PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, 0000

ON CONJUGATION INVARIANTS IN THE DUAL STEENROD ALGEBRA

M. D. CROSSLEY AND SARAH WHITEHOUSE

Abstract. We investigate the canonical conjugation, χ, of the mod 2 dual Steenrod algebra, $\mathcal{A}_*$, with a view to determining the subspace, $\mathcal{A}_*^\chi$, of elements invariant under χ. We give bounds on the dimension of this subspace for each degree and show that, after inverting ξ_1, it becomes polynomial on a natural set of generators. Finally we note that, without inverting ξ_1, $\mathcal{A}_*^\chi$ is far from being polynomial.

1. Introduction.

The mod 2 dual Steenrod algebra, $\mathcal{A}_*$, being a connected commutative Hopf algebra, has a canonical conjugation or anti-automorphism χ. This map was first studied by Thom [T] but most of what we know today about χ is due to Milnor [M]. Our aim is to study the subspace of $\mathcal{A}_*$ consisting of elements invariant under this conjugation map; we denote this subspace by $\mathcal{A}_*^\chi$. While we are unable to give a complete description of $\mathcal{A}_*^\chi$, we have established bounds on its dimension in each degree (Theorem 3.1) and we can show that, after inverting the element $\xi_1 \in \mathcal{A}_*$, the invariant subspace becomes polynomial (Theorem 4.1). Finally, our investigations have also led us to construct a large number of indecomposables in $\mathcal{A}_*^\chi$ (section 5).

We begin by recalling the structure of $\mathcal{A}_*$ and certain well known facts about the map χ, while in section 2 we deduce some elementary properties of χ. In section 3 we derive our bounds on the dimension of the subspace of invariants and in section 4 we study the result of inverting ξ_1. The final section discusses multiplicative generators for the invariants.

The structure of the Hopf algebra $\mathcal{A}_*$ was determined by Milnor [M]. As an algebra, $\mathcal{A}_* = \mathbb{F}_2[\xi_1, \xi_2, \xi_3, \dots]$, where the degree of ξ_i is $2^i - 1$. The coproduct ϕ is determined by the formula

$$\phi(\xi_k) = \sum_{i=0}^{k} \xi_{k-i}^{2^i} \otimes \xi_i \,,$$

where ξ_0 is interpreted as 1.

From [MM] we know that any connected Hopf algebra, H, has a unique bijective linear map, $\chi : H \to H$, called the 'conjugation', with the following properties:
1) $\chi(1) = 1$,
2) $\chi(xy) = \chi(y)\chi(x)$ (i.e. χ is an anti-automorphism),

Received by the editors 16 October 1998.
1991 *Mathematics Subject Classification.* 55S10, 20J06, 20C30.

3) If $\phi(a) = \sum a'_i \otimes a''_i$ where $a \in H^+$ (i.e. $\deg a > 0$), then $\sum a'_i \chi(a''_i) = 0$.

(Since the coproduct ϕ always satisfies the identity $\phi(a) \equiv a \otimes 1 + 1 \otimes a \bmod H^+ \otimes H^+$, the last property determines χ inductively.)

Furthermore, if the Hopf algebra is either commutative or cocommutative, then χ^2 is the identity homomorphism.

In the case of the dual Steenrod algebra, property 3 leads inductively to the following formula for χ (Lemma 10 of [M]).

1.1 Lemma. *In the dual Steenrod algebra $\mathcal{A}_*$,*

$$\chi(\xi_n) = \sum_{\alpha \in Part(n)} \prod_{i=1}^{l(\alpha)} \xi_{\alpha(i)}^{2^{\sigma(i)}} \ ,$$

where $Part(n)$ denotes the set of all ordered partitions of n; and for a given ordered partition $\alpha = (\alpha(1) \,|\, \alpha(2) \,|\, \ldots \,|\, \alpha(l)) \in Part(n)$, $\sigma(i)$ denotes the partial sum $\sum_{j=1}^{i-1} \alpha(j)$. □

This lemma enables us to determine χ on an arbitrary element of $\mathcal{A}_*$, by virtue of multiplicativity (which follows from property 2 since $\mathcal{A}_*$ is commutative) and linearity.

We end this introduction with a few comments on motivation for the problems discussed in this paper. Expressions like $H^m(\Sigma_n, \pi_*(E^{\wedge n}))$ arise in spectral sequences for gamma cohomology of an E_∞-ring spectrum E [RW]. For E suitably nice, this is $H^m(\Sigma_n, (E_*E)^{\otimes(n-1)})$, the Σ_n action here being described in [W]; for $n = 2$, Σ_2 acts by the usual conjugation on E_*E. This paper is therefore concerned with the very special case of this problem where $E = H\mathbb{F}_2$ and $n = 2$. Note that this application requires the whole cohomology $H^*(\Sigma_2; \mathcal{A}_*)$ not just the zero degree part $H^0(\Sigma_2; \mathcal{A}_*) = \mathcal{A}_*^\chi$. With this in mind we shall occasionally comment on the higher cohomology groups although the main concern of this paper is $\mathcal{A}_*^\chi$.

2. Elementary Properties of conjugation.

Now we make some elementary observations on the properties of the conjugation χ. For a connected Hopf algebra $\mathcal{H}$, we denote by $\mathcal{H}^\chi$ the invariant elements of $\mathcal{H}$ under the conjugation map $\chi : \mathcal{H} \to \mathcal{H}$. The identity homomorphism will be denoted by 1, so that $\mathcal{H}^\chi = \mathrm{Ker}(\chi - 1)$.

2.1 Lemma. *If $\mathcal{H}$ is commutative, $\mathcal{H}^\chi$ is a subalgebra of $\mathcal{H}$.*

Proof. The conjugation χ is always an anti-automorphism. So, when $\mathcal{H}$ is commutative, it is a homomorphism of algebras. □

We denote by $\mathcal{H}_d$ the degree d part of a graded object (e.g. Hopf algebra) $\mathcal{H}$.

2.2 Lemma. *If $\mathcal{H}$ is a commutative or cocommutative Hopf algebra over $\mathbb{F}_2$, then* $\dim \mathcal{H}_d^\chi \geq \dim \mathcal{H}_d/2$.

Proof. We have $\chi^2 = 1$ by the (co)commutativity hypothesis. Since we are working over $\mathbb{F}_2$, this gives $(\chi - 1)^2 = 0$, and so $\mathrm{Im}(\chi - 1) \subset \mathrm{Ker}(\chi - 1)$. Since $\dim \mathcal{H}_d = \dim(\mathrm{Im}(\chi - 1)_d) + \dim(\mathrm{Ker}(\chi - 1)_d)$, we have the result. □

2.3 Remark. In the case of the mod 2 (dual) Steenrod algebra, the above dimension constraint is sharp in low degrees, although not in general. It first fails in degree 42. More details are in section 3, particularly Example 3.4.

2.4 Lemma. *In a commutative Hopf algebra $\mathcal{H}$ over $\mathbb{F}_2$,* $\mathrm{Im}(\chi-1)$ *is an ideal in* $\mathrm{Ker}(\chi-1)$. *In particular,* $\mathrm{Im}(\chi-1)$ *is a subalgebra of $\mathcal{H}$.*

Proof. Let $x \in \mathrm{Ker}(\chi-1)$. Then $x(\chi(y)-y) = x\chi(y) - xy = \chi(x)\chi(y) - xy = (\chi-1)(xy)$. The second part can be proved directly: $(\chi(x)-x)(\chi(y)-y) = \chi(z)-z$ mod 2, where $z = xy + x\chi(y)$. □

2.5 Remark. In this situation, the assertion of Lemma 2.1 that $H^0(\Sigma_2;\mathcal{H}) = \mathcal{H}^\chi = \mathrm{Ker}(\chi-1)$ has the structure of an algebra extends to the higher cohomology: $H^n(\Sigma_2;\mathcal{H}) = \mathrm{Ker}(\chi-1)/\mathrm{Im}(\chi-1)$ for $n>0$ (where Σ_2 acts on $\mathcal{H}$ by conjugation) also has an algebra structure.

We now fix our attention on the dual Steenrod algebra, $\mathcal{A}_* = \mathbb{F}_2[\xi_1,\xi_2,\ldots]$, using the notation $(r_1,r_2,\ldots,r_k)$ to denote the monomial $\xi_1^{r_1}\xi_2^{r_2}\ldots\xi_k^{r_k}$. We shall frequently need to order the monomials of a given degree in $\mathcal{A}_*$ and the right lexicographic ordering turns out to be the most useful.

The following unitriangularity property is fundamental and will be used many times without comment.

2.6 Proposition. *With respect to right lexicographic ordering of the monomial basis, the matrix of the conjugation map in each degree, $\chi : (\mathcal{A}_*)_d \to (\mathcal{A}_*)_d$, is unitriangular.*

Proof. It follows from Lemma 1.1 that $\chi(\xi_k) = \xi_k + P_k$ where P_k is a polynomial in $\xi_1,\ldots,\xi_{k-1}$ and hence strictly lower than ξ_k. Consequently for any monomial M in $\xi_1,\ldots,\xi_k$, we have that $\chi(M) = M + Q$ where Q is strictly lower than M. This is because the right lexicographic ordering has the property that if $x<x'$ and $y \le y'$ then $xy < x'y'$. It then follows that the matrix is unitriangular. □

2.7 Remark. This unitriangularity property also holds for certain other orderings. A simple example is left lexicographic ordering. More interestingly, if we define the weight w of the monomial $(r_1,\ldots,r_k)$ to be $r_1+r_2+\cdots+r_k$ then we may obtain further orderings by combining weight and lexicographic orderings. For example, the 'weight/reverse-left lex' order is defined by $a \prec b$ if either $w(a) < w(b)$ or $w(a) = w(b)$ and a *follows* b in left lexicographic ordering. For all such orderings the above proof can be easily modified. In fact, all the proof needs is that for all k, $(\chi-1)(\xi_k)$ is strictly lower than ξ_k (or that $(\chi-1)(\xi_k)$ is always strictly higher) and that the ordering is 'multiplicative', i.e. $x \le x'$ and $y \le y'$ implies that $xy \le x'y'$.

3. Bounds on dimension.

In this section we state and prove the following theorem which gives bounds on the dimension of the invariant subspace $\mathcal{A}_*^\chi$ in a given degree.

3.1 Theorem. *Let the dimension of the (dual) Steenrod algebra in degree d be denoted D_d. Then $D_{d-1}/2 \le \dim((\chi-1)\mathcal{A}_*)_d \le D_d/2$ and hence*

$$D_d/2 \le \dim(\mathcal{A}_*^\chi)_d \le D_d - (D_{d-1}/2)\,.$$

In fact the upper bound on $\dim(\mathcal{A}_*^\chi)_d$ can be improved upon - see Lemma 3.3 and Example 3.4.

The lower bound on $\dim(\mathcal{A}_*^\chi)_d$ was given by Lemma 2.2; the rest of the theorem is a combinatorial corollary of the following proposition. Let a monomial $(r_1, r_2, \ldots, r_k)$ (i.e. $\xi_1^{r_1}\xi_2^{r_2}\ldots\xi_k^{r_k}$) be called 'uniterminal' if $r_k = 1$.

3.2 Proposition. *In $(\mathcal{A}_*)_d$, the uniterminal monomials have linearly independent images under $\chi - 1$.*

Proof. We use right lexicographic ordering and claim that the lowest uniterminal monomial which has $(r_1+1, r_2, \ldots, r_{k-2}, r_{k-1}+2)$ as a summand in its image under $\chi-1$ is $(r_1, \ldots, r_{k-1}, 1)$. Assuming this claim we argue as follows. Let Q be a linear combination of images under $\chi-1$ of uniterminal monomials. So we may write Q as $Q = (\chi-1)(P)$ where P is a linear combination of uniterminal monomials. Suppose that $(r_1, \ldots, r_{k-1}, 1)$ is the highest monomial which appears in P. Then our claim shows that $(\chi-1)(P)$ will have $(r_1+1, r_2, \ldots, r_{k-2}, r_{k-1}+2)$ as a summand, and so cannot be zero. The proposition then follows.

Now to prove the claim. From Lemma 1.1,

$$\chi(\xi_k) = \xi_k + \xi_{k-1}^2\xi_1 + \xi_{k-1}\xi_1^{2^{k-1}} + P_{k-2}\,,$$

where P_{k-2} is some polynomial in $\xi_1, \ldots, \xi_{k-2}$. Looking at the second term on the right hand side of the above expression, we see that the largest monomial in $(\chi-1)(r_1, \ldots, r_{k-1}, 1)$ which does not contain a ξ_k is $(r_1+1, r_2, \ldots, r_{k-2}, r_{k-1}+2)$.

Now we need to see that no earlier uniterminal monomial has this term in its image under $\chi - 1$. Suppose it does appear in the image of $(j_1, \ldots, j_{k'-1}, 1)$, with $(j_1, \ldots, j_{k'-1}, 1) < (r_1, \ldots, r_{k-1}, 1)$ so, in particular, $k' \leq k$. If $k' \leq k-1$ then by 2.6 $(\chi-1)(j_1, \ldots, j_{k'-1}, 1)$ will have no summands with ξ_{k-1}-exponent greater than 1, so cannot have $(r_1+1, r_2, \ldots, r_{k-1}+2)$ as a summand. If $k' = k$ then the fact that $(j_1, \ldots, j_{k'-1}, 1) < (r_1, \ldots, r_{k-1}, 1)$ implies that $(j_1+1, j_2, \ldots, j_{k-1}+2) < (r_1+1, r_2, \ldots, r_{k-1}+2)$. In this case, the image of $(j_1, \ldots, j_{k'-1}, 1)$ cannot contain $(r_1+1, r_2, \ldots, r_{k-1}+2)$ as a summand. □

So $\dim((\chi-1)\mathcal{A}_*)_d \geq R_d$ where R_d is the number of uniterminal monomials in degree d. In order to complete the proof of Theorem 3.1 we now obtain some information about R_d.

3.3 Lemma.
1) $R_d \geq D_{d-1}/2$,
2) $R_d = D_{d-1} - R_{d-1}$.

Proof. We pair up each uniterminal monomial in degree d with another degree d monomial that is not uniterminal by the pairing

$$(r_1, r_2 \ldots, r_{k-2}, r_{k-1}, 1) \longleftrightarrow (r_1+1, r_2, \ldots, r_{k-2}, r_{k-1}+2)\,.$$

The monomials left unpaired are characterized by the fact that they begin with zero and are not uniterminal. The number of these is clearly less than or equal to the total number beginning with zero, which is $D_d - D_{d-1}$. This gives the first claim. The actual number unpaired is given by $(D_d - D_{d-1}) - (R_d - R_{d-1})$, since the number of uniterminal monomials starting with zero in degree d is $R_d - R_{d-1}$. This gives the second part. □

Note that this gives a recursive formula for the R_d's in terms of the D_d's. Alternatively, letting P^i be the polynomial algebra $\mathbb{F}_2[\xi_1, \ldots, \xi_i]$ ($P^0 = \mathbb{F}_2$), it is clear that $R_d = \sum_i \dim(P^{i-1})$

3.4 Example. In degree 42, $\mathcal{A}_*$ has dimension 92. The number of uniterminal monomials, R_{42}, is 44 while D_{41} is 86. So the bounds in Theorem 3.1 tell us that $46 \leq \dim(\mathcal{A}_*^\chi)_{42} \leq 49$. If we are prepared to put in more effort (calculating R_d precisely) then we obtain a sharper upper bound of 48. Further effort (consulting the matrix of $\chi - 1$) shows the actual dimension of the χ invariants to be 47. Note also that the lower bound here is not sharp; in fact 42 is the first degree in which this happens.

4. Conjugation invariants with ξ_1 inverted.

In this section we adjoin a formal inverse to ξ_1, denoting the resulting object by $\mathcal{A}_*[\xi_1^{-1}]$. This is regarded as containing $\mathcal{A}_*$ in the usual way. Since ξ_1 is invariant, $\mathcal{A}_*[\xi_1^{-1}]$ inherits an action of χ and the subspace of invariants turns out to be much more manageable. In fact we show (Theorem 4.1) that it is a polynomial ring on certain natural invariant elements, $\epsilon_2, \epsilon_3, \cdots$. Clearly $\mathcal{A}_*^\chi$ is the intersection of $\mathcal{A}_*$ and $\mathcal{A}_*[\xi_1^{-1}]^\chi$. So one might conclude that, since we have simple descriptions of $\mathcal{A}_*$ and $\mathcal{A}_*[\xi_1^{-1}]^\chi$, we can easily obtain a description of $\mathcal{A}_*^\chi$. However, this turns out to be far from the case - the problem of finding the highest power of ξ_1 dividing a given polynomial in $\xi_1, \epsilon_2, \epsilon_3, \cdots$ seems to be difficult in general. In fact, low degree calculations quickly reveal that the algebra $\mathcal{A}_*^\chi$ is complicated; in particular it is far from being polynomial.

At the end of this section we show how Theorem 4.1 generalizes nicely to give a description of the invariants of $(\mathcal{A}_*/\langle \xi_1, \dots, \xi_{n-1}\rangle)[\xi_n^{-1}]$.

Note that $\mathcal{A}_*[\xi_1^{-1}]^\chi = \mathcal{A}_*^\chi[\xi_1^{-1}]$. That is to say, if we adjoin ξ_1^{-1} to the ring $\mathcal{A}_*^\chi$, we obtain the same object as if we take the χ-invariants of the ring $\mathcal{A}_*[\xi_1^{-1}]$.

4.1 Theorem. *Let $k = \mathbb{F}_2[\xi_1, \xi_1^{-1}]$. Then*

$$\mathcal{A}_*^\chi[\xi_1^{-1}] = k[\epsilon_2, \epsilon_3, \dots]\,,$$

where $\epsilon_2 = \xi_2\chi(\xi_2)$ and, for $n \geq 3$, $\epsilon_n = \xi_2\xi_n + \chi(\xi_2\xi_n)$. Furthermore

$$H^i(\Sigma_2; \mathcal{A}_*[\xi_1^{-1}]) = 0 \qquad \text{for } i > 0\,.$$

The proof of the second statement is straightforward : in $\mathcal{A}_*$ we have $(\chi-1)\xi_2 = \xi_1^3$. It follows that in $\mathcal{A}_*[\xi_1^{-1}]$, 1 is the image under $\chi - 1$ of $\xi_1^{-3}\xi_2$. But $\mathrm{Im}(\chi - 1)$ is an ideal in $\mathrm{Ker}(\chi - 1)$ and so, since $1 \in \mathrm{Im}(\chi - 1)$, these two objects must be equal.

Now we consider the first statement. It is evident that the elements ϵ_n are invariant and we claim that they are also algebraically independent. This follows from the fact that, for each $n \geq 2$, ϵ_n has a summand involving ξ_n, whereas $\epsilon_2, \dots, \epsilon_{n-1}$ have no such summands. (The highest right lexicographic monomial of ϵ_n is $\xi_1^3\xi_n$ if $n \geq 3$ and ξ_2^2 if $n = 2$.) Thus, since the invariants form a subalgebra, $k[\epsilon_2, \epsilon_3, \dots] \subset \mathcal{A}_*^\chi[\xi_1^{-1}]$. The opposite inclusion will follow directly from Proposition 4.3.

4.2 Proposition.

1) *Consider a monomial $(r_1, r_2, \dots, r_k)$. If r_2 is odd then the image of this monomial under $\chi - 1$ cannot be expressed as the image under $\chi - 1$ of a linear combination of lower monomials.*

2) Let $x \in \mathcal{A}_*$ be invariant and let $(r_1, r_2, \dots, r_k)$ be the highest monomial appearing in x. Then r_2 is even.

Proof. We claim that, if r_2 is odd, then the monomial $(r_1, r_2, r_3, \dots, r_k)$ is the first to have $(r_1 + 3, r_2 - 1, r_3, \dots, r_k)$ as a summand of its image under $\chi - 1$. Firstly, these two monomials are adjacent in the right lexicographic ordering, so by 2.6, $(r_1, r_2, r_3, \dots, r_k)$ is the lowest monomial whose image can contain $(r_1 + 3, r_2 - 1, r_3, \dots, r_k)$. Secondly,

$$\begin{aligned}\chi(r_1, r_2, r_3, \dots, r_k) &= \chi(r_1, 0, r_3, \dots, r_k)\chi(\xi_2)^{r_2} \\ &= \chi(r_1, 0, r_3, \dots, r_k)(\xi_2 + \xi_1^3)^{r_2} \quad .\end{aligned}$$

From this, and the fact that $\binom{r_2}{1} \equiv 1 \bmod 2$, it is clear that $(\chi-1)(r_1, r_2, r_3, \dots, r_k)$ does contain a summand $(r_1 + 3, r_2 - 1, r_3, \dots, r_k)$. (Comparison of exponents of $\xi_k, \xi_{k-1}, \dots, \xi_3$ shows that this term cannot arise in any other way.)

The second part follows from the first, for suppose x is invariant, that is $(\chi - 1)(x) = 0$, with highest monomial $(r_1, r_2, \dots, r_k)$. Then $(\chi - 1)(r_1, r_2, \dots, r_k)$ can be expressed as the image under $\chi - 1$ of a linear combination of lower monomials, namely $x - (r_1, r_2, \dots, r_k)$. If r_2 is odd then this contradicts the first part. □

4.3 Proposition. *If $x \in \mathcal{A}_*^\chi$ then there exists some integer $s \geq 0$ such that $\xi_1^s x \in \mathbb{F}_2[\xi_1, \epsilon_2, \epsilon_3, \dots]$.*

Proof. We prove the proposition by a recursion on a well-founded ordering. This will require us to compare monomials and polynomials of different degrees. We do this by using the right lexicographic ordering as a total ordering on *all* monomials (elsewhere we use right lexicographic ordering only to compare monomials of the same degree). Having ordered the monomials, we derive an ordering on polynomials as follows. First compare their highest monomials; if these are equal then compare their next highest monomials and so on. So, for example, the monomial $(4, 5, 1)$ is less than $(1, 0, 0, 1)$, despite the former having a higher degree, and $(1, 6, 0, 1) + (4, 5, 1) + (21, 1)$ is less than $(1, 6, 0, 1) + (1, 0, 0, 1) + (24)$. It is easy to see that this ordering is well-founded, by which we mean that any non-empty set of polynomials has a minimal element. We then claim that, whenever x is such that the proposition is true for all x' less than x, it is true for x. This claim implies the proposition : if the set of elements for which the proposition is false is non-empty then this set will have a least element whose existence contradicts the claim.

We now prove the claim. Let $l = (r_1, r_2, \dots, r_k)$ be the leading monomial of x. By 4.2, r_2 is even. Let $z = \xi_1^{r_1}\epsilon_2^{r_2/2}\epsilon_3^{r_3} \dots \epsilon_k^{r_k}$. Recalling the definition of the ϵ_n's, we see that the leading monomial in z is $\xi_1^{r_1+t}\xi_2^{r_2}\xi_3^{r_3} \dots \xi_k^{r_k}$, where $t = 3(r_3 + r_4 + \dots + r_k)$. This is the leading term of $\xi_1^t x$ and we set $x' = \xi_1^t x + z$, noting that this is invariant, as it is the sum of two invariants. Since the leading monomial of z is equal to that of $\xi_1^t x$, the leading term of x' will be strictly lower. Thus x' is less than x and, by the hypothesis of the claim, the proposition is true for x', say $\xi_1^s x' \in \mathbb{F}_2[\xi_1, \epsilon_2, \epsilon_3, \dots]$. Then $\xi_1^{s+t} x = \xi_1^s x' + \xi_1^s z$ is also in $\mathbb{F}_2[\xi_1, \epsilon_2, \epsilon_3, \dots]$ and the claim is proved. □

4.4 Remark. The only properties of ϵ_n used in the proof are that ϵ_n is invariant and has a certain highest term. In particular we could replace ϵ_2 by $\tilde{\epsilon}_2 = (\chi -$

inverted, since $\tilde{\epsilon}_2 \in \mathrm{Im}(\chi - 1)$ and $\epsilon_n \in \mathrm{Im}(\chi - 1)$ for all $n \geq 3$ and we can re-run the whole programme of the proof of 4.3 with '$\mathrm{Im}(\chi - 1)$' in place of '$\mathrm{Ker}(\chi - 1)$'.

Now we mention a generalization of Theorem 4.1. We consider the situation where we kill off the first $n-1$ generators, $\xi_1, \ldots, \xi_{n-1}$ of $\mathcal{A}_*$ and invert the n-th generator : let $\mathcal{A}_*\langle n \rangle$ denote $(\mathcal{A}_*/\langle \xi_1, \ldots, \xi_{n-1} \rangle)[\xi_n^{-1}]$, where $\langle \xi_1, \ldots, \xi_{n-1} \rangle$ is the ideal generated by $\xi_1, \ldots, \xi_{n-1}$. Note that ξ_n is invariant in $\mathcal{A}_*/\langle \xi_1, \ldots, \xi_{n-1} \rangle$, so $\mathcal{A}_*\langle n \rangle$ inherits a well defined map χ. (In fact, $\xi_n, \xi_{n+1} \ldots \xi_{2n-1}$ are all invariant.)

4.5 Theorem. *Let $k = \mathbb{F}_2[\xi_n, \xi_n^{-1}]$. Then*

$$\mathcal{A}_*\langle n \rangle^\chi = k[\epsilon\langle n \rangle_{n+1}, \epsilon\langle n \rangle_{n+2}, \ldots],$$

where $\epsilon\langle n \rangle_m = \xi_{2n}\xi_m + \chi(\xi_{2n}\xi_m)$ if $m \neq 2n$ and $\epsilon\langle n \rangle_{2n} = \xi_{2n}\chi(\xi_{2n})$. Furthermore

$$H^i(\Sigma_2; \mathcal{A}_*\langle n \rangle) = 0 \qquad \text{for } i > 0\,.$$

The proof of this result is entirely analogous to that of Theorem 4.1. For the second part, it is sufficient to note that the image under $\chi - 1$ of ξ_{2n} is $\xi_n^{2^n+1}$ (modulo $\xi_1, \ldots, \xi_{n-1}$). For the first part, one observes that the $\epsilon\langle n \rangle_m$'s are all invariant and algebraically independent and so $k[\epsilon\langle n \rangle_{n+1}, \epsilon\langle n \rangle_{n+2}, \ldots] \subset \mathcal{A}_*\langle n \rangle^\chi$. Then one shows that if $\theta = \xi_{n+1}^{e_{n+1}} \xi_{n+2}^{e_{n+2}} \ldots \xi_k^{e_k}$ where e_{2n} is even, then there exists an r such that $\xi_n^r \theta$ can be expressed as the leading term of a monomial in the $\epsilon\langle n \rangle_m$'s (modulo $\xi_1, \ldots, \xi_{n-1}$). Using this, one runs through the recursion argument of Proposition 4.3 with the following lemma in place of Proposition 4.2.

4.6 Lemma. *If θ is the leading term of a polynomial in $\mathcal{A}_*/\langle \xi_1, \ldots, \xi_{n-1} \rangle$ which is invariant then the exponent of ξ_{2n} in θ is even.*

The argument is broadly the same as that of Proposition 4.2 : if the exponent of ξ_{2n} in θ is odd then $(\chi - 1)\theta$ contains the summand $\xi_n^{2^n+1}\xi_{2n}^{-1}\theta$ and one checks that there cannot exist any monomial θ' less than θ such that $(\chi - 1)\theta'$ also contains this summand.

5. Some generators.

A natural question to ask is : what is the lowest degree in which we can find an invariant polynomial which involves ξ_n ? For $n = 1$, ξ_1 itself is invariant so the answer is 1. For $n = 2$ one can see that it is 6, since, for example, $\epsilon_2 = \xi_2\chi(\xi_2)$ is invariant. For $n \geq 3$ one might guess that $\epsilon_n = (\chi - 1)(\xi_2\xi_n)$ had the lowest degree among invariants involving ξ_n, yielding the answer $2^n + 2$. However, we shall see that, at least for $n \leq 7$, we can find an invariant in degree $2^n + 1$ with a summand $\xi_1^2\xi_n$. The following lemma implies that no lower degree invariants involve ξ_n.

5.1 Lemma. *The monomials ξ_n and $\xi_1\xi_n$ are not summands of any invariant elements.*

Proof. The image of ξ_n under $\chi - 1$ contains the monomial $\xi_1\xi_{n-1}^2$, which immediately precedes ξ_n in the right lexicographic ordering. Since ξ_n is the highest monomial in its degree, nothing else can have this monomial $\xi_1\xi_{n-1}^2$ in its image. Hence ξ_n cannot be a summand of an invariant polynomial (c.f. the proof of Proposition 4.2). Similarly, $\xi_1\xi_n$ has $\xi_1^2\xi_{n-1}^2$ in its image and is the only monomial which does so. □

However, the above argument cannot be applied to $\xi_1^2\xi_n$. The highest term in its image is $\xi_1^3\xi_{n-1}^2$, but this does not immediately precede $\xi_1^2\xi_n$ in the ordering - $\xi_2\xi_{n-1}^2$ occurs between them and is seen to also have $\xi_1^3\xi_{n-1}^2$ in its image. In fact $\xi_1^2\xi_n$ *is* a summand (and necessarily the leading term) of an invariant for small n and we make the following

5.2 Conjecture. *For each $n \geq 3$, there exists a polynomial d_n in degree $2^n + 1$, invariant under χ and with leading term $\xi_1^2\xi_n$.*

We have been able to construct such elements for $n = 3, 4, 5, 6, 7$. We describe below one particular choice of such elements but first we need some more notation.

Notation. *We define certain elements of $\mathcal{A}_*$, which are evidently invariant.*

$$a_n = \xi_n\chi(\xi_n)\,,$$
$$b_{m_1,m_2,\ldots,m_n} = (\chi - 1)(\xi_{m_1}\xi_{m_2}\ldots\xi_{m_n})\,.$$

The following elements are examples of the d_n's of Conjecture 5.2.

$$\begin{aligned}
d_3 &= b_{2,3}/\xi_1\,,\\
d_4 &= (b_{2,4} + a_2^3)/\xi_1\,,\\
d_5 &= (b_{2,5} + a_2a_3^2 + a_2^2b_{3,4})/\xi_1\,,\\
d_6 &= (b_{2,6} + a_2a_4^2 + a_3^2b_{3,5} + a_2^6a_4 + a_2^4a_3^3 + a_2^{11})/\xi_1\,,\\
d_7 &= (b_{2,7} + a_2a_5^2 + a_4^2b_{3,6} + a_2^2a_3^4a_5 + a_2^9a_3a_5 + a_3^6b_{4,5} + a_2^7a_3^3b_{4,5} + a_2^{14}b_{4,5}\\
&\qquad + a_2^3a_3^4b_{2,3,4,5} + a_2^{10}a_3b_{2,3,4,5} + a_2^3a_4^3b_{3,4} + a_2^{13}a_4b_{3,4} + a_3^5a_4^2 + a_2^{17}a_3^2)/\xi_1\,.
\end{aligned}$$

Note that the above expressions are all quotients by ξ_1 of some sum starting with $b_{2,n}$. In fact a conjecture equivalent to 5.2 is

5.2' Conjecture. *For each $n \geq 3$, there exists an invariant polynomial x_n, not equal to $b_{2,n}$, but such that*

$$x_n \equiv b_{2,n} \bmod \langle\xi_1\rangle\,,$$

where $\langle\xi_1\rangle$ denotes the ideal generated by ξ_1.

We would then obtain d_n by setting $d_n = (b_{2,n} + x_n)/\xi_1$. (The invariance of x_n implies that of d_n since a quotient of one invariant by another is invariant.) Note that we refer to "d_n" rather than "a choice of d_n" because all choices are easily seen to be equivalent modulo invariants in $\xi_1, \cdots, \xi_{n-1}$.

The importance of these elements d_n is that they are indecomposable and hence necessary members of any set of multiplicative generators for $\mathcal{A}_*^\chi$. To prove that they are indecomposable, suppose the converse. Then it would be possible to express the summand $\xi_1^2\xi_n$ as a non-trivial product of two elements which occur as summands in invariant elements. Lemma 5.1 states that this is not the case.

The same argument can be used to show that the elements a_n for $n \geq 2$ are indecomposable too; one considers the summand ξ_n^2. We can also show that 'most' of the elements $b_{m_1,m_2,\ldots,m_n}$ are indecomposable. However, in order to do this we need a lemma.

5.3 Lemma.
1) The monomial $\xi_{n_1}\dots\xi_{n_k}$ where $k\geq 2$ and $1\leq n_1<\dots<n_k$ is not a summand of any invariant polynomial.
2) The monomial $\xi_{n_1}^2\xi_{n_2}\dots\xi_{n_k}$ is not a summand of any invariant polynomial if $n_1+1<n_2<n_3<\dots<n_k$ and either $n_1>1$ or $k>2$.

Proof. The proof of the first part is just a generalization of that of Lemma 5.1. One sees easily that any monomial $\xi_{n_1}\dots\xi_{n_k}$, where $k\geq 2$ and $1\leq n_1<\dots<n_k$, is the highest monomial in its degree with respect to right lexicographic ordering. The image under $\chi-1$ of this monomial has leading term $\xi_1\xi_{n_1-1}^2\xi_{n_2}\dots\xi_{n_k}$ if $n_1>1$ and $\xi_1^2\xi_{n_2-1}^2\xi_{n_3}\dots\xi_{n_k}$ if $n_1=1$. In either case the leading term immediately precedes $\xi_{n_1}\dots\xi_{n_k}$ and hence cannot occur in the image of any other monomial.

For the second part, we consider the cases $k=2$ and $k>2$ separately. In both cases the argument is similar to the one above, but two steps are required.

Suppose $k=2$. Firstly, by considering the partition $(1\,|\,n_2-1)$ of n_2, we see that the image under $\chi-1$ of the monomial $\xi_{n_1}^2\xi_{n_2}$ has $\xi_1\xi_{n_1}^2\xi_{n_2-1}^2$ as a summand. The only other monomial which has this summand in its image is $\xi_{n_1+1}\xi_{n_2-1}^2$. Thus any invariant element which has $\xi_{n_1}^2\xi_{n_2}$ as a summand must also have a summand $\xi_{n_1+1}\xi_{n_2-1}^2$. Secondly, provided $n_1>1$, we can consider the partition $(2\,|\,n_1-1)$ of n_1+1 to see that the latter monomial has $\xi_2\xi_{n_1-1}^4\xi_{n_2-1}^2$ as a summand of its image. One can see that this cannot occur as a summand in the image of any other monomial, hence, for $n_1>1$, there is no invariant with $\xi_{n_1}^2\xi_{n_2}$ as a summand.

Now let $k>2$. By considering the partition $(1\,|\,n_2-1)$ of n_2, we see that the image under $\chi-1$ of the monomial $\xi_{n_1}^2\xi_{n_2}\dots\xi_{n_k}$ has $\xi_1\xi_{n_1}^2\xi_{n_2-1}^2\xi_{n_3}\dots\xi_{n_k}$ as a summand. If $n_1+1<n_2$ then the monomial $\xi_{n_1+1}\xi_{n_2-1}^2\xi_{n_3}\dots\xi_{n_k}$ will also have this as a summand in its image and will be the only other monomial that does. Thus any invariant element with a summand $\xi_{n_1}^2\xi_{n_2}\dots\xi_{n_k}$ must also have a summand $\xi_{n_1+1}\xi_{n_2-1}^2\xi_{n_3}\dots\xi_{n_k}$. Now, considering the partition $(2\,|\,n_k-2)$ of n_k, we see that the latter monomial has $\xi_2\xi_{n_1+1}\xi_{n_2-1}^2\xi_{n_3}\dots\xi_{n_{k-1}}\xi_{n_k-2}^4$ as a summand of its image and again one checks that no other monomial has this in its image. Thus $\xi_{n_1}^2\xi_{n_2}\dots\xi_{n_k}$ cannot be a summand of an invariant polynomial. □

5.4 Proposition. *The element $b_{m_1,m_2,\cdots,m_n}$ is indecomposable if either $2<m_1<\dots<m_n$ and $n\geq 2$ or $2\leq m_1<m_2<\dots<m_n$ and $n>2$. Furthermore, if $n\geq 3$ is such that d_n does not exist then $b_{2,n}$ is indecomposable.*

Proof. Suppose $m_1,\cdots,m_n$ satisfy the above conditions. Then the leading term of $b_{m_1,m_2,\cdots,m_n}$ is either $\xi_1^3\xi_{m_2}\dots\xi_{m_n}$ if $m_1=2$ or $\xi_1\xi_{m_1-1}^2\xi_{m_2}\dots\xi_{m_n}$ if $m_1>2$. Any attempt to write either of these terms as a non-trivial product of monomials will involve at least one factor which, by Lemma 5.1 or Lemma 5.3, cannot occur as a summand of an invariant polynomial. Hence $b_{m_1,m_2,\dots,m_n}$ cannot be decomposable. Finally, if d_n does not exist then $\xi_1^3\xi_n$, the leading term of $b_{2,n}$, cannot be written as a non-trivial product of summands of invariants and $b_{2,n}$ must be indecomposable.□

Now note that the $b_{*\dots*}$ family alone provides $\mathcal{A}_*^\chi$ with far too many generators for it to be polynomial (by transcendence degree considerations).

These three families a_*, $b_{*\dots*}$, d_*, together with ξ_1, are actually sufficient generators up to degree 48. However, in degree 49 a new generator is necessary and our guess is that this is the first of a new infinite family, a generalization in some sense of the mysterious d_* family.

Acknowledgements

We would like to thank Lionel Schwartz and Neil Strickland for helpful conversations and we acknowledge the support of TMR grants from the European Union, held at the Laboratoire d'Analyse, Géométrie et Applications (UMR 7539 au CNRS), Université Paris-Nord.

References

[M] Milnor, John. *The Steenrod algebra and its dual*, Ann. Math., **67**, (1958), 150-171.

[MM] Milnor, J. and Moore, J. *On the structure of Hopf algebras*, Ann. Math., **81**, (1965), 211-264.

[RW] Robinson, Alan and Whitehouse, Sarah. Γ-*homology of commutative rings and of* E_∞*-ring spectra*, Warwick preprint 76/1995.

[T] Thom, R. *Quelques propriétés globales des variétés différentiables*, Comment. Math. Helv. **28**, (1954), 17-86.

[W] Whitehouse, Sarah. *Symmetric group actions on tensor products of Hopf algebroids*, in preparation.

Max-Planck-Institut für Mathematik, P.O. Box 7280, D-53072 Bonn, Germany.
E-mail address: crossley@member.ams.org

Département de Mathématiques, Université d'Artois - Pole de Lens, Rue Jean Souvraz, S. P. 18 - 63207 Lens, France.
E-mail address: whitehouse@poincare.univ-artois.fr