Algebraic & Geometric Topology 17 (2017) 957–982

Hopf ring structure on the mod p cohomology of symmetric groups

LORENZO GUERRA

We describe a Hopf ring structure on $\bigoplus_{n\geq 0} H^*(\Sigma_n;\mathbb{Z}_p)$, discovered by Strickland and Turner, where Σ_n is the symmetric group of n objects and p is an odd prime. We also describe an additive basis on which the cup product is explicitly determined, compute the restriction to modular invariants and determine the action of the Steenrod algebra on our Hopf ring generators. For $p=2$ this was achieved in work of Giusti, Salvatore and Sinha, of which this work is an extension.

20J06

1 Introduction

Let Σ_n be the symmetric group of n objects. Strickland and Turner [8] proved that, for a multiplicative cohomology theory E, the group $A = E\big(\coprod_{n\geq 0} B(\Sigma_n)\big)$ has the structure of a Hopf ring (ie, it admits a coproduct Δ, two products $\odot$ and $\cdot$ and an antipode η, which make it a ring object in the category of coalgebras). Equivalently, the following conditions hold:

- $(A,\Delta,\cdot)$ is a bialgebra.
- $(A,\Delta,\odot,\eta)$ is a Hopf algebra.
- If $\Delta(x)=\sum_i x_i'\otimes x_i''$, then

$$x\cdot(y\odot z)=\sum_i\big[(-1)^{\dim(x_i'')\dim(y)}(x_i'\cdot y)\odot(x_i''\cdot z)\big].$$

Explicitly, the structural maps are defined as follows. The obvious monomorphisms $i_{n,m}\colon \Sigma_n\times\Sigma_m\to\Sigma_{n+m}$ determine the maps $B(\Sigma_n)\times B(\Sigma_m)\to B(\Sigma_{m+n})$, homotopy equivalent to finite coverings. Passing to cohomology and taking their direct sum yields the coproduct Δ. Additionally, $i_{n,m}$ also determines a transfer homomorphism $\mathrm{tr}_{n,m}\colon H^*(\Sigma_n;\mathbb{Z}_p)\otimes H^*(\Sigma_m;\mathbb{Z}_p)\to H^*(\Sigma_{n+m};\mathbb{Z}_p)$. The product $\odot$ is given by $\bigoplus_{n,m\geq 0}\mathrm{tr}_{n,m}$. The product $\cdot$ is the usual cup product. Finally, η is induced by the additive inverse of the sphere spectrum by applying the extended power functor and then cohomology (see [8, pages 140–142]).

Published: 14 March 2017 DOI: 10.2140/agt.2017.17.957

Giusti, Salvatore and Sinha [3] have studied this structure for the ordinary cohomology with coefficients in $\mathbb{Z}_2$ and constructed the following:

- An explicit presentation, in terms of generators and relations, of this Hopf ring.
- An additive basis for the mod 2 cohomology of the symmetric groups in which the products $\cdot$ and $\odot$ and the coproduct Δ defined above can be computed by an explicit rule.

In this presentation, the relations involve only the $\odot$ product. For this reason, all the relations for the cup product in the cohomology of symmetric groups follow, in the mod 2 case, from Hopf ring distributivity. In addition, the authors calculated the restriction to the Dickson invariants and the action of the Steenrod algebra on these groups.

The purpose of this paper is to study the algebraic structure of the cohomology rings $H^*(\Sigma_n;\mathbb{Z}_p)$, where p is an odd prime, as well as the derivation of the mod p analogs of Giusti, Salvatore and Sinha's results. In particular, following their work, we will write a presentation of the Hopf ring $H^*\bigl(\coprod_{n\geq 0} B(\Sigma_n);\mathbb{Z}_p\bigr)$.

The generalizations to the mod p case required overcoming some complications in calculations, especially at odd degrees and when dealing with the more complicated coefficients arising in the description of the Steenrod algebra action. The main differences with the mod 2 case are the following:

- To obtain their Hopf ring presentation, Giusti, Salvatore and Sinha needed to relate the linear duals of $\cdot$, $\odot$ and Δ to the Dyer–Lashof operations. Then they used Nakaoka's description of $H_*(\Sigma_n;\mathbb{Z}_2)$ and dualized to obtain results in cohomology. In the mod p case the need to treat the Bockstein homomorphism separately yields a more complicated structure for the dual of the Dyer–Lashof algebra, which is not a polynomial algebra as in the mod 2 case. This forces us, in the presentation of the Hopf ring $\bigoplus_n H^*(\Sigma_n;\mathbb{Z}_p)$, to use more generators and some nontrivial relations involving the cup product.
- Consider in the cohomology groups $H^*(\Sigma_{2^n};\mathbb{Z}_2)$ the linear duals of the Dyer–Lashof operations with respect to the Nakaoka monomial basis in homology. It is known that the restriction homomorphism onto the ring of Dickson invariants $D_n=\mathbb{Z}_2[x_1,\dots,x_n]^{\mathrm{GL}_n(\mathbb{Z}_2)}$ maps the subalgebra generated by those dual elements surjectively onto D_n. In [3], the computation of the restriction of the Hopf ring generators to D_n relies on this fact. For mod p coefficients this is no longer true; hence, we needed to use a different technique to achieve this goal.

Apart from this introduction, this paper is organized into five sections. In Section 2 we describe a presentation, with generators and relations, of the mod p cohomology of the symmetric groups as a Hopf ring, obtaining the mod p analog of the main theorem in [3]. In Section 3 we obtain an additive basis with a rule for computing the products. In Section 4 we carry out the calculation of the restriction of our Hopf ring generators to the Dickson–Mùi invariant algebras. This will be crucial to the computation of the Steenrod algebra action, which is explained in Section 5. In Section 6 we use our Hopf ring presentation to describe the cup product structure for $H^*(\Sigma_{p^2};\mathbb{Z}_p)$.

Acknowledgments The author would like to thank Professor Frederick Cohen and Professor Dev Sinha for valuable conversations, Professor Mario Salvetti for his guidance, and the referee for helpful comments and suggestions.

2 Hopf ring structure

In this section, we describe $A=\bigoplus_{n\geq 0} H^*(\Sigma_n;\mathbb{Z}_p)$ as a Hopf ring.

Theorem 2.1 [8, Theorem 3.2] *A, with the coproduct Δ, the two products $\odot$ and $\cdot$ and the antipode η described in the introduction, is a Hopf ring.*

We need to describe the homology $H=\bigoplus_{n\geq 0} H_*(\Sigma_n;\mathbb{Z}_p)$, dual to A. In order to establish the notation, we recall the Dyer–Lashof operations, acting on the homology of the symmetric groups. A complete treatment of these operations can be found in Cohen, Lada and May [2], to which we refer for details and proofs. Given a group G, its classifying space is denoted by $B(G)$, its total space (ie a contractible topological space with a free G–action) by $E(G)$. Suppose that X is a space, and we are given a map $\theta\colon E(\Sigma_p)\times_{\Sigma_p} X^p\to X$, where Σ_p acts on X^p by permuting the p factors. Let π_p be a cyclic group of order p, considered a subgroup of Σ_p in the obvious way. Let W_* be the standard resolution of $\mathbb{Z}_p$ with $\mathbb{Z}_p[\pi_p]$–free modules. We can consider the composition map

$$\Theta\colon H_*(W_*\otimes_{\pi_p} C_*(X)^{\otimes p})\to H_*(E(\Sigma_p)\times_{\Sigma_p} X^p;\mathbb{Z}_p)\xrightarrow{\theta_*} H_*(X;\mathbb{Z}_p).$$

For every $i\geq 0$ and $c\in H_d(X;\mathbb{Z}_p)$, we define

$$Q_i(c)=\Theta(e_i\otimes_{\pi_o} c^{\otimes p})\in H_{i+pd}(X;\mathbb{Z}_p),$$

where e_i is the standard generator of W_i.

When θ arises from an action of an E_∞–operad $\mathcal{C}$ on X, Q_i is different from 0 on $H_q(X;\mathbb{Z}_p)$ only if i is congruent to $q(p-1)$ or to $q(p-1)-1$ modulo $2(p-1)$ and $Q_{k(p-1)-1}(x)=\beta Q_{k(p-1)}(x)$, where β is the homology Bockstein homomorphism. Hence, by making a change of indices and defining

$$Q^i=(-1)^{i+\frac{q(q-1)(p-1)}{4}}\left(\tfrac{1}{2}(p-1)!\right)^q Q_{(2i-q)(p-1)}\colon H_q(X;\mathbb{Z}_p)\to H_{q+2i(p-1)}(X;\mathbb{Z}_p),$$

we see that the Q^i and βQ^i generate all the nontrivial operations.

In the category of $\mathcal{C}$–spaces, these operations also satisfy the following properties (see Cohen, Lada and May [2, Theorem 1.1, page 5]):

- Let $*$ denote the product in the homology of a $\mathcal{C}$–space X. The Q_i are $\mathbb{Z}_p$–linear, natural with respect to maps of $\mathcal{C}$–spaces, $Q_0(x) = x^{*p}$ and $Q_i(1_{H_*(X;\mathbb{Z}_p)}) = 0$ for $i > 0$. Hence the operations Q_i can be regarded as homological derived p^{th} powers.
- The following Cartan formula holds for $x \in H_q(X;\mathbb{Z}_p)$ and $y \in H_{q'}(X;\mathbb{Z}_p)$:
$$Q^r(x * y) = \sum_{i+j=r} Q^i(x) * Q^j(x).$$
- The following Adem relations hold:
$$Q^r \circ Q^s = \sum_i (-1)^{r+i} \binom{(p-1)(i-s)-1}{pi-r} Q^{r+s-i} \circ Q^i \qquad \text{if } r > ps,$$
$$\begin{aligned} Q^r \circ \beta Q^s = &\sum_i (-1)^{r+i} \binom{(p-1)(i-s)}{pi-r} \beta Q^{r+s-i} \circ Q^i \\ &- \sum_i (-1)^{r+i} \binom{(p-1)(i-s)-1}{pi-r-1} Q^{r+s-i} \circ \beta Q^i \qquad \text{if } r \geq ps. \end{aligned}$$

By using the Adem relations, we can write an arbitrary composition of k operations $Q_{i_1} \circ \cdots \circ Q_{i_k}$ as a linear combination of sequences $Q_{j_1} \circ \cdots \circ Q_{j_k}$ with nondecreasing j_l. Furthermore, when applied to an even-dimensional class, we can also require that $j_l = \sum_{l<m\leq k} j_m(p-1)$ or $\sum_{l<m\leq k} j_m(p-1) - 1 \bmod 2(p-1)$. We call a sequence of nonnegative integers $J = (j_1, \dots, j_k)$ *admissible* if it satisfies the previous two conditions. We call it *strongly admissible* if, in addition, $j_1 \neq 0$. To simplify the notation, we write Q_J for $Q_{j_1} \circ \cdots \circ Q_{j_k}$. If we translate to the upper-indices notation, a composition $\beta^{\varepsilon_1} Q^{i_1} \circ \cdots \circ \beta^{\varepsilon_k} Q^{i_k}$ is admissible if and only if $pi_l - \varepsilon_l \geq i_{l-1}$ for all l, and is strongly admissible if and only if, in addition, $i_1 - \sum_{l=2}^{k} [2(p-1)i_l - \varepsilon_l] > 0$.

The Dyer–Lashof operations completely describe the structure of $\bigoplus_{n\geq 0} H_*(\Sigma_n;\mathbb{Z}_p)$.

Theorem 2.2 [2, Theorem 4.1, page 40] *Let $\iota \in H_0(\Sigma_1;\mathbb{Z}_p)$ be the homology class of any point in $B(\Sigma_1)$. Let $H = \bigoplus_{n\geq 0} H_*(\Sigma_n;\mathbb{Z}_p)$. Then H, under the product $*$ induced by the inclusions $\Sigma_n \times \Sigma_m \to \Sigma_{n+m}$, is the free graded commutative algebra generated (in appropriate dimensions) by $Q^I(\iota)$ for strongly admissible sequences I. Moreover, the action of the operations Q_i is determined by the properties listed above. In other words, it is isomorphic to the free allowable $\mathcal{R}$–algebra on ι, as defined in* [2, Section I.2].

As a consequence, the basis for this algebra as a $\mathbb{Z}_p$–vector space is given by products of such $Q^I(\iota)$. We call these basis elements *Nakaoka monomials*.

We now define some cohomology classes, which we will prove to be Hopf-ring generators for A.

Definition 2.3 Let the symbol $\vee$ denote the linear dual with respect to the Nakaoka monomial basis of H. Now we define some classes:

$$\begin{aligned}
\alpha_{j,k} &= \big[Q^{p^{k-1}-p^{k-1-j}} \circ \cdots \circ Q^{p^j-1} \circ \beta Q^{p^{j-1}} \circ \cdots \circ Q^p \circ Q^1(\iota)\big]^\vee, \\
\beta_{j,k,m} &= \big[\big(\beta Q^{p^{k-1}-p^{k-1-j}} \circ \cdots \circ Q^{p^{j+1}-p} \circ Q^{p^j-1} \circ \beta Q^{p^{j-1}} \circ \cdots \circ Q^1(\iota)\big)^{*m}\big]^\vee, \\
\gamma_{k,m} &= \big[\big(Q^{p^{k-1}} \circ \cdots \circ Q^p \circ Q^1(\iota)\big)^{*m}\big]^\vee.
\end{aligned}$$

Note that $\alpha_{j,k}$ is an odd-dimensional homogeneous element of A, while $\beta_{j,k,m}$ and $\gamma_{k,m}$ are even-dimensional. Note also that we can easily convert the sequences of operations that appear in the definition above into the lower-index notation. For example, $\gamma_{k,m}$ is the linear dual to

$$(-1)^k Q_{2(p-1)}^{\circ k}(\iota)^{*m}.$$

Similarly, the linear duals of $\alpha_{j,k}$ and $\beta_{j,k,m}$ can be written as nonzero multiples of the elements

$$Q_{p-1}^{\circ k-j} \circ Q_{2p-3} \circ Q_{2(p-1)}^{\circ j-1}(\iota) \quad \text{and} \quad \big[Q_{p-2} \circ Q_{p-1}^{\circ j-i-1} \circ Q_{2p-3} \circ Q_{2(p-1)}^{\circ i-1}(\iota)\big]^{*m}.$$

The structure of A with only the transfer product has a nice description that can be obtained with essentially the same proof adopted by Giusti, Salvatore and Sinha in [3], using the fact that the Bockstein homomorphism is a derivation with respect to the cross product.

Theorem 2.4 [3, Theorem 4.13] *For every sequence I of nonnegative integers, $\Delta_\odot(Q_I(\iota)) = Q_I(\iota) \otimes 1 + 1 \otimes Q_I(\iota)$. In other words, $(H, \Delta_\odot, *)$, the Hopf dual of $(A, \Delta, \odot)$, is freely generated under $*$ by elements that are primitive under $\Delta_\odot$. Hence $(A, \odot)$ is the tensor product*

$$\bigotimes_{\substack{\dim(Q^I)\text{ even} \\ k\in\mathbb{N}}} \frac{\mathbb{Z}_p[(Q^I(\iota)^{p^k})^\vee]}{([(Q^I(\iota)^{p^k})^\vee]^p)} \otimes \textstyle\bigwedge(\{Q^I(\iota)^\vee\}_{\dim(Q^I)\text{ odd}})$$

of a divided power polynomial algebra and an exterior algebra, where the Q^I indexing the tensor products above are the strongly admissible sequences of Dyer–Lashof operations $\beta^{\varepsilon_1} Q^{i_1} \circ \cdots \circ \beta^{\varepsilon_k} Q^{i_k}$. Moreover, the following relations hold:

(1) $\beta_{i,j,m} \odot \beta_{i,j,n} = \binom{n+m}{m} \beta_{i,j,n+m}$,

(2) $\gamma_{k,m} \odot \gamma_{k,n} = \binom{n+m}{m} \gamma_{k,n+m}$.

Thus, as far as the transfer product is concerned, we have relations totally analogous to those described by Sinha, Giusti and Salvatore in the mod 2 case.

However, if the cohomology is taken modulo an odd prime, there are also nontrivial relations for the cup product of the generators, due to the more complicated structure of the dual of the Dyer–Lashof algebra. We state them in the following lemma.

Lemma 2.5 *With the previous notation, the following equalities hold:*

(3) $\alpha_{i,k}\alpha_{j,k} = \gamma_{k,1}\beta_{i,j,p^{k-j}}$ *if* $i < j$.

(4) $\beta_{i,j,p^{k-j}}\alpha_{l,k} = (-1)^{\rho}\beta_{\rho(i),\rho(j),p^{k-\rho(j)}}\alpha_{\rho(l),k}$ *if* i,j,l *are pairwise distinct, where* ρ *is a permutation of the indexes* i,j,l *such that* $\rho(i) < \rho(j)$*, while* $\beta_{i,j,p^{k-j}}\alpha_{l,k} = 0$ *if* i,j,l *are not pairwise distinct.*

(5) $\beta_{i,j,m}\beta_{i',j',m'} = [(-1)^{\rho}]^m\beta_{\rho(i),\rho(j),mp^{j-\rho(j)}}\beta_{\rho(i'),\rho(j'),m'p^{j'-\rho(j')}}$ *if we suppose that* $mp^j = m'p^{j'}$ *and that* i,j,i',j' *are pairwise distinct, where* ρ *is a permutation of the indexes* i,j,i',j' *such that* $\rho(i) < \rho(j)$ *and* $\rho(i') < \rho(j')$*, while* $\beta_{i,j,m}\beta_{i',j',m'} = 0$ *otherwise.*

Proof This is an almost direct consequence of Cohen, Lada and May [2, Theorem 3.7, page 29]. Explicitly, let $\mathcal{R}$ be the Dyer–Lashof algebra as defined in [2]. Let $\mathcal{R}[k]$ be its k^{th} component, so that $\mathcal{R} = \bigoplus_{k\geq 0}\mathcal{R}[k]$. The evaluation of Dyer–Lashof operations on ι gives a morphism of coalgebras $\varphi_k\colon \mathcal{R}[k] \to H_*(\Sigma_{p^k};\mathbb{Z}_p)$, which dualizes to a map of algebras $\varphi_k^*\colon H^*(\Sigma_{p^k};\mathbb{Z}_p) \to \mathcal{R}[k]^*$.

Because of the theorem from [2] cited above, by definition these relations hold in the linear duals of $R[k]$. We are left to check them on the full set of Nakaoka monomials. When m is a power of p this follows immediately from the bialgebra structure of $(H, *, \Delta_\cdot)$, where $\Delta_\cdot$ is the coproduct dual to the cup product. □

Remark The relations described above can be recalled by the properties of the Bockstein homomorphism β in the duals, namely $\beta^2 = 0$ and the fact that β commutes with the product.

Example We provide a very simple example to show how the previous relations work. In $H^*(\Sigma_{p^2};\mathbb{Z}_p)$, relation (3) reduces to

$$\alpha_{2,1}\alpha_{2,2} = \gamma_{2,1}\beta_{1,2,1}.$$

Instead, since we do not have three distinct indices in $\{1,2\}$, the relations in form (4) can be written as $\beta_{1,2,1}\alpha_{1,2} = 0$ and $\beta_{1,2,1}\alpha_{2,2} = 0$. Similarly, (5) only assures that $\beta_{1,2,1}^2 = 0$.

For $H^*(\Sigma_{p^3};\mathbb{Z}_p)$ the relations which can be obtained by Lemma 2.5 are:

$$\alpha_{1,3}\alpha_{2,3}=\gamma_{3,1}\beta_{1,2,p},\alpha_{1,3}\alpha_{3,3}=\gamma_{3,1}\beta_{1,3,1} \quad\text{and}\quad \alpha_{2,3}\alpha_{3,3}=\gamma_{3,1}\beta_{2,3,1},$$
$$\beta_{1,2,p}\alpha_{1,3}=\beta_{1,2,p}\alpha_{2,3}=\beta_{1,3,1}\alpha_{1,3}=\beta_{1,3,1}\alpha_{3,3}=\beta_{2,3,1}\alpha_{2,3}=\beta_{2,3,1}\alpha_{3,3}=0,$$
$$\beta_{1,2,p}\alpha_{3,3}=-\beta_{1,3,1}\alpha_{2,3}=\beta_{2,3,1}\alpha_{1,3},$$
$$\beta_{1,2,p}^2=\beta_{1,2,p}\beta_{1,3,1}=\beta_{1,2,p}\beta_{2,3,1}=\beta_{1,3}^2=\beta_{1,3,1}\beta_{2,3,1}=\beta_{2,3}^2=0.$$

We now turn to the coproduct in A. Using the fact that this is dual to the product of H the following lemma follows from the definitions.

Lemma 2.6 *The following equalities hold:*

- $\Delta(\alpha_{j,k})=\alpha_{j,k}\otimes 1+1\otimes\alpha_{j,k}$
- $\Delta(\beta_{i,j,m})=\sum_{l=0}^{m}(\beta_{i,j,l}\otimes\beta_{i,j,m-l})$
- $\Delta(\gamma_{k,m})=\sum_{l=0}^{m}(\gamma_{k,l}\otimes\gamma_{k,m-l})$

At this point, we have all the ingredients to describe a presentation of A as a Hopf ring analogous to that of Giusti, Salvatore and Sinha [3, Theorem 1.2].

Theorem 2.7 *As a graded commutative Hopf ring, A is generated by the elements $\alpha_{j,k}$, $\beta_{i,j,m}$ and $\gamma_{k,m}$ as defined above (of suitable dimensions) under the relations* (1)–(5) *as explained in Theorem 2.4 and in Lemma 2.5, together with:*

(6) *The product $\cdot$ between two generators belonging to different components is 0.*

Moreover, the value of Δ on generators is determined by the preceding lemma and the antipode is the multiplication by $(-1)^n$ on the component corresponding to Σ_n.

Proof Let $B=(B;\odot_B,\cdot_B,\Delta_B)$ be the graded commutative Hopf ring generated by elements $\alpha_{j,k}$, $\beta_{i,j,m}$ and $\gamma_{k,m}$ (of suitable degree) with the specified relations. There is an obvious morphism $\psi\colon B\to A$.

One can see that, using (3)–(5), B is generated under $\odot$ only by elements that can be written in one of the two following forms:

$$\prod_j\gamma_{k_j,m_j}\cdot\prod_{a=1}^{r}\beta_{i_{2a-1},i_{2a},lp^{-i_{2a}}},$$
$$\prod_j\gamma_{k_j,m_j}\cdot\prod_{a=1}^{r}\beta_{i_{2a-1},i_{2a},p^{c-i_{2a}}}\beta_{i_{2a-1},i_{2a},p^{c-i_{2a}}}\alpha_{i_{2r+1},c}.$$

Here in the first case $1 \le i_1 < \cdots < i_{2r}$, $p^{i_{2r}} \le l$ and $p^{k_j} m_j = l$, while in the second case $1 \le i_1 < \cdots < i_{2r+1} \le c$ and $m_j p^{k_j} = p^c$. We will always suppose that the k_j are arranged in nonincreasing order. Borrowing the notation from [3], we will call these elements *gathered blocks* or simply *blocks*. By relations (3)–(6), these are all the elements that can be obtained from the generators by applying $\cdot_B$. We will call *Hopf monomials* the objects in the form $b_1 \odot_B \cdots \odot_B b_s$, where every b_j is a gathered block.

Then, using relations (1), (2) and (6) and Hopf distributivity, one can prove that for every gathered block b (of even dimension), we have $b^{\odot p} = 0$. Let us define an algebra

$$C = C_{\mathrm{even}} \otimes C_{\mathrm{odd}},$$

with

$$C_{\mathrm{even}} = \bigotimes_{\substack{d,k\ge 0 \\ b\in H^{2d}(\Sigma_{p^k};\mathbb{Z}_p)\text{ block}}} \frac{\mathbb{Z}_p[b]}{b^p},$$

$$C_{\mathrm{odd}} = \bigwedge\big(\{b : b \in H^{2d+1}(\Sigma_{p^k};\mathbb{Z}_p)\text{ block}, d,k \ge 0\}\big),$$

where $\bigwedge(X)$ indicates the exterior algebra generated by the elements of X (in appropriate degrees). By virtue of the above property, there is a morphism $\chi\colon C \to (B,\odot)$. Moreover, notice that, by Hopf distributivity and our coproduct formula for the generators, we have

$$\prod_j \gamma_{k_j,m_j} \cdot \prod_{a=1}^r \beta_{i_{2a-1},i_{2a},lp^{-i_{2a}}} \odot \prod_j \gamma_{k_j,m'_j} \cdot \prod_{a=1}^r \beta_{i_{2a-1},i_{2a},l'p^{-i_{2a}}} = \binom{l+l'}{l} \prod_j \gamma_{k_j,m_j+m'_j} \cdot \prod_{a=1}^r \beta_{i_{2a-1},i_{2a},(l+l')p^{-i_{2a}}}.$$

Hence, every gathered block can be written uniquely as a nonzero multiple of gathered blocks which lie in components indexed by a power of p. This proves that χ is surjective. Theorem 2.2 and Theorem 2.4 imply that the composition $\psi \circ \chi\colon C \to (A,\odot)$ is an isomorphism, proving the theorem. □

3 Presentation of product structures through an additive basis

In this section we will observe that the previous theorem allows us to obtain an additive basis of A as a $\mathbb{Z}_p$–vector space, similar to that in [3]. In order to describe this basis, we need a preliminary definition.

Definition 3.1 Let

$$b = \gamma_{k_1,m_1} \cdots \gamma_{k_s,m_s} \beta_{i_1,i_2,m'_1} \cdots \beta_{i_{2a-1},i_{2a},m'_a}$$

be an even-dimensional gathered block and $r = 2a$. We define the *profile* of b as the pair $(\underline{k}, \underline{e})$, where $\underline{k} = (k_1, \dots, k_s)$, and we suppose that, as usual, k_j is arranged in nonincreasing order, while $\underline{e} = (i_1, \dots, i_r)$.

For example, the profile of $\gamma_{2,2}^3 \gamma_{1,2p} \beta_{1,2,2}$ is determined by $\underline{k} = (2,2,2,1)$, $\underline{e} = (1,2)$.

The following result is an easy consequence of the proof of Theorem 2.7

Corollary 3.2 *Consider the set $\mathcal{M}$ of all Hopf monomials $\bigodot_{i=1}^r b_i$ with the property that the gathered blocks b_i of even dimension have pairwise distinct profiles, and the odd-dimensional blocks are pairwise distinct. This is a bigraded basis for A as a $\mathbb{Z}_p$–vector space.*

It must be noted that the pairing between this basis in cohomology and the Nakaoka monomials in homology is not completely understood. Indeed, the necessity to apply the Adem relations to describe the coproduct dual to $\cdot$ in terms of this basis complicates this pairing. For example, if $p = 3$ then $\gamma_{1,3}^4 = (Q^8 \circ Q^4(\iota))^\vee - (Q^9 \circ Q^3(\iota))^\vee$, because the formula for the coproduct $\Delta.$ of $Q^9 \circ Q^3(\iota)$ yields a summand $Q^3 \circ Q^0(\iota) \otimes Q^6 \circ Q^3(\iota)$, which can be written as $-Q^2 \circ Q^1(\iota) \otimes Q^6 \circ Q^3(\iota)$.

It is helpful to give a graphical description of this basis, similar to that obtained in [3]. First, we describe the generators as rectangles:

- $\gamma_{k,n}$ is a hollow rectangle of width np^k and height $2(1-p^{-k})$.
- $\beta_{j,k,n}$ is a solid rectangle of width np^k and height $2(1-p^{-j}-p^{-k})$.
- $\alpha_{j,k}$ is a solid rectangle of width p^k and height $2(1-p^{-j})-p^{-k}$.

In this way, the area of the rectangle is the homological dimension of the corresponding generator and its width accounts for the component in which the generator lies. Hollow rectangles represent generators whose linear duals in the Nakaoka basis lie in the subalgebra of H generated by sequences of Dyer–Lashof operations $Q^{i_1} \circ \cdots \circ Q^{i_k}(\iota)$ without the Bockstein. In terms of lower-indexed operations, these are written as multiples of $Q_{j_1} \circ \cdots \circ Q_{j_k}(\iota)$ where every j_l is even. These generators behave very similarly to the ones obtained in the mod 2 case. The other generators correspond to solid rectangles. We describe a gathered monomial, which is a product of $\gamma_{k,n}$, $\beta_{j,k,m}$ and possibly $\alpha_{j,k}$ all lying in the same component, as the column obtained by placing the corresponding rectangles on top of each other. A basis element, which is a transfer product of some gathered monomials $b_1, \dots, b_r$, is described by the diagram obtained by arranging the columns corresponding to $b_1, \dots, b_r$ next to each other horizontally. In order to conform to the notation used in [3], we will call these objects *skyline diagrams*. Some examples of skyline diagrams are depicted in Figure 1.

With the aid of this graphical description, we can elucidate the relations (3)–(5) of Lemma 2.5. First, observe that the rectangles of a column associated with a gathered block must satisfy some necessary condition. For example, there must be at most one odd-dimensional solid rectangle. This leads to the following definition.

Definition 3.3 A column made of rectangles with the same width stacked one onto the other is called *admissible* if it is associated with a gathered block.

As we will see at the end of this section, the cup product of two columns is essentially described as a new column obtained by stacking the original ones on top of each other. Hence relation (3) says that, if a column of width l contains two odd-dimensional solid rectangles, we can replace them with a hollow rectangle of height $2(1-l^{-1})$ and another solid rectangle to match the column's height. For the graphical representation of relation (3) see the first example in Figure 1.

Relations (4) and (5) determine how cup products of generators of the form $\beta_{i,j,m}$ and $\alpha_{j,k}$ behave when some indices are permuted. Their graphical interpretation is that if two columns are made only with solid rectangles of which at most one is odd-dimensional, they must be equal up to sign. Given such a column, there are two cases:

- If no admissible all-solid column of the same width and height exists, then it is 0.
- Otherwise it is equal, up to sign, to the (necessarily unique) admissible all-solid column with the same dimensions.

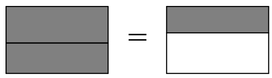
This gives a simple algorithm to write a nonadmissible column as a multiple of an admissible one, which is the graphical counterpart of what we observed in the proof of Theorem 2.7.

With this basis, one can describe the products. For example, in $H^*(\Sigma_{p^2}, \mathbb{Z}_p)$, let x be one of the elements $\gamma_{2,1}$, $\alpha_{1,2}$, $\alpha_{2,2}$ or $\beta_{1,2,1}$. We have $x(\gamma_{1,k} \odot 1_{p(p-k)}) = 0$ for $1 \le k \le p-1$. Indeed, $\Delta(x) = x \otimes 1 + 1 \otimes x$, hence, by Hopf ring distributivity,

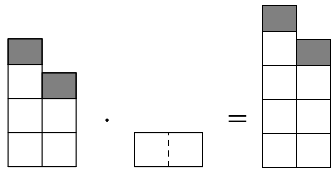
$$x(\gamma_{1,k} \odot 1_{p(p-k)}) = x\gamma_{1,k} \odot 1_{p(p-k)} + \gamma_{1,k} \odot x1_{p(p-k)} = 0 \odot 1_{p(p-k)} + \gamma_{1,k} \odot 0 = 0.$$

Similarly one can prove that $x(\gamma_{1,k-1} \odot \alpha_{1,1} \odot 1_{p(p-k)}) = 0$ for all $1 \le k \le p$.

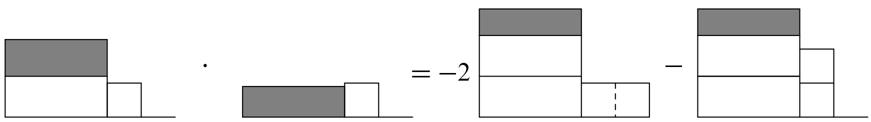
The general case can be derived in the exact same way as described by Giusti, Salvatore and Sinha [3, Section 6] and is indeed a straightforward consequence of the Hopf ring presentation. For this reason, we omit the proofs.



$$\alpha_{1,2}\alpha_{2,2} = \gamma_{2,1}\beta_{1,2,1}$$



$$(\gamma_{1,1}^{i}\alpha_{1,1} \odot \gamma_{1,1}^{j}\alpha_{1,1}) \cdot \gamma_{1,2} = \gamma_{1,1}^{i+1}\alpha_{1,1} \odot \gamma_{1,1}^{j+1}\alpha_{1,1}$$



$$(\gamma_{2,1}\alpha_{2,2} \odot \gamma_{1,1} \odot 1_p) \cdot (\alpha_{1,2} \odot \gamma_{1,1} \odot 1_p) = -2\gamma_{2,1}^2\beta_{1,2,1} \odot \gamma_{1,2} - \gamma_{2,1}^2\beta_{1,2,1} \odot \gamma_{1,1}^2 \odot 1_p$$

Figure 1: Examples of calculations using the graphical representation. The size of the rectangles is correct only for $p = 3$, but the same calculations with classes understood to be in different degrees are actually true for every p.

We begin with the transfer product, which can be described very easily. Given two Hopf monomials $x = b_1 \odot \cdots \odot b_r$ and $y = b'_1 \odot \cdots \odot b'_s$ in $\mathcal{M}$, the transfer product $x \odot y$ is again a Hopf monomial, but it may have gathered blocks with the same profile. However, two even-dimensional gathered blocks with the same profile can be merged together using the formula

$$(\gamma_{k_1,m_1} \cdots \gamma_{k_r,m_r}\beta_{i_1,i_2,n_1} \cdots \beta_{i_{2a-1},i_{2a},n_a}) \odot (\gamma_{k_1,m'_1} \cdots \beta_{i_{2a-1},i_{2a},n'_a}) = \binom{m_1+m'_1}{m_1}\gamma_{k_1,m_1+m'_1} \cdots \beta_{i_{2a-1},i_{2a},n_a+n'_a}.$$

In this way, we can write $x \odot y$ as a multiple of an element of $\mathcal{M}$. Graphically, the transfer product corresponds to placing two skyline diagrams next to each other, merging two columns if they have constituent blocks of the same height and multiplying by $\binom{n+m}{n}$, where n and m are the widths of the two columns.

In order to provide a formula for the coproduct, we need the following:

Definition 3.4 Let $b = \gamma_{l_1,m_1} \cdots \gamma_{l_r,m_r}\beta_{i_1,i_2,n_1} \cdots \beta_{i_{2s-1},i_{2s},n_s}$ be an even-dimensional gathered block. Let $c(b) = p^{l_1}m_1 = \cdots = p^{i_s}n_s$ be the integer corresponding to the component of A in which b lies. We say that a k–tuple $(b_1, \dots, b_k)$ of gathered blocks is a *partition* of b if every b_i has the same profile as b and $\sum_{i=1}^{k} c(b_i) = c(b)$. Some $c(b_i)$ are allowed to be 0, in which case b_i is understood to be 1_0. If b is an odd-dimensional block, a partition is defined in the same way, but we only allow b_i to be equal to 1_0 or to b itself. A partition with $k = 2$ is called a *splitting*.

The coproduct of elements of $\mathcal{M}$ can be calculated with the formula

$$\Delta(b_1 \odot \cdots \odot b_s) = \sum (b'_1 \odot \cdots \odot b'_s) \otimes (b''_1 \odot \cdots \odot b''_s).$$

Here the sum is taken over all the possible splittings $\{b'_i, b''_i\}$ of the constituent blocks b_i. In terms of our graphical representation, the coproduct can be described by dividing each rectangle corresponding to $\gamma_{k,n}$ or $\beta_{j,k,n}$ into n equal parts using vertical dashed lines. The coproduct of a skyline diagram is obtained by cutting each column along the dashed lines that cross it from top to bottom and partitioning them into two to create two other skyline diagrams. This must be done in every possible way and all the outcomes must be summed.

The formula for the cup product of two elements of $\mathcal{M}$ is

$$(b_1 \odot \cdots \odot b_r) \cdot (b'_1 \odot \cdots \odot b'_s) = \sum_{(\mathcal{P},\mathcal{P}')} (-1)^{\varepsilon_{\mathcal{P},\mathcal{P}'}} \bigodot_{j=1}^{s} \bigodot_{i=1}^{r} (b_{i,j} b'_{j,i});$$

the sum is over all pairs of sets $\mathcal{P} = \{(b_{i,1}, \ldots, b_{i,s})\}_{i=1}^{r}$ and $\mathcal{P}' = \{(b'_{i,1}, \ldots, b'_{i,r})\}_{i=1}^{s}$ such that $(b_{i,1}, \ldots, b_{i,s})$ is a partition of b_i and $(b'_{i,1}, \ldots, b'_{i,r})$ is a partition of b'_i. The number $\varepsilon_{\mathcal{P},\mathcal{P}'}$ is given by

$$\varepsilon_{\mathcal{P},\mathcal{P}'} = \sum_{\substack{1 \le i < j \le s \\ 1 \le k \le r}} \dim(b'_{i,k}) \dim(b_{k,j}) + \sum_{\substack{1 \le h < k \le r \\ 1 \le i \le s}} \dim(b'_{i,h}) \dim(b_{k,i}).$$

The coefficient $(-1)^{\varepsilon_{\mathcal{P},\mathcal{P}'}}$ is due to the skew-commutativity of the product. Since the cup product of two gathered blocks, when it is not zero, is equal up to sign to a gathered block, each summand in the previous formula is zero or can be written, up to sign, as a transfer product of gathered blocks. Thus, omitting all the zero summands and eventually merging together the transfer product of gathered blocks with the same profile as before, we can write the desired cup product as a linear combination of elements of $\mathcal{M}$. Note that one can restrict the sum to the $\mathcal{P}$ and $\mathcal{P}'$ such that $b_{i,j}$ and $b'_{j,i}$ lie in the same component, as the other terms are equal to 0.

Graphically, if we are given two skyline diagrams, in order to compute their cup product, we apply the following algorithm:

(1) Divide the rectangles with vertical dashed lines as explained before.

(2) Divide each diagram into columns using both the boundaries of the rectangles and the vertical dashed lines.

(3) Match each column of the first diagram with a column of the second one in all possible ways up to automorphisms, stack the matched columns one on top of

the other and place these newly constructed columns side by side to make new diagrams.

(4) These diagrams may contain a pair of columns with the same profiles. In this case we must use the transfer product formula to merge them. There may also be nonadmissible columns, that we must write as a multiple of admissible ones via the previously described algorithm.

For clarity, we compute two examples, represented graphically in Figure 1:

- Let $x = \gamma_{1,1}^i \alpha_{1,1} \odot \gamma_{1,1}^j \alpha_{1,1}$ and $y = \gamma_{1,2}$. Since x is made of two columns of width p, the only splitting of y which can yield a nontrivial summand in the formula for the cup product is $(\gamma_{1,1}, \gamma_{1,1})$. Hence

$$x \cdot y = \gamma_{1,1}^i \alpha_{1,1} \gamma_{1,1} \odot \gamma_{1,1}^j \alpha_{1,1} \gamma_{1,1} = \gamma_{1,1}^{i+1} \alpha_{1,1} \odot \gamma_{1,1}^{j+1} \alpha_{1,1}.$$

Working graphically, the rectangle corresponding to y should be divided with a dashed line into two equal parts ($\gamma_{1,1}$). Up to automorphisms, there is only one way to match the columns of x with them. Stacking matched columns is equivalent to adding one hollow rectangle of height $2(1-p^{-1})$ to each column of x.

- Let $x = \gamma_{2,1}\alpha_{2,2} \odot \gamma_{1,1} \odot 1_p$ and $y = \alpha_{1,2} \odot \gamma_{1,1} \odot 1_p$. The only two partitions of x that can yield a nontrivial summand in the cup product are $(\gamma_{2,1}\alpha_{2,2}, \gamma_{1,1}, 1_p)$ and $(\gamma_{2,1}\alpha_{2,2}, 1_p, \gamma_{1,1})$. Thus, by our formula,

$$\begin{aligned} x \cdot y &= \gamma_{2,1}\alpha_{2,2}\alpha_{1,2} \odot \gamma_{1,1}^2 \odot 1_p + \gamma_{2,1}\alpha_{2,2}\alpha_{1,2} \odot \gamma_{1,1} \odot \gamma_{1,1} \\ &= -\gamma_{2,1}^2 \beta_{1,2,1} - 2\gamma_{2,1}^2 \beta_{1,2,1} \odot \gamma_{1,2}. \end{aligned}$$

Graphically, there are two possible matches of the columns of x and y because we only need to ensure that the two largest columns match together. When we stack the two large columns one on top of the other we obtain a nonadmissible column that can be transformed as described in the figure. By stacking the remaining columns in the two possible ways, we obtain the two skyline diagrams on the left. In one diagram, two rectangles with the same height have been merged together, and a coefficient of 2 appears.

4 Restriction to modular invariants

Consider the regular representation of $V_n = \mathbb{Z}_p^n$ (the action of V_n on itself given by the usual $\mathbb{Z}_p$–vector space addition). This gives a map $V_n \to \Sigma_{p^n}$, as the set V_n has cardinality p^n. This section is devoted to the computation of the restriction map $\rho_n\colon H^*(\Sigma_{p^n}; \mathbb{Z}_p) \to H^*(V_n; \mathbb{Z}_p)$, induced by this immersion. This is related to the action of the Steenrod algebra on our Hopf ring generators, as we will see in the next section.

First, recall that $H^*(\mathbb{Z}_p;\mathbb{Z}_p)$ is isomorphic as a $\mathbb{Z}_p$–algebra to $\mathbb{Z}_p[y]\otimes\Lambda(x)$, where x and y are generators of the first and the second cohomology groups, respectively. We will also suppose that $\beta(x)=y$, where β is the cohomology Bockstein. Hence, by the Künneth formula,

$$H^*(V_n;\mathbb{Z}_p)=H^*(\mathbb{Z}_p;\mathbb{Z}_p)^{\otimes n}=\mathbb{Z}_p[y_1,\dots,y_n]\otimes\Lambda(x_1,\dots,x_n).$$

Recall that, by a result in Adem and Milgram [1, Corollary 1.8, page 182] the image of ρ_n is contained in the invariant subalgebra $\big[\mathbb{Z}_p[y_1,\dots,y_n]\otimes\Lambda(x_1,\dots,x_n)\big]^{\mathrm{GL}_n(\mathbb{Z}_p)}$, which was determined by Mùi in [7]. In particular, the product gives a $\mathbb{Z}_p$–vector space isomorphism of the previous algebra with $\mathbb{Z}_p[d_{0,n},\dots,d_{n-1,1}]\otimes M$, where M is the $\mathbb{Z}_p$–vector space with basis $\{R_{n,\underline{s}}:0\le s_1<\cdots<s_l<n\}$ indexed by subsets of $\{0,\dots,n-1\}$.

The objects $d_{k,n-k}$ and $R_{n,s_1,\dots,s_l}$ are defined by Mùi in terms of some determinants. More precisely, we can define

$$L_{n,k}=\det\big[y_i^{p^{j-\delta_{j\le k}}}\big]_{1\le i,j\le n},$$

and (letting $\widehat{\cdot}$ denote omission)

$$M_{n,s_1,\dots,s_l}=\frac{1}{l!}\det\begin{bmatrix} x_1 & \dots & x_1 & y_1 & \dots & \widehat{y_1^{p^{s_1}}} & \dots & \widehat{y_1^{p^{s_l}}} & \dots & y_1^{p^{n-1}}\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots\\ x_n & \dots & x_n & y_n & \dots & \widehat{y_n^{p^{s_1}}} & \dots & \widehat{y_n^{p^{s_l}}} & \dots & y_n^{p^{n-1}}\end{bmatrix}.$$

Additionally, we have the equalities

$$d_{k,n-k}=\frac{L_{n,k}}{L_{n,n}}\quad\text{and}\quad R_{n,s_1,\dots,s_l}=M_{n,s_1,\dots,s_l}L_{n,k}^{p-2}.$$

The dimensions of $d_{k,n-k}$ and $R_{n,s_1,\dots,s_l}$ are $2(p^n-p^k)$ and $l+2(p^n-1-\sum_{j=1}^{l}p^{s_j})$, respectively.

Thus, as an algebra, $\big[\mathbb{Z}_p[y_1,\dots,y_n]\otimes\Lambda(x_1,\dots,x_n)\big]^{\mathrm{GL}_n(\mathbb{Z}_p)}$ is generated by these objects $d_{k,n-k}$, which are the classical Dickson invariants, and $R_{n,s_1,\dots,s_l}$ and the product structure are determined by $d_{0,n}$ being a nonzero divisor and the relations

$$R_{n,s_1,\dots,s_l}^2=0\quad\text{and}\quad R_{n,s_1}\dots R_{n,s_l}=(-1)^{\frac{l(l-1)}{2}}R_{n,s_1,\dots,s_l}d_{0,n}^{l-1}.$$

Much is known about these classes. For example, the Steenrod algebra action, which we will need soon, has been determined by Hung and Minh:

Theorem 4.1 [4, page 42] *Let $0 \le r < p^n$. Let $r = \sum_{i=0}^{n-1} a_i p^i$ be the p–adic expansion of r. We agree that $a_{-1} = 0$ by convention. Then:*

- *$\mathcal{P}^r(d_{s,n-s})$ is 0 unless $a_i \ge a_{i-1}$ for all $0 \le i < n$, $i \ne s$ and $a_s + 1 \ge a_{s-1}$. In this case it is given by the formula*
$$\lambda_{r,n,s} \prod_{i=0}^{n-1} d_{i,n-i}^{a_i - a_{i-1} + \delta_{i,s}}, \quad \text{where } \delta_{i,s} = \begin{cases} 1 & \text{if } i = s, \\ 0 & \text{otherwise,} \end{cases}$$
and the following formula for $\lambda_{r,n,s}$ holds:
$$\lambda_{r,n,s} = \frac{(p-1)!}{(p-1-a_{n-1})! \prod_{1 \le i \le n-1, i \ne s} (a_i - a_{i-1})! (a_s + 1 - a_{s-1})!} (a_s + 1).$$
- *$\mathcal{P}^r(R_{n,s})$ is 0 unless $a_i \in \{0,1\}$, $a_i \ge a_{i-1}$ for all $i \ne s$ and $a_s = 0$. This condition is equivalent to $r = (p-1)^{-1}(p^n + p^s - p^{t_1} - p^{t_2})$ for some $t_1 \le s < t_2 \le n$. In this case,*
$$\mathcal{P}^r(R_{n,s}) = R_{n,t_1} d_{t_2,n-t_2} - R_{n,t_2} d_{t_1,n-t_1}.$$
Here, we use the convention that $R_{n,n} = 0$ and $d_{n,0} = 1$.
- *$\mathcal{P}^r(R_{n,s_1,s_2})$ is 0 unless $a_i \in \{0,1\}$, $a_i \ge a_{i-1}$ for $i \ne s_1, s_2$ and $a_{s_1} = a_{s_2} = 0$. This condition is equivalent to $r = (p-1)^{-1}(p^n + p^{s_1} + p^{s_2} - p^{t_1} - p^{t_2} - p^{t_3})$ for some $t_1 \le s_1 < t_2 \le s_2 < t_3 \le n$. In this case, the following formula holds:*
$$\mathcal{P}^r(R_{n,s_1,s_2}) = R_{n,t_1,t_2} d_{t_3,n-t_3} - R_{n,t_1,t_2} d_{t_2,n-t_2} + R_{n,t_2,t_3} d_{t_1,n-t_1}.$$
Again, we agree that $R_{n,s,n} = 0$ and $d_{0,n} = 1$.

Although we will not need this fact, it can be observed that, for $\mathcal{P}^r(d_{s,n-s})$, the coefficients $\lambda_{r,n,s}$ assume a nicer form if we express them as functions of the exponents $e_i = a_i + a_{i-1} + \delta_{i,s}$ that appear in the expression on the right. Explicitly,
$$p\lambda_{r,n,s} = \frac{p!}{\left(p - \sum_{i=0}^{n-1} e_i\right)! \prod_{i=0}^{n-1} e_i!} \sum_{i=0}^{s} e_i.$$
The first factor on the right is the number of choices of disjoint subsets of cardinalities $e_1, \dots, e_{n-1}$ in $\{1, \dots p\}$. After introducing the appropriate notions in Section 5, it will be obvious that $\sum_{i=0}^{n-1} e_i!$ counts the number of factors with an "effective scale" of at least $n - s$.

We now need a preliminary lemma.

Lemma 4.2 *Let $k \in \mathbb{N}$. We define J_k as the k–tuple $(2(p-1), \dots, 2(p-1))$. Let $J = (j_1, \dots, j_k)$ be a sequence of nonnegative integers (not necessarily admissible). If $Q_J = \sum_{J' \text{ admissible}} \lambda_{J,J'} Q_{J'}$ is the expansion of Q_J as a linear combination of admissible sequences of operations, then $\lambda_{J,J_k} = 0$ unless $J = J_k$.*

Proof We recall that $Q_{J_k} = \pm Q^{p^{k-1}} \circ \cdots \circ Q^p \circ Q^1$ and use upper indices, since Adem relations assume a much better form this way. Given a nonadmissible sequence in $\mathcal{R}$, its expansion in the admissible basis is obtained by iterative applications of the Adem relations. Hence, in order to prove the lemma, it is enough to check that for every $\beta^{\varepsilon} Q^r \beta^{\varepsilon'} Q^s$ with $r > ps - \varepsilon'$, when we apply the suitable Adem relation written as in Section 2, the expression we obtain does not contain a summand in the form $\lambda Q^{p^{l+1}} Q^{p^l}$ for some $\lambda \in \mathbb{Z}_p \setminus \{0\}$. This is obvious if $\varepsilon \neq 0$ or $\varepsilon' \neq 0$. If $\varepsilon = \varepsilon' = 0$, then $Q^r \circ Q^s = \sum_i c_i Q^{r+s-i} Q^i$ for some nonzero coefficients c_i only if $pi \geq r$. If there exists $\bar{\imath}$ such that $c_{\bar{\imath}} \neq 0$, $r + s - \bar{\imath} = p^{l+1}$ and $\bar{\imath} = p^l$, then $r + s = p^{l+1} + p^l$ and $r > ps$ implies $r > p^{l+1}$. This is contradictory because $p\bar{\imath} = p^{l+1} < r$. □

We will also need to know how the transfer product behaves with respect to the restriction maps.

Lemma 4.3 *If $x_1 \in H^*(\Sigma_r; \mathbb{Z}_p)$ and $x_2 \in H^*(\Sigma_{p^n - r}; \mathbb{Z}_p)$ are Hopf monomials that are different from 1, then $\rho_n^*(x_1 \odot x_2) = 0$.*

Proof Recall that the inclusion of V_n in Σ_{p^n} factors through the iterated wreath product $\mathbb{Z}_p \wr (\mathbb{Z}_p \wr \cdots \wr (\mathbb{Z}_p \wr \mathbb{Z}_p) \cdots)$ (see Adem and Milgram [1, page 185]). By construction, the image in $H_*(\Sigma_{p^n}; \mathbb{Z}_p)$ of the homology of this subgroup is given by Dyer–Lashof operations of length n. Hence, $H_*(V_n)$ maps onto the linear span of these classes, which are primitive with respect to $\Delta_{\odot}$. As a consequence, they must pair trivially with $x_1 \odot x_2$. □

We are now ready to describe the action of ρ_n on the generators, which is the analog of [3, Corollary 7.6] but is proved using a different technique.

Proposition 4.4 *The following formulas hold:*

$$\begin{aligned}
\rho_{j+k}(\alpha_{j,j+k}) &= (-1)^j R_{j+k,k}, \\
\rho_{j+k}(\beta_{i,j,p^k}) &= (-1)^{k+i} R_{j+k,k,k+j-i}, \\
\rho_{j+k}(\gamma_{j,p^k}) &= (-1)^j d_{k,j}.
\end{aligned}$$

Proof To prove the proposition, we will take advantage of the way Steenrod operations are constructed to inductively compute $\rho_j(\gamma_{j,1})$. Then we will use the naturality of the Steenrod action to work out the remaining cases. The core of this idea was originally used by Mann [5] to compute $\mathrm{im}(\rho_j)$. To a certain extent, we follow his reasoning, but we are also able to reconcile this approach with the Hopf ring structure and to describe in simpler terms the classes in the cohomology of Σ_{p^j} which restrict to $d_{l,j-l}$, $R_{j,l}$ and $R_{j,l,m}$.

First we will prove that $\rho_j(\gamma_{j,1}) = (-1)^j d_{0,j}$, or equivalently, by shifting to the lower-index notation, $\rho_j(Q_{J_j}(\iota)^\vee) = d_{0,j}$, where J_j is the j–tuple defined in Lemma 4.2.

Let us identify $H_*(V_j;\mathbb{Z}_p)$ with $H_*(\mathbb{Z}_p;\mathbb{Z}_p) \otimes H_*(V_{j-1};\mathbb{Z}_p)$. The homomorphism $(\rho_n)_*\colon H_*(V_n;\mathbb{Z}_p) \to H_*(\Sigma_{p^n};\mathbb{Z}_p)$ satisfies, for every $x \in H_s(V_{n-1};\mathbb{Z}_p)$ and for every $r \geq 0$, the formula

$$\begin{aligned}(\rho_n)_*(e_r \otimes x) = \nu(s) \textstyle\sum_k (-1)^k Q_{r+2k-s} \circ \mathcal{P}^k_*(x)& \\ - \delta(r)\nu(s-1) \textstyle\sum_k (-1)^k Q_{r+p+(2pk-s)(p-1)} \circ \mathcal{P}^k_* \beta(x)&.\end{aligned}$$

Here $\mathcal{P}^k_*$ is the linear dual to the k^{th} Steenrod power $\mathcal{P}^k$,

$$\nu(2j+\varepsilon) = (-1)^j \big(\tfrac{1}{2}(p-1)\big)!^{\varepsilon} \quad \text{and} \quad \delta(2j+\varepsilon) = \varepsilon \quad \text{if } \varepsilon \in \{0,1\}.$$

This is stated in May [6, Proposition 9.1, page 205], where it is used as a preliminary step for the proof of Nishida relations, and is essentially the dualization of the original construction of $\mathcal{P}^k$ made by Steenrod.

Note that, by Lemma 4.2, all the summands in the previous formula pair trivially with $Q_{J_j}(\iota)^\vee$, except possibly those in the form $Q_{r+2k-s} \circ \mathcal{P}^k_*(x)$ with $r+2k-s = 2(p-1)$ and $s - 2k(p-1) = 2(p^{j-1}-1)$. This means that $r = (p^{j-1}-l)(p-1)$ and $s = 2(p^{j-1}-1) + 2k(p-1)$. Hence, dually, we have

$$\rho_j(Q_{J_j}(\iota)^\vee) = \sum_{k=0}^{p^{j-1}-1} (-1)^k \mathcal{P}^k \rho_{j-1}(Q^\vee_{J_{j-1}}) y_j^{(p-1)(p^{j-1}-1)}.$$

This implies by induction on j that the right member is equal to $d_{0,j}$. Explicitly, for $j=1$ the statement is trivial. For $j>1$, by the induction hypothesis, $\rho_j(Q_{J_j}(\iota)^\vee)$ is a $\mathrm{GL}_j(\mathbb{Z}_p)$–invariant polynomial in $H^*(V_{j-1};\mathbb{Z}_p)[y_j]$ whose leading coefficient is $d^p_{0,j-1}$. This must be $d_{0,j}$.

The calculations of $\rho_n(x)$ for γ_{n-k,p^k} with $k>0$, $\alpha_{j,n}$ and $\beta_{i,j,p^{n-j}}$ follow directly from the naturality of the Steenrod powers with respect to the restrictions ρ_n and from the formulas in Cohen, Lada and May [2, Theorem 3.9], which determine the Steenrod action on the dual of $\mathcal{R}[n]$. These formulas are true in $H^*(\Sigma_{p^n};\mathbb{Z}_p)$ only up to summands containing nontrivial transfer products, but they still determine $\rho_n \circ \mathcal{P}^r$ on Hopf ring generators because of Lemma 4.3. Comparison with the Steenrod powers of Mùi invariants as determined by Hung and Minh [4, Theorems B and C] yields the result. □

As a corollary, we obtain a known fact about the image of ρ_n.

Corollary 4.5 [5, Theorem A] *The image of ρ_n in $H^*(V_n;\mathbb{Z}_p)^{\mathrm{GL}_n(\mathbb{Z}_p)}$ is the subalgebra generated by $d_{j,n-j}$, $R_{n,j}$ and $R_{n,i,j}$. This can be described as*

$$\bigoplus_{l=0}^{n} \bigoplus_{0\leq s_1<\cdots<s_l<n} \mathbb{Z}_p[d_{0,n},\ldots,d_{n-1,1}]d_{0,n}^{\lceil l/2\rceil,0}R_{n,\underline{s}}.$$

Hence, in general, ρ_k is not surjective.

5 Steenrod algebra action

This section is devoted to the computation of the action of the Steenrod powers on the Hopf ring A. We will achieve this by combining the calculations of Proposition 4.4 with the ideas used by Giusti, Salvatore and Sinha [3, Section 8] for the mod 2 cohomology.

First note that, as in the mod 2 case, the products $\odot$ and $\cdot$, the coproduct Δ and the antipode are induced from stable maps; hence, there are Cartan formulas for all these. This means that A is a Hopf ring over the mod p Steenrod algebra $\mathcal{A}(p)$, so it is sufficient to determine the action of $\beta^\varepsilon\mathcal{P}^l$ ($l\geq 0$ and $\varepsilon\in\{0,1\}$) on the Hopf ring generators $\alpha_{j,j+k}$, β_{i,j,p^k} and γ_{j,p^k}.

In order to describe the Steenrod algebra action on A in terms of our additive basis, we introduce some notation.

Definition 5.1

- The height (ht) of a gathered block b is the number of generators that must be cup-multiplied to obtain b. The height of a Hopf monomial is the largest of the heights of its constituent blocks.
- We define the effective scale (effsc) of a gathered block, which we assume in the form $b=\gamma_{l_1,n_1}\cdots\gamma_{l_r,n_r}\beta_{i_1,i_2,m_1}\cdots\beta_{i_{2s-1},i_{2s},m_s}\alpha_{j,k}^{\varepsilon}$ ($\varepsilon=0,1$) as the largest of the integers $l_1,\ldots,l_r,i_{2s}$ if $\varepsilon=0$, or as k if $\varepsilon=1$. In other words, for $b\in H^*(\Sigma_{p^n};\mathbb{Z}_p)$, effsc$(x)$ is the minimum $k\geq 0$ such that the restriction of x to $\Sigma_{p^k}^{p^{n-k}}$ is not zero. The effective scale of a Hopf monomial is the minimum of the effective scales of its constituent blocks.
- A Hopf monomial is *full-width* if none of its constituent blocks is 1_{Σ_n}.
- We say that a gathered block is of *type A* if all the Hopf ring generators that must be cup-multiplied to obtain it are in the form $\gamma_{l,n}$, except one that is in the form $\alpha_{j,k}$. For example, $\gamma_{1,p^2}^3\alpha_{1,3}$ is of type A. More generally, a Hopf monomial is of type A if all its constituent blocks are of type A.

- We say that a gathered block is of *type B* if all the Hopf ring generators that appear in it are in the form $\gamma_{l,n}$, except one in the form $\beta_{i,j,m}$. For example, $\gamma_{3,1}^5\gamma_{2,p}^2\beta_{1,2,3}$ is of type B. More generally, a Hopf monomial is of type B if all its constituent blocks are of type B.
- We say that a Hopf monomial is of *type C* if it is obtained by applying $\cdot$ and $\odot$ only to elements in the form $\gamma_{l,n}$.

These definitions can be understood graphically. Given a skyline diagram:

- Its height is the maximal number of rectangles stacked one on top of the other that appear in the diagram.
- Its effective scale is the width of the thinnest column among those delineated by the original boundaries and the vertical dashed lines of full height.
- It is full-width if there are no columns of height 0.
- It is of type A if its columns contain exactly one solid rectangle and it is odd-dimensional. It is of type B if its columns contain exactly one solid rectangle and it is even-dimensional, while it is of type C if it is made only of hollow rectangles.

The definitions of height, effective scale and full-width monomial are borrowed from [3] and make sense also for the mod 2 cohomology.

We will also need the following result from Adem and Milgram's book:

Lemma 5.2 [1, Corollary 1.4, page 180] *Let ρ_n and τ_n be the natural restrictions from the cohomology of Σ_{p^n} to $H^*(V_n;\mathbb{Z}_p)$ and $H^*(\Sigma_{p^{n-1}}^p;\mathbb{Z}_p)\cong H^*(\Sigma_{p^{n-1}};\mathbb{Z}_p)^{\otimes p}$, respectively. The following homomorphism, whose components are ρ_n and τ_n, is injective:*

$$H^*(\Sigma_{p^n};\mathbb{Z}_p)\to H^*(V_n;\mathbb{Z}_p)\oplus H^*(\Sigma_{p^{n-1}}^p;\mathbb{Z}_p).$$

This lemma is derived in [1] by proving that elementary abelian subgroups detect the cohomology of Σ_{p^n}, and that all these groups are conjugate to subgroups of $\Sigma_{p^{n-1}}^p$ or to V_n. However, the same result can also be obtained as a consequence of our description. Indeed, the restriction of ρ_n to the linear span of Hopf monomials of height n in $H^*(\Sigma_{p^n};\mathbb{Z}_p)$ is injective by Proposition 4.4. These monomials map trivially to $H^*(\Sigma_{p^{n-1}}^p;\mathbb{Z}_p)$. Recall that a basis for $H^*(\Sigma_{p^{n-1}};\mathbb{Z}_p)^{\otimes p}$ is given by $x_1\otimes\cdots\otimes x_p$, where x_i are Hopf monomials and that τ_n can be identified with the iterated coproduct. Let $x_1\otimes\cdots\otimes x_p$ be such a basis element. By our coproduct formulas, there exists exactly one Hopf monomial $x\in H^*(\Sigma_{p^n};\mathbb{Z}_p)$ of height less than n such that $x_1 \otimes \cdots \otimes x_p$ appears with a nonzero coefficient in the expansion of $\tau_n(x)$. Explicitly, x is the transfer product of the gathered blocks $b \in H^*(\Sigma_m; \mathbb{Z}_p)$ such that, for every $1 \le i \le p$, there is $b_i \in H^*(\Sigma_{m_i}; \mathbb{Z}_p)$ that is a constituent block of x_i with the same profile of b and $\sum_i m_i = m$ (some m_i are allowed to be 0). This implies the lemma.

With these tools, we can obtain formulas for the Steenrod action on A. The idea is to use Theorem 4.1 and Lemma 5.2 and check, case by case, that the two expressions we wish to be equal assume the same value if restricted to $H^*(V_n; \mathbb{Z}_p)$ and $H^*(\Sigma_{p^{n-1}}^p; \mathbb{Z}_p)$.

Lemma 5.3 *$\mathcal{P}^r(\gamma_{n-k,p^k})$ can be expressed as a linear combination of full-width Hopf monomials of Type C with a height of at most p and an effective scale of at least $n-k$.*

Following the notation used by Giusti, Salvatore and Sinha [3], we will call these monomials the *outgrowth monomials* of γ_{n-k,p^k}. We denote the set of such monomials by $\mathrm{Outgrowth}(\gamma_{n-k,p^k})$.

Proof of Lemma 5.3 The proof will follow that of [3, Theorem 8.3]. We proceed by induction on k. First, assume $k = 0$. By Theorem 4.1 and Lemma 5.2, $\mathcal{P}^r(\gamma_{n,1})$ must restrict to

$$\begin{cases} 0 & \text{on } H^*(\Sigma_{p^{n-1}}^p; \mathbb{Z}_p), \\ (-1)^n \lambda_{r,n,0} \prod_{i=0}^{n-1} d_{i,n-i}^{a_i - a_{i-1} + \delta_{i,0}} & \text{on } H^*(V_n; \mathbb{Z}_p). \end{cases}$$

Hence, it must be a multiple of $\prod_{i=0}^{n-1} \gamma_{n-i,p^i}^{a_i - a_{i-1} + \delta_{i,0}}$. This is the only full-width Hopf monomial of Type C, of degree $2(p^n - 1) + 2r(p-1)$ with a height of at most p and an effective scale of at least n.

For $k > 0$, since $\tau_n(\gamma_{n-k,p^k}) = \gamma_{n-k,p^{k-1}}^{\otimes p}$, using the external Cartan formula, we have

$$\tau_n(\mathcal{P}^r(\gamma_{n-k,p^k})) = \sum_{r_1 + \cdots + r_p = r} \mathcal{P}^{r_1}(\gamma_{n-k,p^{k-1}}) \otimes \cdots \otimes \mathcal{P}^{r_p}(\gamma_{n-k,p^{k-1}}).$$

By induction, this is a linear combination of elements $x_1 \otimes \cdots \otimes x_p$, where each x_i is an outgrowth monomial of $\gamma_{n-k,p^{k-1}}$. Recall that, for each $x_1 \otimes \cdots \otimes x_p$ in this form, there exists a unique Hopf monomial $x \in H^*(\Sigma_{p^n}; \mathbb{Z}_p)$ with $\mathrm{effsc}(x) < n$ whose restriction to $H^*(\Sigma_{p^{n-1}}^p; \mathbb{Z}_p)$ has a nonzero multiple of $x_1 \otimes \cdots \otimes x_p$ as a summand. We have described x explicitly above. Moreover, we have $\mathrm{effsc}(x) \le n-1$ and $x \in \mathrm{Outgrowth}(\gamma_{n-k,p^k})$ since height and the fact of being full-width are preserved by the coproduct, and the minimum of the effective scales of x_i must be equal to $\mathrm{effsc}(x)$. A Hopf monomial $x \notin \mathrm{Outgrowth}(\gamma_{n-k,p^k})$ with an effective scale less than n cannot appear in the expression of $\mathcal{P}^r(\gamma_{n-k,p^{k-1}})$, because this would yield summands in

$\tau_n(\mathcal{P}^r(\gamma_{n-k,p^k}))$ that are not tensor products of elements in $\mathrm{Outgrowth}(\gamma_{n-k,p^{k-1}})$. If a Hopf monomial with an effective scale equal to n appear, this must, once again, be an outgrowth monomial of γ_{n-k,p^k}. Otherwise, by applying the restriction to $H^*(V_n;\mathbb{Z}_p)$, we would contradict Theorem 4.1. $\square$

Thus,

$$\mathcal{P}^r(\gamma_{n-k,p^k}) = \sum_{\substack{x\in \mathrm{Outgrowth}(\gamma_{n-k,p^k})\\ \deg(x)=2(p^n-p^k)+2r(p-1)}} c_{n,k,x}x.$$

We are left to determine the coefficients $c_{n,k,x}$. Note that, by restricting to $H^*(V_n;\mathbb{Z}_p)$, using Proposition 4.4 and comparing with the formula in Theorem 4.1, we can directly determine $c_{n,k,x}$ when

$$x = \prod_{i=0}^{n-1} \gamma_{n-i,p^i}^{a_i-a_{i-1}+\delta_{i,k}}$$

is the unique term made by a single gathered block. Explicitly,

$$c_{n,k,\prod_{i=0}^{n-1}\gamma_{n-i,p^i}^{a_i-a_{i-1}+\delta_{i,k}}} = (-1)^{n-k+\sum_{i=0}^{n-1}(a_i-a_{i-1}+\delta_{i,s})(n-i)}\lambda_{r,n,k},$$

where $r=\sum_i a_i p^i$.

In general, let $x=b_1\odot\cdots\odot b_l\in H^*(\Sigma_{p^n};\mathbb{Z}_p)$ be the transfer product of l gathered blocks with pairwise distinct profiles. We assume that $b_i\in H^*(\Sigma_{p^{n_i}m_i};\mathbb{Z}_p)$ with $\mathrm{effsc}(b_i)=n_i$. As a notational convention, given a block b, we denote the (necessarily unique) block which has the same profile and lies in $H^*(\Sigma_{p^{\mathrm{effsc}(b)}};\mathbb{Z}_p)$ by b'. The restriction of x to the cohomology of $\prod_{i=1}^l \Sigma_{p^{n_i}}^{m_i}$ is the symmetrization of the class $b_1'^{\otimes m_1}\otimes\cdots\otimes b_l'^{\otimes m_l}$. By observing that

$$\gamma_{n-k,p^k}|_{\prod_i \Sigma_{p^{n_i}}^{m_i}} = \bigotimes\nolimits_i \gamma_{n-k,p^{k-n+n_i}}^{m_i},$$

we obtain, by application of the naturality of the Steenrod operations and of the external Cartan formula for $\mathcal{P}^r$ as above, that $c_{n,k,x}=\prod_{i=1}^l c_{n-n_i,n_i-n+k,b_i'}$. This reduces the computation of $c_{n,k,x}$ to the previous particular case.

We summarize our calculations in the following proposition.

Proposition 5.4 *Let $0\le k<n$. Let $b=\prod_{i=0}^{n-1}\gamma_{n-i,p^i}^{e_i}\in\mathrm{Outgrowth}(\gamma_{n-k,p^k})$ be the gathered block with an effective scale of n. We define*

$$\begin{aligned} c_{n,k,b} &= (-1)^{n-k+\sum_i e_i(n-i)}\lambda_{(p-1)^{-1}[\sum_i 2(p^n-p^i)-2(p^n-p^k)],n,k} \\ &= (-1)^{n-k+\sum_i e_i(n-i)}\frac{(p-1)!}{(p-\mathrm{ht}(b))!\prod_{i=1}^{n-1}e_i!}\sum_{i=1}^{k} e_i. \end{aligned}$$

Let $x \in \operatorname{Outgrowth}(\gamma_{n-k,p^k})$ *be a general outgrowth monomial. Then* $x = b_1 \odot \cdots \odot b_s$, *with* $b_i \in H^*(\Sigma_{l_i}; \mathbb{Z}_p)$ *that are gathered blocks with pairwise distinct profiles. We define*

$$c_{n,k,x} = \prod_{i=1}^{l} c^{l_i}_{\operatorname{effsc}(b_i),k-n+\operatorname{effsc}(b_i),b'_i}.$$

Then

$$\mathcal{P}^r(\gamma_{n-k,p^k}) = \sum_{\substack{x \in \operatorname{Outgrowth}(\gamma_{n-k,p^k}) \\ \deg(x)=2(p^n-p^k+r(p-1))}} c_{n,k,x}x.$$

Remark Note that, with our proof, we do not need to check inductively that the coefficients agree when we restrict to $H^*(\Sigma_{p^{n-1}}; \mathbb{Z}_p)$ because this is automatically satisfied. However, this can be proved "manually" by observing that $\lambda_{r,n,s} = \lambda_{rp^k,n+k,s+k}$. Because of this, for a block $b = \prod_{i=0}^{n-1} \gamma_{n-i,i}^{a_i-a_{i-1}+\delta_{i,k}} \in H^*(\Sigma_{p^n}; \mathbb{Z}_p)$, not necessarily with $\operatorname{effsc}(b) = n$, we have

$$c_{n,k,b} = (-1)^{n-k+\sum_i (a_i-a_{i-1}+\delta_{i,k})(n-i)} \lambda_{\sum_i a_i p^i,n,k},$$

agreeing with Theorem 4.1. More generally, given a gathered block

$$b = \prod\nolimits_i \gamma_{n-i,mp^i}^{a_i-a_{i-1}+\delta_{i,k}}$$

in $H^*(\Sigma_{p^n m})$ with $\operatorname{effsc}(b) = n$ and given two partitions $(p^{k_1}, \dots, p^{k_1})$, $(p^{k'_1}, \dots p^{k'_{l'}})$ of m with powers of p, the following equality holds in $\mathbb{Z}_p$:

$$\prod_{j=1}^{l} \lambda_{\sum_i a_i p^{i+k_j},n+k_j,k_j} = \prod_{j=1}^{l'} \lambda_{\sum_i a_i p^{i+k'_j},n+k'_j,k'_j}.$$

This implies that the desired coefficients agree in the restriction to $H^*(\Sigma^p_{p^{n-1}}; \mathbb{Z}_p)$.

The computation of $\mathcal{P}^r(\alpha_{j,k})$ and $\mathcal{P}^r(\beta_{i,j,p^k})$ can be done in the same way. Before stating the final results we define the analogous notion of outgrowth monomials for $\alpha_{i,j}$ and β_{i,j,p^k} as the full-width monomials of height one or two with an effective scale of at least j, of types A and B respectively. We will denote the set of such monomials by $\operatorname{Outgrowth}(\alpha_{i,j})$ and $\operatorname{Outgrowth}(\beta_{i,j,p^k})$, respectively.

Proposition 5.5 *Let* $1 \le j \le n$. *For* $x = \gamma_{n-u,p^u}\alpha_{n-t,n} \in \operatorname{Outgrowth}(\alpha_{j,n})$, *we define* $c'_{n,j,x} = (-1)^{j+t+u}(\delta_{t \le n-j} - \delta_{u \le n-j})$. *Here, we allow* $u = n$ *with the convention that* $\gamma_{0,p^n} = 1$. *Then*

$$\mathcal{P}^r(\alpha_{j,n}) = \sum_{\substack{x \in \operatorname{Outgrowth}(\alpha_{j,n}) \\ \deg(x)=2((p-1)r+p^n-p^{n-j})-1}} c'_{n,j,x}x.$$

Let $1 \le i < j \le n$ and let $k = n - j$. Given a gathered block $b = \gamma_{n-v,v}\beta_{n-u,n-t,p^t}$ in $\mathrm{Outgrowth}(\beta_{i,j,p^k})$*, define*

$$c''_{n,i,j,b} = (-1)^{i+k+t+u+v}(\delta_{v>k+j-i} - \delta_{u>k+j-i})\delta_{t\le k+j-i}(\delta_{t\le k} - \delta_{v\le k})\delta_{u>k}.$$

For a general outgrowth monomial $x = b_1 \odot \cdots \odot b_l$ with $b_s \in H^*(\Sigma_{m_s};\mathbb{Z}_p)$ and $\mathrm{effsc}(b_s) = n_s$ *for all $1 \le s \le l$, we define $c''_{n,i,j,x} = \prod_{s=1}^{l}(c''_{n_s,i,j,b_s})^{m_s}$. Then*

$$\mathcal{P}^r(\beta_{i,j,p^k}) = \sum_{\substack{x\in\mathrm{Outgrowth}(\beta_{i,j,p^k})\\ \deg(x)=2((p-1)r+p^n-p^{n-j}-p^{n-i})}} c''_{n,i,j,x}\,x.$$

In this result, the coefficients $c'_{n,j,x}$ and $c''_{n,i,j,x}$ are always equal to -1, 0 or 1.

We close this section with a proposition that describes the action of the Bockstein homomorphism β on Hopf ring generators. This clearly determines β on the whole Hopf ring and follows easily from [6, Theorem 3.9, page 33].

Proposition 5.6 *The following formulas hold:*

- $\beta(\alpha_{j,k}) = \gamma_{k,1}$ *if $j = k$ and is equal to 0 otherwise.*
- $\beta(\beta_{i,j,p^k}) = -\alpha_{i,j}$ *if $k = 0$ and is equal to 0 otherwise.*
- $\beta(\gamma_{j,p^k}) = 0$.

6 An example

As an example we now extract the cup product structure from our Hopf ring presentation in the case of $H^*(\Sigma_{p^2};\mathbb{Z}_p)$. An equivalent description has been given by Mùi [7] by analyzing the restriction to elementary p–subgroups.

First note that, by our results, an additive basis for $H^*(\Sigma_{p^2};\mathbb{Z}_p)$ is given by

$$\mathcal{B} = \Big\{\gamma_{2,1}^a\gamma_{1,p}^b\alpha_{1,2}^{\varepsilon_1}\alpha_{2,2}^{\varepsilon_2}\beta_{1,2,1}^{\varepsilon_3} : a, b, \varepsilon_i \ge 0,\ \sum_{i=1}^{3}\varepsilon_i \le 1\Big\} \\ \cup \Big\{\bigodot_{i=1}^{p}\gamma_{1,1}^{t_i}\alpha_{1,1}^{\varepsilon_i} : t_i \ge 0,\ \varepsilon_i \in \{0,1\} \text{ not all factors equal}\Big\}.$$

The elements of the last set are to be considered up to permutations of the p factors. More simply, we can order the basis for $H^*(\Sigma_p;\mathbb{Z}_p)$ with the rule

$$\gamma_{1,1}^a\alpha_{1,1}^{\varepsilon} > \gamma_{1,1}^b\alpha_{1,1}^{\delta} \iff (a > b) \vee (a = b \wedge \varepsilon > \delta),$$

where we agree that, in the last set, $\gamma_{1,1}^{t_1}\alpha_{1,1}^{\varepsilon_1} \geq \cdots \geq \gamma_{1,1}^{t_p}\alpha_{1,1}^{\varepsilon_p}$ in the given order. It will be useful to order the set of the basis elements in this form with the product order.

We now write the generators and relations in $H^*(\Sigma_{p^2};\mathbb{Z}_p)$ as a ring. We define:

- $x_1 = \gamma_{2,1}$
- $x_2 = \alpha_{1,2}$
- $x_3 = \alpha_{2,2}$
- $x_4 = \beta_{1,2,1}$
- $y_i = \gamma_{1,i} \odot 1_{p^2-pi}$ for $1 \leq i \leq p-1$
- $y_p = \gamma_{1,p}$
- $z_i = \gamma_{1,i-1} \odot \alpha_{1,1} \odot 1_{p^2-pi}$ for $1 \leq i \leq p$

There are equalities $x_2x_3 = x_1x_4$, $x_2x_4 = 0$, $x_3x_4 = 0$ and $x_4^2 = 0$ coming directly from relations (3)–(5) in our Hopf ring presentation. Moreover, we have seen as an example in Section 2 that, for every $1 \leq i \leq 4$, we have $x_i y_j = 0$ for $1 \leq j \leq p-1$ and $x_i z_j = 0$ for $1 \leq j \leq p$. These will be our cup product generators and relations.

Proposition 6.1 *Consider the unital ring*

$$S = \frac{U(x_1, x_2, x_3, x_4, y_1, y_2, y_3, z_1, z_2, z_3)}{I},$$

where $U(X)$ is the free associative skew-commutative algebra generated by the elements of X (in appropriate dimensions) and let $I \subseteq S$ be the bilateral ideal generated by the relations above. There is an isomorphism $\varphi\colon S \to H^*(\Sigma_{p^2};\mathbb{Z}_p)$.

Proof There is a φ defined in the obvious way because we have checked that these relations hold in this cohomology ring. We now prove that φ is bijective. First, let $w = \bigodot_{j=1}^{p} \gamma_{1,1}^{t_j}\alpha_{1,1}^{\varepsilon_j}$, with the factors $\gamma_{1,1}^{t_j}\alpha_{1,1}^{\varepsilon_j}$ ordered from largest to smallest with respect to the product ordering. Consider the set $\mathcal{P}$ of elements $\{(b_{k,1},\dots,b_{k,p})\}_{k=1}^{2}$ where $(b_{1,1},\dots b_{1,p})$ is a partition of $\gamma_{1,i}$ and $(b_{2,1},\dots,b_{2,p})$ is a partition of $1_{p(p-i)}$. Moreover, let $\mathcal{P}'$ be the set of elements $\{(b'_{j,1},b'_{j,2})\}_{j=1}^{p}$ where $(b'_{j,1},b'_{j,2})$ is a splitting of $\gamma_{1,1}^{t_j}$. Using our rule for the cup product explained at the end of Section 2, we have

$$y_i \cdot w = \sum_{\mathcal{P},\mathcal{P}'} \bigodot_{j=1}^{p} b_{1,j}b'_{j,1} \odot \bigodot_{j=1}^{p} b_{2,j}b'_{j,2}.$$

Observe that a partition $(b_{1,1},\dots,b_{1,p})$ of $\gamma_{1,k}$ corresponds to a partition $k_1,\dots,k_p$ of the natural number k with nonnegative integers. Explicitly, the correspondence is given by $b_{1,j} = \gamma_{1,k_j}$. Similarly, a partition $(b_{2,1}, \dots, b_{2,p})$ of $1_{p(p-i)}$ corresponds to a partition $h_1, \dots, h_p$ of $p(p-i)$ by the rule $b_{2,j} = 1_{h_j}$. The only splittings of $\gamma_{1,1}^a \alpha_{1,1}^\varepsilon$ are $(\gamma_{1,1}^a \alpha_{1,1}^\varepsilon, 1_0)$ and $(1_0, \gamma_{1,1}^a \alpha_{1,1}^\varepsilon)$.

Hence, we can write explicitly $y_i \cdot (\bigodot_{j=1}^p \gamma_{1,1}^{t_j})$ as a linear combination of elements of our basis $\mathcal{B}$, and we obtain

$$y_i \cdot w = \lambda_i \bigodot_{k=1}^{p} \gamma_{1,1}^{t_k + \delta_{k \le i}} \alpha_{1,1}^{\varepsilon_k} + \cdots$$

for some $\lambda_i \in \mathbb{Z}_p \setminus \{0\}$, where $\dots$ stands for terms that are smaller than the previous one in the considered ordering. With the same reasoning we can prove that

$$z_i \cdot w = \eta_i \bigodot_{k=1}^{p} \gamma_{1,1}^{t_k + \delta_{k < i}} \alpha_{1,1}^{\varepsilon_k + \delta_{\min\{h \ge i : \varepsilon_h = 0\}}(k)} + \cdots ,$$

where $\eta_i \in \mathbb{Z}_p \setminus \{0\}$ and $\dots$ has the same meaning as before.

An additive basis for S is given by

$$\mathcal{B}' = \Big\{ x_1^a y_p^b x_2^{\varepsilon_1} x_3^{\varepsilon_2} x_4^{\varepsilon_3} : a, b, \varepsilon_i \ge 0,\ \sum_{i=1}^{3} \varepsilon_i \le 1 \Big\} \cup \Big\{ \prod_{i=1}^{p} y_i^{t_i} \prod_{i=1}^{p} z_i^{\varepsilon_i} : t_i \ge 0, \varepsilon_i \in \{0,1\} \Big\}.$$

By induction, using the previous formulas, the expansion in the basis $\mathcal{B}$ of the cohomology class $\varphi\big(\prod_{i=1}^p y_i^{t_i} \prod_{i=1}^p z_i^{\varepsilon_i}\big)$ (with $t_i \ge 0$ and $\varepsilon_i \in \{0,1\}$) is in the form

$$\varphi\Big(\prod_{i=1}^{p} y_i^{t_i} \prod_{i=1}^{p} z_i^{\varepsilon_i}\Big) = \lambda_{\underline{t},\underline{\varepsilon}} \bigodot_{i=1}^{p} \gamma_{1,1}^{\sum_{k=i}^{p} t_k + \sum_{k=i+1}^{p} \varepsilon_k} \alpha_{1,1}^{\varepsilon_i} + \cdots ,$$

where, again, $\lambda_{\underline{t},\underline{\varepsilon}} \neq 0$ in $\mathbb{Z}_p$ and $\dots$ stands for smaller terms. This implies that the matrix associated with the $\mathbb{Z}_p$–linear function

$$\varphi\colon \operatorname{Span}\Big\{ \prod_{i=1}^{p} y_i^{t_i} \prod_{i=1}^{p} z_i^{\varepsilon_i} \Big\} \to \operatorname{Span}\Big\{ \bigodot_{i=1}^{p} \gamma_{1,1}^{t_i} \alpha_{1,1}^{\varepsilon_i} \Big\}$$

with respect to the two bases considered above (if we properly order their elements) is triangular, with all nonzero entries on the diagonal. Hence, $\varphi\colon A \to H^*(\Sigma_{p^2}; \mathbb{Z}_p)$ must be an isomorphism. □

References

[1] **A Adem**, **R J Milgram**, *Cohomology of finite groups*, 2nd edition, Grundl. Math. Wissen. 309, Springer, Berlin (2004) MR

[2] **F R Cohen**, **T J Lada**, **J P May**, *The homology of iterated loop spaces*, Lecture Notes in Mathematics 533, Springer, Berlin (1976) MR

[3] **C Giusti**, **P Salvatore**, **D Sinha**, *The mod-2 cohomology rings of symmetric groups*, J. Topol. 5 (2012) 169–198 MR

[4] **N H V Hung**, **P A Minh**, *The action of the mod p Steenrod operations on the modular invariants of linear groups*, Vietnam J. Math. 23 (1995) 39–56 MR

[5] **B M Mann**, *The cohomology of the symmetric groups*, Trans. Amer. Math. Soc. 242 (1978) 157–184 MR

[6] **J P May**, *A general algebraic approach to Steenrod operations*, from "The Steenrod algebra and its applications" (F P Peterson, editor), Lecture Notes in Mathematics 168, Springer, Berlin (1970) 153–231 MR

[7] **H Mui**, *Modular invariant theory and cohomology algebras of symmetric groups*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 22 (1975) 319–369 MR

[8] **N P Strickland**, **P R Turner**, *Rational Morava E–theory and DS^0*, Topology 36 (1997) 137–151 MR

Scuola Normale Superiore
Piazza dei Cavalieri 7, I-56126 Pisa, Italy

lorenzo.guerra@sns.it

Received: 9 November 2015 Revised: 16 September 2016