Algebraic & Geometric Topology 13 (2013) 2061–2085

The hit problem for $H^*(\mathrm{BU}(2);\mathbb{F}_p)$

DAVID PENGELLEY
FRANK WILLIAMS

The hit problem for a module over the Steenrod algebra $\mathcal{A}$ seeks a minimal set of $\mathcal{A}$–generators ("non-hit elements"). This problem has been studied for 25 years in a variety of contexts, and although complete results have been notoriously difficult to come by, partial results have been obtained in many cases.

For the cohomologies of classifying spaces, several such results possess two intriguing features: sparseness by degree, and uniform rank bounds independent of degree. In particular, it is known that sparseness holds for $H^*(\mathrm{BO}(n);\mathbb{F}_2)$ for all n, and that there is a rank bound for $n \le 3$. Our results in this paper show that both these features continue at all odd primes for $\mathrm{BU}(n)$ for $n \le 2$.

We solve the odd primary hit problem for $H^*(\mathrm{BU}(2);\mathbb{F}_p)$ by determining an explicit basis for the $\mathcal{A}$–primitives in the dual $H_*(\mathrm{BU}(2);\mathbb{F}_p)$, where we find considerably more elaborate structure than in the 2–primary case. We obtain our results by structuring the $\mathcal{A}$–primitives in homology using an action of the Kudo–Araki–May algebra.

16W22, 55R40, 55R45, 55S10; 16W50, 55S05, 57T10, 57T25

1 Summary and statement of results

1.1 Summary

Let $M_* = H_*(\mathrm{BU}(2);\mathbb{F}_p)$, p odd. We consider the problem of determining the subspace $\mathcal{S}$ of $\mathcal{A}$–primitive elements for the (downward) $\mathcal{A}$–action on M_*, ie, the kernel of the action by the positive dimensional elements of the Steenrod algebra $\mathcal{A}$. In the next section we give the background of this problem and explain its equivalence to the hit problem.

It follows by counting from work of Janfada and Wood [3; 4] that the analogous problem to ours at the prime 2 is trivial, in that all primitives in $H_*(\mathrm{BO}(2);\mathbb{F}_2)$ are the 2–fold products of primitives from $H_*(\mathrm{BO}(1);\mathbb{F}_2)$. For p odd, by contrast, there is a plethora of primitives in $H_*(\mathrm{BU}(2);\mathbb{F}_p)$ that are not products of primitives in

Published: 29 May 2013 DOI: 10.2140/agt.2013.13.2061

$H_*(\mathrm{BU}(1);\mathbb{F}_p)$ (we use the product structure of $H_*(\mathrm{BU};\mathbb{F}_p)$ throughout), providing a pleasingly complex richness of structure.

We shall prove that all primitives are concentrated in (complex) degrees τ such that $\widehat{\alpha}(\tau+2)\leq 3$, where $\widehat{\alpha}(n)$ denotes the number of non-zero digits in the p–ary expansion of n. We shall further prove that for all degrees τ, the rank of $\mathcal{S}_\tau$ is bounded by p. To accomplish this, we shall describe in the next section a specific vector space basis for each $\mathcal{S}_\tau$.

Our primary tool in this description will be the self-map of $\mathcal{S}$ (whose definition we shall recall in Section 2) given by the element $d_2 \in \mathcal{K}$, the Kudo–Araki–May algebra. As in [6] we shall see that $\mathcal{S}$ is a free module over d_2, and we shall solve the problem of computing $\mathcal{S}$ by finding a d_2–basis for it. A key ingredient is that for $\tau \geq p-2$ the map $d_2\colon \mathcal{S}_\tau \to \mathcal{S}_{p\tau+(2p-2)}$ is an isomorphism of vector spaces, which restricts the degrees in which d_2–basis elements can occur.

Another valuable tool is that P^{p^n} is a derivation on $\ker P^1 \cap \cdots \cap \ker P^{p^{n-1}}$. This is crucial to establishing our main computational result (Theorem 3.5) on how $\ker P^{p^n}$ can intersect the kernels of lower operations.

Our d_2–basis splits into a "stable" range consisting of degrees above $2p^2-2$ and three lower ranges. In the stable range, d_2–basis elements occur in exactly those degrees τ such that $\widehat{\alpha}(\tau+2)\leq 2$. For each such τ in the stable range, the d_2–basis has very restricted cardinality, at most $(p+3)/2$. In the unstable ranges, the situation is somewhat more complicated, as we shall describe in the next section. In addition to giving a complete description of the d_2–bases, at the end of the next section we provide a table listing the ranks of $\mathcal{S}_\tau$ for all τ.

Section 2 will provide background and the structure of the organizing map d_2, Sections 3 and 4 assemble further the organizational basis for our approach, and the remaining sections analyze the various degree ranges.

1.2 Statement of results

We shall see in Section 2 that we can write a basis for M_* in the form $a_i a_j$, $j \geq i \geq 0$, where the a_i, $i > 0$, are standard polynomial generators of $H_*(\mathrm{BU};\mathbb{F}_p)$ and a_0 is a zero-dimensional place-holder. And we shall see that a vector space basis for M_τ is given by the monomials $a_i a_j$ such that $i+j=\tau$ and $i \leq j$. (By convention, $a_i = 0$ whenever $i < 0$.) In this section we shall give a complete description of the primitives S by providing a d_2–basis, describe how the basis arises, and end with a table giving ranks in all degrees. We begin with the easiest case to describe, the stable range $\tau \geq 2p^2-1$.

We start with the following definitions. For integers i, D_0, l, let

$$v(i, D_0, l) = \sum_{k=1}^{p-D_0+1} \binom{k + D_0 - 2}{D_0 - 1} a_{p(i+1)+(D_0-2)-(p-1)k}\, a_{p(l-i-1)+(p-1)k},$$

in degree $\tau = pl + D_0 - 2$. The formulas are clearly zero except when $1 \le D_0 \le p$, and henceforth D_0 will always be taken to lie in this range. These formulas span much of the kernel of P^1, in fact in the stable range all of it.

As a peek ahead to Definition 3.2, we note that each monomial occurring in these formulas has the sum of the "ones" digits of its subscripts at least $p-1$. We call monomials satisfying this property *Type 1 for* P^1. Each Type 1 monomial occurs in exactly one $v(i, D_0, l)$ formula, and we shall see (Theorem 3.5) that the $v(i, D_0, l)$ that contains a monomial $a_r a_s$ is the smallest linear combination of monomials in $\ker P^1$ that does. However, since $a_r a_s = a_s a_r$, there will be a formula $v(i', D_0, l)$ containing $a_s a_r$ that represents the same element of M_* (up to scalar multiple) as $v(i, D_0, l)$, but with subscripts reversed, and these two formulas will be called *twins*. Further, sometimes a formula $v(i, D_0, l)$ contains both $a_r a_s$ and $a_s a_r$, in which case it is its own twin, and it is possible for it to represent zero in M_* if the coefficients produce cancellation. In the stable range $\ker P^1$ has as a basis the formulas $v(i, D_0, l)$ except for the twinning and sometime zeroing just mentioned. Sometimes we will implicitly identify a formula with the element in M_* that it represents.

It will help in tracking the formulas $v(i, D_0, l)$ and how they interact for each to have an assigned label. Let the *label* of i, D_0, l be the (unordered) set

$$\mathrm{LAB}(i, D_0, l) = \{D_0 - 1 + i, l - 1 - i\} \pmod{p-1}.$$

Note that this set consists of the subscripts of the monomial summands of $v(i, D_0, l)$, which are all identical mod $(p-1)$. Clearly twins have the same label set, and the possible zeroing can happen only if a label set consists of a single element.

The elements represented by the individual formulas $v(i, D_0, l)$ in $\ker P^1$ are generally not in the kernels of the higher P^{p^n}. However, we can identify exactly which linear combinations of them are, as follows.

For integers l and D_0 and for each $0 \le c \le p-2$, define

$$x(c, D_0, l) = \sum_r v(c + r(p-1), D_0, l)$$

in degree $\tau = pl + D_0 - 2$ with $1 \le D_0 \le p$. Clearly every $v(i, D_0, l)$ occurs in exactly one of these formulas. Notice that all the v's in each formula have the same label $\mathrm{LAB}(c, D_0, l)$. And as with the individual v's, reversing subscripts throughout produces a corresponding twin $x(c', D_0, l)$ with the same label, representing the same element of M_* up to scalar multiple.

We can now state the main theorem about d_2–bases in the stable range.

Theorem 1.1 *If $\tau \geq 2p^2 - 1$, then a d_2–basis for S is concentrated in degrees of the form $\tau = D_m p^m + D_0 - 2$, for some $1 \leq D_0, D_m \leq p-1$. In these degrees, a d_2–basis for the primitives is given by the monomial $a_{D_m p^m - 1} a_{D_0 - 1}$ together with elements $x(c, D_0, D_m p^{m-1})$ in the following way:*

1. *If $\mathrm{LAB}(c_1, D_0, D_m) = \mathrm{LAB}(c_2, D_0, D_m)$, $c_1 \neq c_2$, then $x(c_1, D_0, D_m p^{m-1})$ is a unit multiple of $x(c_2, D_0, D_m p^{m-1})$ and so either will serve as a basis element.*
2. *If $\mathrm{LAB}(c, D_0, D_m)$ consists of a single number and D_0 is odd, then we choose $x(c, D_0, D_m p^{m-1})$ as a basis element.*

(If $\mathrm{LAB}(c, D_0, D_m)$ consists of a single number and D_0 is even, then $x(c, D_0, D_m p^{m-1}) = 0$.)

We note that since the $x(c, D_0, D_m p^{m-1})$ are indexed by c, most with distinct twins, there are about $(p-1)/2$ elements in the d_2–basis in the stable range. We further note that every monomial of Type 1 for P^1 in these degrees occurs as a summand of some formula $x(c, D_0, l)$, even though a monomial in the formula may cancel in M_* with the monomial that has reversed subscripts.

We remark on the special role played by P^p among all the higher P^{p^n} in determining the d_2–basis inside $\ker P^1$. Essentially P^p determines what the primitives must look like and restricts degrees somewhat, and then the even higher P^{p^n} reject outright those in most degrees.

We shall prove (Theorem 7.1) that in degrees $\tau = pl + D_0 - 2$ with $D_0 \neq p$, $\ker P^1 \cap \ker P^p$ is concentrated in degrees where l is p–divisible. In such degrees, we shall also prove (Corollary 7.4) that the sum $x(c, D_0, l)$ is always in $\ker P^p$, and is the smallest expression of a $\ker P^1 \cap \ker P^p$ element that contains any of its v's (except individual primitive monomials like those mentioned at the beginning of the theorem). Combined with the twinning and zeroing analysis above, this provides a complete description of $\ker P^1 \cap \ker P^p$ in the stable range; the intersection is spanned by the x's in those degrees where l is p–divisible, along with one additional possible monomial. Then we shall further see that the additional requirement that a primitive should also lie in the kernels of P^{p^n}, $n \geq 2$, has the effect not of forcing the x's to combine further (Remark 2.2), but of disallowing anything in degrees excepting when l is a power of p, leaving only those in degrees $D_m p^m + D_0 - 2$ (Theorem 7.5).

We next consider the *upper-low range* $p^2 + p - 1 \leq \tau \leq 2p^2 - 2$. We have the theorem:

Theorem 1.2 *If $p^2+p-1 \le \tau \le 2p^2-2$, then a d_2–basis for S is concentrated in degrees of the form $\tau = p^2+D_1p+D_0-2$, $1 \le D_0, D_1 \le p-1$, where $D_0-D_1 \ge 1$. In these degrees, a d_2–basis for the primitives is obtained from elements $v(i, D_0, p+D_1)$ for which $p-(D_0-D_1) \le i \le p-1$ in the following way (similar to the stable case):*

(1) *If $\mathrm{LAB}(i_1, D_0, 1+D_1) = \mathrm{LAB}(i_2, D_0, 1+D_1)$, $i_1 \ne i_2$, then $v(i_1, D_0, p+D_1)$ is a unit multiple of $v(i_2, D_0, p+D_1)$ and so either will serve as a basis element.*

(2) *If $\mathrm{LAB}(i, D_0, 1+D_1)$ consists of a single number and D_0 is odd, then we choose $v(i, D_0, p+D_1)$ as a basis element.*

(If $\mathrm{LAB}(i, D_0, 1+D_1)$ consists of a single number and D_0 is even, then $v(i, D_0, p+D_1) = 0$.)

In this case there are about $(D_0-D_1)/2$ elements in the d_2–basis in these degrees. Furthermore, in contrast with the stable case, we note that while all primitive elements are sums of Type 1 monomials, not all such monomials occur in basis elements. The $v(i, D_0, p+D_1)$ for i not in the range $p-(D_0-D_1) \le i \le p-1$ are not summands of any element of ker P^p.

We next consider the *mid-low* range $p-1 \le \tau \le p^2+p-2$. This range is the most complicated for two reasons: (1) it is possible that more than two d_2–basis elements $v(i, D_0, l)$ in a given degree τ can have the same label (so labels cannot be used to specify d_2–basis elements), and (2) there is a new kind of basis element

$$w(u, D_0, l) = \sum_{k=1}^{l+1} (-1)^{k+1} \frac{\binom{D_0-u+k-3}{k-1}}{\binom{u}{k-1}} a_{pl+D_0-2-u-(p-1)(k-1)} a_{u+(p-1)(k-1)}.$$

We have:

Theorem 1.3 *In degrees $\tau = lp+D_0-2$, with $1 \le l \le p$ and $1 \le D_0 \le p$ (so that $p-1 \le \tau \le p^2+p-2$), there are d_2–basis elements only if (1) $D_0 \le p-1$, or (2) $D_0-l \ge 2$.*

Basis elements in the range (1) are given by $v(i, D_0, l)$, for $0 \le i \le [(p+l-D_0-2)/2]$, together with $i = (p+l-D_0-1)/2$ if τ is even and D_0 is odd.

Additional basis elements in the (overlapping) range (2) are given by $w(u, D_0, l)$ for $l \le u \le l+[(D_0-l-3)/2]$, together with $u = l+(D_0-l-2)/2$ if τ and D_0 are both even.

We note that in this range, if $\tau = lp+D_0-2$ is such that l is large and D_0 is small, the vector space dimension of the space of d_2–basis elements can be as large as p, roughly twice the maximum dimension in the other three ranges. Notice that the monomials that occur in d_2–basis elements of the form $w(u, D_0, l)$ have the sum of the "ones" digits of their subscripts less than $p-1$. Again peeking ahead to Definition 3.2, we call monomials of this form *Type 2 for* P^1.

Finally we note that in the *bottom* range $0 \le \tau \le p-2$ all monomials are primitive and none is in the image of d_2, so we have the (trivial) theorem:

Theorem 1.4 *In degrees $0 \le \tau \le p-2$, a d_2–basis can be taken to be all monomials $a_i a_j$ with $i \le j$.*

We close this section with the promised table giving the ranks of all S_τ, $\tau \ge 0$. To organize this table, we use the map $d_2\colon S_{p^k q-2} \to S_{p^{k+1}q-2}$ (recall this is almost always an isomorphism) to split the primitives over d_2 into disjoint degree families $S_{(q)}$, for each q relatively prime to p. So $S_{(q)} = \bigoplus_{k\ge 0} S_{p^k q-2}$ and $S_* = \bigoplus_{\gcd(q,p)=1} S_{(q)}$.

Theorem 1.5 *The following table gives the rank of S_τ in every degree, always writing $\tau = p^k q - 2$ (q relatively prime to p). The table is arranged according to the size of q, corresponding to the division of our d_2–basis into ranges. In degrees not in the table there are no non-zero primitives.*

In the table, $1 \le D_0, D_i \le p-1$ for $i \ge 2$, $1 \le D_1 \le p$ and $k \ge 0$. Let

$$\epsilon = \begin{cases} -1 & \text{when } q \text{ is even and } D_0 \text{ is even,} \\ 0 & \text{when } q \text{ is odd,} \\ 1 & \text{when } q \text{ is even and } D_0 \text{ is odd.} \end{cases}$$

q, relatively prime to p	$\tau = p^k q - 2$	rank(S_τ)
Bottom range: $0 < q < p$		
D_0	$k = 0$	$\left[\frac{D_0}{2}\right]$
	$k \ge 1$	$\frac{p-1}{2}$
Mid-low range: $p < q < p^2 + p$		
$D_1 p + D_0$, $D_1 < D_0$		$\frac{p-1}{2}$
$D_1 p + D_0$, $D_1 \ge D_0$		$\frac{p-D_0+D_1+\epsilon}{2}$
Upper-low range: $p^2 + p < q < 2p^2$		
$p^2 + D_1 p + D_0$, $D_1 < D_0$		$\frac{D_0-D_1+\epsilon}{2}$
Stable range: $q > 2p^2$		
$D_M p^M + D_0$, $M \ge 2$, $(D_M, M) \ne (1,2)$		$\frac{p+1}{2} + \epsilon$

Remark 1.6 The separation of $k \geq 1$ for the bottom range results from the inclusion of the Type 2 w's beginning with $k = 1$ from Theorem 1.3. And the value $q = 1$ is special, in that $k = 0$ is irrelevant, being in negative degree; for $k = 1$ the degree is still below p, and for $k = 2$ no w's are appended, since the degree is beyond them; however, the table values still hold based on the theorems above.

2 Background and booting to organize primitives

2.1 Background

The hit problem for an unstable module over the Steenrod algebra $\mathcal{A}$ asks for a minimal $\mathcal{A}$–module generating set (ie, elements not "hit" by positive Steenrod operations). The problem has been studied at the prime $p = 2$ for polynomial algebras with generators in degree one (cohomology of products of projective spaces), and more recently for algebras of symmetric polynomials in such generators, which are the cohomologies of the classifying spaces $\mathrm{BO}(l)$. The hit problem for various classifying spaces and primes has received considerable attention, and partial results have been obtained in Crossley [1; 2], Janfada and Wood [3; 4], Kameko [5], Pengelley and Williams [6], Peterson [7], Singer [8] and Wood [9]. We refer to [6] for further background.

The few hit problem answers so far for polynomial algebras and their symmetric subalgebras have two interesting features: sparseness by degree, and uniformly bounded rank over all degrees, termed *bounded type*.

Regarding sparseness, Peterson conjectured [7] that mod 2 the $\mathcal{A}$–generators for a product of l real projective spaces could occur only in certain degrees. This was proven true by Wood [9], and later also proven for the symmetric algebras corresponding to the $\mathrm{BO}(l)$, by Janfada and Wood [3]. Both results state that the $\mathcal{A}$–generators are concentrated in degrees τ for which $\tau + l$ has no more than l nonzero digits in its binary expansion, ie, $\widehat{\alpha}(\tau + l) \leq l$.

Regarding explicit ranks, the hit problem for $l = 1$ is easily solved, and the result has rank one in each degree where it is nonzero. Janfada and Wood [4] determined the ranks of $\mathcal{A}$–generators of $H^*(\mathrm{BO}(l);\mathbb{F}_2)$ for $l = 2, 3$, and found that they too are of bounded type, with bounds 1 and 4, respectively.

Our results for $H^*(\mathrm{BU}(2);\mathbb{F}_p)$ address analogous conjectures for p odd. For $H^*(\mathrm{BU}(1);\mathbb{F}_p)$ it is straightforward that the $\mathcal{A}$–generators have rank one in each complex degree τ for which $\tau + 1$ has exactly 1 digit in its p–ary expansion, in analogy to $p = 2$. (At odd primes our cohomology is concentrated in even degrees, so we use 'complex degree', half the topological degree.)

A Peterson-like sparseness conjecture analogous to $p = 2$ would be that the $\mathcal{A}$–generators of $H^*(\mathrm{BU}(2); \mathbb{F}_p)$ are concentrated in complex degrees τ such that $\widehat{\alpha}(\tau+2) \le 2$. A bounded type conjecture would be that the ranks of $\mathcal{A}$–generators of $H^*(\mathrm{BU}(2); \mathbb{F}_p)$ are uniformly bounded over all degrees by approximately $p/2$ or $p-1$. As announced in the summary, the table above shows that the first conjecture is false, but is made true by a mild modification, and that the ranks of $\mathcal{A}$–generators are uniformly bounded by p. However, as stated in the summary, in a stable sense the more ambitious conjectured bounds essentially hold, since the d_2–generators in the stable range satisfy $\widehat{\alpha}(\tau+2) \le 2$ as well as the degree rank bound $(p+3)/2$.

It is instructive to compare our results on $H_*(\mathrm{BU}(2); \mathbb{F}_p)$ with Crossley's work [1; 2] on $H^*(CP(\infty) \times CP(\infty); \mathbb{F}_p)$ and $H_*(CP(\infty) \times CP(\infty); \mathbb{F}_p)$. In particular, the ranges in which he finds primitives in $H_*(CP(\infty) \times CP(\infty); \mathbb{F}_p)$ coincide with our ranges for primitives in $H_*(\mathrm{BU}(2); \mathbb{F}_p)$. There is a rough correspondence between his monomial $\mathcal{A}$–generators $x^i y^j$ for $H^*(CP(\infty) \times CP(\infty); \mathbb{F}_p)$ and our monomial summands $a_i a_j$ of primitive elements in $H_*(\mathrm{BU}(2); \mathbb{F}_p)$. We have not been able to find any way, however, to derive our results from his or vice versa.

2.2 The $\mathcal{A}$–action on M_*

Recall [6] that for any prime p, $H_*(\mathrm{BU}; \mathbb{F}_p)$ is the polynomial algebra with generators $a_n \in H_{2n}(\mathrm{BU}; \mathbb{F}_p)$ for $n \ge 1$, dual to the powers c_1^n of the first Chern class, and that $H_*(\mathrm{BU}(l); \mathbb{F}_p)$ can be thought of as the subspace spanned by monomials in the a_n of length at most l. It is convenient for us, and is usual in the literature, to introduce a placeholder, a_0, of topological degree zero, so that a monomial $a_{i_1} \cdots a_{i_k} \in H_*(\mathrm{BU}(l); \mathbb{F}_p)$ may be written $a_0^{l-k} a_{i_1} \cdots a_{i_k}$. Then $M_* = H_*(\mathrm{BU}(2); \mathbb{F}_p)$ is spanned by monomials of length exactly 2.

Definition 2.1 We categorize monomials in M_* by calling a monomial $a_i a_j$ a 2*–fold* if both i, j are strictly positive, and a 1*–fold* if one of i, j is zero and one of i, j is strictly positive.

The downward right $\mathcal{A}$–action on $H_*(\mathrm{BU}; \mathbb{F}_p)$ is determined via the Cartan formula from
$$a_m * P^r = \binom{m - r(p-1)}{r} a_{m-r(p-1)},$$
the action for $\mathbb{C}P(\infty) = \mathrm{BU}(1)$, in which a_0 is both primitive and never hit by a positive operation, ie, transparent to the $\mathcal{A}$–action. So in M_* the 1–fold and 2–fold subspaces split apart over $\mathcal{A}$. Nonetheless, we will often treat them in a unified way, since they will be tied via our organizing map d_2.

Note from the Cartan formula that the primitives for the $\mathcal{A}$–action form a subalgebra of $H_*(\mathrm{BU};\mathbb{F}_p)$.

Remark 2.2 We may extend the definition of label to monomials via $\mathrm{LAB}(a_i a_j) = \{i, j\} \pmod{p-1}$. Since Steenrod operations change subscripts only by multiples of $p-1$, the subspace spanned by monomials of all degrees having the same label is a sub–$\mathcal{A}$–module of M_*, hence M_* splits over $\mathcal{A}$ according to labels. This elucidates, in our commentary after Theorem 1.1, why the kernels of the higher operations can only eliminate but not combine the x's in $\ker P^1 \cap \ker P^p$.

The operations P^{p^i} of (complex) degree $p^i(p-1)$ generate $\mathcal{A}$, for which it is easy to compute using Lucas's formula for mod p binomial coefficients, namely

$$a_m * P^{p^i} = (m_i + 1) a_{m-p^i(p-1)}, \tag{1}$$

where m_i is the i^{th} p–ary digit of m (ie, $m = \sum_{i\ge 0} m_i p^i$ with $0 \le m_i < p$).

2.3 One-fold primitives and S–decomposable two-fold primitives

The 1–fold $\mathcal{A}$–primitives in M_* are now obvious; they are the $a_0 a_m$ in which m has only trailing digits $p-1$ after the leading digit, ie,

$$\{a_0 a_{jp^n-1} \mid 1 \le j \le p-1,\ n \ge 0,\ (j,n) \ne (1,0)\}.$$

Definition 2.3 By two-fold S–decomposable primitives we mean the subspace spanned by products of primitives in $H_*(\mathrm{BU}(1);\mathbb{F}_p)$.

The twofold S–decomposable primitives are then

$$\{a_{ip^m-1} a_{jp^n-1} \mid 1 \le i, j \le p-1,\ m, n \ge 0,\ (i,m) \ne (1,0) \ne (j,n)\}.$$

Remark 2.4 The positive degrees τ for which $\tau+2$ has no more than two nonzero digits are precisely those containing nonzero 1–fold or S–decomposable 2–fold primitives. The degrees for which $\tau+2$ has three nonzero digits contain only indecomposable 2–fold primitives. They occur only in the upper-low band $p^2 + p < q < 2p^2$ of Theorem 1.5.

2.4 Booting with d_2 to organize primitives

Recall [6] that for any prime p, the action of the element $d_2 \in \mathcal{K}$ on $a_i a_j \in H_*(\mathrm{BU}; \mathbb{F}_p)$ was defined by the formula $d_2(a_i a_j) = a_{pi+p-1} a_{pj+p-1}$ for $i, j \geq 1$, and we extend this definition to $i, j \geq 0$. Kameko [5] and Singer [8] initiated the use of similar operations at the prime 2 for the hit problem, and these have been motivational for our work [6]. It is easy to check that

$$(d_2(a_i a_j)) * P^k = d_2(a_i a_j * P^{k/p}). \tag{2}$$

This ensures that S_* is closed under the action of d_2.

Remark 2.5 The map d_2 takes one-folds to two-folds; $d_2(a_0 a_n) = a_{p-1} a_{pn+p-1}$.

The following lemma is obvious.

Lemma 2.6 *The map d_2 preserves primitives, so*

$$d_2\colon S_{p^k q-2} \rightarrowtail S_{p^{k+1} q-2}.$$

It is easy to see that d_2 is monic and S_* is a free $\mathbb{F}_p[d_2]$–module, so in degrees not congruent to $-2 \bmod p$, a $\mathbb{F}_p$–basis for S_* is also a d_2–basis.

Turning next to degrees $\tau \equiv -2 \bmod p$, the following theorem (to be proved below) and its corollary show that, except for low degrees, there are no d_2–generators for S_*.

Theorem 2.7 *In degrees $\tau \equiv -2 \bmod p$ with $\tau \geq p^2 - 2$, $\ker P^1 = \operatorname{im} d_2$.*

Corollary 2.8 *In degrees $\tau = pl + 2p - 2$ with $l \geq p - 2$,*

$$S_\tau = d_2(S_l).$$

Thus the only d_2–generators that S_* can have in degrees $\tau \equiv -2 \bmod p$ must occur in degrees not exceeding $p^2 - p - 2$, ie, in degrees $pq - 2$ for $q < p$.

Proof That $d_2(S_l) \subseteq S_\tau$ follows from (2) above. Now let $y \in S_\tau$. By the theorem, $y = d_2(x)$ for some $x \in M_l$. By (2) and the monicity of d_2 we have $x \in S_l$. □

Thus we have:

Corollary 2.9 *A d_2–basis for S_* consists of a $\mathbb{F}_p$–basis for primitives in degrees $q - 2$ for q relatively prime to p, along with a $\mathbb{F}_p$–basis complementary to the image of $d_2\colon S_{q-2} \to S_{pq-2}$ for $q < p$.*

Proof The lemma above ensures that for q relatively prime to p, in degree $q-2$ a $\mathbb{F}_p$–basis coincides with a d_2–basis. In degrees of the form $p^k q-2$, $k\geq 1$, the previous corollary assures us that d_2–generators can exist only for $k=1$ and $q<p$. □

Our task then is to find a d_2–basis for the primitives as given by the corollary.

2.5 Monomial terminology and the $\mathcal{A}$–action

When studying the $\mathcal{A}$–action on M_*, we exert care when negative-subscripted a's occur in formulas, since the resulting terms, which must be interpreted as zero, may affect conclusions drawn from other terms in the formula. Also, we need to study which monomials must occur together in representations of elements in the kernel of a Steenrod operation. To assist, we use the following terminology. We note that since p is odd, any element in M_τ can always be expressed in symmetric form in its monomials, ie, the coefficient of $a_i a_j$ is equal to the coefficient of $a_j a_i$.

Definition 2.10

(1) We call a monomial $a_i a_j$ *live* if both its subscripts are nonnegative.

(2) Given $x\in M_*$, we say that a live monomial $a_i a_j$ *appears* in x (or x *contains* $a_i a_j$) if $a_i a_j$ has nonzero $\mathbb{F}_p$ coefficient when x is expressed in its symmetric form.

3 Fundamental theorem on ker P^{p^n} and links

3.1 A filtration of M_* and the kernel of P^{p^n}

Throughout the rest of the paper we shall use the following notation.

Notation 3.1 If n is a nonnegative integer, we shall let n_i denote the i^{th} p–ary digit of n. We shall sometimes write n in the form $(n_0, n_1, \cdots)$.

Definition 3.2 Define nested subspaces M_*^n of M_* as follows. Set $M_\tau^0 = M_\tau$. For $n\geq 1$, define M_τ^n to be the span of those $a_i a_j$ with $i+j=\tau$ and $i_k + j_k \geq p-1$ for $0\leq k\leq n-1$, ie, the monomials whose subscript digit sums are each at least $p-1$ for all digits from the 0^{th} to the $(n-1)^{\text{st}}$.

We call the monomials in M_τ^n *Type 1 for* $P^{p^{n-1}}$, and monomials in M_τ^{n-1} that are not in M_τ^n are called *Type 2 for* $P^{p^{n-1}}$.

Remark 3.3 Alternatively, write $\tau = p^n l + \delta - 1$, $0 \le \delta < p^n$, $l \ge 1$. Then M^n_τ is the subspace of M^{n-1}_τ spanned by

$$\{a_{p^n I+t} a_{p^n J+u} \mid I + J = l - 1,\ 0 \le t, u < p^n,\ t_{n-1} + u_{n-1} = \delta_{n-1} + (p-1)\}.$$

This means that when adding the two subscripts along with 1 to obtain $\tau + 1$, there are "carries" in every digit addition through the one that obtains the n^{th} digit, expressed as $t_m + u_m + 1 = \delta_m + p$ for all $m \le n-1$. This convenient formula will be used frequently.

An important consequence of this definition is given by the following lemma.

Lemma 3.4 *P^{p^n} is a derivation on M^n_τ.*

Proof Let $1 \le k \le n$ and $1 \le b \le p-1$. Using the notation above for spanning monomials for M^n_τ, we consider

$$(a_{p^n I+t}) P^{Bp^k + bp^{k-1}} (a_{p^n J+u}) P^{p^n - Bp^k - bp^{k-1}}.$$

The coefficient of this term contains factors

$$\binom{t_{k-1}+b}{b} \quad \text{and} \quad \binom{u_{k-1}+(p-b)}{p-b}.$$

Assume that $t_{k-1} + b \ge p$. In this case the first of these binomial coefficients is zero. Alternatively assume that $t_{k-1} + b < p$. Then $u_{k-1} + (p-b) > u_{k-1} + t_{k-1} = \delta_{k-1} + (p-1) \ge p-1$, whence the second of these binomial coefficients is zero. □

The next theorem gives the fundamental set of formulas of this paper.

Theorem 3.5 *For $\tau \ge p^{n+1} - 1$, write $\tau = p^{n+1} l + \delta - 1$, $0 \le \delta < p^{n+1}$, $l \ge 1$. Then in degree τ we have $\ker P^{p^n} \cap M^n_\tau$ spanned by elements represented by the formulas*

$$\left\{ \sum_{k=1}^{p-\delta_n} \binom{k+\delta_n+p-1}{\delta_n} a_{p^{n+1} i + p^n \delta_n + t - p^n (p-1)(k-1)} a_{p^{n+1} j + u + p^n (p-1) k} \right. \left| \ i + j = l-1,\ i, j \in \mathbb{Z},\ 0 \le t, u < p^n, t_m + u_m = \delta_m + (p-1) \right\}$$

$$\cup \left\{ \sum_{k=1}^{l+1} (-1)^k \binom{t_n + k - 1}{k-1} \Big/ \binom{u_n}{k-1} a_{p^{n+1} l + t - (p-1)(k-1) p^n} a_{u + (p-1)(k-1) p^n} \right. \left| \ 0 \le t, u < p^{n+1}, t_m + u_m = \delta_m + (p-1) \text{ for } m < n,\ l \le u_n,\ t_n + u_n = \delta_n - 1 \right\}$$

(We shall refer to elements of the first set as being of Type 1 for P^{p^n} *and those of the second set as Type 2 for* P^{p^n}*, since the monomials that occur in the first set of formulas are of Type 1 for* P^{p^n} *and those in the second set of formulas are of Type 2 for* P^{p^n}*.)*

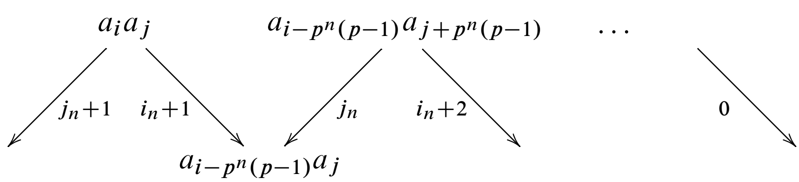
Proof For given $a_i a_j \in M^n_\tau$, we shall completely analyze any $\ker P^{p^n}$ expression containing it. From (1) and the lemma above we have

$$(a_i a_j)P^{p^n} = (i_n + 1)a_{i-p^n(p-1))}a_j + (j_n + 1)a_i a_{j-p^n(p-1)},$$

and the only monomials that could possibly cancel the resulting terms under P^{p^n} are $a_{i-p^n(p-1)}a_{j+p^n(p-1)}$ and $a_{i+p^n(p-1)}a_{j-p^n(p-1)}$, respectively.

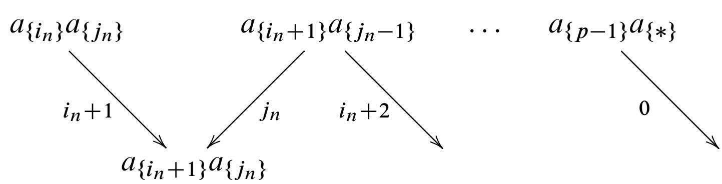
This creates great rigidity, so that if $a_i a_j$ appears in a $\ker P^{p^n}$ expression, there will be a minimal such sum of monomials, uniquely determined up to scalar multiple, and whose subscripts vary consecutively by $p^n(p-1)$.

For cancellation to produce such a sum, the two end terms must each produce a zero coefficient under P^{p^n}, as shown in the part of the cancellation sequence



leading to the right end. The arrows point to monomials arising from P^{p^n}. The resulting coefficients label the arrows, and must be nonzero until the ends.

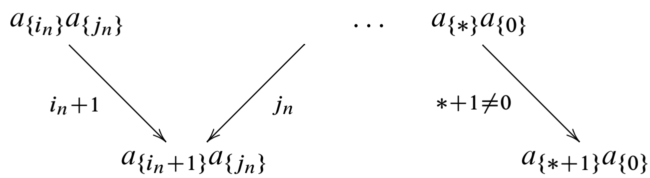
Redisplaying with each subscript replaced by its n^{th} digit placed in braces yields



in which the digits step consecutively to the ends. Notice that since the sum of the two subscript digits is constant for all the monomials, and is at least $p-1$ at the ends, that this cancellation process completes successfully for any $a_i a_j$ of Type 1 for P^{p^n}, and fails for Type 2, showing exactly how the Type 1 $\ker P^{p^n}$ expressions form.

Thus the minimal possible $\ker P^{p^n}$ monomial sums arising from cancellation are the Type 1 formulas listed, normalized to have first coefficient 1, with binomial coefficients proceeding so as to produce the coefficient ratios required for cancellations. Note that it is possible that some monomials in these sums are zero because their indices are negative.

A monomial of Type 2 can still occur in a $\ker P^{p^n}$ sum, but only provided indices in the sequence shown drop below zero in both directions before an obstruction to cancellation arises. The obstructions arise as shown in



because the uncancellable term $a_{\{*+1\}}a_{\{0\}}$ occurs before the cancellation completes successfully, since $i_n + j_n < p-1$.

Thus such a sequence can produce a sum in $\ker P^{p^n}$ precisely if the first subscript of the uncancellable term is negative, and similarly at the other end. The Type 2 formulas above describe exactly this, with every term live, ie, not listing any terms with a negative subscript. □

Definition 3.6 We shall refer to the formulas given in Theorem 3.5 as P^{p^n}*–links*.

Remark 3.7 Type 2 links for P^{p^n} lie in degrees less than $p^{n+2} - p^{n+1} - 1 < p^{n+2}$. Hence they are in the kernels of all P^{p^i} for $i \geq n+1$.

Corollary 3.8 *In degrees τ such that $\tau \geq p^n(p-2)$ we have*

$$\ker P^1 \cap \cdots \cap \ker P^{p^{n-1}} \subseteq M^n_\tau.$$

Proof Consider a monomial summand of an element in $\ker P^{p^{n-1}} \cap M^{n-1}_\tau$, say

$$a_{p^n i + p^{n-1}(\delta_{n-1}-(k-1)(p-1))+t}\, a_{p^n j + p^{n-1}(p-1)k+u},$$

where $i+j = l-1$, $t_m + u_m = \delta_m + (p-1)$, $0 \leq t, u < p^{n-1}$, $0 \leq t_m, u_m \leq p-1$ and $1 \leq k \leq p - \delta_{n-1}$. We may write

$$p^n i + p^{n-1}(\delta_{n-1} - (k-1)(p-1)) + t = p^n(i-k+1) + p^{n-1}(\delta_{n-1}+k-1) + t$$

where we see that

$$0 \leq \delta_{n-1} - 1 \leq \delta_{n-1} + k - 1 \leq \delta_{n-1} + (p - \delta_{n-1}) - 1 = p-1.$$

And we may write

$$p^n j + p^{n-1}(p-1)k + u = p^n(j+k-1) + p^{n-1}(p-k) + u$$

where, again, $0 \le p-k \le p-1$. So $\delta_{n-1}+k-1$ and $p-k$ are the $(n-1)^{\mathrm{st}}$ digits of their respective subscripts. Hence $M_\tau^{n-1} \cap \ker P^{p^{n-1}} \subseteq M_\tau^n$. We may assume, inductively, that $\ker P^1 \cap \cdots \cap \ker P^{p^{n-2}} \subseteq M_\tau^{n-1}$, whence the corollary. □

3.2 Link terminology

Each P^{p^n}–link determines an element of the kernel of P^{p^n}, and each monomial occurs in at most one link. Recall from Section 1 that each link formula *twins* with another formula (possibly itself), obtained by beginning a new link formula by reversing the subscripts of the last monomial of the given formula.

Remark 3.9 A link and its twin must be identical in M_* up to a scalar multiple, which must be given by the last coefficient, since the first coefficient is always one.

Definition 3.10 A *symmetric* link is one that is its own twin. That is, monomials $a_r a_s$ and $a_s a_r$ always occur together in the link formula, but possibly with different coefficients.

Remark 3.11 One checks that any Type 1 link formula, and any symmetric Type 2 link, has its last coefficient simply $(-1)^{r+1}$, where r is the number of monomials in the link. Hence a symmetric link with an even number of terms represents the zero element of M_*, while a symmetric link with an odd number of terms has nonzero symmetric coefficients, ie, the coefficients of $a_r a_s$ and $a_s a_r$ are the same. Then since two non-twin links have no monomials in common, the nonzero link twins produce a basis for $\ker P^{p^n} \cap M_\tau^n$. We also remark that the formulas show that every symmetric link lies in an even degree.

Remark 3.12 A monomial $a_i a_j$ is the summand of a Type 1 P^{p^n}–link with largest (resp. smallest) first index if and only if $j_n = p-1$ (resp. $i_n = p-1$).

Definition 3.13 We call the monomial that has the largest (resp. smallest) first index in a link the *left* (resp. *right*) end of the link.

4 The kernel of P^1 and booting

We specialize Theorem 3.5 to the case $n=0$, setting $\delta_0 = D_0 - 1$.

Theorem 4.1 *In degree $\tau = pl + D_0 - 2$, $l \geq 1$, $1 \leq D_0 \leq p$, we have a spanning set for* $\ker P^1$

$$\left\{ \sum_{k=1}^{p-D_0+1} \binom{k+D_0-2}{D_0-1} a_{pi+D_0+p-2-(p-1)k}\, a_{pj+(p-1)k} \;\middle|\; i+j = l-1,\ i,j \in \mathbb{Z} \right\}$$

$$\bigcup \left\{ \sum_{k=1}^{l+1} (-1)^{k+1} \binom{D_0-u+k-3}{k-1} \Big/ \binom{u}{k-1} a_{pl+D_0-2-u-(p-1)(k-1)} a_{u+(p-1)(k-1)} \;\middle|\; l \leq u \leq D_0 - 2 \right\}.$$

(Note that these are just the Type 1 elements $v(i, D_0, l)$ and the Type 2 $w(u, D_0, l)$ defined in the introduction. We further note that since elements of Type 2 lie in degrees $\tau \leq p^2 - p - 2$ from Remark 3.7, they are all primitive.)

We can now prove the booting Theorem 2.7.

Proof of Theorem 2.7 In these degrees, $\ker(P^1)$ has only Type 1 formulas. Letting $D_0 = p$ in these formulas, we get

$$\left\{ \sum_{k=1}^{1} \binom{k+p-2}{p-1} a_{pi+(2p-2)-(p-1)k} a_{pj+(p-1)k} \;\middle|\; i+j = l-1 \right\},$$

reducing to

$$\{a_{pi+(p-1)} a_{pj+(p-1)} \mid i+j = l\},$$

which is just $\{d_2(a_i a_j) \mid i+j = l\}$. □

5 The mid-low range: proof of Theorem 1.3

To prove Theorem 1.3, we first note that in the mid-low degrees $p-1 \leq \tau \leq p^2+p-2$, the primitives are exactly the kernel of P^1. This is because the only possible action of higher p^{th} powers would be P^p on degrees from p^2 to p^2+p-2. In that range there are no Type 2 formulas for $\ker P^1$ (Remark 3.7), and it is easy to see that Type 1 monomials for P^1 in that range all have both subscripts less than p^2, hence are in the kernel of P^p. Thus we need only identify a d_2–basis for $\ker P^1$ in the mid-low range, accomplished by the following two lemmas.

Lemma 5.1 *Let $p-1 \leq \tau \leq p^2+p-2$. Write $\tau = lp + D_0 - 2$, where $1 \leq l \leq p$ and $1 \leq D_0 \leq p$. The Type 1 d_2–basis elements are given by $v(i, D_0, l)$, for $0 \leq i \leq$*

$[(p+l-D_0-2)/2]$, *together with* $i=(p+l-D_0-1)/2$ *if* τ *is even and* D_0 *is odd, except when* $D_0=p$, *for which there are no* d_2*–basis elements.*

Proof We may arrange the live Type 1 monomials in a $l\times(p-D_0+1)$ matrix in which the $(r,s)^{\text{th}}$ entry $(r,s\geq 1)$ is $a_{p(l-r+1)-s}a_{p(r-1)+D_0-2+s}$. Then the P^1–links correspond to the upper right to lower left diagonals of this matrix (Theorem 4.1). A $\mathbb{F}_p$–basis for $\ker P^1$ follows by checking which of these diagonals represent the same basis element of $\ker P^1$, and which cancel to zero, per Remark 3.11. In degrees with $D_0\neq p$, Corollary 2.9 ensures that this forms a d_2–basis. In degrees with $D_0=p$, the proof of Theorem 2.7, which clearly applies to Type 1 P^1–links in any degree, shows that the $\mathbb{F}_p$–basis is in the image of d_2. □

Lemma 5.2 *Let* $\tau=pl+D_0-2$, $1\leq l\leq p$ *and* $1\leq D_0\leq p$. *(So* $p-1\leq\tau\leq p^2+p-2$.*) Then a* d_2*–basis for the Type 2* $\ker P^1$ *elements consists of* $w(u,D_0,l)$ *for* $l\leq u\leq l+[(D_0-l-3)/2]$, *together with* $u=l+(D_0-l-2)/2$ *if* τ *and* D_0 *are both even.*

Proof From the definition of d_2 it is clear that its image involves only monomials of Type 1 for P^1. Thus a d_2–basis for the Type 2 $\ker P^1$ elements is the same as a $\mathbb{F}_2$–basis. In the formulas for Type 2 elements (Theorem 4.1), we see these formulas are indexed by the variable u, which ranges $l\leq u\leq D_0-2$, so there are D_0-1-l of them, if D_0-1-l is non-negative. By Remark 3.11, if τ is odd, none of these can be symmetric, so there are $(D_0-1-l)/2$ basis elements. If τ is even, there will be exactly one symmetric formula, leaving D_0-2-l non-symmetric ones, from which $(D_0-2-l)/2$ basis elements. Since there are $l+1$ terms in the symmetric formula, if l is even the symmetric terms in this formula cancel pair-wise, so this formula represents the zero element. Similarly, if l is odd, the symmetric terms double up, producing one additional basis element. □

6 The intersection $\ker P^1\cap\ker P^p$ and the upper-low range

We have the following fundamental theorem, from which we will prove Theorem 1.2.

Theorem 6.1 *Let* $\tau=p^2l+D_1p+D_0-2$, *with* $1\leq D_0\leq p-1$, $0\leq D_1\leq p-1$ *and* $l\geq 1$. *Suppose a live monomial* a_ia_j, *with* $j\geq p^2$, *appears in the symmetric expression of an element* $x\in\ker P^1\cap\ker P^p$ *in degree* τ. *Then* $D_1=0$.

The proof of this theorem follows a sequence of technical lemmas.

Lemma 6.2 *Let $\tau = p^2 l + D_1 p + D_0 - 2$, with $1 \le D_0 \le p-1$, $0 \le D_1 \le p-1$ and $l \ge 1$. Suppose that $a_i a_j$ and $a_{i+(p-1)} a_{j-(p-1)}$ both appear in the link $v(I, D_0, l)$, and that $a_{i+p(p-1)} a_{j-p(p-1)}$ and $a_{i+(p^2-1)} a_{j-(p^2-1)}$ appear in $v(I+(p-1), D_0, l)$. Then if both of these links are nonzero summands of an element x expressed in symmetric form of* $\ker P^1 \cap \ker P^p$, *we must have $D_1 = 0$.*

Proof Recall that "appear" means a monomial is live with nonzero coefficient in the symmetric form of an element. Let A and B be the coefficients in $v(I, D_0, l)$ of $a_i a_j$ and $a_{i+(p-1)} a_{j-(p-1)}$ (necessarily the same, respectively, as those of

$$a_{i+p(p-1)} a_{j-p(p-1)} \quad \text{and} \quad a_{i+(p^2-1)} a_{j-(p^2-1)}$$

in $v(I + (p-1), D_0, l)$). And let M and N be the coefficients in x of $v(I, D_0, l)$ and $v(I + (p-1), D_0, l)$.

We calculate the coefficients arising from P^p acting on the four monomials. We have: $(MAa_i a_j)P^p$ has the summand

$$MA\binom{j-p(p-1)}{p} a_{i,j-p(p-1)} = MA(j_1+1) a_{i,j-p(p-1)},$$

and $(NAa_{i+p(p-1)} a_{j-p(p-1)})P^p$ has the summand

$$NA\binom{i}{p} a_{i,j-p(p-1)} = NA(i_1) a_{i,j-p(p-1)},$$

whence, noting that $a_{i,j-p(p-1)}$ is live,

$$MA(j_1+1) + NA(i_1) = 0$$

for x to be in the kernel of P^p. To calculate further, we first need to note that $j_0 \ne p-1$ since $a_i a_j$ is not the left end of its P^1 link, and that therefore $i_0 \ne 0$ since $i_0 + j_0 \ge p-1$.

In similar fashion we now compute that for x to be in the kernel of P^p, we need

$$MB(j_1) + NB(i_1+1) = 0.$$

Combining these two equations, we see that $M = N$, and so

$$(j_1+1) + (i_1) \equiv 0 \bmod p.$$

Now since $a_i a_j$ is Type 1 for P^1, we also have $i_0 + j_0 = D_0 - 2 + p$ (Remark 3.3). Combining the latter two equations with $p(i_1+j_1) + i_0 + j_0 \equiv pD_1 + D_0 - 2 \bmod (p^2)$ yields

$$p(i_1 + j_1 + 1) \equiv pD_1 \bmod p^2, \qquad 0 \equiv D_1 \bmod p,$$

thus $D_1 = 0$. □

We can now eliminate Type 2 links for P^p from consideration in $\ker P^1 \cap \ker P^p$.

Lemma 6.3 *No Type 2 nonzero monomial of* $\ker P^p$ *in any degree* $\tau = p^2 l + D_1 p + D_0 - 2$, $1 \le D_0 \le p-1$, $0 \le D_1 \le p-1$, $l \ge 1$, *appears in any element of* $\ker P^1 \cap \ker P^p$.

Proof If our monomial is not part of a P^p–link, we are done. So consider the Type 2 P^p–link

$$\left\{\sum_{k=1}^{l+1}(-1)^{k+1}\binom{t_1+k-1}{k-1}\Big/\binom{u_1}{k-1}a_{p^2l+t-(p-1)(k-1)p}a_{u+(p-1)(k-1)p}\ \middle|\ 0 \le t,u < p^2, t_0+u_0 = D_0+(p-2),\ l \le u_1,\ t_1+u_1 = D_1-1\right\}.$$

We may assume that $D_1 \ne 0$, since from these formulas there are no Type 2 elements for P^p when $D_1 = 0$. Since $l \ge 1$, there are always at least two nonzero summands. When $k = 1$, we have

$$a_{p^2l+t}a_u,$$

and when $k = 2$, we have

$$-a_{p^2(l-1)+p+t}a_{p^2-p+u}.$$

Write

$$i = p^2(l-1)+p+t \quad \text{and} \quad j = p^2-p+u.$$

Case 1 Assume $u_0 \ne p-1$. In this case, if a_ia_j appears also in some $v(I,D_0,l)$ (from Theorem 4.1 there are no w's in these degrees), then $a_{i+(p-1)}a_{j-(p-1)}$ also appears in $v(I,D_0,l)$. Similarly with $a_{i+p(p-1)}a_{j-p(p-1)}$ and $a_{i+p^2-1}a_{j-(p^2-1)}$, which are live since $u_1 \ge 1$. Hence we have the hypotheses of Lemma 6.2, and arrive at a contradiction to $D_1 \ne 0$.

Case 2 Assume $u_0 = p-1$, so then $t_0 \ne p-1$ (since $D_0 \ne p$). We use a similar calculation to Case 1, this time using the terms for which $k = l$ and $k = l+1$. □

Lemma 6.4 *Suppose* $\tau = p^2l + D_1p + D_0 - 2$, *with* $1 \le D_0, D_1 \le p-1$ *and* $l \ge 1$. *If a live monomial appears in the symmetric expression of an element* $x \in \ker P^1 \cap \ker P^p$ *as the leftmost monomial in a* P^p*–link, then the monomial must lie at the right end of its* P^1*–link.*

Proof First, from Remark 3.7 and Lemma 6.3 above, all links are Type 1 for both P^1 and P^p. Since the monomial a_ia_j is at the left end of a Type 1 P^p link, it must have

$j_1 = p-1$. Suppose the monomial lies elsewhere in its P^1 link than at the right end. Then $i_0 \neq p-1$. The adjacent term to the right in the P^1 link is $a_{i-(p-1)}a_{j+(p-1)}$. It is live since $a_i a_j$ is Type 1 for P^p, ie, $i_1 + j_1 = D_1 + p - 1$ (Remark 3.3), which is in turn at least p by the hypothesis $D_1 \geq 1$. So $i_1 > 0$, and therefore $i \geq p$.

Since $a_{i-(p-1)}a_{j+(p-1)}$ is live, appearing in our symmetric expression of x, it must also appear in a Type 1 P^p link. We compute next from its subscripts. Since $i_0 \neq p-1$, we have $j_0 \neq 0$, since $a_i a_j$ lies in M^1_τ. Now since $j_0 \neq 0$, we have $j + (p-1) = (*, 0, \dots)$. Thus the sum of the p's digits of $i-(p-1)$ and $j+(p-1)$ cannot exceed $p-1$. On the other hand, from Remark 3.3, this sum equals $D_1 + (p-1)$, contradicting our hypothesis that $D_1 \neq 0$. □

Proof of Theorem 6.1 Suppose $D_1 \neq 0$, and consider the nonzero P^1–link that $a_i a_j$ lies in, $v(I, D_0, pl + D_1)$, necessarily of at least two terms since $D_0 < p$.

Case 1 $v(I, D_0, pl + D_1)$ includes the monomial $a_{i+(p-1)}a_{j-(p-1)}$, necessarily live since $j \geq p^2$. Since x lies in $\ker P^{p^n}$ as well as $\ker P^1$, $a_{i+(p-1)}a_{j-(p-1)}$ also appears in a P^p–link. Since $a_{i+(p-1)}a_{j-(p-1)}$ is not the right end of $v(I, D_0, pl + D_1)$, by Lemma 6.4 it is not the left end of its P^p–link. Thus its P^p–link must contain $a_{i+(p-1)+p(p-1)}a_{j-(p-1)-p(p-1)}$, which is live since $j \geq p^2$.

Clearly $a_{i+(p-1)+p(p-1)}a_{j-(p-1)-p(p-1)}$ appears in $v(I + (p-1), D_0, pl + D_1)$ in the same relative position that $a_{i+(p-1)}a_{j-(p-1)}$ does in $v(I, D_0, pl + D_1)$. Hence $a_{i+p(p-1)}a_{j-p(p-1)}$ also appears in $v(I + (p-1), D_0, pl + D_1)$. We now apply Lemma 6.2, obtaining the desired contradiction to the supposition $D_1 \neq 0$.

Case 2 The P^1–link does not include the monomial $a_{i+(p-1)}a_{j-(p-1)}$. In this case, the P^1 link that $a_i a_j$ lies in contains a monomial to the right of $a_i a_j$, so we can replace $a_i a_j$ by the monomial $a_{i-(p-1)}a_{j+(p-1)}$ (provided this monomial is nonzero) and make the argument exactly as above. If the monomial $a_{i-(p-1)}a_{j+(p-1)}$ is zero, we must have $i < p$. Thus $i = (i_0, 0, 0, \dots)$ and $j = (j_0, j_1, \dots)$, and so, since $a_i a_j$ was hypothesized to be of Type 1 for P^p, we have $D_1 + p - 1 = 0 + j_1 \leq p - 1$, whence again $D_1 = 0$. □

Theorem 6.5 *Consider a degree $p^2 + p - 1 \leq \tau \leq 2p^2 - 1$ that is of the form*

$$\tau = p^2 + D_1 p + D_0 - 2, \quad 1 \leq D_0, D_1 \leq p-1.$$

Suppose a monomial $a_i a_j$ appears in the symmetric expression of an element of $\ker P^1 \cap \ker P^p$. Then $i, j < p^2$. Hence $\ker P^1 \cap \ker P^p$ is spanned by those P^1–links, all of whose nonzero monomials have both indices less than p^2.

Proof Suppose a monomial $a_i a_j$ appears in the symmetric expression of an element of $\ker P^1 \cap \ker P^p$, and assume without loss of generality that $i \le j$, and $j \ge p^2$. We apply Theorem 6.1 with $l = 1$ to show $D_1 = 0$, a contradiction. □

We can now prove Theorem 1.2.

Proof of Theorem 1.2 Consider a P^1–link in degree τ. By the previous theorem, the smallest possible second index of a monomial in this link is of the form $(D_1+q)p+(p-1)$ for some $q \ge 0$, and the largest second index of this link is $(D_1+q)p+(p-1)+(p-D_0)(p-1)$. We must also have this index less than p^2. Solving the inequality

$$(D_1+q)p+(p-1)+(p-D_0)(p-1) \le p^2-1,$$

for q, we obtain $q \le D_0 - D_1 - 1$. The number of links is thus $D_0 - D_1$. The theorem follows by using Remark 3.11 to see when these links double up or cancel out, and noting that in this range of degrees the primitives are exactly $\ker P^1 \cap \ker P^p$. □

7 The stable range

We assume $\tau \ge 2p^2-1$ with $\tau = p^2 l + D_1 p + D_0 - 2$, $1 \le D_0 \le p-1$, $0 \le D_1 \le p-1$ and $l \ge 2$. First we see why the primitives all lie in degrees where $D_1 = 0$.

Theorem 7.1 *Consider a degree $\tau \ge 2p^2-1$ that is of the form*

$$\tau = p^2 l + D_1 p + D_0 - 2, \quad 1 \le D_0, D_1 \le p-1.$$

Then $\ker P^1 \cap \ker P^p = 0$. Hence there are no primitives in degree τ.

Proof Suppose a live monomial $a_i a_j$ appears in the symmetric expression of an element of $\ker P^1 \cap \ker P^p$, and assume without loss of generality that $i \le j$. Hence $j \ge \tau/2 \ge p^2$. We apply Theorem 6.1 to show $D_1 = 0$, a contradiction. □

Remark 7.2 When $D_1 = 0$, all monomials are of Type 1 for P^p.

Lemma 7.3 *If $\tau = p^2 l + D_0 - 2$, $1 \le D_0 \le p-1$, $l \ge 2$, then any P^1–link in which the terms $a_i a_j$ and $a_{i+(p-1)} a_{j-(p-1)}$ appear has at least one of these two also appearing in a P^p–link that has a monomial (not necessarily live) with greater first index, and at least one of these two appearing in a P^p–link that has a monomial (not necessarily live) with smaller first index.*

Proof Note first that $i_1 + j_1 = p - 1$ by Remark 3.3. Note next that $i_0 \neq 0$ and $j_0 \neq p-1$ since $a_{i+(p-1)}a_{j-(p-1)}$ is not the right end of its P^1–link.

If neither i_1 nor j_1 is $p-1$, then the P^p–link of which $a_i a_j$ is a summand has monomial summands with both larger and smaller first indices, by Remark 3.12.

Otherwise, if $i_1 = p-1$, then $j_1 = 0$ and the p's–digit of $i + (p-1)$ is 0, hence the P^p–link of which $a_i a_j$ is a summand has a monomial summand with larger first index and the P^p–link of which $a_{i+(p-1)}a_{j-(p-1)}$ is a summand has a monomial summand with smaller first index.

Finally, if $j_1 = p-1$, then the p's digit of $j - (p-1)$ is $p-2$ and $i_1 = 0$, so the P^p–link of which $a_{i+(p-1)}a_{j-(p-1)}$ is a summand has a monomial summand with larger first index and the P^p–link of which $a_i a_j$ is a summand has a monomial summand with smaller first index. □

Corollary 7.4 *As a consequence, if $\tau \geq 2p^2 - 1$ is of the form $\tau = p^2 l + D_0 - 2$, with $1 \leq D_0 \leq p-1$ and $l \geq 2$, then $\ker P^1 \cap \ker P^p$ is spanned by the set*

$$\{x(c, D_0, l) \mid 0 \leq c \leq p-2\},$$

together with $a_{p^2 l - 1} a_{D_0 - 1}$.

Proof First, the elements $x(c, D_0, l)$ are all in $\ker P^1 \cap \ker P^p$, as one sees from the equality of the coefficients M and N on the v's in the proof of Lemma 6.2. The rigidity explained in the proof of Theorem 3.5 dictates that $\ker P^1 \cap \ker P^p$ is spanned by a set of minimal nonoverlapping sums of monomials. The lemma above ensures that each x is minimal, except when the formula has a v with just one live monomial $a_{p^2 l-1} a_{D_0-1}$ (or its twin), to which the lemma does not apply. This monomial is a separate spanning element of $\ker P^1 \cap \ker P^p$, but we may also still leave it in the formula of its x as a convenience. Every Type 1 monomial for P^1 appears in one of the x's, so the listed formulas span. □

Not all of the elements $x(c, D_0, l)$ in the spanning set given in the previous corollary are nonzero, nor are they all distinct. We now proceed to determine a basis for $\ker P^1 \cap \ker P^p$ in the degrees of the corollary.

Since both the entries in $\mathrm{LAB}(c, D_0, l)$ vary through all the integers mod $(p-1)$, we see that if $\mathrm{LAB}(c, D_0, l)$ has two elements, there exists a $c_1 \neq c$ such that $\mathrm{LAB}(c, D_0, l) = \mathrm{LAB}(c_1, D_0, l)$ and $x(c, D_0, l)$ is a unit multiple of $x(c_1, D_0, l)$. Hence we may choose exactly one of these as a basis element for $\ker P^1 \cap \ker P^p$.

Alternatively, if $\mathrm{LAB}(c, D_0, l)$ consists of a single element, then we have $c + D_0 - 1 \equiv l - c - 1 \bmod (p-1)$. In this case, τ must be even, since if $l - D_0$ is odd, this congruence has no solution. With $l - D_0$ even, there are two solutions, $c \equiv (l - D_0)/2$ and $c \equiv (l - D_0 + (p-1))/2 \bmod (p-1)$, with different labels. For one of these, there will be a single symmetric v in the formula for x; in the other the v's all match in twin pairs. Whether or not these cancel or double up depends as in Remark 3.11 on whether the final coefficient in each v is 1 or -1. So if D_0 is even, both values of c give $x(c, D_0, l) = 0$, while for D_0 odd, each of these values of c gives us a distinct basis element for $\ker P^1 \cap \ker P^p$.

This gives us our desired basis for $\ker P^1 \cap \ker P^p$ in all degrees of the form $\tau = p^2 l + D_0 - 2$, $1 \le D_0 \le p-1$, $l \ge 2$. The next theorem determines the primitives in these degrees.

Theorem 7.5 *Let $m \ge 2$ and $p^m - 1 \le \tau \le p^{m+1} - 3$, where $\tau = p^2 l + D_0 - 2$, $1 \le D_0 \le p-1$, $l \ge 2$. Under these hypotheses, M_τ has primitive elements if and only if τ is of the form $\tau = D_m p^m + D_0 - 2$ for some $1 \le D_0, D_m \le p-1$. Conversely, if $\tau = D_m p^m + D_0 - 2$ for some $1 \le D_0, D_m \le p-1$, then $S_\tau = \ker P^1 \cap \ker P^p$.*

Proof Let $2 \le n < m$. Inductively suppose that if a nonzero linear combination of basis elements from $\ker P^1 \cap \ker P^p$ is in $\ker P^1 \cap \dots \cap \ker P^{p^{n-1}}$, then $\tau = \bar{q} p^n + D_0 - 2$ for some $\bar{q} \ge 1$, and $1 \le D_0 \le p-1$. Furthermore assume that if τ is of this form, that $\ker P^1 \cap \dots \cap \ker P^{p^{n-1}} = \ker P^1 \cap \ker P^p$.

Now, to prove the inductive step, we consider P^{p^n} on an element of $\ker P^1 \cap \ker P^p$.

Assume that a nonzero linear combination of basis elements for $\ker P^1 \cap \ker P^p$ is in $\ker P^1 \cap \dots \cap \ker P^{p^{n-1}}$, equivalently by our inductive hypothesis, that τ has the form above. Let $x(c, D_0, l)$ be any of these basis elements. Since $\tau \ge p^{n+1} - 1$, this element is in M^n_τ, by Corollary 3.8. Write

$$R = p(c + r(p-1) + 1) - (p-1)k + D_0 - 2.$$

Applying P^{p^n} to the element $x(c, D_0, l)$, we obtain

$$\sum_r \sum_{k=1}^{p-D_0+1} \binom{k + D_0 - 2}{D_0 - 1} \Bigg[\binom{R - p^n(p-1)}{p^n} a_{R-p^n(p-1)} a_{\tau-R} + \binom{\tau - R - p^n(p-1)}{p^n} a_R a_{\tau-R-p^n(p-1)} \Bigg].$$

We note, by examining the subscripts mod $(p-1)$ in this expression, that they are just those of $\mathrm{LAB}(c, D_0, l)$, so, since the basis elements have distinct labels, the linear combination lies in $\ker P^{p^n}$ if and only if the individual elements $x(c, D_0, l)$ lie in $\ker P^1 \cap \cdots \cap \ker P^{p^n}$. Re-indexing the first of the bracketed terms, we get

$$\sum_{k=1}^{p-D_0+1} \binom{k+D_0-2}{D_0-1} \sum_r \left[\binom{R}{p^n} + \binom{\tau - R - p^n(p-1)}{p^n} \right] a_R a_{\tau - R - p^n(p-1)}.$$

For the $x(c, D_0, l)$ to be in $\ker P^{p^n}$, it is necessary and sufficient that for all such R, the sum

$$\binom{R}{p^n} + \binom{\tau - R - p^n(p-1)}{p^n}$$

is zero.

Case 1 Assume that $D_0 = 1$, so that $\tau = (p-1, \dots, p-1, \tau_n, *, *, \dots)$. Then

$$\binom{\tau - R - p^n(p-1)}{p^n} = \tau_n + 1 - R_n,$$

so the sum

$$\binom{R}{p^n} + \binom{\tau - R - p^n(p-1)}{p^n} = \tau_n + 1,$$

and hence will be zero for all such R if and only if $\tau_n = p-1$, ie, if and only if $\tau = \overline{q_1} p^{n+1} - 1$ for some $\overline{q_1} \geq 1$.

Case 2 Assume that $D_0 \geq 2$, so that $\tau = (D_0 - 2, 0, \dots, \tau_n, *, *, \dots)$. Here, from the form of R above, and since $k \leq p - D_0 + 1$, we have

$$R_0 = D_0 + k - 2 > D_0 - 2 = \tau_0,$$

and get

$$\binom{\tau - R - p^n(p-1)}{p^n} = \tau_n - R_n,$$

whence

$$\binom{R}{p^n} + \binom{\tau - R - p^n(p-1)}{p^n} = \tau_n,$$

and so we are in $\ker P^{p^n}$ if and only if $\tau_n = 0$, ie, if and only if $\tau = \overline{q_1} p^{n+1} + D_0 - 2$ for some $\overline{q_1} \geq 1$. This accomplishes the inductive step.

Finally, note that if $n = m-1$, since $\tau \leq p^{m+1} - 2$ we have $1 \leq q_1 \leq p-1$, so taking $q = q_1$ completes the proof. □

References

[1] **M D Crossley**, *$\mathcal{A}(p)$-annihilated elements in $H_*(\mathbf{CP}^\infty \times \mathbf{CP}^\infty)$*, Math. Proc. Cambridge Philos. Soc. 120 (1996) 441–453 MR1388199

[2] **M D Crossley**, *Monomial bases for $H^*(\mathbf{CP}^\infty \times \mathbf{CP}^\infty)$ over $\mathcal{A}(p)$*, Trans. Amer. Math. Soc. 351 (1999) 171–192 MR1451596

[3] **A S Janfada**, **R M W Wood**, *The hit problem for symmetric polynomials over the Steenrod algebra*, Math. Proc. Cambridge Philos. Soc. 133 (2002) 295–303 MR1912402

[4] **A S Janfada**, **R M W Wood**, *Generating $H^*(\mathrm{BO}(3), \mathbb{F}_2)$ as a module over the Steenrod algebra*, Math. Proc. Cambridge Philos. Soc. 134 (2003) 239–258 MR1972137

[5] **M Kameko**, *Generators of the cohomology of BV_3*, J. Math. Kyoto Univ. 38 (1998) 587–593 MR1661173

[6] **D Pengelley**, **F Williams**, *A new action of the Kudo–Araki–May algebra on the dual of the symmetric algebras, with applications to the hit problem*, Algebr. Geom. Topol. 11 (2011) 1767–1780 MR2821440

[7] **F P Peterson**, *A-generators for certain polynomial algebras*, Math. Proc. Cambridge Philos. Soc. 105 (1989) 311–312 MR974987

[8] **W M Singer**, *Rings of symmetric functions as modules over the Steenrod algebra*, Algebr. Geom. Topol. 8 (2008) 541–562 MR2443237

[9] **R M W Wood**, *Steenrod squares of polynomials and the Peterson conjecture*, Math. Proc. Cambridge Philos. Soc. 105 (1989) 307–309 MR974986

Department of Mathematical Sciences, New Mexico State University
Las Cruces, NM 88003-8001, USA

davidp@nmsu.edu, frank@nmsu.edu

http://www.math.nmsu.edu/~davidp/

Received: 7 October 2012 Revised: 23 January 2013