Adem relations in the Dyer-Lashof algebra and modular invariants

Nondas E. Kechagias
Department of Mathematics
University of Ioannina
45110, Ioannina

December 13, 1999

Abstract

This note deals with Adem relations in the Dyer-Lashof algebra from a modular invariant point of view. An algorithm is provided which has two effects. Firstly, to calculate the hom-dual of an element in the Dyer-Lashof algebra; and secondly, to find the image of a non-admissable element after applying Adem relations. The advandage is that one has to deal with polynomials instead of homology operations. Bockstein operations are excluded.

1. Introduction

The aim of this work is to provide an algorithm for calculating Adem relations in the Dyer-Lashof algebra using modular co-invariants. It is well known that the hom-dual of both Steenrod, P, and Dyer-Lashof, R, algebras are related with subalgebras of the so called *extended Dickson algebras.* The advantage of using modular invariants is that Adem relations are overcome and hidden in their structures.

Using relations between generators of the ring of Upper triangular invariants and the Dickson algebra, an algorithm for finding the hom -dual for elements of R' is given, where R' is a Hopf subalgebra of R containing elements which do not involve Bockstein operations. This is the key point to provide the algorithm described above. This algorithm is also useful in other applications related with the Dyer-Lashof algebra. For example it provides a computational tool for the transfer in the $mod-p$ homology of the symmetric group, since its cohomology is easier described using Dickson invariants. This algorithm becomes complicated when applied to elements involving Bockstein operations. We note that the algorithm mentioned above is a reformulation of May's theorem 3.7, page 29, in [1].

The scheme of this note consists of three sections: sections 2 and 3 recall well known facts about the Dyer-Lashof and Dickson algebras respectively; the algorithms mentioned above are described in the last section.

2. The Dyer-Lashof algebra

Let us briefly recall the construction of the Dyer-Lashof algebra. The symbol p stands for any prime number. Let F be the free graded associative algebra on $\{e^i,\ i \geq 0\}$ and $\{\beta e^i,\ i > 0\}$ over $K := Z/pZ$ with $|e^i| = 2i$ and $|\beta e^i| = 2i-1$. F becomes a coalgebra equipped with coproduct $\psi :\ F \longrightarrow F \otimes F$ given by

$$\psi e^i = \sum e^{i-j} \otimes e^j \text{ and } \psi\beta e^i = \sum \beta e^{i-j} \otimes e^j \ + \ \sum e^{i-j} \otimes \beta e^j.$$

Elements of F are of the form $e^I = \beta^{\epsilon_1} e^{i_1} \dots \beta^{\epsilon_n} e^{i_n}$ where $I = ((\epsilon_1, i_1), \dots (\epsilon_n, i_n))$ with $\epsilon_j = 0$ or 1 and i_j a non negative integer for $j = 1, \ \dots \ , n$. Let $l(I)$ denote the length of e^I and let the excess of e^I be denoted by $exc(e^I) = |e^{i_1}| - \epsilon_1 - |e^{I'}|(p-1)$ where $I' = ((\epsilon_2, i_2), \dots (\epsilon_n, i_n))$; and ∞, if $I = (0, \ \dots, \ 0)$. F admits a Hopf algebra structure with unit $\eta : \ K \longrightarrow F$ and augmentation $\epsilon : F \longrightarrow K$ given by:

$$\epsilon(e^i) = \begin{cases} 1, & \text{if } i = 0 \\ 0, & \text{otherwise.} \end{cases}$$

We define $U = F/I_e$, where I_e is the two sided ideal generated by elements of negative excess. U is a Hopf algebra and if we let $U[n]$ denote the set of all elements of U with length n, then $U[n]$ is a coalgebra of finite type.

We extend the previous construction by restricting the degrees and imposing Adem relations. Let U' be the subalgebra of U generated by $\{e^{(p-1)i},\ i \geq 0\}$ and $\{\beta e^{(p-1)i},\ i > 0\}$. We denote these elements by Q^i and βQ^i respectively, and recall their degrees $|Q^i| = 2i(p-1)$ and $|\beta Q^i| = 2i(p-1) - 1$. Let B be the quotient algebra of U' by the two sided ideal generated by elements of negative excess, where $exc(Q^I) = 2i_1 - \epsilon_1 - |Q^{I'}|$, with $I = ((\epsilon_1, i_1), \dots (\epsilon_n, i_n))$ and $I' = ((\epsilon_2, i_2), \dots (\epsilon_n, i_n))$; and ∞, if $I = (0, \dots, 0)$. B is a Hopf algebra with the induced coproduct and $B[n]$ a coalgebra as before.

Let I be the two sided ideal of B generated by allowing Adem relations everywhere.

Adem relations are given by:

$$\mathbf{Q}^r Q^s = \sum_i (-1)^{\mathbf{r}+k} \binom{(p-1)(k-s)-1}{pk-r} \mathbf{Q}^{r+s-k} Q^k, \qquad \text{if } r > ps; \qquad (2.1)$$

$$\begin{aligned} \mathbf{Q}^r \beta Q^s \;=\; & \sum_i (-1)^{r+k} \binom{(p-1)(k-s)}{pk-r} \beta \mathbf{Q}^{r+s-k} Q^k - \\ & \sum_i (-1)^{r+k} \binom{(p-1)(k-s)-1}{pk-r-1} \mathbf{Q}^{r+s-k} \beta Q^k, \qquad \text{if } r \geq ps. \end{aligned}$$

We denote R the quotient B/I and this quotient algebra is called **the Dyer-Lashof algebra.** Finally, R is a Hopf algebra and $R[n]$ is again a coalgebra. By abuse of notation we use the same symbol for elements of B and R. Since $R[n]$ and $B[n]$ are of finite type, they are isomorphic to their duals as vector spaces and these duals become algebras. We shall describe these duals giving an invariant theoretic description, namely: they are isomorphic to subalgebras of rings of invariants over the appropriate subgroup of $GL(n, K)$. We restrict our study to subalgebras $R' \leq R$ and $B' \leq B$ such that no elements involving Bockstein operations are allowed.

An element Q^I in $R'[n]$ is called admissible, if there are no Adem relations between its factors and primitive if $\psi Q^I = Q^I \otimes Q^0 + Q^0 \otimes Q^I$. Here Q^0 means Q^0 $l(I)$ times. Since the dual of a primitive is a generator, the algebraic structure of the dual algebras is described by the primitives and their relations. Next we discuss the primitives of $B'[n]$, $R'[n]$, and the primitive decomposition of an admissible element. We follow May [1].

Let $\tilde{I}_{i,n} = (p^{i-2}(p-1), \dots, (p-1), 1, 0, \dots, 0)$, where there are $n-i$ zeros. Its degree is $|Q^{\tilde{I}_{i,n}}| = 2p^{i-1}(p-1)$ and $exc(Q^{\tilde{I}_{i,n}}) = 0$. Here $1 \leq i \leq n$.

Let $I_{n-i,n} = (p^{n-i-1}(p^i - 1), \dots, (p^i - 1), p^{i-1}, \dots, p, 1)$. Here $1 \leq i \leq n$ and is the number of p-th powers. The degree $|Q^{I_{n-i,n}}| = 2p^{n-i}(p^i - 1)$ and the $exc(Q^{I_{n-i,n}}) = 0$, if $i < n$, and 1 if $i = n$.

Let the generators be as follows:

$$\begin{aligned} \xi_{0,n} &= ((Q^0)^n)^*, & 0 \leq n. \\ \xi_{n-i,n} &= (Q^{I_{n-i,n}})^*, & 1 \leq i \leq n_j. \end{aligned}$$

Theorem 1. *Let $P'[n]$ be the free associative commutative algebra generated by $\{ \xi_{n-i,n} \ / \ 1 \leq i \leq n$. Then $P'[n] \equiv R'[n]^*$ as algebras.*

3. The Dickson algebra

Let V^k denote a K-dimensional vector space generated by $\{y_1, ..., y_k\}$ and $1 \leq k \leq n$. Let S_n be the graded symmetric algebra of V^n; $S_n = K[y_1, \cdots, y_n]$ and degree $|y_i| = 2$ (if $p = 2$, then $|y_i| = 1$).

The following theorems are well known:

Theorem 1. *[2] $S_n^{GL_n} := D_n = K[d_{n,0}, \cdots, d_{n,n-1}]$ is a polynomial algebra where the degrees are $|d_{n,i}| = 2(p^n - p^i)$.*

Theorem 2. *[4] $S_n^{B_n} := H_n = K\left[h_1^{(p-1)}, \cdots, h_n^{(p-1)}\right]$ is a polynomial algebra where the degrees are $|h_i| = 2p^{i-1}$.*

The generators above are related as follows:

Let $f_{k-1}(x) = \prod_{u \in V^{k-1}} (x - u)$, then $f_{k-1}(x) = \sum_{i=0}^{k-1} (-1)^{n-i} x^{p^i} d_{k-1,i}$ and $h_k = \prod_{u \in V^{k-1}} (y_k - u)$. Moreover,

$$d_{n,n-i} = \sum_{1 \leq j_1 < \cdots < j_i \leq n} \prod_{s=1}^{i} \left(h_{j_s}^{p-1}\right)^{p^{n-i+s-j_s}} \tag{3.1}$$

[3].

Let $\tilde{A} = \{A = (a_{ij})$ an nxn matrix such that $a_{ij} = 0, 1$ for $0 \leq i, j \leq n-1$ and $\sum_{t=0}^{n-1} a_{it} = n - i\}$. For each element of $\tilde{A}$ we define an $n \times n$ matrix $B(A) = (b_{ij}) = \left(b^{(0)}, \cdots, b^{(n-1)}\right)$ such that $b_{ij} = a_{ij} p^{j-1-s+a_{1j}+\cdots+a_{sj}}$. Let us call this collection $\hat{E}(\tilde{A}) = \{B(A) \mid A \in \tilde{A}\}$. Let $M = (m_0, \cdots, m_{n-1})$ be a sequence of zeros or powers of p. Let $\hat{E}^M = \{B(A) = (b_{ij}) \mid A \in \tilde{A}$ and $b_{ij} = a_{ij} m_j p^{j-1-s+a_{1j}+\cdots+a_{sj}}\}$. The following lemma is easily deduced from formula 3.1

Lemma 3. $\prod_{0}^{n-1} d_{n,i}^{m_i} = \sum_{B \in \hat{E}^M} \prod_{t=1}^{n} h_t^{(B\bar{1})_{t-1}}$. *Here* $\bar{1} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$.

The Steenrod algebra acts naturally on D_n and H_n, because S_n is a subalgebra of $H^*(B(Z/pZ)^n; Z/pZ)$. [?]

Theorem 4. *$(R'[n])^* \cong D_n$ as algebra over the Steenrod algebra and the isomorphism Φ is given by $\Phi(\xi_{n-i,n}) = d_{n,n-i}$. Here $1 \le i \le n$.*

4. Calculating the hom-duals and Adem relations

Under isomorphism Φ in theorem 4 we identify $R'[n]^*$ and D_n. Let $\mathbf{A} : B \to R$ be the map which imposes Adem relations and $\mathbf{A} : B'[n] \to R'[n]$ the induced map between the respected coalgebras of length n.

$$\mathbf{A}(Q^I) = \sum a_{I,J} Q^J$$

Let $I = (\varepsilon_1, s_1, \cdots, \varepsilon_n, s_n)$ and $I_j = (\varepsilon_j, s_j, \cdots, \varepsilon_n, s_n)$ for $1 \le j \le n$. Define a total ordering by $I < J$, if $exc(I_j) < exc(J_j)$ for the smallest j such that $exc(I_j) \ne exc(J_j)$.

Let $\hat{\imath} : D_n \hookrightarrow H_n$ be the inclusion of the rings of invariants, then $\hat{\imath}(d^K)$ means the decomposition of d^K in H_n. Firstly, we shall show that $\mathbf{A}^* \equiv \hat{\imath}$ i.e. for any $Q^I \in B[n]$ and $d^K = \prod_{i=0}^{n-1} d_{n,i}^{m_i} \in D_n$,

$$< d^K, \mathbf{A}(Q^I) > = < \hat{\imath}(d^K), Q^I > .$$

Here, $< -, - >$ is the Kronecker product. This is done by studying all monomials in $B[n]$ which map to primitives in $R'[n]$ after applying Adem relations.

Let $n(K) = \sum m_i$. Let $\psi_{n(K)} : R'[n] \to \overset{n(K)}{\otimes} R'[n]$ be the iterated coproduct $n(K)$ times.

$$\begin{aligned} \psi_{n(K)} Q^J &= \sum \pm Q^{J_1} \otimes \cdots \otimes Q^{J_{n(K)}}, \quad \sum J_i = J \\ \mathbf{A}\psi_{n(K)} Q^J &= \sum a_{J_1,\dots,J_{n(K)}} Q^{J'_1} \otimes \cdots \otimes Q^{J'_{n(K)}}. \end{aligned}$$

Since J_i may not be in admissible form, after applying Adem relations we have $J'_i \le J_i$.

$$< d^K, \mathbf{A}Q^I > = < \prod_{i=0}^{n-1} d_{n,i}^{m_i}, \psi_{\sum m_i} \mathbf{A} Q^I > = < \prod_{i=0}^{n-1} d_{n,i}^{m_i}, \mathbf{A}\psi_{\sum m_i} Q^I > =$$
$$< \prod_{i=0}^{n-1} d_{n,i}^{m_i}, \sum_{j=1}^{\sum m_i} \otimes \mathbf{A} Q^{I_j} > = \sum_j \prod_i < d_{n_i}, \mathbf{A} Q^{I_i} >.$$

Lemma 1. *Let $A=(a_{ij})$ be an nxn matrix such that $a_{ij}=0$ or 1 for $0\le i,j\le n-1$ and $\sum\limits_{t=0}^{n-1} a_{it}=n-i$. Let also M be an nx1 matrix such that $M_i=p^{m_i}$ or 0 for $0\le i\le n-1$. Then $\prod\limits_{i=1}^{n} h_i^{(p-1)(AM)_{i-1}}$ is a summand in $\prod\limits_{i=0}^{n-1} d_{n,i}^{M_i}$.*

Proof. This is an application of formula 3.1. ■

Using the lemma above, it is possible to find all summands in $\prod\limits_{i=0}^{n-1} d_{n,i}^{m_i}$.for m_i a non-negative integer.

Lemma 2. *Let $D=\prod\limits_{i=1}^{n} d_{n,i}^{m_i}$. Then $h^{I(D\min)}=\prod\limits_{t=1}^{n} h_t^{(p-1)\sum\limits_{i=0}^{t-1} m_i}$ and $\left(h^{I(D\min)}\right)^*=$*
$$Q^{p^{n-1}m_0+\sum\limits_{i=1}^{n-1}(p^{n-1}-p^{i-1})m_i}\, Q^{p^{n-2}(m_0+m_1)+\sum\limits_{i=2}^{n-1}(p^{n-2}-p^{i-2})m_i}\cdots$$
$$Q^{p^{n-t}(m_0+\ldots+m_{t-1})+\sum\limits_{i=t}^{n-1}(p^{n-t}-p^{i-t})m_i}\ldots Q^{\sum\limits_{0}^{n-1} m_i}.$$

Proof. All possible summands in $\prod\limits_{i=1}^{n} d_{n,i}^{m_i}$ are given by
$$\prod_{i=0}^{n-1}\left(\sum_{1\le j_1<\cdots<j_{n-i}\le n}\ \prod_{s=1}^{n-i}\left(h_{j_s}^{p-1}\right)^{p^{i+s-j_s}}\right)^{m_i}. \ ■$$

Lemma 3. *Let $Q^I\in B'[n]$ be the* hom-dual *of $\left(\prod\limits_{j=1}^{i}\left(h_j^{p-1}\right)^{p^{n-i}}\right)$. Then $Q^I=(d_{n,n-i})^*$ in $R'[n]$ (after applying Adem relations).*

Proof. For the shake of simplicity, we write I instead of Q^I. By hypothesis $I=(p^{n-1},...,p^{n-i},0,...,0)$ (we recall that this is the biggest sequence among those involved in (3.1) after theorem 1.3). Let us call it $I_{\max}(i)$ and we apply Adem relations between the last n-i+1 elements of I $((p^{n-i},0,...,0))$. The last sequence becomes $(p^{n-i}-p^{n-i-1},...,p-1,1)$, because of excess and the binomial coefficients in the Adem relations: $pk-p^{n-t}\le 0$ and $\binom{(p-1)k-1}{pk-p^{n-t}}\ne 0 \bmod p \Rightarrow k=p^{n-t-1}$. Next we consider the first i elements of the new sequence: $(p^{n-1},...,p^{n-i+1},p^{n-i}-p^{n-i-1})$. Again, it becomes $(p^{n-1}-p^{n-i-1},p^{n-2},...,p^{n-i})$ for the same reasons: $pk+p^{n-t-1}-p^{n-i-1}\le p^{n-t}+p^{n-t-1}-p^{n-i-1}$ and $\binom{(p-1)(k-p^{n-t-1}+p^{n-i-1})-1}{pk-p^{n-t}}\ne 0 \bmod p \Rightarrow k \doteq p^{n-t-1}$. Next we consider the first i+1 elements of the new sequence, $(p^{n-1}-p^{n-i-1},p^{n-2},...,p^{n-i},\ p^{n-i-1}-p^{n-i-2})$ which becomes, $(p^{n-1}-$

$p^{n-i-1}, p^{n-2} - p^{n-i-2}, p^{n-3}, ..., p^{n-i-1})$ for the same reasons. After n-i-2 steps, the following sequence is obtained $(p^{n-1} - p^{n-i-1}, p^i - 1, p^{i-1}, ..., p, 1)$ which represents the required element. ■

Lemma 4. *Let $Q^I \in B'[n]$ be the hom-dual of $\left(\prod_{s=1}^{i} \left(h_{j_s}^{p-1}\right)^{p^{n-i+s-j_s}}\right)$ in (3.1) (page -). Here $1 \leq j_1 < ... < j_i \leq n$. Then $\mathbf{A}(Q^I) = (d_{n,n-i})^*$ in $R'[n]$.*

Proof. The sequence I is given by:

$$\left(\begin{array}{l} \underbrace{\sum_{t=1}^{i}(p^{n-i+t-1} - p^{n-i+t-2}), \cdots, p^{n-i+1-j_1} + \sum_{t=2}^{i}(p^{n-i+t-j_1} - p^{n-i+t-j_1-1})}_{j_1}, \underbrace{\cdots}_{j_{i-2}-j_1}, \\ p^{n-j_i}(p^{j_i-j_{i-2}-1} - p^{j_i-j_{i-2}-2}) + p^{n-j_{i-1}-1}(p^{j_{i-1}-j_{i-2}-1} - p^{j_{i-1}-j_{i-2}-2}), \cdots, \\ p^{n-j_i}(p^{j_i-j_{i-1}} - p^{j_i-j_{i-1}-1}) + p^{n-j_{i-1}-1}, \\ \underbrace{p^{n-j_i}(p^{j_i-j_{i-1}-1} - p^{j_i-j_{i-1}-2}), \cdots, p^{n-j_i}(p-1), p^{n-j_i}}_{j_i-j_{i-1}}, \underbrace{0, \cdots, 0}_{n-j_i} \end{array}\right)$$

Here $p^m := 0$, whenever $m < 0$. We shall work out the first steps to describe the idea of the proof. First, we consider the last $n-i+1$ elements of $I_{\max}(i)$: $(p^{n-i}, 0, ..., 0)$ which becomes $(p^{n-i} - p^{n-i-1}, ..., p^{n-j_i+1} - p^{n-j_i}, p^{n-j_i}, 0, ..., 0)$. Applying Adem relations on certain positions on $Q^{I_{\max}(i)}$, Q^I is obtained. Next, the $n-i+2$ elements of the new sequence $(p^{n-i+1}, p^{n-i} - p^{n-i-1}, ..., p^{n-j_i+1} - p^{n-j_i}, p^{n-j_i}, 0, ..., 0)$ becomes $(p^{n-i+1} - p^{n-i-1}, p^{n-i} - p^{n-i-2}, ..., p^{n-j_{i-1}+1} - p^{n-j_{i-1}-1}, p^{n-j_{i-1}}, p^{n-j_{i-1}-1} - p^{n-j_{i-1}-2}, ..., p^{n-j_i}, 0, ..., 0)$.

At each stage a new subsequence I_t of length $n-i+t$ is given by the last one (of length $n-i+t-1$) enlarged by the $i-t$ element of $I_{\max}(i)$. Applying Adem relations between the last $n-i+t-(n-j_t) = j_t - i + t$ elements of I_t, the obtained sequence has the required form. ■

Proposition 5. *Let $Q^I \in B'[n]$ be the hom-dual of a monomial $h^J \in H_n$ such that $|h^J| = 2(p^n - p^{n-i})$ and h^J is not a summand in (3.1) (page -). Then $\mathbf{A}(Q^I) = 0$ in $R'[n]$.*

Proof. Two cases should be considered: 1) $h_{j_1} \cdots h_{j_i}$ divides both $h_1 \cdots h_n$ and h^J, for some $1 \leq j_1 < \cdots < j_i \leq n$; and 2) $h_{j_1} \cdots h_{j_i}$ does divide $h_1 \cdots h_n$ but not h^J, for any $1 \leq j_1 < \cdots < j_i \leq n$. Let j_{i-t} be the biggest index such that

$(h_{j_{i-t}}^{p-1})^{p^{n-t-j_{i-t}}}$ does not divide h^J. Let us start with 1) and recall that $(h^J)^*$ equals

$$\left(\begin{array}{l} \underbrace{p^{n-1} - p^{n-i-1}, \cdots, p^{n-j_1}}_{j_1}, \underbrace{\cdots}_{j_{i-t-1}-j_1}, \underbrace{p^{n-j_{i-t-1}-1} - p^{n-j_{i-t-1}-2-t}, \cdots, p^{n-j_{i-t}}}_{j_{i-t}-j_{i-t-1}}, \\ \underbrace{\cdots}_{j_{i-2}-j_{i-t}}, \underbrace{p^{n-j_{i-2}-1} - p^{n-j_{i-2}-3}, \cdots, p^{n-j_{i-1}}}_{j_{i-1}-j_{i-2}}, \\ \underbrace{p^{n-j_{i-1}-1} - p^{n-j_{i-1}-2}, \cdots, p^{n-j_i}(p-1), p^{n-j_i}}_{j_i-j_{i-1}}, \underbrace{0, \cdots, 0}_{n-j_i} \end{array} \right)$$

Again, we should consider two cases, namely: i) $p^{n-j_{i-t}}$ has been replaced by $p^{n-j_{i-t}} - m(t)$ and ii) $p^{n-j_{i-t}-k} - p^{n-j_{i-t}-k-(t-1)}$ has been replaced by $p^{n-j_{i-t}-k} - p^{n-j_{i-t}-k-(t-1)} + m(t)$.

i) Let us start with $m(t) > 0$. The last $n - j_{i-t} + 1$ elements of the sequence becomes $(p^{n-j_{i-t}} - m(t), p^{n-j_{i-t}-1} - p^{n-j_{i-t}-t}, \cdots, p^{t-1} - 1, p^{t-2}, \cdots, p, 1)$ after applying Adem relations. Because of excess and Adem relations, $p^{n-j_{i-t}-1}$ divides $m(t)$ and hence $p^{n-j_{i-t}-1} = m(t)$ which is case ii).

Now let $m(t) < 0$. As before: $(p^{n-j_{i-t}} - m(t), p^{n-j_{i-t}-1} - p^{n-j_{i-t}-t}, \cdots, p^{t-1} - 1, p^{t-2}, \cdots, p, 1)$ after applying Adem relations. Because of excess and Adem relations, the last sequence becomes: $(p^{n-j_{i-t}} - p^{n-j_{i-t}-t}, p^{n-j_{i-t}-1} - p^{n-j_{i-t}-t-1}, \cdots, p^t + 1, p^{t-2}, \cdots, p, 1)$ and this gives a zero element.

ii) $m(t) < p^{n-j_{i-t}-k-(t-1)}$. Otherwise, this case reduces to the previous one. Excess conditions and Adem relations imply $m(t) = p^{n-j_{i-t}-k-(t-1)}$.

2) The last $n - j_t + 1$ elements of I are given by:
$(p^{n-j_t} - m(t), p^{n-j_t-1} - p^{n-j_t-2}, ..., p^{n-j_i}, 0, ..., 0) \equiv$
$(p^{n-j_t} - m(t), p^{n-j_t-1} - p^{n-j_t-2}, ..., p^{n-j_i} - p^{n-j_i-1}, ..., p-1, 1)$. Because of excess and Adem relations between the first two elements, $m(t) = pm_1(t)$ and the previous subsequence becomes $(p^{n-j_t} - (p-1)m_1(t) - p^{n-j_t-2}, p^{n-j_t-1} - m_1(t), p^{n-j_t-2} - p^{n-j_t-3}, ..., p^{n-j_i} - p^{n-j_i-1}, ..., p-1, 1)$. Finally: $(p^{n-j_t} - (p-1)m_1(t) - p^{n-j_t-2}, p^{n-j_t-1} - (p-1)m_2(t) - p^{n-j_t-3}, ..., p^{n-j_i} - (p-1)m_{j_i-j_t+1}(t) - p^{n-j_i-2}, ..., p - (p-1)m_{n-j_t}(t) - 1, 1)$. Here $m_s(t) = pm_{s+1}(t)$ for $1 \leq s \leq n - j_t$. But the last sequence is equivalent to zero unless $m_{n-j_t} = 0$ and this is a contradiction. ■

Now the following theorem is easily deduced because $R'[n]$ is a coalgebra, the map $\mathbf{A}$ is a coalgebra map, and primitives have been considered.

Theorem 6. *Let $\mathbf{A} : B'[n] \to R'[n]$ be the map which imposes Adem relations. Let $\hat{\imath} : D_n \hookrightarrow H_n$ be the natural inclusion. Then $\mathbf{A}^* \equiv \hat{\imath}$, i.e. for any $Q^I \in B'[n]$*

and $d^K = \prod_{i=0}^{n-1} d_{n,i}^{m_i} \in D_n$,

$$< d^K, \mathbf{A}(Q^I) >=< \hat{\imath}(d^K), Q^I > .$$

Next, the algorithm for calculating the hom-dual in $(R'[n])^*$ is demonstrated.

Example 1. *Let $p = 3$ and $d^I = d_{2,0}^2 d_{2,1}^{19}$, then $I = (2, 19)$ and $'I = (44, 21)$. To calculate its dual the following elements should be considered: $Q^{(48,17)}$, $Q^{(47,18)}$, $Q^{(46,19)}$, $Q^{(45,20)}$, and $Q^{(44,21)}$. The associated elements in D_n should also be considered: $d_{2,0}^{14} d_{2,1}^3$, $d_{2,0}^{11} d_{2,1}^7$, $d_{2,0}^8 d_{2,1}^{11}$, $d_{2,0}^5 d_{2,1}^{15}$, and $d_{2,0}^2 d_{2,1}^{19}$.*

i) $d_{2,0}^{14} d_{2,1}^3 = (Q^{(48,17)})^*$ (there is only one choice).

ii) $d_{2,0}^{11} d_{2,1}^7$. Find the g.c.d.$(d_{2,0}^{14} d_{2,1}^3, d_{2,0}^{11} d_{2,1}^7) = d_{2,0}^{11} d_{2,1}^3$. Consider $\left(d_{2,0}^{14} d_{2,1}^3\right) / (d_{2,0}^{11} d_{2,1}^3) = d_{2,0}^3$ and $(d_{2,0}^{11} d_{2,1}^7)/(d_{2,0}^{11} d_{2,1}^3) = d_{2,1}^4$. Find their decomposition in H_2 and consider their monomials corresponding to the smallest sequences : $h_1^{3\cdot 2} h_2^{3\cdot 2}$, $h_2^{4\cdot 2}$. Find the g.c.d.$(h_1^{3\cdot 2} h_2^{3\cdot 2},\ h_2^{4\cdot 2}) = h_2^{3\cdot 2}$. Consider the following monomials: $(h_1^{3\cdot 2} h_2^{3\cdot 2})/h_2^{3\cdot 2} = h_1^{3\cdot 2}$ and $h_2^{4\cdot 2}/h_2^{3\cdot 2} = h_2^{1\cdot 2}$. Recall that the dual of the second monomial has no Adem relations. Check if $h_1^{3\cdot 2}$ is a summand in $d_{2,1}$. If yes, then $(Q^{(48,17)})^*$ is a summand in $d_{2,0}^{11} d_{2,1}^7$ with the appropriate coefficient: $d_{2,0}^{11} d_{2,1}^7 = (Q^{(47,18)})^* + (Q^{(48,17)})^*$. Otherwise , no.

iii) $d_{2,0}^8 d_{2,1}^{11}$. By repeating steps described above, we obtain: $d_{2,0}^8 d_{2,1}^{11} = (Q^{(46,19)})^* + (Q^{(47,18)})^* + (Q^{(48,17)})^*$.

iv) $d_{2,0}^5 d_{2,1}^{15} = (Q^{(45,20)})^* + (Q^{(46,19)})^* + (Q^{(47,18)})^* + (Q^{(48,17)})^*$.

v) $d_{2,0}^2 d_{2,1}^{19} = (Q^{(44,21)})^* + (Q^{(45,20)})^* + (Q^{(46,19)})^* + (Q^{(47,18)})^* + (Q^{(48,17)})^*$.

Theorem 7. *Let d^I be an element of D_n, then the following algorithm calculates its image in $R'[n]^*$: 1) Find all elements Q^J in $R'[n]$ such that $|d^I| = |Q^J|$ and $'I \leq J$, and their corresponding $d^{J'}$ in D_n. Order them according to the given ordering.*

2) Let d^K be an element in step 1) corresponding to the biggest sequence among those not considered. Find the $\gcd(d^K, d^I)$. If $\gcd(d^K, d^I) = d^K$, then $Q'^K = Q'^I$; otherwise let $d^{K(1)} = d^K / \gcd(d^K, d^I)$, $d^{I(1)} = d^I / \gcd(d^K, d^I)$. Consider $i(d^{I(1)})$ in H_n and find its dual in $B'[n]$. Let $i(d^{I(1)})$ and $i(d^{K(1)})$ in H_n and consider their monomials $h^{I(1)}$ and $h^{K(1)}$ associated with the smallest sequences. Divide both by the greatest common divisor and let $h^{I(2)}$ and $h^{K(2)}$ be the new monomials. Let us recall that $(h^{K(2)})^* = Q'^{K(3)} \in R'[n]$. Let $a_{I,K}$ be the coefficient of $h^{I(2)}$ in $i(d^{K(3)})$. Then d^I contains $a_{I,K}(Q^K)^*$ as a summand. Otherwise, no.

3) Repeat step 2) for all $d^{J'}$ in step 1).

Proof. Let $I = \sum_{t=0}^{n-1} k_t I_{t,n}$ and $k(I) = \sum_{t=0}^{n-1} k_t$. Because of the definition of the hom-dual, we have : $< d^I, Q'^I >= 1$ and $< d^I, Q^J >= a_{(J)}$ for a sequence J such that in the $k(I)$ times iterated coproduct, $\psi Q^J = \sum Q^{J_1} \otimes ... \otimes Q^{J_{k(I)}} \overset{Adem}{=} \sum a_{L_1,...,L_{k(I)}} Q^{L_1} \otimes ... \otimes Q^{L_{k(I)}}$, $a_{(J)} Q'^I$ is a summand. Thus $J \geq' I$. We shall note here that only primitives are involved in the last summand and all elements in $B[n]$ which are mapped to primitives by the map which imposes Adem relations are known.

Let $\psi Q'^{K(1)} = \sum Q^{J_1} \otimes ... \otimes Q^{J_{k(I(1))}}$. If there exists $Q^{M_1} \otimes ... \otimes Q^{M_{k(I(1))}}$ in the last sum such that $Q^{M_i} = Q^{I_{n,t_i}}$ for $i = 1, ..., k(I(1))$ and $\prod_{i=1}^{k(I(1))} d_{n,t_i} = d^{I(1)}$, then Q'^K is a summand in d^I with the same coefficient.

For the sequence J we consider the corresponding element $d^{J'}$ in D_n. Let $d^{J'} = \prod_{t=0}^{n-1} d_{t,n}^{m_t}$ such that $J \geq' I$. Then $k(I) \geq k(J')$. Consider the common elements between d^I and $d^{J'}$, their associated elements in $R[n]$ will not contribute anything more in the iterated coproduct. Hence, only the non-common elements must be consider. However, we must check if the associated sequence of $d^{J'}/\gcd(d^{J'}, d^I)$ after the appropriate (the number of common elements are not considered) iterated coproduct is applied and Adem relations are considered provides the associated sequence of $d^I/\gcd(d^{J'}, d^I)$. But since all elements which map to primitives after applying Adem relations are known, this is true exactly when the conditions of the last part of step 2) are fulfilled. ■

Next, the algorithm which calculates Adem relations using modular invariants is demonstrated.

Example 2. *Let $p = 3$ and $I = (50, 15)$. Then $\mathbf{A}(Q^I) = 2Q^{(47,18)} + Q^{(46,19)}$ using Adem relations in the Dyer-Lashof algebra. We shall also evaluate $\mathbf{A}(Q^I)$ using the following algorithm.*

1) Find all $d^{K'} \in D_n$ and corresponding $Q^K \in R[n]$ such that $|d^{K'}| = |Q^I| = 2(p-1)(50+15)$. Using their decomposition in H_n check those which contain $(Q^I)^* = h_1^{20(p-1)} h_2^{15(p-1)}$ as a summand. Those are

$d_{2,0}^{14} d_{2,1}^{3}$, $Q^{(48,17)}$, *no;*

$d_{2,0}^{11} d_{2,1}^{7}$, $Q^{(47,18)}$, *yes with coefficient 2;*

$d_{2,0}^{8} d_{2,1}^{11}$, $Q^{(46,19)}$, *no;*

$d_{2,0}^{5} d_{2,1}^{15}$, $Q^{(45,20)}$, *no;*

$d_{2,0}^{2} d_{2,1}^{19}$, $Q^{(44,21)}$, *no.*

2) Calculating their duals:

$d^{14}_{2,0}d^{3}_{2,1} = (Q^{(48,17)})^*$ *(there is only one choice).*

$d^{11}_{2,0}d^{7}_{2,1}$. *Find the g.c.d.*$(d^{14}_{2,0}d^{3}_{2,1}, d^{11}_{2,0}d^{7}_{2,1}) = d^{11}_{2,0}d^{3}_{2,1}$. *Consider* $\left(d^{14}_{2,0}d^{3}_{2,1}\right)/(d^{11}_{2,0}d^{3}_{2,1}) = d^{3}_{2,0}$ *and* $(d^{11}_{2,0}d^{7}_{2,1})/(d^{11}_{2,0}d^{3}_{2,1}) = d^{4}_{2,1}$ *and their corresponding sequences in* H_2: $h_1^{3\cdot 2}h_2^{3\cdot 2}$, $h_2^{4\cdot 2}$. *Find the g.c.d.*$(h_1^{3\cdot 2}h_2^{3\cdot 2},\ h_2^{4\cdot 2}) = h_2^{3\cdot 2}$. *Consider* $(h_1^{3\cdot 2}h_2^{3\cdot 2})/h_2^{3\cdot 2} = h_1^{3\cdot 2}$ *and* $h_2^{4\cdot 2}/h_2^{3\cdot 2} = h_2^{1\cdot 2}$. *Check if* $h_1^{3\cdot 2}$ *is a summand in* $d_{2,1}$. *If yes, then* $(Q^{(48,17)})^*$ *is a summand in* $d^{11}_{2,0}d^{7}_{2,1}$ *with the appropriate coefficient:* $d^{11}_{2,0}d^{7}_{2,1} = (Q^{(47,18)})^* + (Q^{(48,17)})^*$. *Otherwise , no.*

$d^{8}_{2,0}d^{11}_{2,1}$. *repeating steps described above, we obtain:* $d^{8}_{2,0}d^{11}_{2,1} = (Q^{(46,19)})^* + (Q^{(47,18)})^* + (Q^{(48,17)})^*$.

$d^{5}_{2,0}d^{15}_{2,1} = (Q^{(45,20)})^* + (Q^{(46,19)})^* + (Q^{(47,18)})^* + (Q^{(48,17)})^*$.

$d^{2}_{2,0}d^{19}_{2,1} = (Q^{(44,21)})^* + (Q^{(45,20)})^* + (Q^{(46,19)})^* + (Q^{(47,18)})^* + (Q^{(48,17)})^*$.

3) Use the Kronecker product to evaluate $\mathbf{A}(Q^I)$.

Start with $d^{K'}$ *such that* K' *is the biggest sequence where the first non-zero coefficient of* $(Q^I)^* = h_1^{20(p-1)}h_2^{15(p-1)}$ *in* $d^{K'}$ *appears.*

$< d^{11}_{2,0}d^{7}_{2,1}, \mathbf{A}(Q^I) >=< \hat{i}(d^{11}_{2,0}d^{7}_{2,1}), \mathbf{Q}^I >= 2 \Rightarrow Q^{(47,18)}$ *has coefficient* 2 *in* $\mathbf{A}(Q^I)$.

$< d^{8}_{2,0}d^{11}_{2,1}, \mathbf{A}(Q^I) >=< \hat{i}(d^{8}_{2,0}d^{11}_{2,1}), \mathbf{Q}^I >= 0 \Rightarrow Q^{(46,19)}$ *has coefficient* 1 *in* $\mathbf{A}(Q^I)$.

$< d^{5}_{2,0}d^{15}_{2,1}, \mathbf{A}(Q^I) >=< \hat{i}(d^{5}_{2,0}d^{15}_{2,1}), \mathbf{Q}^I >= 0 \Rightarrow Q^{(45,20)}$ *has coefficient* 0 *in* $\mathbf{A}(Q^I)$.

$< d^{2}_{2,0}d^{19}_{2,1}, \mathbf{A}(Q^I) >=< \hat{i}(d^{2}_{2,0}d^{19}_{2,1}), \mathbf{Q}^I >= 0 \Rightarrow Q^{(44,21)}$ *has coefficient* 0 *in* $\mathbf{A}(Q^I)$.

Hence $\mathbf{A}(Q^I) = 2Q^{(47,18)} + Q^{(46,19)}$.

Now, the following proposition is obvious.

Proposition 8. *Let* $Q^I \in B[n]$. *The following algorithm computes* $\mathbf{A}(Q^I)$ *in* $R'[n]$.

i) Find all sequences K *according to the given ordering such that* $Q^K \in R'[n]$ *and* $|Q^K| = |Q^I|$. *Let* $b_{I,K}$ *be the coefficients of* $h^{I'}$ *in* $i(d^{K'})$.

ii) Compute the duals of $d^{K'}$ *in* $(R'[n])^*$.

iii) Use the Kronecker product to evaluate $\mathbf{A}(Q^I)$:

Start with the first non-zero b_{I,K_1}, *according to the ordering, then* $\mathbf{A}(Q^I)$ *contains* $a_{I,K}Q^{K_1}$; $< d^{K_1'}, \mathbf{A}(Q^I) >= a_{I,K_1} = b_{I,K_1}$. *Proceed to the next sequence* K_2 *and use* b_{I,K_2} *(whether or not is zero) and the dual of* $d^{K_2'}$ *to compute the coefficient* a_{I,K_2} *of* Q^{K_2} *in* $\mathbf{A}(Q^I)$. *Repeat last step for all remaining sequences.*

References

[1] F. Cohen, T. Lada, and J. P. May, **The homology of iterated loop spaces.** LNM 533, (1975).

[2] L. E. Dickson, *A fundamental system of invariants of the general modular linear group with a solution of the form problem.* Trans. A. M. S. **12** (1911), 75-98.

[3] Nondas E. Kechagias, *Extended Dyer-Lashof algebras and modular coinvariants.* Manuscripta Math. 84, 1994 pp. 261-290.

[4] Huyhn Mui, *Modular invariant theory and the cohomology algebras of the symmetric groups*, J. Fac. Sci. Univ. Tokyo, **IA** (1975), 319-369.

E-MAIL: NKECHAG@CC.UOI.GR