line we used Milnor's recursive formula for the anti-automorphism. □

In analogy to [**S3**] we make the following more general definitions:

Definition 5.3. *For $k\geqslant 1$, let $\mathcal{I}(k)$ be the set of non-decreasing sequences $(i_0,i_1,\ldots,i_{k-1})$ of positive integers. For $\tau\in\mathfrak{S}(k)$ and $I\in\mathcal{I}(k)$ we define*

$$Z_I(k;\tau) := \sum_{j=0}^{k-1} p^j B(i_{\tau(j)}+\tau(j)-j)\,,$$

$$X_I(k;\tau) := \xi[Z_I(k;\tau)] \;=\; \prod_{j=0}^{k-1}\xi_{i_{\tau(j)}+\tau(j)-j}^{p^j}\,,$$

and

$$\mathcal{X}_I(k) := \sum_{\tau\in\mathfrak{S}(k)} \operatorname{sign}(\tau)\, X_I(k;\tau)\,.$$

We further define

$$P_I(k;\tau) := \sum_{j=0}^{k-1} p^{j+i_0} B(i_{\tau(j)} + \tau(j) - (j+i_0))\,,$$

$$R_I(k;\tau) := \xi[P_I(k;\tau)] \;=\; \prod_{j=0}^{k-1} \xi_{i_{\tau(j)}+\tau(j)-(j+i_0)}^{p^{j+i_0}}\,,$$

and

$$\mathcal{R}_I(k) := \sum_{\tau\in\mathfrak{S}(k)} \operatorname{sign}(\tau)\, R_I(k;\tau)\,.$$

Observations 5.4. *1. If $I = (i,i,\dots,i) \in \mathcal{I}(k)$ is a constant sequence then we obtain $Z_I(k;\tau) = Z_i(k;\tau)$ and consequently $X_I(k;\tau) = X_i(k;\tau)$. Moreover, for such a sequence I and $\tau \neq \mathrm{Id}_k$ we have $P_I(k;\tau) = *$ and consequently $\mathcal{R}_I(k) = R_I(k;\mathrm{Id}_k) = 1$.*

2. If $I = (i_0, i_1, \dots, i_{k-1}) \in \mathcal{I}(k)$ and $i_0 > 1$ let $I[-1]$ denote the sequence $(i_0 - 1, i_1 - 1, \dots, i_{k-1} - 1) \in \mathcal{I}(k)$. Then $\mathcal{R}_I(k) = \big(\mathcal{R}_{I[-1]}(k)\big)^p$.

Theorem 5.5. *Let $k \geqslant 1$. Then $\hat{\mathcal{X}}_I(k) \equiv (-1)^{i_0 k}\xi_k^{\gamma(i_0)} \cdot \hat{\mathcal{R}}_I(k)$ modulo monomials of length $> k$.*

Proof. First recall that we have the following expression for $\hat{\mathcal{X}}_I(k)$:

$$\begin{aligned}\hat{\mathcal{X}}_I(k) &= \sum_{\rho\in\mathfrak{S}(k)} \operatorname{sign}(\rho) \prod_{j=0}^{k-1} \hat{\xi}_{i_{\rho(j)}+\rho(j)-j}^{p^j}\\ &= \sum_{\rho\in\mathfrak{S}(k)} \operatorname{sign}(\rho)\; \hat{\xi}_{i_{\rho(0)}+\rho(0)} \cdot \prod_{j=1}^{k-1} \hat{\xi}_{i_{\rho(j)}+\rho(j)-j}^{p^j}\,.\end{aligned}$$

Applying Milnor's recursive formula for the anti-automorphism we obtain

$$-\hat{\xi}_{i_{\rho(0)}+\rho(0)} \equiv \sum_{n=1}^{k} \xi_n \cdot \hat{\xi}_{i_{\rho(0)}+\rho(0)-n}^{p^n}$$

modulo monomials of length $> k$. So we have

$$\hat{\mathcal{X}}_I(k) \equiv -\sum_{n=1}^{k}\sum_{\rho\in\mathfrak{S}(k)} \operatorname{sign}(\rho)\; \xi_n \cdot \hat{\xi}_{i_{\rho(0)}+\rho(0)-n}^{p^n} \cdot \prod_{j=1}^{k-1} \hat{\xi}_{i_{\rho(j)}+\rho(j)-j}^{p^j}\,.$$

For each $\rho \in \mathfrak{S}(k)$ we define ρ' by

$$\rho'(l) = \begin{cases} \rho(0) & \text{if } l = k-1\\ \rho(l+1) & \text{if } 0 \leqslant l \leqslant k-2.\end{cases}$$

Note that $\operatorname{sign}(\rho) = (-1)^{k-1}\operatorname{sign}(\rho')$. So

$$\hat{\mathcal{X}}_I(k) \equiv (-1)^k \sum_{n=1}^{k}\sum_{\rho'\in\mathfrak{S}(k)} \operatorname{sign}(\rho')\; \xi_n \cdot \hat{\xi}_{i_{\rho'(k-1)}+\rho'(k-1)-n}^{p^n} \cdot \prod_{l=0}^{k-2} \hat{\xi}_{i_{\rho'(l)}+\rho'(l)-(l+1)}^{p^{l+1}}$$

modulo monomials of length $> k$.

For the proof of the theorem, we fix k and use induction on i_0. First suppose that $i_0 = 1$. Then

$$\xi_k \cdot \hat{\mathcal{R}}_I(k) = \sum_{\tau \in \mathfrak{S}(k)} \operatorname{sign}(\tau)\, \xi_k \cdot \hat{\xi}^{p^k}_{i_{\tau(k-1)}+\tau(k-1)-k} \cdot \prod_{j=0}^{k-2} \hat{\xi}^{p^{j+1}}_{i_{\tau(j)}+\tau(j)-(j+1)}$$

so that

$$\begin{aligned} &\hat{\mathcal{X}}_I(k) - (-1)^k \xi_k \cdot \hat{\mathcal{R}}_I(k) \\ &\qquad \equiv (-1)^k \sum_{n=1}^{k-1} \sum_{\rho' \in \mathfrak{S}(k)} \operatorname{sign}(\rho')\, \xi_n \cdot \hat{\xi}^{p^n}_{i_{\rho'(k-1)}+\rho'(k-1)-n} \cdot \prod_{l=0}^{k-2} \hat{\xi}^{p^{l+1}}_{i_{\rho'(l)}+\rho'(l)-(l+1)} . \end{aligned} \tag{14}$$

It can easily be verified that the summand in (14) associated to n and ρ' is the negative of the term associated to n and ρ'' where

$$\rho''(l) = \begin{cases} \rho'(l) & \text{if } l \neq n-1 \text{ and } l \neq k-1 \\ \rho'(n-1) & \text{if } l = k-1 \\ \rho'(k-1) & \text{if } l = n-1 \end{cases}$$

(note that $\operatorname{sign}(\rho') = -\operatorname{sign}(\rho'')$). So the difference $\hat{\mathcal{X}}_I(k) - (-1)^k \xi_k \cdot \hat{\mathcal{R}}_I(k)$ vanishes modulo monomials of length $> k$ and the theorem holds for $i_0 = 1$.

The proof for general I is similar. By induction we can assume that the statement is true for $(i_0 - 1, i_1 - 1, \ldots, i_k - 1) = I[-1]$. By Observation 5.4(2)

$$\xi_k^{\gamma(i_0)} \cdot \hat{\mathcal{R}}_I(k) = \left(\xi_k^{\gamma(i_0-1)} \cdot \hat{\mathcal{R}}_{I[-1]}(k)\right)^p \cdot \xi_k$$

which modulo terms of length $> k$ is

$$\begin{aligned} &\equiv \left((-1)^{k(i_0-1)} \hat{\mathcal{X}}_{I[-1]}(k)\right)^p \cdot \xi_k \\ &= (-1)^{k(i_0-1)} \xi_k \cdot \sum_{\tau \in \mathfrak{S}(k)} \operatorname{sign}(\tau) \prod_{j=0}^{k-1} \hat{\xi}^{p^{j+1}}_{i_{\tau(j)}-1+\tau(j)-j} \\ &= (-1)^{k(i_0-1)} \sum_{\tau \in \mathfrak{S}(k)} \operatorname{sign}(\tau)\, \xi_k \cdot \hat{\xi}^{p^k}_{i_{\tau(k-1)}+\tau(k-1)-k} \cdot \prod_{j=0}^{k-2} \hat{\xi}^{p^{j+1}}_{i_{\tau(j)}+\tau(j)-(j+1)} . \end{aligned}$$

Now one can define ρ'' as before and proceed as in the case $i_0 = 1$ in order to establish the inductive step. □

An especially interesting formula arises from Theorem 5.5 if we set $I = (i, i, \ldots, i)$, a constant sequence:

Theorem 5.6. *Let $i, k > 0$. Modulo monomials of length $> k$ we have*

$$\hat{\xi}_i^{\gamma(k)} \equiv (-1)^{ik} \xi_k^{\gamma(i)} - \sum_{\mathrm{Id}_k \neq \tau \in \mathfrak{S}(k)} \operatorname{sign}(\tau) \prod_{j=0}^{k-1} \hat{\xi}^{p^j}_{i+\tau(j)-j} .$$

In particular, if $0 \leqslant f < \gamma(k+1)$ then

$$\hat{\xi}_k^{\gamma(i)} \cap \mathrm{P}[i; f] = (-1)^{ik} \xi_i^{\gamma(k)} \cap \mathrm{P}[i; f] \;=\; (-1)^{ik} \mathrm{P}[i; f - \gamma(k)] .$$

Proof. The first part follows immediately from Theorem 5.5 and Observation 5.4(1), so it only remains to prove the second statement. By the part already proved we have the following equality:

$$\hat{\xi}_i^{\gamma(k)} \cap \hat{\mathrm{P}}[i; f] = (-1)^{ik} \xi_k^{\gamma(i)} \cap \hat{\mathrm{P}}[i; f] - \Bigl(\sum_{\mathrm{Id}_k \neq \tau \in \mathfrak{S}(k)} \operatorname{sign}(\tau) \prod_{j=0}^{k-1} \hat{\xi}^{p^j}_{i+\tau(j)-j} \Bigr) \cap \hat{\mathrm{P}}[i; f]$$

Now observe that for any $\mathrm{Id}_k \neq \tau \in \mathfrak{S}(k)$ the product $\prod_{j=0}^{k-1} \xi_{i+\tau(j)-j}^{p^j}$ is of length strictly greater than i, so for any such τ we get

$$\Big(\prod_{j=0}^{k-1} \hat{\xi}_{i+\tau(j)-j}^{p^j}\Big) \cap \hat{\mathrm{P}}[i;f] = \chi\Big[\Big(\prod_{j=0}^{k-1} \xi_{s+\tau(j)-j}^{p^j}\Big) \cap \mathrm{P}[i;f]\Big] \;=\; 0\,.$$

Using Cor. 3.3(3) we thus obtain $\hat{\xi}_i^{\gamma(k)} \cap \hat{\mathrm{P}}[i;f] = \hat{\mathrm{P}}[i;f-\gamma(k)] = (-1)^{ik}\xi_k^{\gamma(i)} \cap \hat{\mathrm{P}}[i;f]$. The claim now follows by application of $(-1)^{ik}\chi$ to this formula. □

Finally, we note that Theorem 5.5 provides us with useful information regarding the behaviour of the stripping operations $D(\hat{\mathcal{X}}_I(k))$:

Corollary 5.7. *1. If* $\mathrm{len}(\theta) < k$, *then* $\hat{\mathcal{X}}_I(k) \cap \theta = 0$ *for all* $I \in \mathcal{I}(k)$.

2. If $\mathrm{len}(\theta) = k$, *then* $\hat{\mathcal{X}}_I(k) \cap \theta = (-1)^{i_0 k}\hat{\mathcal{R}}_I(k) \cap (\xi_k^{\gamma(i_0)} \cap \theta)$.

3. In particular, $\hat{\mathcal{X}}_I(k) \cap \mathrm{P}[k;f] = (-1)^{i_0 k}\hat{\mathcal{R}}_I(k) \cap \mathrm{P}[k;f-\gamma(i_0)]$.

Proof. This follows immediately from the theorem by invoking Prop. 3.1 and Cor. 3.3. □

References

[CWW] D. P. Carlisle, G. Walker and R. M. W. Wood. The intersection of the admissible basis and the Milnor basis of the Steenrod algebra. *J. Pure Appl. Algebra* **128** (1998), no.1, 1–10

[G] A. M. Gallant. Excess and conjugation in the Steenrod algebra. *Proc. Amer. Math. Soc.* **76** (1979), no.1, 161–166

[Ka1] I. Karaca. The nilpotence height of P_t^s for odd primes. *Trans. Amer. Math. Soc.* **351** (1999), no.2, 547–558

[Ka2] I. Karaca. On the action of Steenrod operations on polynomial algebras. *Turkish J. Math.* **22** (1998), no.2, 163–170

[Ka3] I. Karaca. Conjugation in the mod p Steenrod algebra and its dual. *(preliminary version, oct. 1998)*

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

[M] D. M. Meyer. Hit polynomials and excess in the mod p Steenrod algebra. *(prépublication numéro 1999-19, Université Paris–Nord)*

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

[S1] J. H. Silverman. Conjugation and excess in the Steenrod algebra. *Proc. Am. Math. Soc.* **119** (1993), no.2, 657–661

[S2] J. H. Silverman. Stripping and conjugation in the Steenrod algebra. *J. Pure Appl. Algebra* **121** (1997), no.1, 95–106

[S3] J. H. Silverman. Hit polynomials and conjugation in the dual Steenrod algebra. *Math. Proc. Camb. Philos. Soc.* **123** (1998), no.3, 531–547

[WW] G. Walker and R. M. W. Wood. The nilpotence height of Sq^{2^n}. *Proc. Am. Math. Soc.* **124** (1996), no.4, 1291–1295

[W] R. M. W. Wood. Problems in the Steenrod algebra. *Bull. London Math. Soc.* **30** (1998), no.5, 449–517

This article may be accessed via WWW at http://www.rmi.acnet.ge/hha/ or by anonymous ftp at ftp://ftp.rmi.acnet.ge/pub/hha/volumes/2000/n1/n1.(dvi,ps,dvi.gz,ps.gz)

Dagmar M. Meyer `dagmar@math.univ-paris13.fr` `meyerd@member.ams.org`

LAGA, Institut Galilée, Univ. Paris-Nord