Proceedings of the Edinburgh Mathematical Society (2001) **44**, 323–350 ©

HIT POLYNOMIALS AND EXCESS IN THE MOD *P* STEENROD ALGEBRA

DAGMAR M. MEYER

Laboratoire Analyse, Géométrie et Applications, Université Paris 13,
93430 Villetaneuse, France (meyerd@member.ams.org)

(Received 28 March 2000)

Abstract Let p be an odd prime. The primary purpose of this paper is to determine the excess of the conjugates of the Steenrod operations $\mathrm{P}[k;f]$, which are defined as $\mathrm{P}[k;f] := \mathrm{P}(p^{k-1}f)\cdot\mathrm{P}(p^{k-2}f)\cdot\cdots\cdot\mathrm{P}(pf)\cdot\mathrm{P}(f)$. The result is then used to obtain sufficient conditions for an element in the polynomial algebra $\mathbb{F}_p[x_1,\dots,x_s]$ to be in the image under the standard action of the Steenrod algebra. Results and methods are generalizations of previous work by Judith Silverman and by myself with Judith Silverman.

Keywords: hit polynomials; excess; Steenrod algebra

AMS 2000 *Mathematics subject classification:* Primary 55S10
Secondary 55S05

1. Introduction

Let p be an *odd* prime. The purpose of this paper is to determine the excess of the conjugates of the Steenrod operations $\mathrm{P}[k;f]$ defined below; these operations are the odd-primary analogues of the elements $\mathrm{Sq}[k;f]$ which were studied by Silverman in [**7**] and [**8**]. The result is then used to obtain sufficient conditions for an element $\theta \in \mathbb{P}_s := H^*(BT^s;\mathbb{F}_p)$ to be hit under the standard action of the mod p Steenrod algebra $\mathcal{A}^*$, where $BT^s = \prod_{i=1}^{s} \mathbb{C}P^\infty$ is the classifying space of the s-dimensional torus. This question is obviously related to the problem of determining a minimal set of generators of $\mathbb{P}_s$, as an $\mathcal{A}^*$-module, which has been studied extensively by Crossley, Wood and others.

Let $\mathcal{P}^* \subset \mathcal{A}^*$ be the sub-Hopf algebra of the mod p Steenrod algebra 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 $\mathrm{P}(0) := 1$. The elements $\mathrm{P}[k;f]$ are defined as

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

for any $k \geqslant 1$ and $f \geqslant 0$. In particular, $\mathrm{P}[1;f] = \mathrm{P}(f)$.

$\mathcal{P}^*$ inherits the canonical anti-automorphism χ of $\mathcal{A}^*$; in order to simplify notation we denote the image of an element $\theta \in \mathcal{P}^*$ under χ by $\hat{\theta}$, following notation introduced in [**9**]. In particular, $\hat{\mathrm{P}}[k;f] := \chi(\mathrm{P}[k;f])$.

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

We are interested in the excess of the operations $\hat{\mathrm{P}}[k;f]$: the excess of any operation θ in $\mathcal{P}^*$ can be defined as $\mathrm{ex}(\theta) = \min\{n \mid \theta(\iota_n) \neq 0 \in H^*(K(\mathbb{Z}/p,n);\mathbb{F}_p)\}$, where $\iota_n \in H^*(K(\mathbb{Z}/p,n);\mathbb{F}_p)$ is the fundamental class. Alternatively, write $\mathbb{P}_s \cong \mathbb{F}_p[x_1,\dots,x_s]$ with $|x_i| = 2$. Then the excess of θ can be characterized by $\mathrm{ex}(\theta) = 2\min\{s \mid \theta(x_1x_2\cdots x_s) \neq 0 \in \mathbb{P}_s\}$.

For $m \geqslant 0$ we define the numbers $\gamma(m)$ by

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

Given a non-negative integer f, we denote by $\mu(f)$ the minimal number of summands in any representation of f as a sum of the $\gamma(i)$, i.e.

$$\mu(f) := \min\left\{\sum_{i\geqslant 1} a_i \;\middle|\; f = \sum_{i\geqslant 1} a_i\gamma(i)\right\}.$$

It is known that $\mathrm{ex}(\hat{\mathrm{P}}(f)) = 2\mu(f)$ (cf. [**3**, Corollary 5], where the '2' is accidentally missing). Our result generalizes this formula to monomials of the form $\mathrm{P}[k;f]$ for arbitrary $k \geqslant 1$. Since we need more notation in order to state the theorem in its full form, we only give a simplified version here and refer the reader to § 2 for the complete statement.

Theorem 1.1 (weak version). *Let f and k be integers with $k \geqslant 1$, $f \geqslant 0$. Then*

$$\mathrm{ex}(\hat{\mathrm{P}}[k;f]) = 2\gamma(k)\mu(f).$$

This is the analogue of [**8**, Theorem 1.1] for odd primes.

Now let s be a positive integer and suppose that P is a monomial in $\mathbb{P}_s$. Throughout this paper we will always denote monomials by capital letters and then use the corresponding small letter to denote the degree, so that for example $|P| = 2p$, $|M| = 2m$, etc. We say that P is *hit* if it is in the image of the induced action $\bar{\mathcal{P}}^* \otimes \mathbb{P}_s \to \mathbb{P}_s$, where $\bar{\mathcal{P}}^*$ denotes the augmentation ideal of $\mathcal{P}^*$. An immediate consequence of Theorem 1.1 is the following result, which is the odd primary version of [**8**, Theorem 1.2].

Theorem 1.2. *Let s and k be positive integers and suppose that $P \in \mathbb{P}_s$ is of the form $E \cdot F^{p^k}$, where E and F are polynomials of degrees e and f, respectively. Suppose that $e < \gamma(k)\mu(f)$. Then P is hit.*

Evidently, any monomial $M \in \mathbb{P}_s$ which is of the form $M = F^p$ is hit. If M does not have this special form, then there is a unique description of M as

$$M = a\prod_{j=0}^{n(M)} (L_j)^{p^{k_j}},$$

where $0 \neq a \in \mathbb{F}_p$, $n(M) \geqslant 0$, each L_j is a product of the form $x_1^{c_1}x_2^{c_2}\cdots x_s^{c_s}$ with $0 \leqslant c_i \leqslant p-1$, not all c_i equal to 0, and $0 = k_0 < k_1 < \cdots < k_{n(M)}$. For $1 \leqslant J \leqslant n(M)$

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

we define decompositions

$$D_J(M) := \left[a \prod_{j=0}^{J-1} (L_j)^{p^{k_j}}\right] \cdot \left[\prod_{j=J}^{n(M)} (L_j)^{p^{k_j - k_J}}\right]^{p^{k_J}}.$$

For any non-negative integer x, let $\alpha(x)$ denote the sum of the coefficients in the p-adic expansion of x, i.e. if $x = \sum_{i \geqslant 0} a_i p^i$ with $0 \leqslant a_i < p$, then $\alpha(x) = \sum_{i \geqslant 0} a_i$. As a consequence of Theorem 1.2 we obtain the following set of conditions that a monomial *necessarily* has to fulfil in order to qualify as a possible generator of $\mathbb{P}_s$ as a $\mathcal{P}^*$-module:

Proposition 1.3. *Let $s > 0$. Then $\mathbb{P}_s$ is generated as a module over $\mathcal{P}^*$ by monomials M fulfilling the following condition.*

> *For all $1 \leqslant J \leqslant n(M)$, the decompositions $D_J(M)$ as defined above satisfy the inequality*
> $$\alpha\left((p-1)f_J + \left[\frac{e_J}{\gamma(k_J)}\right]\right) \leqslant \left[\frac{e_J}{\gamma(k_J)}\right].$$

Here

$$e_J = \sum_{j=0}^{J-1} p^{k_j} l_j \quad \text{and} \quad f_J = \sum_{j=J}^{n(M)} p^{k_j - k_J} l_j$$

(with l_j the degree of L_j); we use the notation $[x] := \max\{z \in \mathbb{Z} \mid z \leqslant x\}$.

The condition corresponding to $J = 1$ is the single condition given in Theorem 2 of [**1**]. In § 5 we will provide an example which shows that our result indeed improves on the one by Chen and Shen: for $s = 3$ we find a monomial M such that $n(M) = 3$, M satisfies the conditions corresponding to $J = 1$ and $J = 2$, but it fails to fulfil the requirement for $J = 3$.

I thank Martin Crossley for pointing out to me that Theorem 2 in [**1**] and his own Theorem 2.2 in [**2**] imply the following fact, which allows us to identify dimensions in which we do not have to look for generators of $\mathbb{P}^s$ as a $\mathcal{P}^*$-module.

Proposition 1.4. *If $\alpha((p-1)(d+s)) > s(p-1)$ or if $\alpha(d+s) > s(s+1)(p-1)/2$, then in dimension $2d$ the graded $\mathbb{F}_p$-vector space $\mathbb{F}_p \otimes_{\mathcal{P}^*} \mathbb{P}_s$ is trivial.*

Our example $M \in \mathbb{P}_3$ is not covered by these conditions, i.e. Proposition 1.4 does not imply that there are *no* generators in the dimension of M. Hence the example shows that our results genuinely provide us with new information on the structure of $\mathbb{P}_s$ as a $\mathcal{P}^*$-module (and hence as a module over the Steenrod algebra).

The reader familiar with [**8**] and [**5**] may be wondering how far the analogy between the work presented here and the content of those two papers actually goes. In fact, the overall structure and the proofs of some of the results are quite similar. However, as so often is the case when trying to translate a result that is known for $p = 2$ to the odd-primary setting, the difficulty arises from the uncertainty of whether a 1 in the statement or proof of the known (mod 2) result corresponds in the mod p case to a 1, to $(p-1)$, or maybe to some or any number c with $1 \leqslant c \leqslant (p-1)$. In particular this means that *a*

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

priori non-trivial coefficients could appear just about anywhere. Once this problem has been solved on a case-to-case basis, many of the arguments indeed carry over nicely to the case of an odd prime.

2. Preliminaries and complete statement of Theorem 1.1

2.1. The monoid $\mathcal{S}$ of finite sequences

Let $\mathcal{S}$ be the set consisting of all sequences $S = (s_1, \dots, s_n, \dots)$ of non-negative integers with only finitely many non-zero entries. Under componentwise addition $\mathcal{S}$ is a commutative monoid; the neutral element is denoted by $0_{\mathcal{S}}$. We write $S = (s_1, s_2, \dots, s_L)$ if $s_j = 0$ for $j > L$. For $0 < a \leqslant b$ we denote by $S\{a, b\}$ the sequence whose ith coordinate is s_i if $a \leqslant i \leqslant b$, and 0 otherwise. Degree, excess and length of elements in $\mathcal{S}$ are defined by $|S| = \sum_{i \geqslant 1} s_i(p^i - 1)$, $\operatorname{ex}(S) = \sum_{i \geqslant 1} s_i$, and $\operatorname{len}(S) = \min\{i \geqslant 0 \mid s_j = 0,\ \forall j > i\}$, respectively, and we use the notation $S \succ S'$ to express that S is greater than S' in the right-lexicographical order. For notational convenience we adjoin a special element $*$ to $\mathcal{S}$ which has the property that $* + x = x + * = *$ for every $x \in \mathcal{S} \cup \{*\} =: \mathcal{S}^*$. Finally, for $j \in \mathbb{Z}$ we define the element $B(j) \in \mathcal{S}^*$ as the sequence with ith coordinate equal to δ_{ij} if $j \geqslant 0$, and as the special element $*$ if $j < 0$.

2.2. *E*-notation for admissibles and *M*-notation for Milnor basis elements

We will work both with the admissible and with the Milnor basis of $\mathcal{P}^*$, which are induced from those of the Steenrod algebra $\mathcal{A}^*$. For the admissible basis of $\mathcal{P}^*$ we use the parametrization which is given by the sequences $S \in \mathcal{S}$ in the following way: if $S = (s_1, \dots, s_n)$, then $E[S] = \mathrm{P}(a_1) \cdot \dots \cdot \mathrm{P}(a_n)$, where $a_n = s_n$ and $a_i = pa_{i+1} + s_i$ for $1 \leqslant i \leqslant n - 1$. In particular, $E[(0, \dots, 0, s_k = f)] = \mathrm{P}[k; f]$.

The Milnor basis of $\mathcal{P}^*$ is also parametrized by the sequences in $\mathcal{S}$: the dual $\mathcal{P}_*$ is a polynomial $\mathbb{F}_p$-algebra on generators ξ_i $(i \geqslant 1)$ in dimension $2(p^i - 1)$; we set $\xi_0 := 1$. For $S = (s_1, \dots, s_n)$ we write $\xi[S]$ for the monomial $\xi_1^{s_1} \cdot \dots \cdot \xi_n^{s_n}$, with $\xi_i^0 := 1$. The Milnor basis is the basis of $\mathcal{P}^*$ that is dual to the basis of $\mathcal{P}_*$ given by all the $\xi[S]$ with $S \in \mathcal{S}$; we denote the basis element dual to $\xi[S]$ by $M[S]$.

We also use the convention $M[S] = 0 = E[S]$ and $\xi[S] = 0$ if $S = *$ or if S is a finite sequence of integers with at least one negative entry.

The definitions of length, excess and right-lexicographical order for the elements of $\mathcal{S}$ induce analogous definitions for the elements both of the admissible basis and the Milnor basis. We set

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

and

$$E[S] \succ_E E[S'] :\Longleftrightarrow S \succ S' \Longleftrightarrow: M[S] \succ_M M[S'].$$

Thus we obtain notions of length, excess and order for all homogeneous elements of $\mathcal{P}^*$ (and of $\mathcal{P}_*$ by dualizing): let $\mathcal{B}$ denote either the admissible basis or the Milnor basis,

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

and, respectively, let B stand either for E or for M. Now suppose θ is a homogeneous element of $\mathcal{P}^*$ with a representation $\theta = \sum_{i=1}^{n} \alpha_i B[S_i]$ in basis elements in $\mathcal{B}$, with $S_1 \succ S_2 \succ \cdots \succ S_n$ and $0 \neq \alpha_i \in \mathbb{F}_p$ (we say '$B[S_i]$ appears in θ (with coefficient α_i)'). Then we set

$$\begin{aligned}\operatorname{len}_B(\theta) &:= \max_i\{\operatorname{len}_B(B[S_i])\} = \max_i\{\operatorname{len}(S_i)\},\\ \operatorname{ex}_B(\theta) &:= \min_i\{\operatorname{ex}_B(B[S_i])\} = 2\min_i\{\operatorname{ex}(S_i)\}.\end{aligned}$$

Furthermore, if θ' is another homogeneous element of $\mathcal{P}^*$ with a representation

$$\theta' = \sum_{i=1}^{n'} \alpha'_i B[S'_i],$$

with $S'_1 \succ S'_2 \succ \cdots \succ S'_{n'}$, then we define $\theta \succ_B \theta'$ if and only if there exists r with $1 \leqslant r \leqslant n$ such that

$$\begin{aligned} S_i = S'_i \quad &\text{and} \quad \alpha_i = \alpha'_i, \quad &&\text{for } 1 \leqslant i < r,\\ \alpha_r > \alpha'_r, \quad & &&\text{if } S_r = S'_r \text{ and } r \leqslant n',\\ S_r \succ S'_r, \quad & &&\text{if } S_r \neq S'_r \text{ and } r \leqslant n',\end{aligned}$$

i.e. θ and θ' are compared in descending order of their $\mathcal{B}$-summands.

The definition of excess of θ given here coincides with the one given in § 1 (cf. [**3**]); in particular $\operatorname{ex}_E(\theta) = \operatorname{ex}(\theta) = \operatorname{ex}_M(\theta)$. Also, the change-of-basis matrix X in each dimension between the admissible and the Milnor basis is upper triangular with diagonal entries $x_{SS} = \pm 1$, if we use the orderings $\succ_E$ and $\succ_M$, respectively (cf. [**6**, Lemma 8]). From this it follows that for any $S \in \mathcal{S}$ we have $E[S] \succ_E E[S] - x_{SS}M[S]$ and $M[S] \succ_M M[S] - x_{SS}E[S]$, and one easily deduces that for any $\theta \in \mathcal{P}^*$ we have $\operatorname{len}_M(\theta) = \operatorname{len}_E(\theta)$, which we therefore simply write as $\operatorname{len}(\theta)$.

In Example 2.2 we will show that the relation $\theta \succ_E \theta'$ does *not* in general imply $\theta \succ_M \theta'$ or vice versa. However, we have the following result which shows that the maximal summand of a given element is parametrized by the same sequence in $\mathcal{S}$ in both the admissible basis representation and the Milnor basis representation.

Lemma 2.1. *Let $\theta \in \mathcal{P}^*$ and suppose that θ is represented in the admissible basis as*

$$\theta = \sum_{i=1}^{n} \alpha_i E[R_i], \quad \textit{with } R := R_1 \succ R_2 \succ \cdots \succ R_n, \quad \alpha_i \in \mathbb{F}_p$$

and in the Milnor basis as

$$\theta = \sum_{j=1}^{m} \varphi_j M[S_j], \quad \textit{with } S := S_1 \succ S_2 \succ \cdots \succ S_m, \quad \varphi_j \in \mathbb{F}_p.$$

Then $S = R$ and $\varphi_1 = x_{RR}\alpha_1$, where $x_{RR} = \pm 1$ is the Rth diagonal entry in the change-of-basis matrix from admissible basis to Milnor basis.

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

Proof. $M[R]$ appears in $E[R]$ with coefficient $x_{RR} = \pm 1$, but it does not appear in $E[R_i]$ for $2 \leqslant i \leqslant n$ since $R \succ R_i$; hence its coefficient in the Milnor basis representation of θ is $x_{RR}\alpha_1$. On the other hand, $M[S]$ appears in θ with coefficient φ_1, so it must appear in at least one of the $E[R_i]$ for $1 \leqslant i \leqslant n$. If it appears in $E[R_i]$ for some $2 \leqslant i \leqslant n$, then $R \succ S$, which is impossible because of maximality of S. Hence $M[S]$ appears in $E[R]$, and again by maximality $R = S$. From this it also follows that $\varphi_1 = x_{RR}\alpha_1$. □

Here is the example promised above.

Example 2.2. Let $S \in \mathcal{S}$; the Milnor basis element $M[S]$ has a representation in the admissible basis given by $M[S] = \sum_{i=1}^{n} \alpha_i E[S_i]$ with $S_1 \succ \cdots \succ S_n$ (we can assume that $n > 1$). Now consider $M[S_n]$ with representation $M[S_n] = \sum_{j=1}^{m} \varphi_j E[R_j]$ with $R_1 \succ \cdots \succ R_m$ and set $\theta := M[S]$ and $\omega := M[S] + ((p - \alpha_n)/\varphi_1)M[S_n]$. So we have $\omega \succ_M \theta$. However, by Lemma 2.1, $S_n = R_1$, and so the admissible basis representation of ω is

$$\omega = \sum_{i=1}^{n} \alpha_i E[S_i] + \frac{p - \alpha_n}{\varphi_1} \sum_{j=1}^{m} \varphi_j E[R_j] = \sum_{i=1}^{n-1} \alpha_i E[S_i] + \frac{p - \alpha_n}{\varphi_1} \sum_{j=2}^{m} \varphi_j E[R_j]$$

with $S_1 \succ \cdots \succ S_{n-1} (\succ S_n = R_1) \succ R_2 \succ \cdots \succ R_m$. Hence $\theta \succ_E \omega$.

2.3. Elements of minimal excess

In § 1 we defined

$$\mu(f) = \min\biggl\{\sum_{i \geqslant 1} a_i \biggm| f = \sum_{i \geqslant 1} a_i \gamma(i)\biggr\}$$

for any non-negative integer f. Clearly, $\mu(f)$ can also be defined as the least excess of all sequences in $\mathcal{S}$ of degree $(p - 1)f$. Let

$$\Lambda(f) := \max\{\lambda : \gamma(\lambda) \leqslant f\}.$$

Then it is not hard to see that for any $f \geqslant 0$ there exists a unique sequence $R_1(f) = (r_1, \dots, r_{\Lambda(f)}) \in \mathcal{S}$ of length $\Lambda(f)$ and of degree $(p - 1)f$ such that $0 \leqslant r_i < p$ for all i, except that the first non-trivial r_i satisfies $0 < r_i \leqslant p$; this sequence has $\operatorname{ex}(R_1(f)) = \mu(f)$. Also, $R_1(f)$ is the right-lexicographically maximal element in $\mathcal{S}$ which has degree $(p - 1)f$. The corresponding admissible element $E[R_1(f)]$ is thus of minimal excess $(= 2\mu(f))$ and also the maximal element among all elements of the admissible basis in dimension $2(p - 1)f$. The analogous statement holds for the Milnor basis element $M[R_1(f)]$.

For $k \geqslant 1$, set

$$R_k(f) := (\gamma(k)r_1, \gamma(k)r_2, \dots, \gamma(k)r_{\Lambda(f)}).$$

Then $R_k(f)$ has excess $\gamma(k)\mu(f)$ and degree $(p^k - 1)f$, while the corresponding admissible basis element $E[R_k(f)]$ and the Milnor basis element $M[R_k(f)]$ both have excess $2\gamma(k)\mu(f)$ and dimension $2(p^k - 1)f$.

The sequence $R_1(f)$ may be constructed inductively by increasing the $\Lambda(f)$th entry of $R_1(f - \gamma(\Lambda(f)))$ by one. More generally, we have the following result.

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

Lemma 2.3. *Choose $1 \leqslant c \leqslant p$ such that $c\gamma(\Lambda(f)) \leqslant f < (c+1)\gamma(\Lambda(f))$; note that if $c = p$, then $f = p\gamma(\Lambda(f))$ by definition of $\Lambda(f)$. Then for any $k \geqslant 1$ the sequence $R_k(f)$ can be constructed inductively by increasing the $\Lambda(f)$th entry of $R_k(f - c\gamma(\Lambda(f)))$ by $c\gamma(k)$.*

Proof. Since $R_k(f)$ is obtained from $R_1(f)$ by multiplying each entry by $\gamma(k)$, it evidently suffices to prove the lemma for $k = 1$. The assertion is clear for $c = 1$. So suppose $c > 1$, which implies $\Lambda(f - \gamma(\Lambda(f))) = \Lambda(f)$. Now by induction we know that $R_1(f - \gamma(\Lambda(f)))$ can be constructed from $R_1(f - c\gamma(\Lambda(f)))$ by increasing the $\Lambda(f)$th entry by $c-1$, and $R_1(f)$ is constructed by increasing this same entry once again by one, i.e. by increasing the $\Lambda(f)$th entry of $R_1(f - c\gamma(\Lambda(f)))$ by c. □

2.4. Complete statement of Theorem 1.1

We are now in a position to give the full version of Theorem 1.1.

Theorem 1.1 (complete statement). *Let f and k be positive integers. Then the Milnor basis element $M[R_k(f)]$ has a non-trivial coefficient in the Milnor basis representation of $\hat{\mathrm{P}}[k; f]$. Moreover, it is both minimal in excess and maximal with respect to $\succ_M$ among all Milnor basis elements appearing in $\hat{\mathrm{P}}[k; f]$. Likewise, the admissible basis element $E[R_k(f)]$ has non-trivial coefficient in the admissible basis representation of $\hat{\mathrm{P}}[k; f]$; furthermore it is both minimal in excess and maximal with respect to $\succ_E$ among all admissible basis elements appearing in $\hat{\mathrm{P}}[k; f]$. In particular,* $\mathrm{ex}(\hat{\mathrm{P}}[k; f]) = 2\gamma(k)\mu(f)$.

3. *k*-reductions

Theorem 1.1 will be proved by induction on f, using the 'stripping' technique in $\mathcal{P}^*$, which will be reviewed briefly in § 4 and which is discussed in detail in [**4**]. In order for the inductive argument to work we need to have enough information on the sequences parametrizing the Milnor and the admissible basis elements, respectively, i.e. information on the monoid $\mathcal{S}$. The purpose of this section is to study the properties of the sequences in $\mathcal{S}$ with respect to 'k-reducibility'; in particular we will identify the maximal elements in certain subsets of $\mathcal{S}$ which consist of sequences satisfying given reducibility conditions. In § 4 the results obtained here will be combined with the stripping technique.

The concept of k-reducibility was first introduced in [**8**]. However, it turned out that the ideas used in that paper were not quite sufficient to lead to a correct proof of the analogue of Theorem 1.1 for $p = 2$; in fact they needed to be developed in substantially more depth in order to lead to success (cf. [**5**]). We present here a version of the theory for odd primes p.

3.1. Basic definitions and properties

Let $0 \leqslant \zeta < k$ and denote by $\mathcal{I}(k, \zeta)$ the set of non-decreasing sequences $(i_\zeta, i_1, \dots, i_{k-1})$ of positive integers. For τ an element in the symmetric group $\mathfrak{S}(k - \zeta)$

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

and $I \in \mathcal{I}(k,\zeta)$ we set

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

Definition 3.1.

(i) Let $T \in \mathcal{S}$, and suppose that $I(1), \dots, I(n) \in \mathcal{I}(k,\zeta)$ are sequences such that all coefficients of $T - \sum_{r=1}^{n} Z_{I(r)}(k,\zeta;\mathrm{Id}_{k-\zeta})$ are non-negative. Then T is (k,ζ)-reducible via $\bar{I} := \{I(1), \dots, I(n)\}$.

(ii) Suppose furthermore that $\tau_1, \dots, \tau_n \in \mathfrak{S}(k-\zeta)$ satisfy $P_{I(r)}(k,\zeta;\tau_r) \neq *$ for $1 \leqslant r \leqslant n$. We set

$$U := T - \sum_{r=1}^{n} Z_{I(r)}(k,\zeta;\mathrm{Id}_{k-\zeta}),$$
$$P := \sum_{r=1}^{n} P_{I(r)}(k,\zeta;\tau_r).$$

Then $[U;P] \in \mathcal{S} \times \mathcal{S}$ is the (k,ζ)-reduction of T via $\bar{I}$ and $\bar{\tau} = \{\tau_1, \dots, \tau_n\}$. The degree of this (k,ζ)-reduction is defined to be the sum $|[U;P]| := |U| + |P|$.

(iii) A sequence $T \in \mathcal{S}$ is (k,ζ)-irreducible if it fails to be (k,ζ)-reducible via $\{I\}$ for any $I \in \mathcal{I}(k,\zeta)$.

The degree of $[U;P]$ can be determined by the following formula.

Lemma 3.2. *With notation as above*

$$|[U;P]| = |T| - (p^k - p^\zeta) \sum_{r=1}^{n} \gamma(i_\zeta(r)),$$

where $i_\zeta(r)$ is the ζth coordinate of $I(r)$. In particular, $|[U;P]|$ is independent of $\bar{\tau}$, and any (k,ζ)-reduction of T has degree $\equiv |T|$ modulo $(p^k - p^\zeta)$.

Observations 3.3.

(i) If $\zeta = 0$ then $\mathcal{I}(k,\zeta)$ coincides with $\mathcal{I}(k)$ in the notation of [**4**]; this will be the case in most of our considerations. In this case we will leave the parameter ζ out of the notation. In particular, we will write $Z_I(k;\tau)$ instead of $Z_I(k,0;\tau)$ and $P_I(k;\tau)$ instead of $P_I(k,0;\tau)$ and speak of k-reducibility instead of $(k,0)$-reducibility.

(ii) If T is k-reducible via $\bar{I} := \{I(1), \dots, I(n)\}$ then one may obtain a k-reduction of T by taking $\tau_r = \mathrm{Id}_k$ for all r. Moreover, if the $I(r)$ are constant sequences, then this is the only corresponding k-reduction of T, since in this case $P_{I(r)}(k;\tau_r) = *$ for $\tau_r \neq \mathrm{Id}_k$.

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

(iii) If $t_i \geqslant \gamma(k)$ for some i, then $[T - \gamma(k)B(i); 0_{\mathcal{S}}]$ is a k-reduction of T via the constant sequence $(i, \dots, i) \in \mathcal{I}(k)$ and the constant sequence of permutations $\bar{\tau} = (\mathrm{Id}_k, \dots, \mathrm{Id}_k)$. Consequently, every $T \in \mathcal{S}$ has a k-reduction $[U; 0_{\mathcal{S}}]$ with $u_i < \gamma(k)$ for all i.

Given any $I \in \mathcal{I}(k)$ we define $\delta(I)$ to be the largest index r for which $i_r = i_0$. The following lemma is obvious.

Lemma 3.4. *If T is k-reducible via I, then we must have $t_{i_0} \geqslant \gamma(\delta(I) + 1)$.*

For the rest of § 3 we will assume that $k \geqslant 2$ is fixed and that all reducing sequences are k-reducing sequences, if not stated otherwise.

Definition 3.5.

(i) Suppose that $T \in \mathcal{S}$ is k-reducible by some $I \in \mathcal{I}(k)$. Then we define $I[T]$ to be the right-lexicographically maximal k-reducing sequence for T; this sequence may be constructed inductively.

(ii) We define sequences $T^r \in \mathcal{S}$ and $I^r[T] \in \mathcal{I}(k)$ inductively as follows:

$$I^1[T] := I[T] \qquad \text{and} \quad T^1 := T - Z_{I^1[T]}(k; \mathrm{Id}_k)$$

and if $r \geqslant 2$ and T^{r-1} is k-reducible, then

$$I^r[T] := I[T^{r-1}] \quad \text{and} \quad T^r := T^{r-1} - Z_{I^r[T]}(k; \mathrm{Id}_k).$$

(iii) Suppose that n is the largest index for which $I^n[T]$ is defined. Then we set $\bar{I}[T] := \{I^1[T], \dots, I^n[T]\}$. For $1 \leqslant r \leqslant n$ we define q_r to be i_0^r, the 0th coordinate of $I^r[T]$, and we set $\bar{Q}[T] := \{q_1, \dots, q_n\}$. It will also be convenient to set $q_0 := \mathrm{len}(T)$ and to write $\bar{Q}^+[T] := \{q_0, q_1, \dots, q_n\}$. Finally, we define $\bar{\Delta}[T] := \{\delta(I^1[T]), \dots, \delta(I^n[T])\}$.

Assume now that every term of T is less than $\gamma(k)$; this implies that $i_0^r < i_{k-1}^r$ for $1 \leqslant r \leqslant n$. Since the right-lexicographical maximality of $I^r[T]$ implies that $i_{k-1}^r \leqslant i_0^{r-1}$, we find that $q_r < q_{r-1}$ for $1 \leqslant r \leqslant n$ and that all entries of $I^r[T]$ lie in the interval $[q_r, q_{r-1}]$.

We summarize some consequences of the above paragraph for future reference.

Lemma 3.6. *Suppose that every term of T is less than $\gamma(k)$.*

(i) *If I is any k-reducing sequence of T, then $\delta(I) < k - 1$.*

Furthermore, for $1 \leqslant r \leqslant n$ we have

(ii) $q_r < q_{r-1}$,

(iii) $t_{q_r}^r = t_{q_r} - \gamma(\delta(I^r[T]) + 1)$, *where $t_{q_r}^r$ is the q_rth component of T^r,*

(iv) $I^r[T] = I[T^{r-1}\{1, q_{r-1}\}] = I[T^{r-1}\{q_r, q_{r-1}\}]$.

We will see in Proposition 3.9 that not just any descending sequence of positive integers qualifies as $\bar{Q}^+[T]$ for some $T \in \mathcal{S}$. Instead, there is a condition on the maximal length of 'runs' appearing in $\bar{Q}^+[T]$ as follows.

Definition 3.7. Let $\bar{Q}^+ = \{q_0, q_1, \dots, q_s\}$ be a sequence of integers. A run of length m starting from q_r is a subsequence $\{q_r, \dots, q_{r+m-1}\}$ of $\bar{Q}^+$ with the property that $q_{t+1} = q_t - 1$ for all $r + m - 1 > t \geqslant r$. Furthermore, if $r > 1$ then we require that $q_{r-1} - 1 > q_r$, and if $s > r + m - 1$ we require that $q_{r+m-1} - 1 > q_{r+m}$. The run starting from q_0 will be referred to as the initial run, any other run will be called non-initial.

For the proof of Proposition 3.9 below we will need an estimate for the δ appearing in the sequence $\bar{\Delta}[T]$ associated to $T \in \mathcal{S}$.

Lemma 3.8. *Let $T \in \mathcal{S}$ be of length L. Assume that $t_i < \gamma(k)$ for all i and choose $1 \leqslant j \leqslant k$ such that $\gamma(k) - \gamma(j) \leqslant t_L < \gamma(k) - \gamma(j-1)$. Write $\bar{\Delta}[T] =: \{\delta_1, \dots, \delta_n\}$ and suppose that $\{q_r, q_{r+1}, \dots, q_{r+m-1}\} \subset \bar{Q}^+[T]$ is a run of length m. Then for $0 \leqslant \nu \leqslant m-1$ we have*

$$\delta_{r+\nu} \geqslant \begin{cases} \nu, & \text{if } r > 0, \\ j + \nu - 2, & \text{if } r = 0 \text{ and } 0 < \nu. \end{cases}$$

If $r = 0$ and $0 < \nu$, then the minimal value of δ_ν is achieved if and only if

$$t_{q_{\hat{\nu}}} \geqslant \gamma(k) - (p-1)\gamma(\hat{\nu} + j - 1) - 1 \quad \text{for all } 1 \leqslant \hat{\nu} < \nu;$$

if $r > 0$, the minimal value of $\delta_{r+\nu}$ is achieved if and only if $\delta_r = 0$ and

$$t_{q_{r+\hat{\nu}}} \geqslant \gamma(k) - (p-1)\gamma(\hat{\nu} + 1) - 1 \qquad \text{for all } 0 \leqslant \hat{\nu} < \nu.$$

Proof. The proof is by induction on ν and is left to the reader. □

Now the condition on the maximal length of 'runs' appearing in $\bar{Q}^+[T]$ that was announced earlier on is the following.

Proposition 3.9. *We fix integers $n \geqslant 0$, $L > 0$, and $1 \leqslant j \leqslant k$ and choose a sequence $\bar{Q}^+ = \{L = q_0, q_1, \dots, q_n\}$. Assume that there exists a $T \in \mathcal{S}$ for which $\bar{Q}^+ = \bar{Q}^+[T]$; assume further that $t_L < \gamma(k) - \gamma(j-1)$ and that the other terms of T are less than $\gamma(k)$. Then $\bar{Q}^+$ contains no non-initial runs of length greater than $k-1$. Moreover, $\bar{Q}^+$ contains no initial run of length greater than $k - j + 1$.*

Proof. Suppose that we have a run of length m in $\bar{Q}^+$ starting from q_r, and write $\bar{\Delta}[T] =: \{\delta_1, \dots, \delta_n\}$. By Lemma 3.8, we have $\delta_{r+m-1} \geqslant m - 1$ if $r > 0$, and $\delta_{r+m-1} \geqslant j + m - 3$ if $r = 0$ and $m > 1$. The conclusions follow from Lemma 3.4, which states that we must have $\gamma(\delta_{r+m-1} + 1) \leqslant t_{q_{r+m-1}} < \gamma(k)$. □

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

3.2. The subsets $\mathcal{F}$, $\mathcal{H}$ and $\mathcal{W}$ of $\mathcal{S}$ and their maximal elements

We start with the subset $\mathcal{F}$ of $\mathcal{S}$.

Lemma 3.10. *For fixed integers (ζ, j, e, q, L) with $L > 0$, $1 \leqslant j \leqslant k$, $0 \leqslant e < p^{j-1}$, $0 \leqslant \zeta \leqslant j-1$, and $0 \leqslant q \leqslant L-1$, let $\mathcal{F} = \mathcal{F}(\zeta, j, e, q, L)$ be the set of all sequences $F \in \mathcal{S}$ for which*

(i) *F has length $\leqslant L$,*

(ii) *$f_L = \gamma(k) - \gamma(j) + e$,*

(iii) *F is (k, ζ)-irreducible, and*

(iv) *$f_i = 0$ for $1 \leqslant i \leqslant q$.*

Define $\tilde{F} = \tilde{F}(\zeta, j, e, q, L) \in \mathcal{S}$ by

$$\tilde{f}_n = \begin{cases} \gamma(k) - \gamma(j) + e, & \text{if } n = L, \\ \gamma(j) - \gamma(\zeta) - 1, & \text{if } n = L-1 \text{ and } q < L-1, \\ p^{\zeta} - 1, & \text{if } q < n < L-1, \\ 0, & \text{otherwise.} \end{cases}$$

Then $\tilde{F} \in \mathcal{F}$, and for any $F \in \mathcal{F}$ we have $|F| \leqslant |\tilde{F}|$.

Proof. It is clear that $\tilde{F}$ belongs to $\mathcal{F}$. In order to see that $|F| \leqslant |\tilde{F}|$ for any $F \in \mathcal{F}$, we first consider the case $f_L = 0$, or equivalently $j = k$ and $e = 0$. In this case the claim can easily be proved by induction on L. For general sequences $F \in \mathcal{F}$, note that the condition $f_L = \gamma(k) - \gamma(j) + e$ implies that $F\{1, L-1\}$ is (j, ζ)-irreducible. Hence $F\{1, L-1\}$ satisfies the conditions of the lemma with k replaced by j, and since the Lth coordinate of $F\{1, L-1\}$ is zero, we can apply the case that has already been proved. The details are left to the reader. □

Below we will see that Lemma 3.10 provides us with a condition on those sequences $T \in \mathcal{S}$ such that the associated Milnor basis element $M[T]$ can possibly appear in $\hat{\mathrm{P}}(k; f)$. First we recall a result from [**4**, Corollary 4.7] as follows.

Proposition 3.11. *Let $s \geqslant 1$ and $t \geqslant 0$. If $\gamma(t) \leqslant f < \gamma(t+1)$, then the operations $\hat{\mathrm{P}}[s; f]$ are all of length exactly t, independent of s.*

Using this result, we derive from Lemma 3.10 the following condition.

Proposition 3.12. *Fix positive integers $k \geqslant 2$ and $f \geqslant 1$, and let $T \in \mathcal{S}$ be a sequence such that $M[T]$ has non-trivial coefficient in the Milnor basis representation of $\hat{\mathrm{P}}(k; f)$. Then T is k-reducible.*

Proof. Let $\Omega := \mathrm{len}(T)$, and suppose that T is k-irreducible. Applying Lemma 3.10 with $(\zeta, j, e, q, L) = (0, k, 0, 0, \Omega + 1)$, we then obtain

$$|T| \leqslant |\tilde{F}(0, k, 0, 0, \Omega + 1)| = (p^{\Omega} - 1)(\gamma(k) - 1).$$

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

On the other hand we know that $2|T| = |\hat{\mathrm{P}}(k; f)| = 2(p^k - 1)f$, so that $(p^k - 1)f = |T| < (p^{\Omega} - 1)\gamma(k)$. Hence $(p - 1)f < (p^{\Omega} - 1)$, and so $f < \gamma(\Omega)$. By Proposition 3.11 this implies that $\mathrm{len}(T) < \Omega$, contradicting the definition of Ω. □

Next we introduce the subset $\mathcal{H}$ of $\mathcal{S}$.

Lemma 3.13. *For fixed integers (j, e, q, L) with $1 \leqslant q \leqslant L - 1$, $1 \leqslant j \leqslant k$, and $0 \leqslant e < p^{j-1}$, let $\mathcal{H} = \mathcal{H}(j, e, q, L)$ be the set of all sequences $H \in \mathcal{S}$ for which*

(i) *H has length $\leqslant L$,*

(ii) *$h_i = 0$ for $1 \leqslant i \leqslant q - 1$,*

(iii) *$h_L = \gamma(k) - \gamma(j) + e$,*

(iv) *$H\{q + 1, L\}$ is k-irreducible, and*

(v) *$H\{q, L\}$ is k-reducible and $h_q = \gamma(\delta(I[H]) + 1)$, so that after reducing by $I[H]$ we have $h_q^1 = 0$.*

Let

$$\tilde{\delta} := \begin{cases} j - 1, & \text{if } q = L - 1, \\ 0, & \text{if } q < L - 1, \end{cases}$$

and define $\tilde{H} = \tilde{H}(j, e, q, L)$ by

$$\tilde{H} := B(q) + \tilde{F}(0, j, e, 0, L).$$

Then $\delta(I[\tilde{H}]) = \tilde{\delta}$ and $\tilde{H} \in \mathcal{H}$. Moreover, for any $H \in \mathcal{H}$, we have $|H| \leqslant |\tilde{H}|$ and $\tilde{\delta} \leqslant \delta(I[H])$.

Proof. Note that we can rewrite $\tilde{H}$ as $B(q) + (\gamma(j) - 1)B(L - 1) + (\gamma(k) - \gamma(j) + e)B(L)$; from this description it is easily verified that $\delta(I[\tilde{H}]) = \tilde{\delta}$ and $\tilde{H} \in \mathcal{H}$.

Next we prove the inequalities: if $q = L - 1$ then one observes that the assumptions force $H = \tilde{H}$, so we are done. On the other hand, if $q \leqslant L - 2$ then $\tilde{\delta} = 0$ and so obviously $\tilde{\delta} \leqslant \delta(I[H]) =: \delta$. Furthermore, $H\{q + 1, L\}$ is (k, δ)-irreducible, so, by Lemma 3.10, $|H\{q + 1, L\}| \leqslant |\tilde{F}(\delta, j, e, q, L)|$. Now a short calculation shows that $|H| = |\gamma(\delta + 1)B(q)| + |H\{q + 1, L\}| \leqslant |\tilde{H}|$. □

Now we fix integers (j, e, L) with $L > 0$, $1 \leqslant j \leqslant k$, and $0 \leqslant e < p^{j-1}$, and a sequence $\bar{Q} = \{q_1, \ldots, q_n\}$ such that $\bar{Q}^+ = \{L, q_1, \ldots, q_n\}$ satisfies the conditions of Proposition 3.9 for the given parameters. We define a sequence $\bar{\Delta} = \{\delta_1, \ldots, \delta_n\}$ as follows: each q_c, $1 \leqslant c \leqslant n$, belongs to a unique run. We write $r(c)$ for the index of the initial term of the run to which q_c belongs, and set $\nu(c) := c - r(c)$. Hence q_c is the $(\nu(c) + 1)$th member in the run starting at $q_{r(c)}$; note that $\nu(c)$ could be zero if the run starts at q_c itself.

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

We define δ_c for $1 \leqslant c \leqslant n$ by

$$\delta_c := \begin{cases} \nu(c), & \text{if } r(c) > 0, \\ j + \nu(c) - 2, & \text{if } r(c) = 0; \end{cases} \tag{3.1}$$

the conditions of Proposition 3.9 ensure that $\delta_c < k - 1$ for $1 \leqslant c \leqslant n$ (cf. Lemma 3.6 (i)).

With $\bar{\Delta}$ at hand, we define the sequence $\tilde{W}(j, e, \bar{Q}, L) \in \mathcal{S}$ by

$$\tilde{W}(j, e, \bar{Q}, L) := \begin{cases} \tilde{F}(0, j, e, 0, L), & \text{if } n = 0, \\ \tilde{H}(j, e, q_1, L) + \displaystyle\sum_{r=1}^{n-1} \tilde{H}(\delta_r + 2, p^{\delta_r + 1} - 1, q_{r+1}, q_r) & \\ \qquad\qquad + \tilde{F}(0, \delta_n + 2, p^{\delta_n + 1} - 1, 0, q_n), & \text{if } n > 0 \end{cases}$$

(notice that $n > 0$ implies $L > 1$ so that the definition makes sense).

It will be useful to have an explicit description of the entries of $\tilde{W}(j, e, \bar{Q}, L) =: \tilde{W}$. If $\bar{Q} = \emptyset$ this description has been given in Lemma 3.10; for $\bar{Q} \neq \emptyset$ one has to assemble the different pieces in the definition of $\tilde{W}(j, e, \bar{Q}, L)$, which leads to the following formula:

$$\tilde{w}_i = \begin{cases} \gamma(k) - \gamma(j) + e, & \text{if } i = L, \\ \gamma(k) - 1, & \text{if } i = q_r \text{ for some } 1 \leqslant r \leqslant n, \\ \gamma(m+1) - 1, & \text{if for some } 0 < r \leqslant n \text{ there is a run of length } m \\ & \text{starting from } q_r \text{ and terminating in } q_{r+m-1} = i + 1, \\ \gamma(j + m - 1) - 1, & \text{if the initial run starting from } q_0 \text{ has length} \\ & m \text{ and terminates in } q_{m-1} = i + 1, \\ 0, & \text{otherwise.} \end{cases} \tag{3.2}$$

Examples 3.14. It is instructive to visualize the definition of $\tilde{W}(j, e, \bar{Q}, L)$ with a few examples.

(1) Let $(k, j, e, L) = (5, 2, 2, 7)$ and $\bar{Q} = \{q(1) = 6,\ q(2) = 5,\ q(3) = 2\}$. Then $\bar{Q}^+ = \{q(0) = 7,\ q(1) = 6,\ q(2) = 5,\ q(3) = 2\}$, so that we have two runs: the initial one of length 3 starting from $q(0) = 7$ and terminating in $q(2) = 5$, and one other run of length 1 starting from and also terminating in $q(3) = 2$. The sequence $\tilde{W}(j, e, \bar{Q}, L)$ looks like

$$(\gamma(2) - 1, \gamma(5) - 1, 0, \gamma(4) - 1, \gamma(5) - 1, \gamma(5) - 1, \gamma(5) - \gamma(2) + 2).$$

(2) Let $(k, j, e, L) = (8, 1, 0, 4)$ and $\bar{Q} = \{q(1) = 3,\ q(2) = 2,\ q(3) = 1\}$. Then $\bar{Q}^+ = \{q(0) = 4,\ q(1) = 3,\ q(2) = 2,\ q(3) = 1\}$, so that we have only one run, the initial one of length 4 starting from $q(0) = 4$ and terminating in $q(3) = 1$. The sequence $\tilde{W}(k, j, e, \bar{Q}, L)$ looks like

$$(\gamma(8) - 1, \gamma(8) - 1, \gamma(8) - 1, \gamma(8) - 1).$$

The following facts are easily verified.

Lemma 3.15. *Let L, j, e, $\bar{Q}$ and $\bar{\Delta}$ be as above.*

(i) $\bar{Q}[\tilde{W}(j,e,\bar{Q},L)] = \bar{Q}$ *and* $\bar{\Delta}[\tilde{W}(j,e,\bar{Q},L)] = \bar{\Delta}$.

(ii) *Suppose that* $\bar{Q} \neq \emptyset$. *Let* $\bar{Q}_2 := \{q_2,\dots,q_n\}$ *and* $\tilde{\delta} := \delta(I[\tilde{H}(j,e,q_1,L)])$. *Then* $\tilde{\delta} = \delta_1$ *and* $\tilde{W}(j,e,\bar{Q},L) = \tilde{W}(\tilde{\delta}+2, p^{\tilde{\delta}+1}-1, \bar{Q}_2, q_1) + \tilde{H}(j,e,q_1,L)$.

We now investigate some properties of the degrees of the sequences $\tilde{W}(j,e,\bar{Q},L)$.

Lemma 3.16. *Fix $L > 0$ and a sequence $\bar{Q} = \{q_1,\dots,q_n\}$ of positive integers. Denote by J the set of all those j with $1 \leqslant j \leqslant k$ such that the parameters $(n,j,L,\bar{Q}^+)$ satisfy the conditions of Proposition 3.9; we assume that $J \neq \emptyset$. Then*

(i) *for fixed $j \in J$, the degree $|\tilde{W}(j,e,\bar{Q},L)|$ is a strictly increasing function of e with $0 \leqslant e < p^{j-1}$,*

(ii) *the degree $|\tilde{W}(j,p^{j-1}-1,\bar{Q},L)|$ is a strictly decreasing function of $j \in J$, and*

(iii) *for all $j \in J$ and $0 \leqslant e < p^{j-1}$ we have*

$$|\tilde{W}(j,e,\bar{Q},L)| \leqslant \gamma(k)\sum_{r=1}^{n}(p^{q_r}-1) + (\gamma(k)-p^{j-1}+e)(p^L-1);$$

the inequality is strict unless $n = 0$ and $j = 1$.

Proof. Part (i) follows immediately from (3.2). To prove part (ii), choose $j_1, j_2 \in J$ with $1 \leqslant j_1 < j_2 \leqslant k$; then for $i = 1,2$ the sequence $\tilde{W}_i := \tilde{W}(j_i, p^{j_i-1}-1, \bar{Q}, L)$ is defined. Let m be the length of the initial run of $\bar{Q}^+$. If $m = L$ then $\tilde{W}_1$ and $\tilde{W}_2$ differ only in the Lth place, and it follows immediately from Formula (3.2) that $|\tilde{W}_1| > |\tilde{W}_2|$. If $m < L$ then $\tilde{W}_1$ and $\tilde{W}_2$ differ in the Lth and $(L-m)$th places, and a short calculation reveals that $|\tilde{W}_1| - |\tilde{W}_2| > 0$, proving part (ii).

The third part of the lemma is proved by induction on n. The case $n = 0$ follows easily from the definition, since in this case $\tilde{W}(j,e,\emptyset,L)$ is defined to be $\tilde{F}(0,j,e,0,L)$. For the general case, recall from Lemma 3.15 (ii) that $\tilde{W}(j,e,\bar{Q},L)$ can be rewritten as the sum of $\tilde{W}(\tilde{\delta}+2, p^{\tilde{\delta}+1}-1, \bar{Q}_2, q_1)$ and $\tilde{H}(j,e,q_1,L)$, where $\tilde{\delta} = \delta(I[\tilde{H}(j,e,q_1,L)])$ and $\bar{Q}_2 = \{q_2,\dots,q_n\}$. To complete the proof one applies the inductive hypothesis to $\tilde{W}(\tilde{\delta}+2, p^{\tilde{\delta}+1}-1, \bar{Q}_2, q_1)$ and the case $n = 0$ to $|\tilde{H}(j,e,q_1,L)| = |B(q_1)| + |\tilde{W}(j,e,\emptyset,L)|$. □

As the notation already suggests, the sequence $\tilde{W}(j,e,\bar{Q},L)$ appears as the maximal element (with respect to degree) of a certain subset $\mathcal{W}(j,e,\bar{Q},L)$ of $\mathcal{S}$ which we now define.

Lemma 3.17. *Fix integers (j,e,L) with $L > 0$, $1 \leqslant j \leqslant k$ and $0 \leqslant e < p^{j-1}$. Fix also a sequence $\bar{Q} = \{q_1,\dots,q_n\}$ such that the associated sequence $\bar{Q}^+$ satisfies the conditions of Proposition 3.9 for (n,L,j). Consider the set $\mathcal{W} = \mathcal{W}(j,e,\bar{Q},L)$ of sequences W such that*

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

(i) *W has length $\leqslant L$,*

(ii) *$w_i < \gamma(k)$ for $1 \leqslant i \leqslant L$,*

(iii) *$w_L = \gamma(k) - \gamma(j) + e$, and*

(iv) *$\bar{Q}[W] = \bar{Q}$.*

Let $\tilde{W} = \tilde{W}(j, e, \bar{Q}, L)$ as defined above. Then $\tilde{W} \in \mathcal{W}$ and $|W| \leqslant \tilde{W}$ for all $W \in \mathcal{W}$.

Proof. That $\tilde{W} \in \mathcal{W}$ follows from the explicit description given in equation (3.2) and Lemma 3.15 (i). The inequality will be proven by induction on n. Suppose that $n = 0$, and choose $W \in \mathcal{W}$. Then W is k-irreducible, which is to say $(k, 0)$-irreducible, so

$$|W| \leqslant |\tilde{F}(0, j, e, 0, L)| = |\tilde{W}(j, e, \emptyset, L)|$$

by Lemma 3.10 and the definition of $\tilde{W}(j, e, \bar{Q}, L)$. This proves the lemma for $n = 0$.

Now let $n \geqslant 1$ and suppose that the result is known for $0 \leqslant \hat{n} \leqslant n-1$. Choose $W \in \mathcal{W}$, and set $\delta := \delta(I[W])$. By definition of W^1 and by Lemma 3.6, we have

$$w_i^1 = \begin{cases} w_{q_1} - \gamma(\delta + 1), & \text{for } i = q_1, \\ w_i, & \text{for } i < q_1. \end{cases}$$

We can now write

$$W = W^1\{1, q_1\} + [\gamma(\delta + 1)B(q_1) + W\{q_1 + 1, L\}]. \tag{3.3}$$

For typographical convenience denote the sum in brackets by P; then $I[P] = I[W]$. Evidently $P \in \mathcal{H}(j, e, q_1, L)$ as in Lemma 3.13, and so is no greater in degree than $\tilde{H}(j, e, q_1, L)$. Let $\tilde{\delta} := \delta(I[\tilde{H}(j, e, q_1, L)])$; since $\delta(I[P]) = \delta(I[W]) = \delta$, Lemma 3.13 further implies that $\delta \geqslant \tilde{\delta}$.

We now turn our attention to the first summand in (3.3). Since, by assumption, $w_{q_1} < \gamma(k)$, we find that

$$\begin{aligned} w_{q_1}^1 &= w_{q_1} - \gamma(\delta + 1) \\ &\leqslant (\gamma(k) - 1) - \gamma(\tilde{\delta} + 1) \\ &= \gamma(k) - \gamma(\tilde{\delta} + 2) + (p^{\tilde{\delta}+1} - 1); \end{aligned} \tag{3.4}$$

this maximum value is achieved only if δ takes its minimum possible value, $\tilde{\delta}$, and w_{q_1} takes its maximum possible value, $\gamma(k) - 1$. Define j' and e' by $w_{q_1}^1 =: \gamma(k) - \gamma(j') + e'$ with $1 \leqslant j' \leqslant k$ and $0 \leqslant e' < p^{j'-1}$; by (3.4), we must have $j' \geqslant \tilde{\delta} + 2$.

Let $\bar{Q}_2 := (q_2, \ldots, q_n)$. From the definition of $\bar{Q}[T]$ and from Lemma 3.6 (iv) we find that $\bar{Q}_2 = \bar{Q}[W^1\{1, q_1\}]$; hence $W^1\{1, q_1\} \in \mathcal{W}(j', e', \bar{Q}_2, q_1)$, so that the inductive hypothesis implies that $|W^1\{1, q_1\}| \leqslant |\tilde{W}(j', e', \bar{Q}_2, q_1)|$. In particular, we have $\bar{Q}_2 = \bar{Q}[\tilde{W}^1\{1, q_1\}]$, and since $w_{q_1}^1 \leqslant \gamma(k) - \gamma(\tilde{\delta} + 2) + (p^{\tilde{\delta}+1} - 1)$ by (3.4), we know

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

that $\bar{Q}_2^+$ satisfies the conditions of Proposition 3.9 for $(L, j) = (q_1, \tilde{\delta} + 2)$. Hence both parts (i) and (ii) of Lemma 3.16 are applicable and now imply that

$$|\tilde{W}(j', e', \bar{Q}_2, q_1)| \leqslant |\tilde{W}(\tilde{\delta} + 2, p^{\tilde{\delta}+1} - 1, \bar{Q}_2, q_1)|.$$

Since $\tilde{H}(j, e, q_1, L)$ and $\tilde{W}(\tilde{\delta} + 2, p^{\tilde{\delta}+1} - 1, \bar{Q}_2, q_1)$ add up to $\tilde{W}(j, e, \bar{Q}, L)$ by Lemma 3.15 (ii), we obtain $|W| \leqslant |\tilde{W}(j, e, \bar{Q}, L)|$ as claimed. □

3.3. *k*-reductions of small degree

We now use the results obtained in the first two parts of this section in order to prove the following result.

Proposition 3.18. *Let $T \in \mathcal{S}$ and assume that T is not of the form $\gamma(k)S$ for some $S \in \mathcal{S}$. Let L be the largest index n for which t_n is not divisible by $\gamma(k)$. Then T has a (possibly trivial) k-reduction $[U; P]$ of degree less than $\gamma(k)(p^L - 1)$ with $u_L > 0$.*

Proof. If T is k-irreducible, then by Lemma 3.10 we have

$$|T| \leqslant |\tilde{F}(0, k, 0, 0, L + 1)| = (p^L - 1)(\gamma(k) - 1) < \gamma(k)(p^L - 1),$$

so the trivial reduction $[T; 0_{\mathcal{S}}]$ satisfies the requirements of the proposition. Otherwise, we may assume, after reducing by constant sequences if necessary, that $t_i < \gamma(k)$ for all i, and consequently that T has length L. We write the leading term as $t_L = \gamma(k) - \gamma(j) + e$ for some $1 \leqslant j \leqslant k$ and $0 \leqslant e < p^{j-1}$.

If $e > 0$, then the U-term of any k-reduction of T has $u_L > 0$; this follows directly from the definitions. Write $\bar{Q}[T] =: \{q_1, \dots, q_n\}$. Then $T \in \mathcal{W}(j, e, \bar{Q}[T], L)$ as in Lemma 3.17, so by Lemmas 3.16 and 3.17 we find that

$$|T| \leqslant \gamma(k) \sum_{r=1}^{n} (p^{q_r} - 1) + (\gamma(k) - p^{j-1} + e)(p^L - 1).$$

Lemma 3.2 then implies that the reduction $[U; P]$ of T by $\bar{I}[T]$ satisfies

$$|[U; P]| \leqslant (\gamma(k) - p^{j-1} + e)(p^L - 1) \leqslant (\gamma(k) - 1)(p^L - 1),$$

since $e \leqslant p^{j-1} - 1$. This proves the proposition in the case $e > 0$.

If $e = 0$, then the U-term resulting from reducing T by $\bar{I}[T]$ has leading term 0, so the preceding argument will not work. Instead let $S := T - p^j B(L)$. Observe that if S is k-reducible, then T is k-reducible, although not optimally, by $\bar{I} := \bar{I}[S]$. Let $[V; P]$ be some k-reduction of S by $\bar{I}$; if S is k-irreducible we understand $[V; P]$ to be $[S; 0_{\mathcal{S}}]$. The corresponding k-reduction of T by $\bar{I}$ is $[U; P] = [V + p^j B(L); P]$, so that U has leading term $u_L \geqslant p^j$, with equality holding if S is k-reducible or if $j = k - 1$.

To estimate $|[U; P]|$, write $\bar{Q}[S] =: \{q_1, \dots, q_n\}$. We have $s_i = 0$ for $i > L$ and $s_L = \gamma(k) - \gamma(j + 1)$, so that $S \in \mathcal{W}(j + 1, 0, \bar{Q}[S], L)$ as in Lemma 3.17. By Lemmas 3.16 and 3.17, we find that

$$|S| < \gamma(k) \sum_{r=1}^{n} (p^{q_r} - 1) + (\gamma(k) - p^j)(p^L - 1)$$

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

(note that we have strict inequality since $j+1>1$). Lemma 3.2 then implies that

$$|[V;P]| < (\gamma(k)-p^j)(p^L-1),$$

so that

$$\begin{aligned}|[U;P]| &= |p^jB(L)| + |[V;P]| \\ &< p^j(p^L-1) + (\gamma(k)-p^j)(p^L-1) \\ &= \gamma(k)(p^L-1),\end{aligned}$$

which completes the proof of the proposition. □

4. *k*-reductions and stripping

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

The stripping technique is a process that can be applied to any Hopf algebra, in particular to the Steenrod algebra $\mathcal{A}^*$ or to the sub-Hopf algebra $\mathcal{P}^*$ that we are working with. It was studied in detail in [**7**] and [**4**]. Let Δ^* denote the diagonal map of $\mathcal{P}^*$ and $\langle\cdot,\cdot\rangle$, the inner product. Using the maps

$$\mathcal{P}^* \xrightarrow{\Delta^*} \mathcal{P}^* \otimes \mathcal{P}^* \xrightarrow{\mathrm{id}\otimes\langle\xi,\cdot\rangle} \mathcal{P}^*$$

we associate to each element $\xi \in \mathcal{P}_*$ an endomorphism $D(\xi)$ of the graded vector space $\mathcal{P}^*$; this endomorphism is determined by

$$\theta \mapsto \sum\langle\xi,\theta''\rangle\theta', \quad \text{where } \Delta^*(\theta) =: \sum\theta'\otimes\theta''.$$

One easily verifies that $D(\xi)$ satisfies $\langle\xi\cdot\varphi,\theta\rangle = \langle\varphi, D(\xi)\theta\rangle$ for all $\varphi\in\mathcal{P}_*$ and $\theta\in\mathcal{P}^*$.

Since the construction is analogous to the construction of the cap-product of a cohomology class ξ with a homology class θ, the notation

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

has become customary. With this notation we have

$$\langle\xi[S+T],\hat{\theta}\rangle = \langle\hat{\xi}[S+T],\theta\rangle = \langle\hat{\xi}[S],\hat{\xi}[T]\cap\theta\rangle;$$

in particular, if $|T|=|\theta|$ then $\langle\xi[T],\hat{\theta}\rangle = \langle 1,\hat{\xi}[T]\cap\theta\rangle$. This implies that $M[T]$ appears in $\hat{\theta}$ with coefficient $c\in\mathbb{F}_p$ if and only if $\hat{\xi}[T]\cap\theta = c$.

In what follows, let $\phi_*:\mathcal{P}_*\to\mathcal{P}_*\otimes\mathcal{P}_*$ denote the comultiplication of $\mathcal{P}_*$; we write $\phi_*(y) =: \sum y'\otimes y''$.

Proposition 4.1 (see [7]). *The stripping operations have the following properties:*

(i) $(y_1+y_2)\cap\theta = y_1\cap\theta + y_2\cap\theta$,

(ii) $(y_1\cdot y_2)\cap\theta = (y_2\cdot y_1)\cap\theta = y_1\cap(y_2\cap\theta) = y_2\cap(y_1\cap\theta)$,

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

(iii) $y \cap (\theta_1 \cdot \theta_2) = \sum (y' \cap \theta_1) \cdot (y'' \cap \theta_2)$,

(iv) $\hat{y} \cap (\theta_1 \cdot \theta_2) = \sum (\widehat{y''} \cap \theta_1) \cdot (\widehat{y'} \cap \theta_2)$, *and*

(v) $\hat{y} \cap \hat{\theta} = \widehat{y \cap \theta}$

Since the comultiplication $\varDelta^*$ in $\mathcal{P}^*$ is determined by the formula

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

(see [**6**]), it follows directly from the definitions that for any $R, S \in \mathcal{S}$ we have

$$\xi[R] \cap M[S] = M[S-R]. \tag{4.1}$$

Thus stripping in $\mathcal{P}^*$ can be described very easily if we are working in the Milnor basis. From (4.1) it follows in particular that stripping does not increase length, and one easily deduces the following property.

Lemma 4.2. *If $\theta \in \mathcal{P}^*$ has length n, then $\xi_k \cap \theta = 0$ for all $k > n$.*

If we are working in the admissible basis things become slightly more complicated. For the following results, see [**4**, Corollary 3.3].

Lemma 4.3.

(1) *If* $\mathrm{P}(a_1) \cdot \dots \cdot \mathrm{P}(a_k)$ *is admissible of excess* $2e$, *then*

$$\xi_k \cap (\mathrm{P}(a_1) \cdot \dots \cdot \mathrm{P}(a_k)) = \mathrm{P}(a_1 - p^{k-1}) \cdot \mathrm{P}(a_2 - p^{k-2}) \cdot \dots \cdot \mathrm{P}(a_k - 1),$$

which is again admissible and has excess $2e-2$. *Consequently, if* $R = (r_1, \dots, r_k) \in \mathcal{S}$, *then* $\xi_k \cap E[R] = E[(r_1, \dots, r_{k-1}, r_k - 1)]$.

(2) *In particular,*

$$\xi_k \cap \mathrm{P}[k; f] = \mathrm{P}[k; f-1] \quad \textit{and} \quad \hat{\xi}_k \cap \hat{\mathrm{P}}[k; f] = \hat{\mathrm{P}}[k; f-1].$$

4.2. A divisibility result

For $I \in \mathcal{I}(k)$ and $\tau \in \mathfrak{S}(k)$ we set

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

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

and

$$\mathcal{X}'_I(k) := \sum_{\mathrm{Id}_k \neq \tau \in \mathfrak{S}(k)} \operatorname{sgn}(\tau)\, X_I(k; \tau),$$

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

We will make use of the following formula, which was proved in [**4**, Theorem 5.5].

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

Theorem 4.4. *Let $k \geqslant 1$. Then*

$$\hat{X}_I(k;\mathrm{Id}_k) \equiv (-1)^{i_0 k}\xi_k^{\gamma(i_0)} \cdot \hat{\mathcal{R}}_I(k) - \hat{\mathcal{X}}'_I(k)$$

modulo monomials of length $> k$.

For the rest of this section let $k \geqslant 2$ and $f \geqslant 1$ be fixed, unless stated otherwise. We denote by $W \in \mathcal{S}$ the sequence for which $M[W]$ is maximal with respect to $\succ_M$ among all summands of minimal excess in the Milnor basis representation of $\hat{\mathrm{P}}[k;f]$, and by $\tilde{W} \in \mathcal{S}$ the sequence for which $M[\tilde{W}]$ is maximal with respect to $\succ_M$ among *all* Milnor basis elements appearing in $\hat{\mathrm{P}}[k;f]$. We will now combine the stripping technique reviewed above with the results obtained in § 3. The outcome will be a divisibility result both for W and for $\tilde{W}$.

As we have seen in Proposition 3.12, the sequence W is k-reducible via some sequence $I \in \mathcal{I}(k)$. Since $\mathrm{P}[k;f] = E[(0,\dots,0,r_k = f)]$ is of length exactly k, Theorem 4.4 together with Lemma 4.3 implies

$$\begin{aligned} 0 &\neq \langle \hat{\xi}[W], \mathrm{P}[k;f]\rangle \\ &= \langle \hat{\xi}[W - Z_I(k;\mathrm{Id}_k)], \hat{\xi}[Z_I(k;\mathrm{Id}_k)] \cap \mathrm{P}[k;f]\rangle \qquad (4.2)\\ &= -\langle \hat{\xi}[W - Z_I(k;\mathrm{Id}_k)], \hat{\mathcal{X}}'_I(k) \cap \mathrm{P}[k;f]\rangle \\ &\qquad + (-1)^{i_0 k}\langle \hat{\xi}[W - Z_I(k;\mathrm{Id}_k)], \hat{\mathcal{R}}_I(k) \cap \mathrm{P}[k;f-\gamma(i_0)]\rangle. \qquad (4.3)\end{aligned}$$

We claim that the first summand in (4.3) vanishes. Indeed,

$$\begin{aligned}&\langle \hat{\xi}[W - Z_I(k;\mathrm{Id}_k)], \hat{\mathcal{X}}'_I(k) \cap \mathrm{P}[k;f]\rangle \\ &\qquad = \sum_{\mathrm{Id}_k \neq \tau \in \mathfrak{S}(k)} \mathrm{sgn}(\tau)\langle \hat{\xi}[W - Z_I(k;\mathrm{Id}_k) + Z_I(k;\tau)], \mathrm{P}[k;f]\rangle. \qquad (4.4)\end{aligned}$$

If $Z_I(k;\tau) = *$, then $W - Z_I(k;\mathrm{Id}_k) + Z_I(k;\tau) = *$ and so $\hat{\xi}[W - Z_I(k;\mathrm{Id}_k) + Z_I(k;\tau)] = 0$, so the corresponding summand is zero. On the other hand, it follows directly from the definition that for $\tau \neq \mathrm{Id}_k$ any non-$*$ $Z_I(k;\tau)$ is strictly $\succ$ than $Z_I(k;\mathrm{Id}_k)$ and of the same excess. Thus every non-$*$ term $W - Z_I(k;\mathrm{Id}_k) + Z_I(k;\tau)$ of (4.4) is strictly $\succ$ than W and of the same excess. By definition of W then, none of the elements $M[W - Z_I(k;\mathrm{Id}_k) + Z_I(k;\tau)]$ appears in $\hat{\mathrm{P}}[k;f]$ and each summand in (4.4) vanishes.

We thus obtain

$$0 \neq \langle \hat{\xi}[W - Z_I(k;\mathrm{Id}_k)], \hat{\mathcal{R}}_I(k) \cap \mathrm{P}[k;f-\gamma(i_0)]\rangle, \qquad (4.5)$$

which means that $M[W - Z_I(k;\mathrm{Id}_k)]$ appears in the Milnor basis representation of $\mathcal{R}_I(k) \cap \hat{\mathrm{P}}[k;f-\gamma(i_0)]$. We claim that $W - Z_I(k;\mathrm{Id}_k)$ satisfies conditions analogous to W.

Lemma 4.5. *$M[W - Z_I(k;\mathrm{Id}_k)]$ is maximal with respect to $\succ_M$ among all summands of minimal excess in the Milnor basis representation of $\mathcal{R}_I(k) \cap \hat{\mathrm{P}}[k;f-\gamma(i_0)]$.*

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

Proof. First suppose there is a sequence $T \in \mathcal{S}$ such that $M[T]$ appears in $\mathcal{R}_I(k) \cap \hat{\mathrm{P}}[k; f - \gamma(i_0)]$ but with $\mathrm{ex}(T) < \mathrm{ex}(W - Z_I(k; \mathrm{Id}_k))$. We have

$$\langle \hat{\xi}[T], \hat{\mathcal{X}}'_I(k) \cap \mathrm{P}[k; f] \rangle = \sum_{\mathrm{Id}_k \neq \tau \in \mathfrak{S}(k)} \mathrm{sgn}(\tau) \langle \hat{\xi}[T + Z_I(k; \tau)], \mathrm{P}[k; f] \rangle,$$

which is zero since for any $\mathrm{Id}_k \neq \tau \in \mathfrak{S}(k)$ either $Z_I(k; \tau) = * = T + Z_I(k; \tau)$ or $\mathrm{ex}(T + Z_I(k; \tau)) < \mathrm{ex}(W - Z_I(k; \mathrm{Id}_k) + Z_I(k; \tau)) = \mathrm{ex}(W)$. Thus

$$\begin{aligned} 0 &\neq (-1)^{i_0 k} \langle \hat{\xi}[T], \hat{\mathcal{R}}_I(k) \cap \mathrm{P}[k; f - \gamma(i_0)] \rangle \\ &= \langle \hat{\xi}[T], \hat{X}_I(k; \mathrm{Id}_k) \cap \mathrm{P}[k; f - \gamma(i_0)] \rangle \\ &= \langle \hat{\xi}[T + Z_I(k; \mathrm{Id}_k)], \mathrm{P}[k; f] \rangle. \end{aligned}$$

This means that $M[T + Z_I(k; \mathrm{Id}_k)]$ appears in $\hat{\mathrm{P}}[k; f]$, which is impossible since $\mathrm{ex}(T + Z_I(k; \mathrm{Id}_k)) < \mathrm{ex}(W)$. Hence $M[W - Z_I(k; \mathrm{Id}_k)]$ has minimal excess among all summands in the Milnor basis representation of $\hat{\mathcal{R}}_I(k) \cap \mathrm{P}[k; f - \gamma(i_0)]$. Now suppose there is a sequence $S \in \mathcal{S}$ such that $M[S]$ appears in $\hat{\mathcal{R}}_I(k) \cap \mathrm{P}[k; f - \gamma(i_0)]$, with $\mathrm{ex}(S) = \mathrm{ex}(W - Z_I(k; \mathrm{Id}_k))$ but $S \succ W - Z_I(k; \mathrm{Id}_k)$. Then an argument similar to the one just given again leads to a contradiction. This proves the claim. □

Lemma 4.5 shows that we can iterate the argument that we used in order to arrive at expression (4.5) in the following way: suppose that W is k-reducible by a set of sequences $\bar{I} = \{I(1), \dots, I(n)\}$. Then the reasoning described in equations (4.2) and (4.3) can be applied successively to each sequence $I(r)$, $1 \leqslant r \leqslant n$, where each time the summand involving stripping by $\hat{\mathcal{X}}'_{I(r)}(k)$ vanishes. The end result in this case is

$$0 \neq \left\langle \hat{\xi}\left[W - \sum_{r=1}^{n} Z_{I(r)}(k; \mathrm{Id}_k)\right], \left(\prod_{r=1}^{n} \hat{\mathcal{R}}_{I(r)}(k)\right) \cap \mathrm{P}\left[k; f - \sum_{r=1}^{n} \gamma(i_0(r))\right] \right\rangle.$$

Since

$$\prod_{r=1}^{n} \hat{\mathcal{R}}_{I(r)}(k) = \sum_{\sigma_1 \in \mathfrak{S}(k)} \cdots \sum_{\sigma_n \in \mathfrak{S}(k)} \prod_{r=1}^{n} (\mathrm{sgn}(\sigma_r) \hat{R}_{I(r)}(k; \sigma_r)),$$

we know that for some parameter $\bar{\tau} = \{\tau_1, \dots, \tau_n\} \subset \mathfrak{S}(k)$ we have

$$\begin{aligned} 0 &\neq \left\langle \hat{\xi}\left[W - \sum_{r=1}^{n} Z_{I(r)}(k; \mathrm{Id}_k)\right], \left(\prod_{r=1}^{n} \hat{R}_{I(r)}(k; \tau_r)\right) \cap \mathrm{P}\left[k; f - \sum_{r=1}^{n} \gamma(i_0(r))\right] \right\rangle \\ &= \left\langle \hat{\xi}\left[W - \sum_{r=1}^{n} Z_{I(r)}(k; \mathrm{Id}_k) + \sum_{r=1}^{n} P_{I(r)}(k; \tau_r)\right], \mathrm{P}\left[k; f - \sum_{r=1}^{n} \gamma(i_0(r))\right] \right\rangle. \end{aligned}$$

We write

$$U := W - \sum_{r=1}^{n} Z_{I(r)}(k; \mathrm{Id}_k) \quad \text{and} \quad P := \sum_{r=1}^{n} P_{I(r)}(k; \tau_r).$$

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

Then $[U;P]$ is a k-reduction of W via $\bar{I}$ and $\bar{\tau}$, and the Milnor basis element $M[U+P]$ appears with non-trivial coefficient in $\hat{\mathrm{P}}[k; f - \sum_{r=1}^{n} \gamma(i_0(r))]$.

Our results are summarized in Proposition 4.6, where we separately treat the constant and the non-constant sequences in $\bar{I}$. First observe that if $T \in \mathcal{S}$ is written in the form $T = \gamma(k)G + H$ for some $G, H \in \mathcal{S}$, then, by Observation 3.3 (ii), $(H; 0_{\mathcal{S}})$ is the unique k-reduction of T via the constant sequences corresponding to the entries of G. Also note that if $M[T]$ appears in $\hat{\mathrm{P}}[k; f]$, then $|T| = (p^k - 1)f$, and so, by Lemma 3.2, we know that $|H| = (p^k - 1)\eta$ for some non-negative integer $\eta \leqslant f$.

Proposition 4.6. *Write $W = \gamma(k)G + H$ with $G, H \in \mathcal{S}$, so that $|H| = (p^k - 1)\eta$ for some $\eta \leqslant f$. Then $M[H]$ appears in $\hat{\mathrm{P}}[k; \eta]$.*

Suppose moreover that H is k-reducible via $\bar{I} = \{I_1, \dots, I_n\}$. Then for some k-reduction $[U;P]$ of H via $\bar{I}$, the Milnor basis element $M[U+P]$ appears in $\hat{\mathrm{P}}[k; \eta - \sum_{r=1}^{n} \gamma(i_0(r))]$.

A similar argument yields the analogous conclusions concerning the sequence $\tilde{W}$.

Finally, we can prove the divisibility result announced earlier on.

Theorem 4.7. *Fix positive integers k and f, and suppose that $W \in \mathcal{S}$ is the sequence for which $M[W]$ is maximal with respect to $\succ_M$ among all summands of minimal excess in the Milnor basis representation of $\hat{\mathrm{P}}[k; f]$. Then $W = \gamma(k)Q$ for some $Q \in \mathcal{S}$ of degree $(p-1)f$. Similarly, if $\tilde{W} \in \mathcal{S}$ is the sequence for which $M[W]$ is maximal with respect to $\succ_M$ among all summands in the Milnor basis representation of $\hat{\mathrm{P}}[k; f]$, regardless of excess, then $\tilde{W} = \gamma(k)\tilde{Q}$ for some $\tilde{Q} \in \mathcal{S}$ of degree $(p-1)f$.*

Proof. For $k = 1$ the theorem is trivial, we may thus assume $k \geqslant 2$. We give the proof for W; the argument for $\tilde{W}$ is identical. Suppose that the theorem is not true, and let L be the largest index i for which w_i is not divisible by $\gamma(k)$. We take $[U;P]$ to be a k-reduction of W via $\bar{I}$ and $\bar{\tau}$ which satisfies the conclusion of Lemma 3.18, namely that $|[U;P]| < \gamma(k)(p^L - 1)$ and $u_L > 0$. Since $|W| = (p^k - 1)f$ and $|[U;P]| \equiv |W|$ modulo $(p^k - 1)$ by Lemma 3.2, we can write $|[U;P]| = (p^k - 1)\phi$ for some $\phi < \gamma(L)$; recall that the degree $|[U;P]|$ is independent of the choice of the parameter $\bar{\tau}$. By Proposition 4.6 we can find a parameter $\bar{\tau}'$ such that for the k-reduction $[U;P']$ corresponding to the parameters $\bar{I}$ and $\bar{\tau}'$ the Milnor basis element $M[U+P']$ appears in $\hat{\mathrm{P}}[k;\phi]$. But by Theorem 3.11 this implies that $U + P'$ has length less than L so that $u_L + p'_L = 0$, contradicting the assumption that $u_L > 0$. We conclude that indeed $w_i \equiv 0$ modulo $\gamma(k)$ for all i. □

5. Proofs of Theorems 1.1 and 1.2 and Proposition 1.3

We split Theorem 1.1 into two parts which will be proved separately. The first half reads as follows.

Theorem 5.1. *Let f and k be positive integers. Then the operation $E[R_k(f)]$ has a non-trivial coefficient in the admissible basis representation of $\hat{\mathrm{P}}[k; f]$. Likewise, the operation $M[R_k(f)]$ has a non-trivial coefficient in the Milnor basis representation of $\hat{\mathrm{P}}[k; f]$. Consequently $\mathrm{ex}(\hat{\mathrm{P}}[k; f]) \leqslant 2\gamma(k)\mu(f)$.*

Remark 5.2. The proof of this result is modelled on the proof of [**7**, Theorem 4]. In fact, only the 'admissible version' of the theorem is proved there, although exactly the same strategy works for the 'Milnor version'. This is particularly noteworthy since in [**8**, Theorem 9.1] the (mod 2) Milnor version is quoted and used.

For the proof we need the following two results, which were proved in [**4**, Theorem 4.6] and [**4**, Theorem 5.6], respectively.

Theorem 5.3. *For all positive integers s, t and c with $1 \leqslant c \leqslant p$ the following conjugation formula holds:*

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

Theorem 5.4. *Let $k, s > 0$. If $f < \gamma(s+1)$ is a non-negative integer, then*

$$\hat{\xi}_s^{\gamma(k)} \cap \mathrm{P}[k; f] = (-1)^{ks}\xi_k^{\gamma(s)} \cap \mathrm{P}[k; f] = (-1)^{ks}\,\mathrm{P}[k; f - \gamma(s)].$$

Proof of Theorem 5.1. If f is of the form $c\gamma(t)$ with $1 \leqslant c \leqslant p$ and $t \geqslant 1$, then by Theorem 5.3 we have

$$\hat{\mathrm{P}}[k; c\gamma(t)] = (-1)^{tkc}\,\mathrm{P}[t; c\gamma(k)] = (-1)^{tkc}E[R_k(c\gamma(t))].$$

Additionally, we know that $M[R_k(c\gamma(t))]$ appears in the Milnor basis representation of $E[R_k(c\gamma(t))]$, so both parts of the theorem are certainly true for f of this specific form. In particular the theorem holds for $f = 1 = \gamma(1)$.

Now we assume that the theorem has been shown to be true for all f with $1 \leqslant f \leqslant \gamma(s)$ for some $s \geqslant 1$; we will show that it also holds for $\gamma(s) < f \leqslant \gamma(s+1)$. Since we have already proven the theorem for all f of the form $c\gamma(t)$ with $1 \leqslant c \leqslant p$ and $t \geqslant 1$, we can assume that $c\gamma(s) < f < (c+1)\gamma(s)$ for some $1 \leqslant c \leqslant p-1$.

c-fold application of Theorem 5.4 implies that $D\hat{\xi}_k^{c\gamma(s)}$ and $(-1)^{ksc}D\xi_s^{c\gamma(k)}$ agree on $\hat{\mathrm{P}}[k; f]$, i.e.

$$\xi_s^{c\gamma(k)} \cap \hat{\mathrm{P}}[k; f] = (-1)^{ksc}\hat{\xi}_k^{c\gamma(s)} \cap \hat{\mathrm{P}}[k; f] = (-1)^{ksc}\hat{\mathrm{P}}[k; f - c\gamma(s)].$$

Since $0 < f - c\gamma(s) < \gamma(s)$, we know from Proposition 3.11 that all admissible basis elements appearing in $\hat{\mathrm{P}}[k; f - c\gamma(s)]$ have length less than s, while all those appearing in $\hat{\mathrm{P}}[k; f]$ have length less than or equal to s. The same is true with 'admissible basis elements' replaced by 'Milnor basis elements'. So suppose we have some $E[(r_1, \ldots, r_s)]$ appearing in $\hat{\mathrm{P}}[k; f]$ (where r_s could be 0). If we strip $\hat{\mathrm{P}}[k; f]$ by $\xi_s^{c\gamma(k)}$, then by Lemma 4.3 this basis element is mapped either to 0 (if $r_s < c\gamma(k)$) or to $E[(r_1, \ldots, r_s - c\gamma(k))]$ in $(-1)^{ksc}\hat{\mathrm{P}}[k; f - c\gamma(s)]$, though the latter is only possible if $r_s = c\gamma(k)$, since this basis element must have length less than s.

Therefore, consider the assignment

$$\kappa : E[(r_1, \ldots, r_{s-1})] \mapsto E[(r_1, \ldots, r_{s-1}, c\gamma(k))],$$

which assigns to every admissible basis element appearing in $(-1)^{ksc}\hat{\mathrm{P}}[k; f - c\gamma(s)]$ an admissible basis element with last entry $c\gamma(k)$ appearing in $\hat{\mathrm{P}}[k; f]$. By induction,

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

$E[R_k(f-c\gamma(s))]$ appears in $(-1)^{ksc}\hat{\mathrm{P}}[k;f-c\gamma(s)]$. Since $c\gamma(s)<f<(c+1)\gamma(s)$ we have $\Lambda(f)=s$, and by Lemma 2.3 increasing the sth entry of $R_k(f-c\gamma(s))$ by $c\gamma(k)$ yields $R_k(f)$. Therefore the above assignment maps each copy of $E[R_k(f-c\gamma(s))]$ in the admissible basis representation of $(-1)^{ksc}\hat{\mathrm{P}}[k;f-c\gamma(s)]$ to a copy of $E[R_k(f)]$ in the admissible basis representation of $\hat{\mathrm{P}}[k;f]$.

Similarly, by (4.1) we know that any element $M[(r_1,\dots,r_s)]$ appearing in the Milnor basis representation of $\hat{\mathrm{P}}[k;f]$ is mapped under stripping by $\xi_s^{c\gamma(k)}$ either to 0 or to $M[(r_1,\dots,r_s-c\gamma(k))]$ in the Milnor basis representation of $(-1)^{ksc}\hat{\mathrm{P}}[k;f-c\gamma(s)]$. Hence the same argument as for the admissible basis elements leads to the conclusion that each copy of $M[R_k(f-c\gamma(s))]$ appearing in $(-1)^{ksc}\hat{\mathrm{P}}[k;f-c\gamma(s)]$ corresponds to a copy of $M[R_k(f)]$ appearing in $\hat{\mathrm{P}}[k;f]$, so again by induction we can conclude that $M[R_k(f)]$ appears in $\hat{\mathrm{P}}[k;f]$. This proves the theorem. □

With Theorem 5.1 in hand, the remaining part of Theorem 1.1 follows easily from Theorem 4.7 and Lemma 2.1 as follows.

Theorem 5.5. *Suppose that f and k are positive integers. Then the Milnor basis element $M[R_k(f)]$ is both minimal in excess and maximal with respect to $\succ_M$ among all Milnor basis elements appearing in $\hat{\mathrm{P}}[k;f]$. Likewise, the admissible basis element $E[R_k(f)]$ is both minimal in excess and maximal with respect to $\succ_E$ among all admissible basis elements appearing in $\hat{\mathrm{P}}[k;f]$. In particular, $\mathrm{ex}(\hat{\mathrm{P}}[k;f])=2\gamma(k)\mu(f)$.*

Proof. We first prove the statement for the Milnor basis elements. Milnor's formula [**6**] states that

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

which proves the theorem in the case $k=1$, since $R_1(f)$ is minimal in excess and maximal in right-lexicographical order among all sequences R in $\mathcal{S}$ with $|R|=(p-1)f$.

Suppose then that $k>1$, and as in § 4.2 let W (respectively, $\tilde{W}$) be the sequence in $\mathcal{S}$ such that $M[W]$ is maximal among all Milnor basis elements of minimal excess appearing in $\hat{\mathrm{P}}[k;f]$ (respectively, such that $M[\tilde{W}]$ is maximal among *all* Milnor basis elements appearing in $\hat{\mathrm{P}}[k;f]$). Since $M[R_k(f)]$ appears in $\hat{\mathrm{P}}[k;f]$ by Theorem 5.1, we have $\mathrm{ex}(W)\leqslant\mathrm{ex}(R_k(f))$. By Theorem 4.7, there exists some $Q\in\mathcal{S}$ of degree $(p-1)f$ such that $W=\gamma(k)Q$. We have $\mathrm{ex}(Q)\geqslant\mathrm{ex}(R_1(f))$, which implies $\mathrm{ex}(W)\geqslant\mathrm{ex}(R_k(f))$ and thus $\mathrm{ex}(W)=\mathrm{ex}(R_k(f))$. Now if we had $W\succ R_k(f)$ then we would also have $Q\succ R_1(f)$, which is impossible. So $W=R_k(f)$. On the other hand, if $\tilde{W}\neq W$ then $\tilde{W}\succ W=R_k(f)$. Again by Theorem 4.7, there exists some $\tilde{Q}\in\mathcal{S}$ of degree $(p-1)f$ such that $\tilde{W}=\gamma(k)\tilde{Q}$, and then $\tilde{Q}\succ R_1(f)$, which is again impossible. Hence we also have $\tilde{W}=R_k(f)$ which proves the theorem for the Milnor basis elements.

For the admissible version, note that we have already proved that $\mathrm{ex}(\hat{\mathrm{P}}[k;f])=2\,\mathrm{ex}(R_k(f))$. Hence we already know that $E[R_k(f)]$ has minimal excess among all admissible basis elements appearing in $\mathrm{ex}(\hat{\mathrm{P}}[k;f])$. The fact that it is also maximal with respect to $\succ_E$ follows from Lemma 2.1. □

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

From Theorem 1.1 we easily derive Theorem 1.2.

Proof of Theorem 1.2. As in [**10**] we use the fact that for any element $\theta \in \mathcal{P}^*$ and any two polynomials U and V in $\mathbb{P}_s$ we have $U\theta(V) \equiv (\hat{\theta}U)V$ modulo hit elements. Since $\mathrm{P}[k; f]F = F^{p^k}$ we have

$$E \cdot F^{p^k} = E \cdot \mathrm{P}[k; f]F \equiv (\hat{\mathrm{P}}[k; f]E) \cdot F$$

modulo hit elements. But since $\mathrm{ex}(\hat{\mathrm{P}}[k; f]) = 2\gamma(k)\mu(f)$ by Theorem 1.1 and since by assumption $|E| = 2e < 2\gamma(k)\mu(f)$, we have $\hat{\mathrm{P}}[k; f]E = 0$ as claimed. □

Of course, the monomial P from Theorem 1.2 could be decomposed in many different ways, and the question is whether we really have to study every possible such decomposition.

Definition 5.6. Let $M \in \mathbb{P}_s$ be a monomial with decomposition $M = E \cdot F^{p^k}$. If $e < \gamma(k)\mu(f)$ then we say that the decomposition satisfies the k-criterion for being hit.

Proposition 5.7. *If the decomposition $(EG^{p^k}) \cdot H^{p^k}$ satisfies the k-criterion then so does $E(GH)^{p^k}$. If the decomposition $E \cdot (G^p)^{p^k}$ satisfies the k-criterion then the decomposition $E \cdot G^{p^{k+1}}$ satisfies the $(k+1)$-criterion.*

Proof. The implications corresponding to the claims are $e + p^k g < \gamma(k)\mu(h) \implies e < \gamma(k)\mu(g + h)$ and $e < \gamma(k)\mu(pg) \implies e < \gamma(k+1)\mu(g)$; they are an easy consequence of the following lemma. □

Lemma 5.8. *Let f, g and h be non-negative integers. Then*

(i)

$$\mu(f+1) = \begin{cases} \mu(f) - (p-1), & \textit{if the first non-zero entry of } R_1(f) \textit{ is } p, \\ \mu(f) + 1, & \textit{otherwise,} \end{cases}$$

(ii) *$\mu(h) \leqslant \mu(g + h) + (p - 1)g$, and*

(iii) *for any integer $s \geqslant 0$ we have $\mu(sf) \leqslant s\mu(f)$.*

Proof. Part (i) follows immediately from the definitions of $\mu(f)$ and $R_1(f)$, part (ii) follows from part (i) by induction, and part (iii) is obvious. □

Recall the decompositions $D_J(M)$ that were defined in the introduction: if we write $M \in \mathbb{P}_s$ as

$$M = a \prod_{j=0}^{n(M)} (L_j)^{p^{k_j}},$$

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

where $0 \neq a \in \mathbb{F}_p$, $n(M) \geqslant 0$, each L_j is a product of the form $x_1^{c_1}x_2^{c_2}\cdots x_s^{c_s}$ with $0 \leqslant c_i \leqslant p-1$, not all c_i equal to 0, and $0 = k_0 < k_1 < \cdots < k_{n(M)}$, then for $1 \leqslant J \leqslant n(M)$ we have decompositions

$$D_J(M) = \Bigl[a \prod_{j<J} (L_j)^{p^{k_j}}\Bigr] \cdot \Bigl[\prod_{j\geqslant J} (L_j)^{p^{k_j - k_J}}\Bigr]^{p^{k_J}}.$$

Proposition 5.7 implies that if some decomposition $E \cdot F^{p^k}$ of M satisfies the k-criterion, and if J is defined by $k_{J-1} < k \leqslant k_J$, then $D_J(M)$ satisfies the k_J-criterion. Hence, as in the case $p = 2$, we have the following test.

Hitness test. *Let $M \in \mathbb{P}_s$ be a monomial which is not of the form F^p, and let $D_J(M)$, $1 \leqslant J \leqslant n(M)$, be its decompositions as above. Then in order to obtain the maximal benefit from Theorem 1.2 it is not necessary to apply it to every possible decomposition of M; it suffices to apply the k_J-criterion to $D_J(M)$ for $1 \leqslant J \leqslant n(M)$.*

For any non-negative integer x, let $\alpha(x)$ denote the sum of the coefficients in the p-adic expansion of x. Then for any integer $z \geqslant 0$ the number $\mu(z)$ can be defined in a different way as follows.

Lemma 5.9. *Let x, y and k be non-negative integers with $k \geqslant 1$. Then the relation*

$$\alpha\biggl((p-1)x + \biggl[\frac{y}{\gamma(k)}\biggr]\biggr) \leqslant \biggl[\frac{y}{\gamma(k)}\biggr]$$

holds if and only if $y \geqslant \gamma(k)\mu(x)$. In particular, $\mu(x)$ can be characterized as the smallest non-negative integer y which satisfies $\alpha((p-1)x + y) \leqslant y$.

Proof. First assume $k = 1$. Let $x = \sum_{j\geqslant 0} a_j\gamma(j)$ be a description of x such that $\sum_{j\geqslant 0} a_j = \mu(x)$. Then

$$\begin{aligned}(p-1)x + \mu(x) &= (p-1)\sum_{j\geqslant 0} a_j\gamma(j) + \mu(x)\\ &= \sum_{j\geqslant 0} a_j(p^j - 1) + \sum_{j\geqslant 0} a_j = \sum_{j\geqslant 0} a_j p^j.\end{aligned}$$

Here we do not necessarily have $0 \leqslant a_j < p$, but in any case we obtain

$$\alpha((p-1)x + \mu(x)) \leqslant \sum_{j\geqslant 0} a_j = \mu(x).$$

So the inequality holds for $\mu(x)$. It also holds for any $y \geqslant \mu(x)$, since obviously

$$\alpha((p-1)x + y) \leqslant \alpha((p-1)x + \mu(x)) + (y - \mu(x)).$$

To prove the converse, suppose that we have some $y \geqslant 0$ with the property that $b := \alpha((p-1)x + y) \leqslant y$; we show that $\mu(x) \leqslant y$. We can write $(p-1)x + y = \sum_{r=1}^{b} p^{i_r}$ for certain $i_r \geqslant 0$, so that

$$(p-1)x + (y - b) = \sum_{r=1}^{b}(p^{i_r} - 1) = (p-1)\sum_{r=1}^{b}\gamma(i_r).$$

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

In particular, $y-b$ is divisible by $(p-1)$, and

$$x+\frac{y-b}{p-1}=\sum_{r=1}^{b}\gamma(i_r).$$

By Lemma 5.8 (ii) we now have

$$\mu(x)-(y-b)\leqslant\mu\left(x+\frac{y-b}{p-1}\right)\leqslant b,$$

so that $\mu(x)\leqslant y$.

The case $k>1$ immediately follows from what we have already proved by replacing $[y/\gamma(k)]$ for y. □

The following proposition can easily be deduced from Theorem 1.2.

Proposition 5.10. *Let $s>0$. Then $\mathbb{P}_s$ is generated as a module over $\mathcal{P}^*$ by monomials M satisfying the following condition: for any decomposition $M=E\cdot F^{p^k}$ with $k\geqslant 1$, we have*

$$\alpha\left((p-1)f+\left[\frac{e}{\gamma(k)}\right]\right)\leqslant\left[\frac{e}{\gamma(k)}\right].$$

Proof. Suppose that we have a monomial M which for some $k\geqslant 1$ has a decomposition as $E\cdot F^{p^k}$ which does not satisfy the above inequality. By Lemma 5.9 this implies that $e<\gamma(k)\mu(f)$. Hence by Theorem 1.2 the monomial $M=E\cdot F^{p^k}$ is hit and cannot be a generator. □

Finally, we can prove Proposition 1.3 from § 1.

Proof of Proposition 1.3. Because of the 'Hitness test' given above, it suffices to check the condition of Proposition 5.10 only for the decompositions $D_J(M)$ for $1\leqslant J\leqslant n(M)$. □

We end this paper with the example that was promised in § 1.

Example 5.11. Suppose $s=3$ and let

$$M=x_1^{p^2-1}x_2^{p^3+2p-1}x_3^{p^3+2}.$$

Then $n(M)=3$ and M has the following three decompositions

$$D_i(M)=E_i\cdot F_i^{p^{k_i}},\quad i=1,2,3:$$

(i) $D_1(M)=(x_1^{p-1}x_2^{p-1}x_3^2)\cdot[(x_1^{p-1}x_2)(x_2x_3)^{p^2}]^p$ with $k_1=1$, $e_1=2p$, $f_1=2p^2+p$,

(ii) $D_2(M)=[(x_1^{p-1}x_2^{p-1}x_3^2)(x_1^{p-1}x_2)^p]\cdot[(x_2x_3)^p]^{p^2}$ with $k_2=2$, $e_2=p^2+2p$, $f_2=2p$, and

(iii) $D_3(M)=[(x_1^{p-1}x_2^{p-1}x_3^2)(x_1^{p-1}x_2)^p]\cdot(x_2x_3)^{p^3}$ with $k_3=3$, $e_3=p^2+2p$, $f_2=2$.

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

Hence M satisfies the condition given in [**1**], which is the first condition in Proposition 1.3, since we have $\alpha((p-1)(2p^2+p)+2p) = p+1 \leqslant 2p$. So using this condition alone, M cannot be excluded as a generator. M also satisfies the condition corresponding to $J = 2$, since

$$\alpha\biggl((p-1)2p + \biggl[\frac{p^2+2p}{p+1}\biggr]\biggr) = p \leqslant \biggl[\frac{p^2+2p}{p+1}\biggr].$$

However, given that

$$\alpha\biggl((p-1)2 + \biggl[\frac{p^2+2p}{p^2+p+1}\biggr]\biggr) = p \nleqslant \biggl[\frac{p^2+2p}{p^2+p+1}\biggr],$$

the third and last condition is not satisfied, and M can in fact be excluded from the list of possible generators of $\mathbb{P}_s$ as a $\mathcal{P}^*$-module.

Finally, we note that our example is not covered by Proposition 1.4: we have $|M| = 2(2p^3+p^2+2p)$, and $s \geqslant 3$. One easily sees that for $s \geqslant 3$ we have $\alpha((p-1)s) \leqslant (s-2)(p-1)$. Hence

$$\begin{aligned}\alpha((p-1)(2p^3+p^2+2p+s)) &\leqslant \alpha((p-1)(2p^3+p^2+2p)) + \alpha((p-1)s)\\ &\leqslant 2p-2+(s-2)(p-1) = s(p-1),\end{aligned}$$

which shows that the first condition in Proposition 1.4 is not satisfied, and

$$\begin{aligned}\alpha(2p^3+p^2+2p+s) &\leqslant \alpha(2p^3+p^2+2p) + \alpha(s)\\ &\leqslant 5+s \leqslant s(s+1)(p-1)/2\end{aligned}$$

since $s \geqslant 3$, which contradicts the second condition in Proposition 1.4.

Acknowledgements. I had numerous clarifying email conversations with Judith Silverman on the subject of this paper, and I would like to thank her for sharing her ideas with me. Most of the work presented in this paper was carried out while I was supported by a 'bourse post-doctorale Alfred Kastler' from the French Ministry of Foreign Affairs. The final writing was done while I held a 'Marie Curie fellowship' from the European Union.

References

1. S. M. Chen and X. Y. Shen, On the action of Steenrod powers on polynomial algebras, in *Algebraic topology (San Feliu de Guíxols, 1990)* (ed. J. Aguadé, M. Castellet and F. R. Cohen), pp. 326–330, Lecture Notes in Mathematics, vol. 1509 (Springer, 1992).
2. M. D. Crossley, H^*V is of bounded type over $\mathcal{A}(p)$, in *Group representations: cohomology, group actions, and topology (Seattle, WA, 1996)* (ed. A. Adem, J. Carlson, S. Priddy and P. Webb), *Proc. Symp. Pure Math.*, vol. 63, pp. 183–190 (American Mathematical Society, Providence, RI, 1998).
3. D. Kraines, On excess in the Milnor basis, *Bull. Lond. Math. Soc.* **3** (1971), 363–365.
4. D. M. Meyer, Stripping and conjugation in the mod p Steenrod algebra and its dual, *Homology Homotopy Appl.* **2** (2000), 1–16.

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press

5. D. M. Meyer and J. H. Silverman, Corrigendum to 'Hit polynomials and conjugation in the dual Steenrod algebra' (by J. H. Silverman, *Math. Proc. Camb. Phil. Soc.* **123** (1998), 531–547), *Math. Proc. Camb. Phil. Soc.* **129** (2000), 277–289.
6. J. Milnor, The Steenrod algebra and its dual, *Ann. Math.* **67** (1958), 150–171.
7. J. H. Silverman, Stripping and conjugation in the Steenrod algebra, *J. Pure Appl. Algebra* **121** (1997), 95–106.
8. J. H. Silverman, Hit polynomials and conjugation in the dual Steenrod algebra, *Math. Proc. Camb. Phil. Soc.* **123** (1998), 531–547.
9. G. Walker and R. M. W. Wood, The nilpotence height of Sq^{2^n}, *Proc. Am. Math. Soc.* **124** (1996), 1291–1295.
10. R. M. W. Wood, Steenrod squares of polynomials and the Peterson conjecture, *Math. Proc. Camb. Phil. Soc.* **105** (1989), 307–309.

https://doi.org/10.1017/S0013091500000353 Published online by Cambridge University Press