

MONOMIAL BASES FOR $H^*(CP^\infty \times CP^\infty)$ OVER $\mathcal{A}(p)$

M. D. CROSSLEY

ABSTRACT. We consider the polynomial algebra $H^*(CP^\infty \times CP^\infty; \mathbf{F}_p)$ as a module over the mod p Steenrod algebra, $\mathcal{A}(p)$, p being an odd prime. We give a minimal set of generators consisting of monomials and characterise all such ‘monomial bases’.

1. INTRODUCTION

We are concerned with the problem of finding minimal sets of generators for $H^*(BV; \mathbf{F}_p)$ as a module over the mod p Steenrod algebra $\mathcal{A}(p)$, where V is an elementary abelian p -group.

Some reasons for studying this problem are the following. All simple representations of $GL(V)$ over \mathbf{F}_p can be found as composition factors in the vector space spanned by a minimal set of generators, as explained in [10] for the prime 2, the argument being valid for odd primes as well. There is also a map to the $GL(V)$ invariants of this space of generators from the dual of the E_2 term of the classical Adams spectral sequence for the stable homotopy groups of spheres, which, at least in low degrees, is an isomorphism - see [7] and [4]. The central rôle that $H^*(BV; \mathbf{F}_p)$ plays in the theory of unstable modules over the Steenrod algebra, see [6], also adds interest to this problem.

However the problem is seen to be particularly difficult in general, as is gauged by our progress. It is known how to construct sets of generators for any such V (e.g. the ‘regular’ monomials of [2] and [5]) but these are far from minimal in general. On the other hand, it is known how to construct minimal sets of generators for some such V , but only if V has rank ≤ 2 (or ≤ 3 if $p = 2$) [1], [3].

This paper is concerned with odd primes, for which there is an intermediate problem. $H^*(BV; \mathbf{F}_p)$ is a tensor product, $S(V^*) \otimes \Lambda(V^*)$, of a symmetric algebra and an exterior algebra. As an algebra over the Steenrod algebra, $S(V^*)$ may be identified with $H^*(CP^\infty \times \cdots \times CP^\infty; \mathbf{F}_p)$, the cohomology of a product of rank V copies of infinite complex projective space. Thus we have the intermediate problem of finding minimal sets of generators for $H^*(CP^\infty \times \cdots \times CP^\infty; \mathbf{F}_p)$. In [3] we calculated the subring $M_*(2)$ of $H_*(CP^\infty \times CP^\infty; \mathbf{F}_p)$ that consists of all elements annihilated by the right action of $\mathcal{A}(p)$ defined by

$$\langle \xi\theta, \zeta \rangle = \langle \xi, \theta\zeta \rangle$$

where $\theta \in \mathcal{A}(p)$, $\xi \in H_*(CP^\infty \times CP^\infty; \mathbf{F}_p)$ and $\zeta \in H^*(CP^\infty \times CP^\infty; \mathbf{F}_p)$.

Received by the editors November 12, 1996.

1991 *Mathematics Subject Classification*. Primary 55S10.

The author was supported by a DGICYT grant and Leibniz Fellowship and gratefully acknowledges the hospitality of the Centre de Recerca Matemàtica in Barcelona.

©1999 American Mathematical Society

From this it is possible to describe the space

$$M^*(2) = \mathbf{F}_p \otimes_{\mathcal{A}(p)} H^*(CP^\infty \times CP^\infty; \mathbf{F}_p),$$

whose bases correspond to minimal sets of generators for $H^*(CP^\infty \times CP^\infty; \mathbf{F}_p)$ as a module over $\mathcal{A}(p)$, since $M^*(2)$ is the vector space dual of $M_*(2)$. However, the generators one obtains by this method consist of large intractable polynomials (cf. Table 1 of the first version of [4] - C.R.M. preprint **323**, Centre de Recerca Matemàtica, Barcelona). So, in practice, the results of [3] serve only to tell us the dimension of $M^n(2)$ in each degree n , that is, they give us the Poincaré series of $M^*(2)$. In order to perform calculations we ideally require a basis for $M^*(2)$ that consists of *monomials* and it is the purpose of this paper to provide such a basis. An example of the type of calculation that a monomial basis facilitates is contained in [5]: conjecture 5.3 of that paper is quickly seen to be false using the basis given by Theorem 1.1 (and Statement 1.2) below. As it turns out, the calculations required to obtain this basis easily yield all possible monomial bases. Thus rather than just describing one monomial basis this paper describes all possible monomial bases.

The original intention of the author was to obtain such a basis from the polynomials derived from [3]. As the work progressed, however, it became apparent that one should ignore these polynomials and work, more or less, from first principles. Thus we offer a proof, independent of [3], of the following theorem.

Theorem 1.1. *As far as it goes, Table 1 gives a monomial basis for $M^*(2)$.*

That is to say, if n can be found in the left hand column of Table 1, then the right hand column gives a basis for $M^n(2)$. In Table 1 we have chosen two elements $x, y \in H^2(CP^\infty \times CP^\infty; \mathbf{F}_p)$ such that $H^*(CP^\infty \times CP^\infty; \mathbf{F}_p)$ is isomorphic to the polynomial algebra on x and y . We also use the same symbol for an element in $H^*(CP^\infty \times CP^\infty; \mathbf{F}_p)$ as for its image under the natural projection

$$H^*(CP^\infty \times CP^\infty; \mathbf{F}_p) \rightarrow M^*(2).$$

TABLE 1

Degree, n	Basis for $M^n(2)$
$\leq 2(p-2), n$ even	$\{x^i y^{n/2-i} \mid 0 \leq i \leq n\}$
$2(((i+1)p + j + 1)p^s - 2)$ $0 \leq i, j \leq p-1, s \geq 0$	$\{x^{(k+1)p^s-1} y^{n/2-(k+1)p^s+1} \mid \min(i+1, j) \leq k \leq p-1\}$ $\cup \{x^{(k+1)p^{s+1}-1} y^{n/2-(k+1)p^{s+1}+1} \mid 0 \leq k \leq i\}$
$2(((i+1)p^r + j + 1)p^s - 2)$ $1 \leq i, j + 1 \leq p-1,$ $r \geq 2, s \geq 0$	$\{x^{(k+1)p^{s+1}-1} y^{n/2-(k+1)p^{s+1}+1} \mid 1 \leq k \leq p-1\}$ $\cup \{x^{(j+1)p^s-1} y^{(i+1)p^{r-s}-1}, x^{(i+1)p^{r-s}-1} y^{(j+1)p^s-1}\}$
$2((p^2 + ip + j + 1)p^s - 2)$ $1 \leq i \leq j \leq p-2, s \geq 0$	$\{x^{(k+1)p^{s+1}-1} y^{n/2-(k+1)p^{s+1}+1} \mid i \leq k \leq j\}$

However, in addition to this theorem we need the following complementary result.

Statement 1.2. *In the degrees, n , not dealt with by Table 1, $M^n(2)$ is 0.*

So, for example, Theorem 1.1 tells us nothing about $M^n(2)$ when $n = 2(p^2 + p - 1)$ but Statement 1.2 reassures us that there is nothing to tell in this case: $M^n(2) = 0$.

One can view this statement 1.2 as a conclusion of [3], or one could attempt to re-work the proof given in [3] for the cohomological setting. (Note that this proof was an induction on degree, using the given description of $M_*(2)$ in an essential way, so such a re-working could be expected to be a large task.) What we would like to do, but have so far been unable to, is to give a bare-handed proof, independent of the results of Theorem 1.1.

As mentioned earlier, we have, in fact, gone further than Theorem 1.1; we have calculated all possible monomial bases for $M^*(2)$. However it would not be feasible to state the conclusions of this study in tabular form. Instead we will describe the other possible monomial bases, for each row of Table 1, in the section concerned with that row; see Propositions 3.2, 4.5, 5.2 and 6.3.

The author would like to express his gratitude to the referee for his/her comments which, the author believes, have enabled this version to be a significant improvement on earlier versions of this paper.

2. NOTATION AND SOME PRELIMINARY RESULTS

Binomial coefficients play a large part in what follows, since the action of $\mathcal{A}(p)$ on $H^*(\mathbf{C}P^\infty \times \mathbf{C}P^\infty; \mathbf{F}_p)$ can be succinctly expressed by

$$\mathcal{P}^i(x^s) = \binom{s}{i} x^{s+i(p-1)}$$

and the Cartan formula. We will use the convention that binomial coefficients take integer arguments but give values in \mathbf{F}_p . We will frequently need the following well-known formula for determining binomial coefficients modulo p :

$$(1) \quad \binom{n}{r} = \prod \binom{n_s}{r_s}$$

where $n_0 + pn_1 + p^2n_2 + \dots$ and $r_0 + pr_1 + p^2r_2 + \dots$ are the p -adic expansions for n and r respectively.

Another convention we wish to introduce concerns non-zero scalars. These are painfully ubiquitous and, since we frequently wish to multiply them but only rarely to add them, they are essentially irrelevant. For this reason we use the notation

$$\mathcal{P}^{p^q}(A) = B + C + \dots$$

to indicate that $\mathcal{P}^{p^q}(A) = \xi B + \xi' C + \dots$, where ξ and ξ' are some non-zero scalars. Thus, if we can establish that $\binom{q}{1} \neq 0$, and $\binom{r}{1} \neq 0$, we may write $\mathcal{P}^1(x^q y^r) = x^{q+(p-1)} y^r + x^q y^{r+(p-1)}$.

The following result highlights the periodic facet of $M^*(2)$.

Lemma 2.1. *Let $f : H^*(\mathbf{C}P^\infty \times \mathbf{C}P^\infty; \mathbf{F}_p) \rightarrow H^*(\mathbf{C}P^\infty \times \mathbf{C}P^\infty; \mathbf{F}_p)$ be the linear map defined by $f(X) = x^{p-1} y^{p-1} X^p$ for all $X \in H^*(\mathbf{C}P^\infty \times \mathbf{C}P^\infty; \mathbf{F}_p)$. Then f induces a map $M^n(2) \rightarrow M^{pn+2(2p-2)}(2)$ for all $n \geq 0$, which we will also denote by f , and if $n \geq 2(p-1)$, then this induced map is an isomorphism.*

In the terminology of Table 1, this lemma implies that we need only consider the case where $s = 0$, for it enables us to vary s while leaving $M^*(2)$ unchanged, up to an isomorphism given by f . For example, in row 2, if $n = 2(((i+1)p^r + j+1)p^s - 2)$ with $s > 0$, then $n = pm + 2(2p-2)$ where $m = 2(((i+1)p^r + j+1)p^{s-1} - 2)$ and f maps $M^m(2)$ isomorphically onto $M^n(2)$. So by iterating this we need only study $M^{n_0}(2)$ where $n_0 = 2(((i+1)p^r + j+1) - 2)$.

The proof of this lemma is rather involved, and requires a few results which will be used many more times in this work.

The first of these is the ‘short Cartan formula’. In order to state this result concisely we introduce the term *hit* to signify elements in the image of the map

$$\bar{\mathcal{A}}(p) \otimes H^*(CP^\infty \times CP^\infty; \mathbf{F}_p) \longrightarrow H^*(CP^\infty \times CP^\infty; \mathbf{F}_p),$$

where $\bar{\mathcal{A}}(p)$ denotes the augmentation ideal of $\mathcal{A}(p)$. More explicitly, an element is hit if it can be written as $\sum_{i>0} \mathcal{P}^i X_i$ for some polynomials $X_i \in H^*(CP^\infty \times CP^\infty; \mathbf{F}_p)$. Since every Steenrod operation \mathcal{P}^i is decomposable unless i is a power of p , we can conclude that an element is hit if and only if it can be written as $\sum_{i \geq 0} \mathcal{P}^{p^i} X_i$ for some polynomials X_i . Furthermore, we say an element is *hit by \mathcal{P}^j* if it can be written as $\sum_{i=1}^j \mathcal{P}^i X_i$. This is a weaker condition than saying that an element is in the image of \mathcal{P}^j , but turns out to be more useful for our purposes. We can now state the short Cartan formula:

Lemma 2.2 (Short Cartan formula). *For any $q, s, t \geq 0$,*

$$\mathcal{P}^{p^q}(x^s y^t) \equiv \mathcal{P}^{p^q}(x^s) y^t + x^s \mathcal{P}^{p^q}(y^t)$$

modulo elements hit by \mathcal{P}^{p^q-1} .

Proof. Note first that if $q = 0$, then the lemma is just the usual Cartan formula for \mathcal{P}^1 . Now let χ denote the anti-automorphism of $\mathcal{A}(p)$, let $s, t \geq 0$ and let $q \geq 1$. We first show that

$$(2) \quad \mathcal{P}^{p^q}(x^s y^t) \equiv \chi(\mathcal{P}^{p^q})(x^s) y^t + x^s \mathcal{P}^{p^q}(y^t) \text{ modulo elements hit by } \mathcal{P}^{p^q-1}.$$

To prove this, we use the (standard) Cartan formula to evaluate $\mathcal{P}^i(\chi(\mathcal{P}^{p^q-i})(x^s) y^t)$ for each $i \leq p^q$:

$$\mathcal{P}^i(\chi(\mathcal{P}^{p^q-i})(x^s) y^t) = \sum_{j=0}^i \mathcal{P}^{i-j} \chi(\mathcal{P}^{p^q-i})(x^s) \mathcal{P}^j(y^t)$$

and then take the sum over i running from 0 to p^q :

$$(3) \quad \sum_{i=0}^{p^q} \mathcal{P}^i(\chi(\mathcal{P}^{p^q-i})(x^s) y^t) = \sum_{i=0}^{p^q} \sum_{j=0}^i \mathcal{P}^{i-j} \chi(\mathcal{P}^{p^q-i})(x^s) \mathcal{P}^j(y^t).$$

Now recall the recursive definition of $\chi(\mathcal{P}^r)$ for any integer r :

$$\sum_{i=0}^r \mathcal{P}^i \chi(\mathcal{P}^{r-i}) = \begin{cases} 0 & \text{if } r > 0, \\ 1 & \text{if } r = 0. \end{cases}$$

Then by reordering the summations on the right side of equation (3) and using this defining formula for $\chi(\mathcal{P}^r)$, we have

$$\sum_{i=0}^{p^q} \mathcal{P}^i(\chi(\mathcal{P}^{p^q-i})(x^s) y^t) = x^s \mathcal{P}^{p^q}(y^t).$$

Separating out the $i = 0$ and $i = p^q$ terms from the left hand summation we have

$$\chi(\mathcal{P}^{p^q})(x^s) y^t + \mathcal{P}^{p^q}(x^s y^t) + Z = x^s \mathcal{P}^{p^q}(y^t),$$

where $Z = \sum_{i=1}^{p^q-1} \mathcal{P}^i(\chi(\mathcal{P}^{p^q-i})(x^s) y^t)$. Thus, in the terminology introduced above, Z is hit by \mathcal{P}^{p^q-1} and the proof of equation (2) is complete. (Note that in (2)

we are employing the non-zero scalar convention introduced earlier - otherwise $\chi(\mathcal{P}^{p^q})(x^s)y^t$ would have coefficient -1 .)

The proof of the lemma is completed by the following identity:

$$\chi(\mathcal{P}^{jp^q})(x^s) = \mathcal{P}^{jp^q}(x^s) \text{ for } j \leq p.$$

The proof of this identity is achieved by a straightforward double induction on j and q , based on Straffin's formula [9] :

$$\chi(\mathcal{P}^{jp^q}) = -\mathcal{P}^{jp^q} - \sum_{l=1}^j \mathcal{P}^{(j-l)p^q} \chi(\mathcal{P}^{lp^q}).$$

Note that we are not asserting that $\chi(\mathcal{P}^{jp^q})$ is equal to \mathcal{P}^{jp^q} as an element of $\mathcal{A}(p)$; this is certainly not true. We are merely claiming that they give the same value when evaluated on $x^s \in H^*(\mathbf{C}P^\infty \times \mathbf{C}P^\infty; \mathbf{F}_p)$. \square

Note that in the above proof we could have replaced y^t by $x^u y^t$, thus obtaining the formula

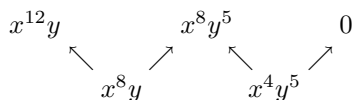
$$(4) \quad \mathcal{P}^{p^q}(x^{s+u}y^t) \equiv \mathcal{P}^{p^q}(x^s)x^u y^t + x^s \mathcal{P}^{p^q}(x^u y^t) \text{ modulo elements hit by } \mathcal{P}^{p^q-1}$$

which we will need later in the proof of Lemma 2.1.

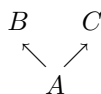
The second preliminary tells us precisely which elements are hit by \mathcal{P}^1 . Let \bar{s} denote the residue class modulo p of s if $s \geq 0$ and 0 if $s < 0$.

Lemma 2.3. $x^q y^r$ is hit by \mathcal{P}^1 if and only if $\bar{q} + \bar{r} < p - 1$ and either $q > (p - 1)(1 + \bar{r})$ or $r > (p - 1)(1 + \bar{q})$. In particular, if $q + r > p^2 - p$, then $x^q y^r$ is hit by \mathcal{P}^1 if and only if $\bar{q} + \bar{r} < p - 1$.

Proof. The reasoning behind this lemma is as follows. At first glance one may think that $x^q y^r$ is hit by \mathcal{P}^1 if and only if it is the image of $x^{q-(p-1)}y^r$ or $x^q y^{r-(p-1)}$ under \mathcal{P}^1 . But further consideration shows that things are not so straightforward. For example, let $p = 5$ and consider the element $x^4 y^5 + x^8 y$: $\mathcal{P}^1(x^4 y^5 + x^8 y) = (4x^8 y^5 + 5x^4 y^9) + (8x^{12} y + x^8 y^5) = 3x^{12} y$. Thus $x^{12} y$ is hit by \mathcal{P}^1 . We depict this situation by a 'chain', with $x^{12} y$ at one end and 0 at the other:



using the notation



to signify that $\mathcal{P}^1(A) = \xi B + \xi' C$ for some non-zero scalars ξ and ξ' (i.e. $\mathcal{P}^1(A) = B + C$ in the notation introduced earlier).

Extending this argument we see that $x^q y^r$ will be hit by \mathcal{P}^1 whenever there is such a chain, of arbitrary length, linking $x^q y^r$ at one end with 0 at the other:

$$(5) \quad \begin{array}{ccccccc} x^q y^r & & x^{q-(p-1)} y^{r+(p-1)} & & \dots & & x^{q-m(p-1)} y^{r+m(p-1)} & & 0 \\ & \swarrow & \nearrow & & & & \swarrow & \nearrow & \\ & x^{q-(p-1)} y^r & & x^{q-2(p-1)} y^{r+(p-1)} & & & x^{q-(m+1)(p-1)} y^{r+m(p-1)} & & \end{array}$$

where $m \geq 0$. For, if we have such a chain, then

$$\mathcal{P}^1(x^{q-(p-1)}y^r + x^{q-2(p-1)}y^{r+(p-1)} + \dots + x^{q-(m+1)(p-1)}y^{r+m(p-1)}) = x^qy^r$$

where, as usual, we are suppressing non-zero scalar coefficients.

Moreover, x^qy^r will be hit by \mathcal{P}^1 if *and only if* there is such a chain or its ‘mirror image’—obtained by swapping x with y and q with r . Clearly we need only consider the first possibility, dealing with the second by symmetry.

For the above chain, (5), to exist it is necessary and sufficient to find m such that if $1 \leq i \leq m$, then

$$\mathcal{P}^1(x^{q-i(p-1)}y^{r+(i-1)(p-1)}) = x^{q-(i-1)(p-1)}y^{r+(i-1)(p-1)} + x^{q-i(p-1)}y^{r+i(p-1)}$$

and, if $i = m + 1$,

$$\mathcal{P}^1(x^{q-(m+1)(p-1)}y^{r+m(p-1)}) = x^{q-m(p-1)}y^{r+m(p-1)}.$$

Recalling that $\mathcal{P}^1(x^syt) = \binom{s}{1}x^{s+p-1}yt + \binom{t}{1}x^syt+p-1 = \bar{s}x^{s+p-1}yt + \bar{t}x^syt+p-1$, we see that these conditions for the existence of (5) are equivalent to:

1. $\overline{(q - i(p - 1))} \neq 0$ for $1 \leq i \leq m$,
2. $\overline{(r + (i - 1)(p - 1))} \neq 0$ for $1 \leq i \leq m$,
3. $\overline{q - (m + 1)(p - 1)} \neq 0$,
4. $r + m(p - 1) = 0$.

We now wish to find a more tractable way of expressing these conditions. First note that $\overline{r + (i - 1)(p - 1)}$ will be zero if and only if $i \equiv r + 1$. By definition, $0 \leq \overline{r + 1} \leq p - 1$ so if $m \geq p$, then either $\overline{r + 1}$ or $\overline{r + 1} + p$ will lie in the interval $1, \dots, m$ and condition 2 cannot hold. So if condition 2 holds, then $m \leq p - 1$. Condition 4 states that $m \equiv r \pmod p$ so if conditions 2 and 4 hold, then $m = \bar{r}$. Conversely, if $m = \bar{r}$, then this implies that both conditions 2 and 4 hold.

Now we turn to the remaining two conditions, 1 and 3. Since \bar{s} is defined to be 0 if $s < 0$, it follows that if condition 3 holds, then $q > (m + 1)(p - 1)$. Now if we assume this to be the case, then $\overline{q - i(p - 1)} = \overline{q + i}$ and conditions 1 and 3 together assert that $q + i \not\equiv 0 \pmod p$ for $1 \leq i \leq m + 1$, i.e. $q \not\equiv p - 1, p - 2, \dots, p - (m + 1)$. Since $\bar{q} \leq p - 1$ by definition, this condition is equivalent to $\bar{q} < p - (m + 1)$. Thus conditions 1 and 3 imply that $q > (m + 1)(p - 1)$ and $\bar{q} < p - 1 - m$. Conversely, if $q > (m + 1)(p - 1)$ and $\bar{q} < p - 1 - m$, then conditions 1 and 3 are seen to hold.

Thus we conclude that the chain exists if and only if $\bar{q} + \bar{r} < p - 1$ and $q > (p - 1)(1 + \bar{r})$, with $m = \bar{r}$.

Now we need to symmetrise to cover the second possible chain, but this simply means replacing the second condition with $r > (p - 1)(1 + \bar{q})$.

The second statement of the lemma is a consequence of the first. Suppose that $\bar{q} + \bar{r} < p - 1$, so $\bar{q} + \bar{r} \leq p - 2$. If $r \leq (p - 1)(1 + \bar{q})$ and $q \leq (p - 1)(1 + \bar{r})$, then $q + r \leq (p - 1)(2 + \bar{q} + \bar{r}) \leq (p - 1)(p) = p^2 - p$. Thus if $q + r > p^2 - p$, it follows that either $r > (p - 1)(1 + \bar{q})$ or $q > (p - 1)(1 + \bar{r})$. □

Now we are in a position to prove Lemma 2.1.

Proof of Lemma 2.1. Recall that $M^*(2)$ is the quotient of $H^*(CP^\infty \times CP^\infty; \mathbf{F}_p)$ by the subspace of ‘hit’ elements, that is, elements which can be written as $\sum_{i>0} \mathcal{P}^i X_i$ for some polynomials $X_i \in H^*(CP^\infty \times CP^\infty; \mathbf{F}_p)$. Thus to show that f induces a map $M^*(2) \rightarrow M^*(2)$, we need to show that if X is hit, then so is $f(X)$.

Suppose that X is hit. By linearity of f and the Steenrod operations, we may assume that $X = \mathcal{P}^i(x^q y^r)$ for some $i \geq 1$. Moreover, since the operation \mathcal{P}^i is decomposable unless i is a power of p , we may assume that $X = \mathcal{P}^{p^t}(x^q y^r)$ for some $t \geq 0$. Then $f(X) = x^{p-1} y^{p-1} (\mathcal{P}^{p^t}(x^q y^r))^p$. We will show that, modulo hit elements, $f(X)$ is congruent to $\mathcal{P}^{p^{t+1}}(x^{p-1+qp} y^{p-1+rp})$ and hence $f(X)$ is hit.

To do this, we first use equation (4) to evaluate $\mathcal{P}^{p^{t+1}}(x^{p-1+qp} y^{p-1+rp})$:

$$(6) \quad \mathcal{P}^{p^{t+1}}(x^{p-1+qp} y^{p-1+rp}) \equiv \mathcal{P}^{p^{t+1}}(x^{p-1}) x^{qp} y^{p-1+rp} + x^{p-1} \mathcal{P}^{p^{t+1}}(x^{qp} y^{p-1+rp}).$$

Since $t \geq 0$, it follows that $\mathcal{P}^{p^{t+1}}(x^{p-1}) = 0$ and so we need only consider the second term on the right hand side, which we expand using the (standard) Cartan formula, twice.

$$\begin{aligned} x^{p-1} \mathcal{P}^{p^{t+1}}(x^{qp} y^{p-1+rp}) &= x^{p-1} \sum_{j=0}^{p^{t+1}} \mathcal{P}^j(x^{qp}) \mathcal{P}^{p^{t+1}-j}(y^{p-1+rp}) \\ &= x^{p-1} \sum_{j=0}^{p^{t+1}} \mathcal{P}^j(x^{qp}) \sum_{k=0}^{p^{t+1}-j} \mathcal{P}^k(y^{rp}) \mathcal{P}^{p^{t+1}-j-k}(y^{p-1}). \end{aligned}$$

Now $\mathcal{P}^j(x^{qp}) = \binom{qp}{j} x^{qp+j(p-1)}$ will be zero unless j is a multiple of p by equation (1). Similarly, $\mathcal{P}^k(y^{rp})$ will be zero unless k is a multiple of p . If j and k are both multiples of p , then so will $p^{t+1} - j - k$ be, but then $\mathcal{P}^{p^{t+1}-j-k}(y^{p-1})$ will be zero unless $p^{t+1} - j - k = 0$. Hence

$$x^{p-1} \mathcal{P}^{p^{t+1}}(x^{qp} y^{p-1+rp}) = x^{p-1} y^{p-1} \sum_{j=0}^{p^t} \mathcal{P}^{jp}(x^{qp}) \mathcal{P}^{(p^t-j)p}(y^{rp}).$$

Next we observe that, for any $i, s \geq 0$,

$$(7) \quad (\mathcal{P}^i(x^s))^p = \left(\binom{s}{i} x^{s+i(p-1)}\right)^p = \binom{sp}{ip} x^{sp+ip(p-1)} = \mathcal{P}^{ip}(x^{sp}).$$

So

$$\begin{aligned} x^{p-1} \mathcal{P}^{p^{t+1}}(x^{qp} y^{p-1+rp}) &= x^{p-1} y^{p-1} \sum_{j=0}^{p^t} (\mathcal{P}^j x^q)^p (\mathcal{P}^{p^t-j} y^r)^p \\ &= x^{p-1} y^{p-1} \left(\sum_{j=0}^{p^t} \mathcal{P}^j x^q \mathcal{P}^{p^t-j} y^r\right)^p \\ &= x^{p-1} y^{p-1} (\mathcal{P}^{p^t}(x^q y^r))^p \\ &= f(\mathcal{P}^{p^t}(x^q y^r)) \\ &= f(X) \end{aligned}$$

and, recalling equation (6), we see that $f(X)$ is congruent to $\mathcal{P}^{p^{t+1}}(x^{p-1+qp} y^{p-1+rp})$ as claimed. Thus $f(X)$ is hit and f does induce a map $M^*(2) \rightarrow M^*(2)$.

Having shown that f induces a map $M^*(2) \rightarrow M^*(2)$, we now show that it is injective. We will work by induction on i , showing that if X is a polynomial such that $f(X)$ is hit by \mathcal{P}^i , then X is hit.

The first step is to show that if $f(X)$ is hit by \mathcal{P}^1 , then X is hit. To do this notice that, by the definition of f , every monomial in $f(X)$ will have both exponents

congruent to $p - 1$ modulo p . But no such monomial can be in the image of \mathcal{P}^1 , since $\mathcal{P}^1(x^s) = \binom{s}{1}x^{s+p-1}$ and if $s + p - 1$ is congruent to $p - 1$ modulo p , then s is congruent to 0 and $\binom{s}{1} = 0$. Thus there are no polynomials X such that $f(X)$ is hit by \mathcal{P}^1 and the claim is vacuously proved in this case.

Now we assume that whenever X is such that $f(X)$ is hit by \mathcal{P}^{N-1} , then X is hit. We suppose then that Y is some polynomial such that $f(Y)$ is hit by \mathcal{P}^N . If N is not a power of p , then \mathcal{P}^N is decomposable and $f(Y)$ is hit by \mathcal{P}^{p^k} where p^k is the largest power of p that is less than N . Then by the inductive hypothesis Y is hit and so the inductive step is proven immediately. So, instead, we suppose that $N = p^i$, with $i > 0$. By the usual arguments of linearity of f and the Steenrod operations we may assume that $f(Y) = \mathcal{P}^{p^i}(Z)$ for some polynomial Z . Suppose that $Z = \sum_j x^{q_j} y^{r_j}$ for some integers $q_j, r_j \geq 0$.

By applying the short Cartan formula to each monomial of each Z , we have

$$f(Y) \equiv \sum_j (\mathcal{P}^{p^i}(x^{q_j})y^{r_j} + x^{q_j}\mathcal{P}^{p^i}(y^{r_j}))$$

modulo elements hit by \mathcal{P}^{p^i-1} . Now, as we noted earlier, when we write $f(Y)$ as a polynomial in x and y , it is clear from the definition of f that every exponent must be congruent to $p - 1$. So we must have $\bar{q}_j = \bar{r}_j = p - 1$, since applying \mathcal{P}^{p^i} will not change this residue class. Define \tilde{q}_j, \tilde{r}_j by $q_j = p - 1 + p\tilde{q}_j$ and $r_j = p - 1 + p\tilde{r}_j$ and note that for $i > 0$, $\mathcal{P}^{p^i}(x^{p-1+p\tilde{q}_j}) = x^{p-1}\mathcal{P}^{p^i}(x^{p\tilde{q}_j})$ and similarly, $\mathcal{P}^{p^i}(y^{p-1+p\tilde{r}_j}) = y^{p-1}\mathcal{P}^{p^i}(y^{p\tilde{r}_j})$.

Thus,

$$f(X) \equiv \sum_j x^{p-1}y^{p-1}(\mathcal{P}^{p^i}(x^{p\tilde{q}_j})y^{p\tilde{r}_j} + x^{p\tilde{q}_j}\mathcal{P}^{p^i}(y^{p\tilde{r}_j}))$$

modulo elements hit by \mathcal{P}^{p^i-1} . It follows from (7) that

$$\begin{aligned} f(X) &\equiv \sum_j x^{p-1}y^{p-1}(\mathcal{P}^{p^i-1}(x^{\tilde{q}_j})y^{\tilde{r}_j} + x^{\tilde{q}_j}\mathcal{P}^{p^i-1}(y^{\tilde{r}_j}))^p \\ &\equiv f(\sum_j \mathcal{P}^{p^i-1}(x^{\tilde{q}_j})y^{\tilde{r}_j} + x^{\tilde{q}_j}\mathcal{P}^{p^i-1}(y^{\tilde{r}_j})). \end{aligned}$$

Let W denote $\sum_j \mathcal{P}^{p^i-1}(x^{\tilde{q}_j})y^{\tilde{r}_j} + x^{\tilde{q}_j}\mathcal{P}^{p^i-1}(y^{\tilde{r}_j})$. We have shown that $f(X)$ is equivalent to $f(W)$ modulo elements hit by \mathcal{P}^{p^i-1} . So $f(X - W)$ is hit by \mathcal{P}^{p^i-1} and, by the inductive hypothesis, $X - W$ is hit.

Now from the short Cartan formula we have

$$\mathcal{P}^{p^i-1}(\sum_j x^{\tilde{q}_j}y^{\tilde{r}_j}) \equiv \sum_j \mathcal{P}^{p^i-1}(x^{\tilde{q}_j})y^{\tilde{r}_j} + x^{\tilde{q}_j}\mathcal{P}^{p^i-1}(y^{\tilde{r}_j}) = W,$$

the equivalence being modulo elements hit by \mathcal{P}^{p^i-1-1} . Thus W is hit and consequently so is X . This concludes the proof of the inductive step and, with it, the proof that f is injective on $M^*(2)$.

Finally, we show that the induced map is onto in the stated range. If $n = pm + 2(2p - 2)$ and $x^q y^r$ is a monomial of degree n , then $q + r \equiv 2p - 2 \pmod p$ so $\bar{q} + \bar{r} = p - 2$ or $p + p - 2$. In the latter case, since both \bar{q} and \bar{r} cannot exceed $p - 1$, they must both be equal to $p - 1$, and then $x^q y^r$ will be in the image of f .

In the former case, if $m \geq 2(p-1)$ then $q+r = n/2 \geq (p^2-p) + (2p-2) > p^2-p$, and Lemma 2.3 asserts that $x^q y^r$ is hit.

This completes the proof. □

The last preliminary result we wish to mention is the following.

Theorem 2.4. *As an $\mathcal{A}(p)$ module, $H^*(\mathbf{C}P^\infty \times \mathbf{C}P^\infty; \mathbf{F}_p)$ splits as a $\mathbf{Z}/(p-1)$ -bigraded direct sum $\bigoplus_{i,j} H_{i,j}^*(2)$, where $H_{i,j}^*(2)$ is the subspace spanned by monomials $x^q y^r$ where $q \equiv i \pmod{p-1}$ and $r \equiv j \pmod{p-1}$.*

In fact $H^(\mathbf{C}P^\infty \times \mathbf{C}P^\infty; \mathbf{F}_p)$ splits further : $H_{i,0}^*(2)$ has an $\mathcal{A}(p)$ -submodule consisting of monomials $x^q y^0$, and the complementary subspace spanned by monomials $x^q y^r$ where $(p-1)$ divides r but $r \neq 0$, is also an $\mathcal{A}(p)$ -submodule. Similarly $H_{0,j}^*(2)$ splits as a direct sum of two components.*

This is an easy consequence of the fact that each Steenrod power operation \mathcal{P}^i increases the exponent by a multiple of $(p-1)$.

The main use we will have for this theorem is in proving linear independence of certain elements: If two monomials, $x^q y^r$ and $x^{q'} y^{r'}$ are such that $q \not\equiv q' \pmod{p-1}$ or $r \not\equiv r' \pmod{p-1}$, then they must be linearly independent. This solves the question of linear independence in almost all cases.

The remainder of the paper is concerned with the proof of Theorem 1.1, which is dealt with in a piece-wise fashion. In fact the proof splits into the following parts (which correspond approximately to the rows of Table 1): the *toddler* stage, in degrees 1 to $2(p-2)$, the *adolescence* stage, in degrees $2(p-1)$ to $2(p^2+p-2)$, the *thirtysomething* stage, in degrees $2(p^2+p)$ to $2(2p^2-p-3)$ and finally the *retirement* stage, which covers all higher degrees except those congruent to $2(p-2) \pmod{2p}$, which are dealt with by Lemma 2.1. Each of these stages has a section to itself except the retirement stage, which is split over the two final sections of this paper as it is rather long, and the toddler stage which is trivial: there are no hit elements so $M^*(2) = H^*(\mathbf{C}P^\infty \times \mathbf{C}P^\infty; \mathbf{F}_p)$ in these degrees and the only possible monomial basis is the one given in Table 1.

3. ADOLESCENCE

In this section we consider the cases where $n = (i+1)p+j-1$, with $0 \leq i, j \leq p-1$.

In most such cases $n < p^2$ and so we will only need to consider \mathcal{P}^1 , whose image we can describe without much difficulty. This section is split into 4 subsections, according to whether $i = p-1$ or $i \leq p-1$ and $j = 0$ or $j > 0$.

3.1. $i = p-1, j = 0$. In this case $n = p^2 - 1 < p^2$ and we need only consider \mathcal{P}^1 . We first show that there are no hit monomials in this degree. For if $x^q y^r$ has degree $2n$, i.e. $q+r = n$, then $\bar{q} + \bar{r}$ must be congruent to $n = p^2 - 1$ modulo p and so must equal $p-1$ or $2p-1$. In either case Lemma 2.3 states that this monomial is not hit.

Now note that, by the splitting Theorem 2.4, x^n and y^n cannot be constituents of any hit polynomial. Therefore they are indispensable basis elements but play no further part in our calculations, so we can concentrate on the other terms. (This phenomenon will reappear in later cases.)

Let $\phi(m, k) = x^{m(p-1)+k} y^{n-k-m(p-1)}$ for $1 \leq k \leq p-1$ and $0 \leq m \leq p$, unless $k = p-1$ in which case we restrict m to $\leq p-1$. The motivation for this definition comes from the splitting Theorem 2.4. For if $k \neq k'$, then $\phi(m, k)$ and $\phi(m', k')$

lie in different components of the splitting given by the theorem, and so must be linearly independent. Hence we need only consider relations between $\phi(m, k)$ and $\phi(m', k')$ if $k = k'$.

Since the only Steenrod operation we have to consider is \mathcal{P}^1 , we need only look for relations between $\phi(m, k)$ and $\phi(m+1, k)$. Now $\mathcal{P}^1(x^{m(p-1)+k}y^{n-k-(m+1)(p-1)}) = \frac{(n-k-(m+1)(p-1))\phi(m, k) + (m(p-1)+k)\phi(m+1, k)}{(n-k-(m+1)(p-1))\phi(m, k) + (m(p-1)+k)\phi(m+1, k)}$, so $\phi(m, k) + \phi(m+1, k)$ will be hit if and only if $(n-k-(m+1)(p-1)) \neq 0$ and $(m(p-1)+k) \neq 0$. These two conditions are seen to be equivalent when $n = p^2 - 1$, and equivalent to $m \not\equiv k \pmod{p}$. Because of the ranges that k and m are restricted to, this is equivalent to $m \neq k$. So if $m, m' \leq k$, then $\phi(m, k) \equiv \phi(m', k)$ modulo elements hit by \mathcal{P}^1 , and if $m, m' > k$, then $\phi(m, k) \equiv \phi(m', k)$ modulo elements hit by \mathcal{P}^1 . Thus, modulo hit elements, we have at most two distinct equivalence classes of monomials:

$$\{\phi(m, k) \mid 0 \leq m \leq k\} \quad \{\phi(m, k) \mid k+1 \leq m \leq p\}$$

for each value of k , as well as the two classes $\{x^n\}$ and $\{y^n\}$. In fact, if $k = p-1$, then the second class is empty, for we made the extra restriction above that m could not be p when $k = p-1$. (If we had allowed m to equal p when $k = p-1$, then $\phi(m, k)$ would be y^n , which we've already dealt with.) Since we have entirely calculated the space of hit elements in this degree, these equivalence classes correspond to bases for $M^{2n}(2)$. So for each value of k satisfying $1 \leq k \leq p-2$, we have two basis elements, for $k = p-1$ we have one, and we have two other basis elements x^{p^2-1} and y^{p^2-1} . Thus we see that $\dim M^{2n}(2) = 2(p-2) + 1 + 2 = 2p-1$ and any monomial basis for $M^{2n}(2)$ is formed by taking one member from each equivalence class. That is, every basis is of the form

$$\begin{aligned} & \{\phi(m_k^-, k), \phi(m_k^+, k) \mid 1 \leq k \leq p-2\} \cup \{\phi(m_{p-1}^-, p-1), x^{p^2-1}, y^{p^2-1}\} \\ &= \{\phi(m_k^-, k) \mid 1 \leq k \leq p-1\} \cup \{\phi(m_k^+, k) \mid 1 \leq k \leq p-2\} \cup \{x^{p^2-1}, y^{p^2-1}\} \end{aligned}$$

where, for $1 \leq k \leq p-1$, m_k^- and m_k^+ satisfy $0 \leq m_k^- \leq k$, $k+1 \leq m_k^+ \leq p$.

3.2. $i = p-1, j > 0$. Now we assume that $j > 0$, so $n = p^2 + j - 1 \geq 0$ and we need to consider \mathcal{P}^p as well as \mathcal{P}^1 . However it turns out that \mathcal{P}^p plays practically no part in the calculations, since any elements that are hit by \mathcal{P}^p are also hit by \mathcal{P}^1 , as we will now show. Suppose $x^q y^r$ is a monomial such that $\mathcal{P}^p(x^q y^r)$ has degree $2n$. By the short Cartan formula, Lemma 2.2, $\mathcal{P}^p(x^q y^r) \equiv \mathcal{P}^p(x^q) y^r + x^q \mathcal{P}^p(y^r)$ modulo elements hit by \mathcal{P}^1 . Now $\mathcal{P}^p(x^q) y^r = \binom{q}{p} x^s y^r$ where $s = q + p(p-1)$. If this is non-zero, then $\binom{q}{p} \neq 0$, so $q \geq p$ and $s \geq p^2$. Thus, since $s+r = n = p^2 + j - 1$, we see that $\bar{s} + \bar{r} = j - 1 < p - 1$ and, since $s+r > p^2 - p$, Lemma 2.3 shows that $x^s y^r$ is hit by \mathcal{P}^1 . Similarly, $x^q \mathcal{P}^p(y^r)$ is hit by \mathcal{P}^1 and we conclude that $\mathcal{P}^p(x^q y^r)$ is hit by \mathcal{P}^1 . Hence any element hit by \mathcal{P}^p is, in fact, hit by \mathcal{P}^1 . So we need only consider \mathcal{P}^1 .

Note that, by Lemma 2.3 since $n > p^2 - p$, $x^q y^{n-q}$ is hit if $q \leq j-1$ or $q \geq n - (j-1)$ for, in either case, $\bar{q} + \bar{n-q} = j-1 < p-1$. As before, let $\phi(m, k) = x^{m(p-1)+k} y^{n-k-m(p-1)}$ for $1 \leq k \leq p-1, 0 \leq m \leq p$. Then $\phi(m, k)$ is hit if and only if $(m(p-1)+k) + (n-k-m(p-1)) < p-1$. Since the sum of these residue classes is congruent to n modulo p , it must be $j-1$ or $p+j-1$. But neither residue class can exceed $p-1$, so it follows that if one residue class is $\leq j-1$, then the sum must be $j-1$. Conversely, if the sum is $j-1$, then both

must be $\leq j - 1$. Hence $\phi(m, k)$ is hit if and only if $\overline{(m(p-1) + k)} \leq j - 1$, i.e. if $k - m \equiv 0, 1, \dots, j - 1 \pmod p$.

Similarly, $\phi(m, k) + \phi(m + 1, k)$ is hit if and only if $\overline{(m(p-1) + k)} \neq 0$ and $\overline{(n - k - (m + 1)(p - 1))} \neq 0$. This is equivalent to $k - m \not\equiv 0 \pmod p$ and $k - m \not\equiv j - 1 \pmod p$. Thus we have at most two equivalence classes of monomials:

$$\{\phi(m, k) \mid m < k - (j - 1)\} \quad \{\phi(m, k) \mid m > k\}$$

for each value of k . The first will be empty if $k < j$, while the second will never be empty. So for each value of k in the range $1 \leq k \leq j - 1$ we get one equivalence class, while for each k such that $j \leq k \leq p - 1$ we get two. Hence $\dim M^{2n}(2)$ is equal to $(j - 1) + 2(p - j) = 2p - j - 1 = p + i - j$ and all monomial bases have the form

$$\begin{aligned} & \{\phi(m_k^+, k) \mid 1 \leq k \leq j - 1\} \cup \{\phi(m_k^-, k), \phi(m_k^+, k) \mid j \leq k \leq p - 1\} \\ & = \{\phi(m_k^+, k) \mid 1 \leq k \leq p - 1\} \cup \{\phi(m_k^-, k) \mid j \leq k \leq p - 1\} \end{aligned}$$

where $0 \leq m_k^- \leq k - j, k + 1 \leq m_k^+ \leq p$.

3.3. $i < p - 1, j = 0$. Now we assume that $i < p - 1$ and $j = 0$. As in the case where $i = p - 1, j = 0$, we see from Lemma 2.3 that no monomials are hit and the monomials x^n, y^n are indispensable basis elements but play no part in our calculations.

Again, we set $\phi(m, k) = x^{m(p-1)+k}y^{n-k-m(p-1)}$ for $1 \leq k \leq p - 1, 0 \leq m \leq M$ where M is equal to $i + 1$ if $k < i$ and equal to i if $k \geq i$. This range is designed to ensure that we always have $1 \leq m(p - 1) + k \leq n - 1$. By the usual processes, we see that $\phi(m, k) + \phi(m + 1, k)$ is hit if and only if $m \neq k$. It follows that for $k < i$ we get two equivalence classes while for $k \geq i$ we get only one. Recalling that we also need x^n and y^n in order to form a basis, we conclude that $\dim M^{2n}(2)$ is equal to $2 + 2(i - 1) + (p - i) = p + i = p + i - j$ and any monomial basis is of the form

$$\begin{aligned} & \{\phi(m_k^-, k), \phi(m_k^+, k) \mid 1 \leq k < i\} \cup \{\phi(m_k^-, k) \mid i \leq k \leq p - 1\} \cup \{x^n, y^n\} \\ & = \{\phi(m_k^-, k) \mid 1 \leq k \leq p - 1\} \cup \{\phi(m_k^+, k) \mid 1 \leq k < i\} \cup \{x^{(i+1)p-1}, y^{(i+1)p-1}\} \end{aligned}$$

where $0 \leq m_k^- \leq k, k + 1 \leq m_k^+ \leq p$.

3.4. $i < p - 1, j > 0$. We again set $\phi(m, k) = x^{m(p-1)+k}y^{n-k-m(p-1)}$ for $1 \leq k \leq p - 1$. However, it is not clear what the range for m should be. We want the range to be $0 \leq m \leq M$ where M is such that if $m > M$, then $\phi(m, k)$ is hit. We now proceed to calculate M .

By Lemma 2.3, $x^q y^{n-q}$ is hit if $n - q \leq j - 1$ and $q > (p - 1)(1 + n - q)$. For if $n - q \leq j - 1$, then $\overline{n - q} \leq j - 1$ and, since $\overline{n - q} + \bar{q} \equiv n \equiv j - 1 \pmod p$, we must have that $\overline{n - q} + \bar{q} = j - 1 < p - 1$.

The condition $q > (p - 1)(1 + n - q)$ is equivalent to $qp > p(n + 1) - (n + 1) = p(n + 1) - (i + 1)p - j = p(n - i) - j$, i.e. $q \geq n - i$ (since $j > 0$). Thus the conditions $n - q \leq j - 1$ and $q > (p - 1)(1 + n - q)$ can be combined as

$$\begin{aligned} q & \geq \max(n - (j - 1), n - i) = \max((i + 1)p, (i + 1)p + j - i - 1) \\ & = \max((i + 1)(p - 1) + i + 1, (i + 1)(p - 1) + j) = (i + 1)(p - 1) + \max(i + 1, j). \end{aligned}$$

So M must be such that $m > M$ implies that $m(p - 1) + k \geq (i + 1)(p - 1) + \max(i + 1, j)$. Thus we see that we should define M by:

$$M = \begin{cases} i & \text{if } k \geq \max(i + 1, j), \\ i + 1 & \text{if } k < \max(i + 1, j). \end{cases}$$

Now, by Lemma 2.3, $\phi(m, k)$ is hit if and only if the following conditions hold:

$$\overline{(m(p - 1) + k)} + \overline{(n - k - m(p - 1))} < p - 1$$

and either

$$m(p - 1) + k > (p - 1)(1 + \overline{(n - k - m(p - 1))})$$

or

$$n - k - m(p - 1) > (p - 1)(1 + \overline{(m(p - 1) + k)}).$$

The following lemma provides equivalent, but more tractable, expressions for these conditions and is proved by straightforward methods.

Lemma 3.1. *If i, j, k, m are such that $0 \leq i < p - 1, 1 \leq j \leq p - 1, 1 \leq k \leq p - 1, 0 \leq m \leq M$, then they satisfy $\overline{(m(p - 1) + k)} + \overline{(n - k - m(p - 1))} < p - 1$ and either $m(p - 1) + k > (p - 1)(1 + \overline{(n - k - m(p - 1))})$ or $n - k - m(p - 1) > (p - 1)(1 + \overline{(m(p - 1) + k)})$ if and only if they satisfy either $1 \leq k + 1 - j \leq m \leq k, 0 \leq m \leq k \leq \min(i, j - 1)$ or $p + 1 + k - j \leq m \leq M$.*

So we conclude that $\phi(m, k)$ is hit if and only if $1 \leq k + 1 - j \leq m \leq k, 0 \leq m \leq k \leq \min(i, j - 1)$, or $p + 1 + k - j \leq m \leq M$. Thus $\phi(m, k)$ is *not* hit if and only if:

$$(8) \quad \begin{aligned} k < j - 1, & \quad k \leq i, & \quad k + 1 \leq m \leq \min(p + k - j, M), \\ k < j - 1, & \quad k > i, & \quad 0 \leq m \leq \min(p + k - j, M), \\ k = j - 1, & \quad k \leq i, & \quad k + 1 \leq m \leq M, \\ k = j - 1, & \quad k > i, & \quad 0 \leq m \leq M, \\ k > j - 1, & \quad k \leq i, & \quad 0 \leq m \leq k - j, \text{ or } k + 1 \leq m \leq M, \\ k > j - 1, & \quad k > i, & \quad 0 \leq m \leq k - j. \end{aligned}$$

Now if $\phi(m, k)$ and $\phi(m + 1, k)$ are not themselves hit, then $\phi(m, k) + \phi(m + 1, k)$ will be hit if and only if $\overline{(m(p - 1) + k)} \neq 0$ and $\overline{(n - k - (m + 1)(p - 1))} \neq 0$. For if these conditions hold, then $\phi(m, k) + \phi(m + 1, k) = \mathcal{P}^1(x^{m(p-1)+k}y^{n-k-(m+1)(p-1)})$.

That is, $\phi(m, k) + \phi(m + 1, k)$ is hit unless $m \equiv k$, or $m \equiv k - j \pmod p$. Using this criterion, one checks that in each row of (8) above, if m and m' are in the same interval, then $\phi(m, k) \equiv \phi(m', k)$ modulo hit elements. Thus the number of intervals above corresponds to the number of equivalence classes. So, we always have at least one equivalence class corresponding to k , while if $j - 1 < k \leq i$, we have two. Thus if $j \leq i$, $\dim M^{2n}(2) = (p - 1) + (i + 1 - j) = p + i - j$, while if $j > i$, then $\dim M^{2n}(2) = p - 1$.

Now note that the conclusions of subsections 3.1, 3.2 and 3.3 can be incorporated into those of this subsection, as follows:

Proposition 3.2. *If $n = (i + 1)p + j - 1$, with $0 \leq i, j \leq p - 1$, then any monomial basis for $M^{2n}(2)$ is given by the following recipe. If $j > 0$, then for each k in the range $1 \leq k \leq p - 1$, take one member m from each interval given in the appropriate row of (8), and the set of monomials $\{\phi(m, k)\}$ will form a basis. If $j = 0$, then to obtain a basis we follow the same recipe but augment the set $\{\phi(m, k)\}$ by the element $\{y^n\}$.*

It is easily seen that the basis given in Table 1 can be obtained in this way : m is taken to be 0 if $k > j - 1$ or $k > i$, and $k + 1$ if $k \leq i$.

4. THIRTYSOMETHING

Now we deal with the cases where $n = p^2 + p(i + 1) + j$ with $0 \leq i \leq j \leq p - 3$.

Note first that x^n and y^n are hit by \mathcal{P}^1 , by Lemma 2.3, since $n \equiv j \not\equiv p - 1 \pmod p$. As in section 3 we define $\phi(m, k)$ to be $x^{m(p-1)+k}y^{n-k-m(p-1)}$, for $1 \leq k \leq p - 1$, $0 \leq m \leq M$, where $M = \lfloor (n - k - 1)/(p - 1) \rfloor$. In fact, one easily sees that

$$M = \begin{cases} p + i + 1 & \text{if } i + 1 \leq k - j - 1, \\ p + i + 2 & \text{if } k - j \leq i + 1 \leq p - 2 + k - j, \\ p + i + 3 & \text{if } p - 1 + k - j \leq i + 1. \end{cases}$$

In particular, note that $M \leq 2p$.

Lemma 4.1. $\phi(m, k)$ is hit by \mathcal{P}^1 if and only if $m \equiv k - j, k + 1 - j, \dots, k - 1$ or $k \pmod p$.

Proof. Since $n > p^2 - p$, the second part of Lemma 2.3 asserts that $\phi(m, k)$ is hit by \mathcal{P}^1 if and only if $\overline{(m(p - 1) + k) + (n - k - m(p - 1))} < p - 1$. Since $n \equiv j \pmod p$ and $j < p - 1$, it follows that $\phi(m, k)$ is hit if and only if $\overline{(m(p - 1) + k)} \leq j$ or, equivalently $\overline{(n - k - m(p - 1))} \leq j$. Now $n - k - m(p - 1) \equiv j - k + m \pmod p$ and so $\overline{(n - k - m(p - 1))} \leq j$ if and only if $m \equiv k - j, k + 1 - j, \dots, k - 1$, or $k \pmod p$. \square

Lemma 4.2. If neither $\phi(m, k)$ nor $\phi(m + 1, k)$ are hit by \mathcal{P}^1 , then $\phi(m, k) + \phi(m + 1, k)$ is hit by \mathcal{P}^1 .

Proof. The sum $\phi(m, k) + \phi(m + 1, k)$ will be hit by \mathcal{P}^1 if and only if $\binom{m(p-1)+k}{1} \neq 0$ and $\binom{n-k-(m+1)(p-1)}{1} \neq 0$. If $\binom{m(p-1)+k}{1} = 0$, then $\binom{m}{1} = k$, and $\phi(m, k)$ will be hit by \mathcal{P}^1 , by Lemma 4.1. Similarly, if $\binom{n-k-(m+1)(p-1)}{1} = 0$, then $\phi(m + 1, k)$ is hit by \mathcal{P}^1 . \square

Thus the values of m for which $\phi(m, k)$ are not hit by \mathcal{P}^1 come in blocks : $0, \dots, k - j$, then $k + 1, \dots, p - 1 + k - j$, then $p + k + 1, \dots, 2p - 1 + k - j$. Within each of these blocks, all terms are equivalent to each other modulo elements hit by \mathcal{P}^1 —this is the import of the preceding lemma.

Next we consider the effect of \mathcal{P}^p . The following two lemmas are immediate consequences of applying the short Cartan formula to $\mathcal{P}^p(x^{m(p-1)+k}y^{n-k-(m+p)(p-1)})$.

Lemma 4.3. $\phi(m, k)$ is hit by \mathcal{P}^p if $m = 0$ or $m = M$.

Lemma 4.4. If $1 \leq m \leq M - p - 1$, then $\phi(m, k) + \phi(m + p, k)$ is hit by \mathcal{P}^p .

Now that we have assembled the necessary facts about hit elements, we make our analysis of what is happening.

If $k \geq j + 2$, then we have two intervals of values of $m \leq M$ such that $\phi(m, k)$ is not hit by \mathcal{P}^1 : $0 \leq m \leq k - j - 1$ and $k + 1 \leq m \leq p + k - j - 1$. (The assumption that $k \geq j + 2$ ensures that any higher values of m such that $\phi(m, k)$ is hit by \mathcal{P}^1 , are out of range, since $p + k + 1 \geq p + j + 3 \geq p + i + 3$ and $M \leq p + i + 2$ because $k \geq j + 2$.) Moreover, for any m, m' belonging to the same interval, $\phi(m, k) \equiv \phi(m', k)$ modulo elements hit by \mathcal{P}^1 , by Lemma 4.2.

Now Lemma 4.3 states that $\phi(0, k)$ is hit by \mathcal{P}^p and so every value in the first interval corresponds to a hit monomial.

On the other hand, if $1 \leq M - p - 1$, then Lemma 4.4 says that $\phi(1, k) + \phi(p + 1, k)$ is hit by \mathcal{P}^p . Since $k \geq j + 2$, we see that 1 lies in the first interval, so this relation links the first interval to the second, and so implies that for each value in the second interval, the corresponding monomial is hit. If $1 > M - p - 1$, then $M = p + 1$ and $\phi(p + 1, k)$ is hit by Lemma 4.3. So, again, every monomial corresponding to a value of m in the second interval is hit.

So we see that if $k \geq j + 2$, then all monomials $\phi(m, k)$ are hit.

If $k \leq i$, then there are again two intervals of values of m such that $\phi(m, k)$ is not hit by \mathcal{P}^1 : $k + 1 \leq m \leq p - 1 + k - j$ and $p + k + 1 \leq m \leq \min(M, 2p - 1 + k - j)$. Also, as before, if m, m' belong to the same interval, then, by Lemma 4.2, $\phi(m, k) \equiv \phi(m', k)$ modulo elements hit by \mathcal{P}^1 .

If $M \leq 2p - 1 + k - j$, then the second interval contains M , which corresponds to a monomial hit by \mathcal{P}^p , so every value in the second interval corresponds to a hit monomial. Moreover, the second interval also contains $p + k + 1$, which is strictly less than M (since $k \leq i$ implies that $k \leq j$ and hence that M is either $p + i + 2$ or $p + i + 3$ and so $M \geq p + k + 2$). Thus $\phi(k + 1, k) + \phi(p + k + 1, k)$ is hit by \mathcal{P}^p , by Lemma 4.4, and we have a link between first and second intervals; thus all monomials in both intervals are hit in this case.

If $M > 2p - 1 + k - j$, then both $k + 1$ and $k + 2$ are strictly less than $M - p - 1$ so we get two links between the first and second intervals: $\phi(k + 1, k) + \phi(p + k + 1, k)$ and $\phi(k + 2, k) + \phi(p + k + 2, k)$ are both hit by \mathcal{P}^p according to Lemma 4.4. We will show that this ‘double-bond’ implies that all monomials in both intervals are hit. For once, the non-zero scalars play a significant rôle and so, for the next paragraph only, we abandon our notation convention of suppressing the scalars.

Now $\mathcal{P}^1(x^{(k+1)p-1}y^{n+2-(k+2)p}) = (j + 2)\phi(k + 1, k) + (p - 1)\phi(k + 2, k)$. Similarly, $\mathcal{P}^1(x^{(p+k)p-1}y^{n+2-(p+k+1)p}) = (j + 2)\phi(p + k + 1, k) + (p - 1)\phi(p + k + 2, k)$. On the other hand, using the short Cartan formula, $\mathcal{P}^p(x^{(k+1)p-1}y^{n+1-(k+p)p}) \equiv (i + 1 - k)\phi(k + 1, k) + k\phi(p + k + 1, k)$ and $\mathcal{P}^p(x^{(k+2)p-2}y^{n+2-(k+p+1)p}) \equiv (i - k)\phi(k + 2, k) + (k + 1)\phi(p + k + 2, k)$. Now define \mathbf{A} to be the matrix

$$\mathbf{A} = \begin{pmatrix} j + 2 & 0 & i + 1 - k & 0 \\ p - 1 & 0 & 0 & i - k \\ 0 & j + 2 & k & 0 \\ 0 & p - 1 & 0 & k + 1 \end{pmatrix}$$

so that each entry of the row vector

$$(\phi(k + 1, k) \quad \phi(k + 2, k) \quad \phi(p + k + 1, k) \quad \phi(p + k + 2, k)) \mathbf{A}$$

is hit. But \mathbf{A} is seen to be non-singular (it has determinant $-(i + 1)(j + 2)$), i.e. invertible, so each of the monomials $\phi(k + 1, k)$, $\phi(k + 2, k)$, $\phi(p + k + 1, k)$ and $\phi(p + k + 2, k)$ can be written as linear combinations of hit monomials. It follows that $\phi(m, k)$ is hit for every m if $k \leq i$.

Thus we have seen that if $k \leq i$ or $k \geq j + 2$, every monomial $\phi(m, k)$ is hit. Finally, if $i + 1 \leq k \leq j + 1$, then the only values of m for which $\phi(m, k)$ is not hit by \mathcal{P}^1 are those satisfying $k + 1 \leq m \leq p + k - j - 1$ or $p + k + 1 \leq m \leq M$. As usual, if m, m' both belong to the same interval, then $\phi(m, k)$ and $\phi(m', k)$ are equivalent modulo elements hit by \mathcal{P}^1 .

Now, since $i + 1 \leq k \leq j + 1$, we see that $M = p + i + 2 \leq p + k + 1$. So the second interval contains at most one value, which corresponds to a hit monomial, according to Lemma 4.3. We claim that all monomials corresponding to values in the first interval are not hit, and hence form an equivalence class modulo hit elements, i.e. a basis element for $M^{2n}(2)$.

To see this, note that, by the short Cartan formula, the space of elements hit by \mathcal{P}^p , modulo that of elements hit by \mathcal{P}^1 , is spanned by $\Phi(m, k)$, for $0 \leq m \leq M - p$, where

$$\begin{aligned} \Phi(m, k) &= \binom{m(p-1)+k}{p} \phi(m, k) + \binom{n-k-(m+p)(p-1)}{p} \phi(m+p, k) \\ &\equiv \mathcal{P}^p(x^{m(p-1)+k}y^{n-k-(m+p)(p-1)}) \text{ modulo elements hit by } \mathcal{P}^1. \end{aligned}$$

If $\phi(m, k)$, with $k + 1 \leq m \leq p + k - j - 1$, appears as a non-trivial summand of $\Phi(m', k)$, then either $m' = 0$ (and $m = p$) or $m' = k + 1$ (and $m = k + 1$). But in both of these cases we see that the coefficient of $\phi(m, k)$ in $\Phi(m', k)$ is zero. So none of these monomials $\phi(m, k)$ with $k + 1 \leq m \leq p + k - j - 1$ can be hit by \mathcal{P}^p , and hence none can be hit.

Our conclusion is then:

Proposition 4.5. *If $n = p^2 + ip + j - 1$, with $1 \leq i \leq j \leq p - 2$, then any monomial basis for $M^{2n}(2)$ can be formed by taking, for each $k \in \{i + 1, \dots, j + 1\}$, some monomial $\phi(m_k, k)$ such that $k + 1 \leq m_k \leq p + k - j - 1$.*

It is easily seen that the basis given in Table 1 is obtained in this way.

5. RETIREMENT I

In this section we consider the case where $n = (i + 1)p^r - 1$ with $1 \leq i \leq p - 1$, $r \geq 2$.

First we note that x^n and y^n are not hit. For if x^n were hit, then, by the second part of the splitting Theorem 2.4, it would be the image under some operation \mathcal{P}^{p^s} of $x^{n-p^s(p-1)}$. But, by considering the p -adic expansion for n , one sees from equation (1) that $\binom{n-p^s(p-1)}{p^s} = 0$ for any s . Similarly, y^n cannot be hit. They also cannot be constituent terms in any hit polynomial, again by Theorem 2.4. Thus they are necessary members of any basis but, having said that, they play no further rôle in our calculations.

As in the previous sections, define $\phi(m, k) = x^{m(p-1)+k}y^{n-k-m(p-1)}$, for $1 \leq k \leq p - 1$ and $0 \leq m \leq M$, where $M = \lfloor (n - k - 1)/(p - 1) \rfloor$.

Theorem 5.1. *For $1 \leq k \leq p - 1$, if $0 \leq m < M$, then there exists some m' such that $m < m' \leq M$ and $\phi(m, k) + \phi(m', k)$ is hit.*

From this it follows that, for each value of k , the monomials $\phi(m, k)$ and $\phi(m', k)$ are equivalent, modulo hit elements, for any m and m' . Thus any basis of monomial elements can be formed by taking x^n and y^n , and then any set $\{\phi(m_k, k) \mid k \in K\}$ where K is some subset of the set of integers $\{1, \dots, p - 1\}$ and $0 \leq m_k \leq M$. In fact, we have the following result, that K must, in fact, be the whole set $\{1, \dots, p - 1\}$, which we will prove after we prove the theorem.

Proposition 5.2. *If $n = (i + 1)p^r - 1$ for some $1 \leq i \leq p - 1$, $r \geq 2$, then any monomial basis for $M^{2n}(2)$ consists of x^n , y^n and a set $\{\phi(m_k, k) \mid 1 \leq k \leq p - 1\}$, where each m_k is any integer such that $0 < m_k(p - 1) + k < n$.*

Again one checks, without difficulty, that the basis given in Table 1 is of this form.

Proof of the theorem. First note that $\phi(m, k) + \phi(m + 1, k)$ will be hit by \mathcal{P}^1 if $\binom{m(p-1)+k}{1} \neq 0$, $\binom{n-k-(m+1)(p-1)}{1} \neq 0$ and $n - k - (m + 1)(p - 1) \geq 0$. But if the third condition holds, then the first and second conditions are equivalent. For these binomial coefficients are precisely the residue classes of $m(p - 1) + k$ and $n - k - (m + 1)(p - 1)$ (providing that $n - k - (m + 1)(p - 1) \geq 0$). The sum of these residue classes must be congruent modulo p to the residue class of the sum. The sum is $n - (p - 1)$, which has residue class 0. So in particular, if one of the residue classes is zero, then the other one must also be zero. In other words, $\binom{m(p-1)+k}{1} \neq 0$ if and only if $\binom{n-k-(m+1)(p-1)}{1} \neq 0$.

Hence if $\binom{m(p-1)+k}{1} \neq 0$ and $n - k - (m + 1)(p - 1) \geq 0$, then setting $m' = m + 1$ will complete the proof of the theorem in this case.

Now consider when $\phi(m, k) + \phi(m + p, k)$ is hit by \mathcal{P}^p . We apply the short Cartan formula to $\mathcal{P}^p(x^{m(p-1)+k}y^{n-k-(m+p)(p-1)})$ to see that $\phi(m, k) + \phi(m + p, k)$ will be hit when $\binom{m(p-1)+k}{p} \neq 0$, $\binom{n-k-(m+p)(p-1)}{p} \neq 0$ and $n - k - (m + p)(p - 1) \geq 0$. Again, if the third condition holds, then the first and second conditions are equivalent. To see this, let $m(p - 1) + k$ have p -adic expansion $a_0 + a_1p + a_2p^2 + \dots$ and let $n - k - (m + p)(p - 1)$ have p -adic expansion $b_0 + b_1p + b_2p^2 + \dots$. Then $a_0 + b_0 \equiv n - p(p - 1) \equiv p - 1 \pmod{p}$. So, since a_0 and b_0 are both $\leq p - 1$, we must have that $a_0 + b_0 = p - 1$. Thus $a_1 + b_1 \equiv 0$, since the p -adic expansion for $n - p(p - 1)$ starts $(p - 1) + 0p + (p - 1)p^2 + \dots$. In particular, $a_1 = 0$ if and only if $b_1 = 0$. But this proves the claim, since $a_1 = \binom{m(p-1)+k}{p}$ and $b_1 = \binom{n-k-(m+p)(p-1)}{p}$, by equation (1).

Thus if $\binom{m(p-1)+k}{p} \neq 0$ and $n - k - (m + p)(p - 1) \geq 0$, we can set $m' = m + p$ and the theorem will be proved in this case.

We can continue this line of reasoning. Applying the short Cartan formula to $\mathcal{P}^{p^q}(x^{m(p-1)+k}y^{n-k-(m+p^q)(p-1)})$ we see that $\phi(m, k) + \phi(m + p^q, k)$ will be hit when $\binom{m(p-1)+k}{p^q} \neq 0$, $\binom{n-k-(m+p^q)(p-1)}{p^q} \neq 0$ and $n - k - (m + p^q)(p - 1) \geq 0$. If the third condition holds, then the first and second conditions will be equivalent; this is seen by generalising the argument given above. Let $a_0 + a_1p + \dots$ be the p -adic expansion of $m(p - 1) + k$, as before, let $b_0 + b_1p + \dots$ be that of $n - k - (m + p^q)(p - 1)$ and note that $n - p^q(p - 1)$ has p -adic expansion

$$(p - 1) + (p - 1)p + \dots + (p - 1)p^{q-1} + 0p^q + (p - 1)p^{q+1} + \dots + (p - 1)p^{r-1} + ip^r.$$

Thus $a_0 + b_0 \equiv p - 1$, so $a_0 + b_0 = p - 1$ and hence $a_1 + b_1 \equiv p - 1$. This in turn implies that $a_1 + b_1 = p - 1$, and so $a_2 + b_2 \equiv p - 1$, etc., until we see that $a_{q-1} + b_{q-1} = p - 1$. Then $a_q + b_q \equiv 0$, which implies $a_q = 0$ if and only if $b_q = 0$, as required.

Thus if $\binom{m(p-1)+k}{p^q} \neq 0$ and $n - k - (m + p^q)(p - 1) \geq 0$, then $\binom{n-k-(m+p^q)(p-1)}{p^q}$ must also be non-zero, so we can set $m' = m + p^q$ to prove the theorem in this case.

Thus we have proved the theorem in almost all cases. The remaining cases correspond to those m such that, for each q ($0 \leq q \leq r - 1$), either $\binom{m(p-1)+k}{p^q} = 0$ or $n - k - (m + p^q)(p - 1) < 0$. The latter condition is equivalent to $n - k - m(p - 1) < p^q(p - 1)$ and, clearly, if $n - k - m(p - 1) < p^q(p - 1)$, then $n - k - m(p - 1) < p^s(p - 1)$ for every $s \geq q$. So let q_0 now denote the smallest integer such that

$n - k - m(p - 1) < p^{q_0}(p - 1)$. Then $\binom{m(p-1)+k}{p^s} = 0$ for all $s < q_0$ and so p^{q_0} divides $m(p - 1) + k$. Since $m(p - 1) + k > n - p^{q_0}(p - 1)$, by the minimality of q_0 , and $n - p^{q_0}(p - 1)$ has p -adic expansion

$$(p - 1) + (p - 1)p + \cdots + (p - 1)p^{q_0-1} + 0p^{q_0} + (p - 1)p^{q_0+1} + \cdots + (p - 1)p^{r-1} + ip^r,$$

and $m(p - 1) + k$ is divisible by p^{q_0} , it follows that $m(p - 1) + k$ must have p -adic expansion

$$0 + 0p + \cdots + 0p^{q_0-1} + jp^{q_0} + (p - 1)p^{q_0+1} + (p - 1)p^{q_0+2} + \cdots + (p - 1)p^{r-1} + ip^r,$$

where $1 \leq j \leq p - 1$. In other words, $m(p - 1) + k = n - (p^{q_0+1} - 1) + jp^{q_0}$.

If $q_0 = 0$, then $n - k - m(p - 1) < p - 1$ so $(m + 1)(p - 1) > n - k$ and $m + 1 > \lfloor (n - k - 1)/(p - 1) \rfloor$, i.e. $m \geq M$, which contradicts the hypotheses of the theorem. Hence we conclude that $q_0 \geq 1$.

We first assume that $q_0 \geq 2$. Our strategy in this case is to show that $\phi(m, k) + \phi(m - 1, k)$ is hit by \mathcal{P}^1 , and then that $\phi(m - 1, k) + \phi(p^{q_0-1} + m - 1, k)$ is hit. Since $q_0 \geq 2$, it follows that $p^{q_0-1} + m - 1 > m$ and we can take m' to be $p^{q_0-1} + m - 1$. The details are as follows.

As observed earlier, $\binom{m(p-1)+k}{p^s} = 0$ for all $s < q_0$ so, in particular, $\binom{m(p-1)+k}{1} = 0$, which implies that $\binom{(m-1)(p-1)+k}{1} = 1 \neq 0$. Also $n - k - m(p - 1) \geq p^{q_0-1}(p - 1)$ (by minimality of q_0) so $n - k - m(p - 1) > 0$ and, by the reasoning used at the start of this proof, $\phi(m - 1, k) + \phi(m, k)$ is hit by \mathcal{P}^1 .

Using the p -adic expansion for $m(p - 1) + k$ given above, $(m - 1)(p - 1) + k$ must equal

$$1 + (p - 1)p + \cdots + (p - 1)p^{q_0-1} + (j - 1)p^{q_0} + (p - 1)p^{q_0+1} + \cdots + (p - 1)p^{r-1} + ip^r$$

and this will be a p -adic expansion, at least up to (and including) the coefficient of p^{q_0-1} . Therefore $\binom{(m-1)(p-1)+k}{p^{q_0-1}} = p - 1 \neq 0$. Also, $n - k - (m - 1)(p - 1) \geq p^{q_0-1}(p - 1) + p - 1$ by minimality of q_0 . So $n - k - (m - 1)(p - 1) > 0$ and, by the same argument as earlier, $\phi(m - 1, k) + \phi(m + p^{q_0} - 1, k)$ is hit by $\mathcal{P}^{p^{q_0}}$. This completes the proof in this case.

We are left with the case where $q_0 = 1$. In this case we show that $\phi(m, k) + \phi(m - (j + 1), k)$ is hit by \mathcal{P}^1 and then that $\phi(m - (j + 1), k) + \phi(m + p - (j + 1), k)$ is hit by \mathcal{P}^p , using the same techniques as above. If $j < p - 1$, then $m + p - (j + 1) > m$ and by setting $m' = m + p - (j + 1)$ the proof of the theorem is complete in this case. If $j = p - 1$, then $n - k - m(p - 1) = (p - 1)$, so $m + 1 > \lfloor (n - k - 1)/(p - 1) \rfloor$, i.e. $m \geq M$, contradicting the hypotheses of the theorem. \square

Now we turn to the proof of Proposition 5.2. It follows from the following

Lemma 5.3. *There are no hit monomials in these degrees.*

For, if it were possible to form a basis $\{x^n, y^n\} \cup \{\phi(m_k, k) \mid k \in K\}$ for some proper subset $K \subset \{1, \dots, p - 1\}$, then, by virtue of the splitting Theorem 2.4, this would imply that for any $k' \in \{1, \dots, p - 1\}$ not present in K , $\phi(m, k')$ is hit for all m , in contradiction of Lemma 5.3.

Proof of the lemma. For the proof of this lemma it is necessary to abandon the convention about suppressing non-zero scalars introduced in section 2. Thus, in this proof, $\mathcal{P}^{p^t}(A) = B + C$ means absolute equality, not just up to scalar multiple of the individual terms.

Consider $\mathcal{P}^{p^t}(x^q y^r)$ where q and r are such that $q + r + p^t(p - 1) = n$. Let $m = n - p^t(p - 1)$, which has p -adic expansion

$$(p - 1) + (p - 1)p + \cdots + (p - 1)p^{t-1} + 0p^t + (p - 1)p^{t+1} + \cdots + (p - 1)p^{r-1} + ip^r.$$

Let q, r have p -adic expansions $\sum q_j p^j$ and $\sum r_j p^j$. As in the proof of Theorem 5.1, one can easily see by induction that $q_j + r_j = p - 1$ for $0 \leq j \leq t - 1$ and $q_t + r_t \equiv 0 \pmod p$. So $r_t \equiv -q_t \pmod p$ and, using Lemma 2.2, we see that

$$\mathcal{P}^{p^t}(x^q y^r) \equiv \mathcal{P}^{p^t}(x^q) y^r + x^q \mathcal{P}^{p^t}(y^r) = q_t(x^{q+p^t(p-1)} y^r - x^q y^{r+p^t(p-1)})$$

modulo elements hit by $\mathcal{P}^{p^{t-1}}$.

Thus the image of any monomial under \mathcal{P}^{p^t} is, modulo elements hit by $\mathcal{P}^{p^{t-1}}$, a (possibly zero) scalar multiple of $\phi(m, k) - \phi(m - p^t, k)$ for some m, k . Then by the linearity of the Steenrod operations and the fact that \mathcal{P}^i is decomposable whenever i is not a power of p , we see that the space of hit elements in these degrees is spanned by terms of the form $\phi(m, k) - \phi(m - p^t, k)$ for some t, m, k . Thus any hit element can be written in this form. Clearly we cannot write $\phi(m, k)$ in this form for any m, k and there cannot be any $\phi(m, k)$ which is hit. Thus the lemma is proven. \square

6. RETIREMENT II

Finally we turn to the case $n = (i + 1)p^r + j - 1$ where $r \geq 2, 1 \leq i \leq p - 1$ and $1 \leq j \leq p - 2$.

As always, we define $\phi(m, k)$ by $\phi(m, k) = x^{m(p-1)+k} y^{n-k-m(p-1)}$ for $1 \leq k \leq p - 1$ and for a certain range of m , the range being dependent on k . Before deciding what this range should be, we make some observations about certain monomials in these degrees.

Consider $x^s y^t$ where $s < j$, so $t \geq (i + 1)p^r$. Then $0 \leq \bar{t} \leq j - 1$ so $\bar{s} + \bar{t} = j - 1$ and, by Lemma 2.3, $x^s y^t$ is hit by \mathcal{P}^1 . Similarly, $x^t y^s$ is hit by \mathcal{P}^1 . On the other hand, if $s = j$, then $t = (i + 1)p^r - 1$ and, as we saw in the previous section, y^t is not hit. Since $j < p$, we also see that x^s is not hit, so $x^s y^t$ cannot be hit, nor can it be a constituent monomial in any hit polynomial. Therefore $x^j y^{(i+1)p^r-1}$ is an indispensable basis element, but it plays no further part in our calculations. The same is true for $x^{(i+1)p^r-1} y^j$.

So we wish the range on m to ensure that we always have $j + 1 \leq m(p - 1) + k \leq (i + 1)p^r - 2$. Thus we insist that $M_0 \leq m \leq M_1$ where $M_0 = 0$ if $k > j$ and $M_0 = 1$ if $k \leq j$ and $M_1 = \lfloor ((i + 1)p^r - 2 - k)/(p - 1) \rfloor$.

We now consider the image of \mathcal{P}^1 .

Lemma 6.1. *If $M_0 \leq m \leq M_1$, then $\phi(m, k)$ is hit by \mathcal{P}^1 if and only if $m \equiv k, k - 1, \dots, k - (j - 2)$ or $k - (j - 1) \pmod p$. In particular, note that if $m \leq M_1 - p$, then $\phi(m, k)$ is hit by \mathcal{P}^1 if and only if $\phi(m + p, k)$ is hit by \mathcal{P}^1 . If $M_0 \leq m \leq M_1 - 1$ and neither $\phi(m, k)$ nor $\phi(m + 1, k)$ are hit by \mathcal{P}^1 , then $\phi(m, k) + \phi(m + 1, k)$ is hit by \mathcal{P}^1 .*

Proof. Since $n > p^2 - p$, Lemma 2.3 tells us that $\phi(m, k)$ is hit by \mathcal{P}^1 if and only if $\overline{(m(p-1) + k) + (n - k - m(p-1))} < p - 1$. The sum of these residue classes must be congruent to n modulo p , i.e. congruent to $j - 1$. Thus if $\overline{(m(p-1) + k)} \leq j - 1$, then, since $\overline{(n - k - m(p-1))} \leq p - 1$, the sum must be equal to $j - 1$ and hence less than $p - 1$. Conversely, if the sum is less than $p - 1$, then it must equal $j - 1$ and so $\overline{(m(p-1) + k)} \leq j - 1$. But if $m \geq 0$, then, by definition, $\overline{(m(p-1) + k)} \leq j - 1$ if and only if $k - m \equiv j - 1, j - 2, \dots, 0$, which is equivalent to the condition stated in the lemma.

Now $\phi(m, k) + \phi(m + 1, k)$ will be equal to $\mathcal{P}^1(x^{m(p-1)+k}y^{n-k-(m+1)(p-1)})$ if $\overline{(m(p-1) + k)} \neq 0$ and $\overline{(n - k - (m + 1)(p - 1))} \neq 0$. If $\overline{(m(p-1) + k)} = 0$, then, by the first part of the lemma, $\phi(m, k)$ is hit by \mathcal{P}^1 , while $\phi(m + 1, k)$ will be hit by \mathcal{P}^1 if $\overline{(n - k - (m + 1)(p - 1))} = 0$. \square

Lemma 6.2. *If $M_0 \leq m \leq M_1 - p$ and $\phi(m, k)$ is not hit by \mathcal{P}^1 , then $\phi(m, k) + \phi(m + p, k)$ is hit by \mathcal{P}^p .*

Combining Lemmas 6.1 and 6.2 we see that, for any k , if m, m' are such that neither $\phi(m, k)$ nor $\phi(m', k)$ are hit by \mathcal{P}^1 , then they are equivalent modulo hit elements.

Then, as in the previous section, any monomial basis must consist of $x^{(i+1)p^r-1}y^j$, $x^jy^{(i+1)p^r-1}$ and a set $\{\phi(m_k, k) \mid k \in K\}$ where X is some subset of $\{1, \dots, p - 1\}$, and m_k are chosen subject to $0 \leq m_k \leq M$ and $\overline{(m_k(p-1) + k)} \geq j$. As before, we will see that K must be the whole set $\{1, \dots, p - 1\}$ and we have the following conclusion.

Proposition 6.3. *If $n = (i + 1)p^r + j - 1$ with $r \geq 2$, $1 \leq i \leq p - 1$, $1 \leq j \leq p - 2$, then any monomial basis for $M^{2n}(2)$ will consist of $x^{(i+1)p^r-1}y^j$, $x^jy^{(i+1)p^r-1}$ and $\{\phi(m_k, k) \mid 1 \leq k \leq p - 1\}$, where each m_k is any integer such that $j < m_k(p - 1) + k < n - j$ and $\overline{(m_k(p-1) + k)} \geq j$.*

We will prove this after we have proved Lemma 6.2. However, before we can prove Lemma 6.2 we need one preliminary result.

Lemma 6.4. *If $M_0 \leq m \leq M_1 - p$, $\phi(m, k)$ is not hit by \mathcal{P}^1 , then $\phi(m, k) + \phi(m + p, k)$ is hit by \mathcal{P}^p if either $\binom{m(p-1)+k}{p} \neq 0$ or $\binom{n-k-(m+p)(p-1)}{p} \neq 0$.*

Proof. Applying the short Cartan formula to $\mathcal{P}^p(x^{m(p-1)+k}y^{n-k-(m+p)(p-1)})$, we see that $\phi(m, k) + \phi(m + p, k)$ is hit by \mathcal{P}^p if $\binom{m(p-1)+k}{p} \neq 0$ and $\binom{n-k-(m+p)(p-1)}{p} \neq 0$. So it will suffice to show that these two conditions are equivalent. Suppose that $m(p-1) + k$ has p -adic expansion $a_0 + a_1p + a_2p^2 + \dots$ and that $n - k - (m + p)(p - 1)$ has p -adic expansion $b_0 + b_1p + b_2p^2 + \dots$. Then $a_0 + b_0 \equiv n - p(p - 1) \equiv j - 1 \pmod{p}$, i.e. $a_0 + b_0 = j - 1$ or $p + j - 1$. By assumption, $\phi(m, k)$ is not hit, so, by Lemma 6.1, $a_0 \geq j$ and thus $a_0 + b_0 = p + j - 1$. It follows that $(p + j - 1) + (a_1 + b_1)p \equiv n - p(p - 1) \equiv p + j - 1 \pmod{p^2}$. Thus $a_1 + b_1 = 0$ or $a_1 + b_1 = p$. In either case, $a_1 \neq 0$ if and only if $b_1 \neq 0$. By equation (1), this implies that $\binom{m(p-1)+k}{p} \neq 0$ if and only if $\binom{n-k-(m+p)(p-1)}{p} \neq 0$. \square

Proof of Lemma 6.2. We first suppose that $M_0 + 1 \leq m \leq M_1 - p - 1$ and that $\phi(m, k)$ is not hit by \mathcal{P}^1 . If $\binom{m(p-1)+k}{p} \neq 0$, then, by Lemma 6.4, $\phi(m, k) + \phi(m + p, k)$ is hit by \mathcal{P}^p and the proof is complete in this case.

If $\binom{m(p-1)+k}{p} = 0$, then let $m(p-1)+k$ have p -adic expansion $a_0+a_1p+a_2p^2+\dots$. Since $\phi(m, k)$ is not hit by \mathcal{P}^1 , we have, by Lemma 6.1, that $a_0 \geq j$ and, since $\binom{m(p-1)+k}{p} = 0$ we have, by equation (1), that $a_1 = 0$. Thus

$$(m+1)(p-1)+k = (a_0-1) + 1p + a_2p^2 + \dots$$

and this will be a p -adic expansion. Hence $\binom{(m+1)(p-1)+k}{p} = 1 \neq 0$ and, if $\phi(m+1, k)$ is not hit by \mathcal{P}^1 , then Lemma 6.4 tells us that $\phi(m+1, k)+\phi(m+p+1, k)$ is hit by \mathcal{P}^p . Assuming that this is the case, Lemma 6.1 states that $\phi(m, k)+\phi(m+1, k)$ is hit by \mathcal{P}^1 and that $\phi(m+p, k)+\phi(m+p+1, k)$ is hit by \mathcal{P}^1 , and hence $\phi(m, k)+\phi(m+p, k)$ is hit by \mathcal{P}^1 . Thus the proof is complete unless $\phi(m+1, k)$ is hit by \mathcal{P}^1 .

Using the p -adic expansions for $m(p-1)+k$ and $(m+1)(p-1)+k$ given above, if $\phi(m, k)$ is not hit by \mathcal{P}^1 but $\phi(m+1, k)$ is, then $a_0 = j$. Hence $(m-1)(p-1)+k = (a_0+1) + (p-1)p + (a_2-1)p^2 + \dots$ and this will be a p -adic expansion, at least up to (and including) the coefficient of p . In particular, $\binom{(m-1)(p-1)+k}{p} = p-1 \neq 0$. Further, $1 \leq a_0+1 = j+1 \leq p-1$ so, by Lemma 6.1, $\phi(m-1, k)$ is not hit by \mathcal{P}^1 . Hence, by Lemma 6.4, $\phi(m-1, k)+\phi(m+p-1, k)$ is hit by \mathcal{P}^p . Then we also have that $\phi(m-1, k)+\phi(m, k)$ and $\phi(m+p-1, k)+\phi(m+p, k)$ are both hit by \mathcal{P}^1 , by Lemma 6.1, and hence that $\phi(m, k)+\phi(m+p, k)$ is hit by \mathcal{P}^p .

It only remains to deal with $m = M_0$ or $m = M_1 - p$. Suppose first that $m = M_0$. If $k > j$, then $M_0 = 0$. By Lemma 6.1, $\phi(1, k)$ is not hit by \mathcal{P}^1 and, since $\binom{(p-1)+k}{p} = 1 \neq 0$, Lemma 6.4 shows that $\phi(1, k)+\phi(p+1, k)$ is hit by \mathcal{P}^1 . Since neither $\phi(0, k)$ nor $\phi(1, k)$ are hit by \mathcal{P}^1 , it follows from Lemma 6.1 that both $\phi(0, k)+\phi(1, k)$ and $\phi(p, k)+\phi(p+1, k)$ are hit by \mathcal{P}^1 . Thus $\phi(0, k)+\phi(p, k)$ is hit by \mathcal{P}^p and the proof is complete in this case.

If $k \leq j$, then $M_0 = 1$. But $\binom{1+(p-1)+k}{1} = k-1 \leq j-1$ and so $\phi(1, k)$ is hit by \mathcal{P}^1 , by Lemma 6.1. So there is nothing to prove in this case.

Finally, we deal with the case where $m = M_1$. By definition,

$$M_1 = \lfloor ((i+1)p^r - 2 - k)/(p-1) \rfloor,$$

i.e.

$$M_1 = \begin{cases} (i+1)(p^{r-1} + \dots + 1) + k & \text{if } k \leq i-1, \\ (i+1)(p^{r-1} + \dots + 1) + k - 1 & \text{if } k \geq i. \end{cases}$$

In either case $(i+1)p^r - p \leq M_1(p-1) + k < (i+1)p^r$, so $\binom{M_1(p-1)+k}{p} = p-1 \neq 0$. By Lemma 6.4 this shows that $\phi(M_1-p, k)+\phi(M_1, k)$ is hit by \mathcal{P}^p , which completes the proof. □

Now we prove Proposition 6.3. Exactly as in the previous section, it follows from:

Lemma 6.5. *The only hit monomials in these degrees are those $x^q y^r$ where $\binom{q}{1} \leq j-1$.*

Proof. The main idea of the proof is similar to that of Lemma 5.3 - we describe a set of polynomials which spans the space of hit elements in these degrees and show that the only monomials which can be expressed as linear combinations of these polynomials are those given in the statement of the lemma. As in Lemma 5.3, we suspend the convention about non-zero scalars, so equality will mean exact equality throughout this proof, not just up to a non-zero scaling.

We will prove that all hit elements in these degrees can be expressed as linear combinations of:

$$\begin{aligned} & \{\bar{\phi}(m, k) \mid \overline{(m(p-1)+k)} \leq j-1\} \cup \\ & \{\bar{\phi}(m, k) - \bar{\phi}(m+1, mk) \mid \overline{(m(p-1)+k)} \geq j, \text{ and } \overline{((m+1)(p-1)+k)} \geq j\} \cup \\ & \{\bar{\phi}(m, k) - \bar{\phi}(m+p^s, k) \mid 1 \leq s, \} \end{aligned}$$

where we have replaced $\phi(m, k)$ by some (non-zero) scalar multiple of it, $\bar{\phi}(m, k)$, to simplify the expressions above.

It is then easily seen that the only monomials in these degrees which are hit are those $\bar{\phi}(m, k)$, (or $\phi(m, k)$) for which $\overline{(m(p-1)+k)} \leq j-1$, and the proof of the lemma follows.

We will demonstrate this claim by proving, by induction on q , that the space of elements in these degrees hit by \mathcal{P}^{p^q} is spanned by the set S_q defined by :

$$\begin{aligned} S_q = & \{\bar{\phi}(m, k) \mid \overline{(m(p-1)+k)} \leq j-1\} \cup \\ & \{\bar{\phi}(m, k) - \bar{\phi}(m+1, mk) \mid \overline{(m(p-1)+k)} \geq j, \text{ and } \overline{((m+1)(p-1)+k)} \geq j\} \cup \\ & \{\bar{\phi}(m, k) - \bar{\phi}(m+p^s, k) \mid 1 \leq s \leq q, \}. \end{aligned}$$

We start with the case where $q = 0$. The image of \mathcal{P}^1 has been described in Lemma 6.1. Rephrasing the results of that lemma, since we are no longer suppressing non-zero scalars, it says that $\phi(m, k)$ is hit by \mathcal{P}^1 if $m \equiv k, k-1, \dots, k-(j-1) \pmod p$ and if neither $\phi(m, k)$ nor $\phi(m+1, k)$ are hit by \mathcal{P}^1 , then $\lambda_{m,k}\phi(m, k) + \lambda'_{m+1,k}\phi(m+1, k)$ is hit for some non-zero scalars $\lambda_{m,k}$ and $\lambda'_{m+1,k}$. These scalars are determined by

$$\mathcal{P}^1(x^{m(p-1)+k}y^{n-k-(m+1)(p-1)}) = \lambda_{m,k}\phi(m, k) + \lambda'_{m+1,k}\phi(m+1, k).$$

Now we wish to define $\bar{\phi}(m, k) = \mu_{m,k}\phi(m, k)$ for some (non-zero) scalar $\mu_{m,k}$ so as to arrange that $\lambda_{m,k}\phi(m, k) + \lambda'_{m+1,k}\phi(m+1, k)$ is a multiple of $\bar{\phi}(m, k) - \bar{\phi}(m+1, k)$. To do this, define $\mu_{m,k} = 1$ if $m \equiv k+1 \pmod p$ and then, assuming that $m \equiv k+2, \dots, k+p-j-1 \pmod p$ and that $\mu_{m,k}$ has been defined, define $\mu_{m+1,k}$ by

$$\mu_{m+1,k} = -\mu_{m,k}\lambda'_{m+1,k}/\lambda_{m,k}.$$

It is then seen that

$$\lambda_{m,k}(\bar{\phi}(m, k) - \bar{\phi}(m+1, k)) = \mu_{m,k}(\lambda_{m,k}\phi(m, k) + \lambda'_{m+1,k}\phi(m+1, k)).$$

Finally, if $m \equiv k, k-1, \dots, k-(j-1) \pmod p$, we define $\mu_{m,k} = 1$, i.e. $\bar{\phi}(m, k) = \phi(m, k)$.

Thus we see that the space of elements hit by \mathcal{P}^1 is spanned by

$$\begin{aligned} & \{\bar{\phi}(m, k) \mid \overline{(m(p-1)+k)} \leq j-1\} \cup \\ & \{\bar{\phi}(m, k) - \bar{\phi}(m+1, mk) \mid \overline{(m(p-1)+k)} \geq j, \text{ and } \overline{((m+1)(p-1)+k)} \geq j\}, \end{aligned}$$

which is precisely S_0 , and the start of the inductive proof is complete.

Now we assume, as an inductive hypothesis, that the space of elements hit by $\mathcal{P}^{p^{q-1}}$ is spanned by the set of polynomials S_{q-1} and we consider those elements which are hit by \mathcal{P}^{p^q} . Suppose that $s+t = n - p^q(p-1)$. By the short Cartan formula, Lemma 2.2,

$$\mathcal{P}^{p^q}(x^s y^t) \equiv \mathcal{P}^{p^q}(x^s)y^t + x^s \mathcal{P}^{p^q}(y^t)$$

modulo elements hit by \mathcal{P}^{p^q-1} . Note that since all the operations \mathcal{P}^d are decomposable unless d is a power of p , any element hit by \mathcal{P}^{p^q-1} is, in fact, hit by \mathcal{P}^{p^q-1} and thus can be described using the inductive hypothesis. So it only remains to show that $\mathcal{P}^{p^q}(x^s)y^t + x^s\mathcal{P}^{p^q}(y^t)$ can be written as a linear combination of elements in S_q .

Now, if $\bar{s} \leq j - 1$, then $\overline{(s + p^q(p - 1))} = \bar{s} \leq j - 1$ and $\mathcal{P}^{p^q}(x^s)y^t$ is hit by \mathcal{P}^1 . Moreover, if this is the case, then, since $\bar{t} + \bar{s} \equiv n - p^q(p - 1) \equiv j - 1 \pmod{p}$, we have that $\bar{t} \leq j - 1$ and hence $x^s\mathcal{P}^{p^q}(y^t)$ is also hit by \mathcal{P}^1 . So in this case $\mathcal{P}^{p^q}(x^s)y^t, x^s\mathcal{P}^{p^q}(y^t) \in S_0$ and the inductive proof is clear.

If $\bar{s} \geq j$, then, as in the proof of Lemma 5.3, by considering the p -adic expansions of s and t , we see that $\binom{s}{p^q} = -\binom{t}{p^q}$. For if $s = s_0 + s_1p + \dots$ and $t = t_0 + t_1p + \dots$, then, since $s + t = n - p^q(p - 1)$, we see that $\bar{s} = s_0 \geq j$ implies that $s_0 + t_0 = p + j - 1$, so $s_1 + t_1 = p - 1$, $s_2 + t_2 = p - 1$, etc. and $s_q + t_q = 0$, i.e. $\binom{s}{p^q} + \binom{t}{p^q} = 0$. Thus

$$\begin{aligned} \mathcal{P}^{p^q}(x^s)y^t + x^s\mathcal{P}^{p^q}(y^t) &= \binom{s}{p^q}(x^{s+p^q(p-1)}y^t - x^s y^{t+p^q(p-1)}) \\ &= \binom{s}{p^q}(\phi(m, k) - \phi(m + p^q, k)) \\ &= \binom{s}{p^q}\mu_{m,k}^{-1}(\bar{\phi}(m, k) - \bar{\phi}(m + p^q, k)) \end{aligned}$$

for some m, k , and the proof is complete. □

REFERENCES

1. M. A. Alghamdi, M. C. Crabb, J. R. Hubbuck, Representations of the homology of BV and the Steenrod algebra I, In *Adams Memorial Symposium*, eds. N. Ray, G. Walker, L.M.S. Lect. Notes **176** C.U.P. (1992), 217-234. MR **94i**:55022
2. D. P. Carlisle, R. M. W. Wood, The boundedness conjecture for the action of the Steenrod algebra on polynomials, In *Adams Memorial Symposium*, eds. N. Ray, G. Walker, L.M.S. Lect. Notes **176** C.U.P. (1992), 203-216. MR **95f**:55015
3. M. D. Crossley, $\mathcal{A}(p)$ -annihilated elements in $H_*(CP^\infty \times CP^\infty)$, *Math. Proc. Camb. Phil. Soc.* **120** (1996), 441-453. MR **97d**:55029
4. M. D. Crossley, $\mathcal{A}(p)$ generators for H^*V and Singer's homological transfer, To appear in *Math. Z.*
5. M. D. Crossley, H^*V is of bounded type over $\mathcal{A}(p)$, *Proc. Sympos. Pure Math.*, **63**, Amer. Math. Soc., Providence, RI, 1998. CMP 98:08
6. L. Schwartz, Unstable modules over the Steenrod algebra and Sullivan's fixed point set conjecture, *Chicago Lectures in Math.*, Univ. of Chicago Press (1994). MR **95d**:55017
7. W. M. Singer, The transfer in homological algebra, *Math. Z.* **202** (1989), 493-524. MR **90i**:55035
8. N. E. Steenrod, *Cohomology Operations*, *Annals of Math. Studies* **50**, Princeton Univ. Press (1962). MR **26**:3056
9. P. D. Straffin, Jr., Identities for conjugation in the Steenrod algebra, *Proc. A.M.S.* **49** (1975), 253-255. MR **52**:1693
10. R. M. W. Wood, Steenrod squares of polynomials, In *Advances in Homotopy Theory*, eds. Salamon, S. M. et al., L.M.S. Lect. Notes, **139** C.U.P. (1989), 173-177. MR **91c**:55030

CENTRE DE RECERCA MATEMÀTICA, INSTITUT D'ESTUDIS CATALANS, APARTAT 50, E-08193, BELLATERRA, BARCELONA, SPAIN

Current address: Laboratoire d'Analyse, Géométrie et Applications, Université Paris Nord, 93430 Villentaneuse, France

E-mail address: crossley@math.univ-paris13.fr