THE CONNER-FLOYD MAP FOR FORMAL A-MODULES

KEITH JOHNSON

ABSTRACT. A generalization of the Conner-Floyd map from complex co-bordism to complex K-theory is constructed for formal A-modules when A is the ring of algebraic integers in a number field or its p-adic completion. This map is employed to study the Adams-Novikov spectral sequence for formal A-modules and to confirm a conjecture of D. Ravenel.

0. Introduction. Let BP be the spectrum representing Brown-Peterson coho-mology with respect to a prime p and let E be the Adams summand of complex K-theory with respect to this prime. The BP version of the Conner-Floyd map is a map of spectra $\mathrm{BP} \to E$ which induces a natural equivalence

$$\mathrm{BP}_* X \otimes_{\mathrm{BP}_*} E_* \simeq E_* X.$$

In particular this induces an isomorphism

$$E_* \otimes_{\mathrm{BP}_*} \mathrm{BP}_* \mathrm{BP} \otimes_{\mathrm{BP}_*} E_* \simeq E_* E$$

and so provides a way of computing the Hopf algebra of stable co-operations for E from those for BP. Using this one can obtain a description of $E_* E$ similar to that for $K_* K$ contained in [**AHS**]. The study of BP and the computation of $\mathrm{BP}_* \mathrm{BP}$ are based on a study of formal group law, in particular the p-typical formal group law.

In [**R1**] Ravenel studied a generalization of this situation where the formal group law is replaced by a formal A-module where A is the ring of integers in an algebraic number field K or its p-adic completion. The purpose of the present paper is to describe the corresponding generalization of the map $(\mathrm{BP}_*, \mathrm{BP}_* \mathrm{BP}) \to (E_*, E_* E)$ induced by the Conner-Floyd map, and to compute the generalization of $E_* E$. This is of interest because it provides some information about a conjecture (3.10) made in [**R1**]. This conjecture concerned the value of a certain Ext group $\mathrm{Ext}_{V_A T}(V_A, V_A)$ when K is an extension of the field Q_p of p-adic numbers. Here $(V_A, V_A T)$ is the Hopf algebroid corresponding to the A-typical formal A module. This group was conjectured to be, up to small factor, $A/J^A_{n(q-1)}$. Here $J^A_{n(q-1)}$ is the ideal of A generated by the elements of the form $a^n - 1$ for units a of A congruent to $1 \bmod(\pi)$ and (π) is the unique prime ideal in A. We will show, using the generalization of the Conner-Floyd map, that $A/J^A_{n(q-1)}$ occurs as $E_1^{1,0}$ in the chromatic spectra sequence for formal A-modules [**R1**, Lemma 2.10] and that the small factor in the conjecture is contributed by the nontriviality of the differential d_1 originating from this group. We will analyze this differential and show that it is nonzero for A

the ring of integers in a totally ramified extension of degree a power of p, p^l, of the field obtained by adjoining pth roots of unity to Q_p, but zero for all other A (thus the small factor is nontrivial for $K = Q_2$ ($p = 2$, $l = 0$) and $K = Q_3[\sqrt{-3}]$ ($p = 3$, $l = 0$), the two special cases considered in [**R1**]). For A of this type we also identify those dimensions in which the small factor is nontrivial and give an estimate of its size in terms of that of J^A and the number of roots of unity of pth power order contained in A.

The paper is organized as follows:

In §1 we define the Hopf algebroid $(E_A, E_A T)$ which is our generalization of $(E_*, E_* E)$ and a map of Hopf algebroids $(V_A, V_A T) \to (E_A, E_A T)$. We also define a second map of Hopf algebroids

$$(E_A, E_A T) \to (K[v, v^{-1}], K[u, u^{-1}, v, v^{-1}])$$

and study $E_A T$ by studying the image of the composition map

$$\Phi \colon V_A T \to K[u, u^{-1}, v, v^{-1}].$$

In §2, we define a certain subalgebra C of the ring of Laurent polynomials. This algebra consists of those Laurent polynomials satisfying a certain integrality condition and is related to similar rings studied by Georg Pólya and Alexander Ostrowski over 60 years ago. We show that in dimension 0 the image of Φ is equal to C and then show that the map $(E_A T)_0 \to C$ is an isomorphism. Using this description of $E_A T$ we compute the Ext group $\text{Ext}_{E_A T}(E_A, E_A)$ in §3 and show that this is isomorphic, via a v_1 local change of rings theorem, to the group $\text{Ext}_{V_A T}(V_A, M^1)$ in the chromatic spectral sequence. We then do the number theory necessary to identify those extensions for which the relevant differential is nontrivial.

I would like to thank Doug Ravenel for his comments on a preliminary version of this paper. The calculations in §3 (Corollaries 27 and 28) in particular owe a great deal to his suggestions.

1. The map Φ and generators for $\text{Im}\,\Phi$. We will suppose that A is the ring of integers in a finite extension K of Q_p, the p-adic numbers, with maximal ideal (π) and residue field F_q. If $q = p^f$, and e is the ramification index of p in A, i.e. $(\pi^e) = (p)$, then $e \cdot f$ is the index of the extension [**CF**].

In analogy with definition 3.6 of [**M-R**], we define

$$E_A = A[v, v^{-1}]$$

with degree(v) $= 2(q - 1)$ and give it the structure of a V_A algebra via the map

$$\phi' \colon V_A \to E_A, \qquad v_i \mapsto \begin{cases} v & \text{if } i = 1, \\ 0 & \text{if } i > 1. \end{cases}$$

We also define

$$E_A T = E_A \otimes_{V_A} V_A T \otimes_{V_A} E_A$$

which forms with E_A, a Hopf algebroid. There is by extension a map of Hopf algebroids

$$(\phi', \Phi') \colon (V_A, V_A T) \to (E_A, E_A T).$$

It is $E_A T$ which we wish to describe. For this we will require the auxiliary Hopf algebroid $(K[v, v^{-1}], K[u, u^{-1}, v, v^{-1}])$. The structure maps here are given by

$$\eta_R(v) = v, \quad \eta_L(v) = u, \quad \psi(u) = u \otimes 1, \quad \psi(v) = 1 \otimes v, \quad c(u) = v.$$

To describe $E_A T$ we will examine its image in $K[u, u^{-1}, v, v^{-1}]$ under the canonical map $E_A T \to E_A T \otimes K$ and show that this map is injective. We will concentrate first on identifying the image of this map, and postpone the proof of injectivity to the end of §2. Since the image of this map is the same as that of the composition

$$V_A T \to E_A T \to E_A T \otimes K = K[u, u^{-1}, v, v^{-1}]$$

it is this that we study, i.e. the Hopf algebroid map

$$(\phi, \Phi) \colon (V_a, V_A T) \to (K[v, v^{-1}], K[u, u^{-1}, v, v^{-1}]).$$

Recall [**R1**, 2.8] that

$$V_A T = V_A[t_1, t_2, \ldots] \quad \text{where } \deg(t_n) = 2(q^n - 1).$$

To describe the image of Φ we will obtain a recursive formula for $\Phi(t_n)$ in terms of $\Phi(t_j)$ for $j < n$. To do this we must first determine the value of the unique extension of ϕ

$$\overline{\phi} \colon V_A \otimes K \to K[v, v^{-1}]$$

on the coefficients of the logarithm of the formal A-module.

LEMMA 1. *If the log of the A-typical formal A-module is $\sum \lambda_i x^{q^i}$ then*

$$\overline{\phi}(\lambda_n) = v^{(q^n - 1)/(q-1)} / \pi^n.$$

PROOF. We have, from [**R1**, 2.9], the formula

$$\pi \lambda_n = \sum_{0 \le i < n} \lambda_i v_{n-i}^{q^i}.$$

Applying $\overline{\phi}$ we obtain

$$\pi \overline{\phi}(\lambda_n) = \overline{\phi}(\lambda_{n-1}) \cdot v^{q^{n-1}}$$

and the result follows. □

PROPOSITION 2. *The degree 0 component of the image of Φ is generated over $A[w, w^{-1}]$ by the set of polynomials $\{g_n | n = 0, 1, 2, \ldots\}$ which are determined by the recursive formula*

$$g_n = \sum_{i=0}^{n-1} \frac{1}{\pi^{i+1}} \left(g_{n-i-1}^{q^i} \cdot w^{q^{n-1}} - g_{n-i-1}^{q^{i+1}} \right).$$

Here we have used the notation $w = v/u$.

PROOF. Starting with the same formula as in the proof above and applying η_R yields

$$\pi \eta_R(\lambda_n) = \sum_{0 \le i < n} \eta_R(\lambda_i) \eta_R(v_{n-i})^{q^i}$$

or

$$\pi \cdot \sum_{i=0}^{n} \eta_L(\lambda_i) \cdot t_{n-i}^{q^i} = \sum_{i=0}^{n-1} \sum_{j=0}^{i} \eta_L(\lambda_j) t_{i-j}^{q^i} \eta_R(v_{n-i})^{q^i}.$$

Applying Φ to both sides of this we obtain

$$\pi \cdot \sum_{i=0}^{n} \phi(\eta_L(\lambda_i)) \Phi(t_{n-i})^{q^i} = \sum_{i=0}^{n-1} \phi(\eta_L(\lambda_i)) \Phi(t_{n-i-1})^{q^i} v^{q^{n-1}}$$

since $\Phi(\eta_R(v_{n-i})) = 0$ unless $n - i = 1$. This can be rewritten as

$$\pi \cdot \sum_{i=0}^{n} \frac{1}{\pi^i} u^{(q^i-1)/(q-1)} \Phi(t_{n-1})^{q^i} = \sum_{i=0}^{n-1} \frac{1}{\pi^i} u^{(q^i-1)/(q-1)} \Phi(t_{n-i-1})^{q^i} \cdot v^{q^{n-1}}.$$

To analyze this further we introduce the notation

$$g_i = \Phi(t_i) \cdot u^{-(q^i-1)/(q-1)}.$$

Making this substitution we obtain, after some computation

$$\sum_{i=0}^{n} \frac{1}{\pi^i} g_{n-i}^{q^i} = \sum_{i=0}^{n-1} \frac{1}{\pi^{i+1}} g_{n-i-1}^{q^i} \cdot w^{q^{n-1}}.$$

Solving this for g_n yields the result. □

2. Integral valued polynomials and the image of Φ. To analyze further the image of Φ, we introduce certain subalgebras of the algebra Laurent polynomials:

$$C = \{f \in K[w, w^{-1}] | f(1 + \pi A) \subseteq A\},$$
$$B = C \cap K[w],$$
$$\overline{B} = \{f \in K[x] | f(A) \subseteq A\}.$$

Note that the algebras B and $\overline{B}$ are isomorphic via the unique map of algebras sending w to $1 + \pi x$. In view of our observations in the preceding section concerning the polynomials $\{g_n\}$, showing that $(\text{Im}\,\Phi)_0 \subseteq C$ is equivalent to showing that $g_n \in B$ or, writing $h_n(x) = g_n((x - 1)/\pi)$, that $h_n \in \overline{B}$. In terms of these polynomials the recurrence formula of Proposition 2 becomes

$$h_n = \sum_{i=0}^{n-1} \frac{1}{\pi^{i+1}} \left(h_{n-i-1}^{q^i} (\pi x + 1)^{q^{n-1}} - h_{n-i-1}^{q^{i+1}} \right).$$

What we will show is

LEMMA 3. *If $h \in \overline{B}$, $i < n$, then*

$$\frac{1}{\pi^{i+1}} \left(h^{q^i} \cdot (\pi x + 1)^{q^{n-1}} - h^{q^{i+1}} \right) \in \overline{B}.$$

PROOF. We begin by noting two facts about A. First, if u is a unit in A, then $u^{q-1} \equiv 1 \bmod \pi$. This is because the group of units modulo π has order $q - 1$. Second, the binomial theorem implies that if $y \equiv 1 \bmod \pi^\nu$ then $y^q \equiv 1 \bmod \pi^{\nu+1}$. It follows from this, by induction, that for any $x \in A$,

$$(1 + x\pi)^{q^{n-1}} \equiv 1 \quad \bmod \pi^{i+1}$$

for any $i < n$.

From these two facts we see that for any $x \in A$,

$$h^{q^i} \cdot (\pi x + 1)^{q^{n-1}} - h^{q^{i+1}} \equiv h^{q^i}(x) - h^{q^{i+1}}(x) \quad \bmod \pi^{i+1}$$
$$\equiv h^{q^i}(x)(1 - h^{(q-1)q^i}(x)) \quad \bmod \pi^{i+1}$$
$$\equiv 0 \quad \bmod \pi^{i+1}. \quad \square$$

We next examine the algebras B and $\overline{B}$ more closely using techniques developed by G. Pólya and A. Ostrowski, published in 1919 [**O, P**]. The results in these papers

are stated for the case of the ring of integers in an algebraic number field, but, as remarked in [C], they all extend directly to the case of any Dedekind ring with finite residue fields, including the discrete valuation ring, A, that we are concerned with. Our aim is to develop a way of recognizing a generating set for these algebras (which we will apply to $\{g_n\}$ or $\{h_n\}$).

DEFINITION 4. (i) Let $\{p_i | i = 0, \ldots, q-1\}$ be a complete set of residues for π in A.

(ii) Let $\{\alpha_i | i = 0, 1, 2, \ldots\}$ and $\{\bar{\alpha}_i | i = 0, 1, 2, \ldots\}$ be subsets of A defined by

$$\bar{\alpha}_n = \sum_{i=0}^{k} p_{c_i} \pi^i \quad \text{and} \quad \alpha_n = 1 + \pi \bar{\alpha}_n$$

if the expression of the integer n in base q is $n = \sum_{i=0}^{k} c_i q^i$.

(iii) Let $\psi \colon Z^+ \to Z^+$ be defined by

$$\psi(n) = \sum_{i=1}^{k} \left[\frac{n}{q^i} \right].$$

We can make the following observations concerning these definitions. First, the elements $\{\bar{\alpha}_i\}_{i=0}^{q^k-1}$ form a complete set of residues for π^k in A for any positive integer k. Next the elements $\{\alpha_i\}_{i=0}^{q^k-1}$ form a complete set of residues mod π^{k+1} of those elements of A congruent to $1 \mod \pi$. Finally, the function ψ could equally well be defined by the formula

$$\psi(n) = \left(n - \sum_{i=0}^{k} c_i \right) \bigg/ (q-1).$$

Given these observations, we may define some polynomials which form bases for B and $\overline{B}$.

DEFINITION 5. Let $\hat{g}_0(w) = 1 = \bar{g}_0(x)$ and, for $n > 0$,

$$\hat{g}_n(w) = \prod_{i=0}^{n-1} \frac{w - \alpha_i}{\pi^{n+\psi(n)}}$$

and

$$\bar{g}_n(x) = \prod_{i=0}^{n-1} \frac{x - \bar{\alpha}_i}{\pi^{\psi(n)}}.$$

PROPOSITION 6 [P, O]. (i) $\{\bar{g}_n | n = 0, 1, 2, \ldots\}$ is a basis for $\overline{B}$ as an A-module.

(ii) $\{\hat{g}_n | n = 0, 1, 2, \ldots\}$ is a basis for B as an A-module.

PROOF. In view of the isomorphism $B \simeq \overline{B}$ mentioned at the beginning of this section it suffices to prove (i).

That $\bar{g}_n \in \overline{B}$ for all n follows from the fact that if $a \in A$, then

$$\prod_{i=0}^{n-1} a - \bar{\alpha}_i \equiv 0 \quad \mod \pi^{\psi(n)}.$$

This can be found in [P, p. 106].

To show that the polynomials $\{\bar{g}_n | n = 0, 1, \ldots\}$ span $\overline{B}$, we require the additional fact from [**P**, Satz IV], that if $f \in \overline{B}$ is of degree n then $\pi^{\psi(n)} \cdot f \in A[x]$. Thus, since the leading term of $\bar{g}_n$ is $1/\pi^{\psi(n)}$, f can be expressed as a linear combination of $\bar{g}_0, \ldots, \bar{g}_n$. Linear independence follows from the fact that degree $(\bar{g}_n) = n$. □

To deduce information about the multiplicative structure of these algebras from this result it is convenient to introduce some auxiliary polynomials which yield different bases for B and $\overline{B}$. Let $\{f_i(x) | i = 0, 1, \ldots\}$ be the polynomials given recursively by

$$f_0(x) = x,$$
$$f_1(x) = (x^q - x)/\pi,$$
$$f_{n+1}(x) = f_1 \circ f_n(x).$$

Also, if $n = \sum_{i=0}^k c_i q^i$ let

$$\bar{f}_n(x) = \prod_i (f_i(x))^{c_i} \quad \text{and} \quad \hat{f}_n(x) = \bar{f}\left(\frac{w-1}{\pi}\right).$$

PROPOSITION 7.   *The polynomials* $\{\bar{f}_n | n = 0, 1, 2, \ldots\}$ *and* $\{\hat{f}_n | n = 0, 1, 2, \ldots\}$ *are bases for the algebras* $\overline{B}$ *and* B *respectively. The polynomials* $\{f_n | n = 0, 1, 2, \ldots\}$ *are a generating set for* $\overline{B}$.

PROOF. It suffices to prove the first of these three assertions. Since $\sum_{i=0}^k c_i \psi(q^i)$ $= \psi(n)$ the leading coefficient of $\bar{f}_n$ is $1/\pi^{\psi(n)}$. Thus, for each n, the matrix expressing the polynomials $\{\bar{f}_i | i = 0, 1, \ldots, n\}$ as A linear combinations of $\{\bar{g}_i | i = 0, 1, \ldots, n\}$ is triangular with units of A along its diagonal. It is, therefore, invertible over A by Cramer's rule. The result follows.   □

We are now ready to return to studying $\mathrm{Im}(\Phi)_0$ and to show that it equals C. For this we show that the polynomials $\{h_n(x) | n = 0, 1, \ldots\}$ generate $\overline{B}$. This is sufficient since B generated C over $A[w^{\pm 1}]$ and $B \cong \overline{B}$. Our approach is to compare this prospective generating set with the one for $\overline{B}$ constructed above.

DEFINITION 8.   Denote by R_n the subalgebra of $\overline{B}$ generated by $\{f_i | i = 0, 1, \ldots, n\}$.

These subalgebras have the property

LEMMA 9.   (i) *If* $f \in \overline{B}$, *and* $\deg(f) < q^{n+1}$, *then* $f \in R_n$.
(ii) *If* $k < q^{n+2}$ *is given, then there exists* $f \in R_n$ *with the properties that* $\deg(f) = k$, *and that the leading coefficient of* f *is* $1/\pi^{\psi(k)-1}$.

PROOF. The subgroup of $\overline{B}$ of polynomials of degree less than q^{n+1} has as a basis $\{\bar{f}_i | i = 1, 2, \ldots, q^{n+1} - 1\}$. Since each of these is constructed as a product of polynomials in R_n the first assertion is clear. Some arithmetic with the function ψ shows that if $k = \sum_{i=0}^{n+1} c_i q^i$ then

$$f = \prod_{i=0}^{n-1} (f_i)^{c_i} \cdot f_n^{c_n + q \cdot c_{n+1}}$$

has the property claimed in the second assertion.   □

We are now ready to prove the following proposition.

PROPOSITION 10. R_n is generated by $\{h_i | i = 1, 2, \ldots, n+1\}$.

PROOF. We begin with a result concerning the coefficients of h_n. Suppose that

$$h_n = \sum_{i=0}^{(q^n-1)/(q-1)} a_{i,n} x^n$$

and that γ is the π-adic valuation on K as in [**R1**, p. 340], i.e. γ is the extension to K of the usual valuation on the p-adic numbers. We claim that $\gamma(a_{i,n}) \geq -\psi(q^{n-1})/e$ with strict inequality if $i > q^{n-1}$ and equality if $i = q^{n-1}$. We will prove this by induction on n. For $n = 1$ the result follows from direct computation. Suppose the result holds for h_n and consider h_{n+1}.

Note that ψ has the property

$$\psi(q^n) = q \cdot \psi(q^{n-1}) + 1 > q^2 \psi(q^{n-2}) + 2, \quad \text{etc.}$$

Now h_{n+1} is given by

$$h_{n+1} = \sum_{i=0}^{n} \left(\frac{h_{n-i}^{q^i}(\pi x + 1)^{q^n}}{\pi^{i+1}} - \frac{h_{n-i}^{q^{i+1}}}{\pi^{i+1}} \right)$$

and the π-adic norm of the coefficients of $h_{n-i}^{q^i}(\pi x + 1)^{q^n}/\pi^{i+1}$ are all greater than $-(q^i \psi(q^{n-i-1}) + (i+1))/e$ while those of $h_{k-i}^{q^{i+1}}/\pi^{i+1}$ will all be greater than $-(q^{i+1} \cdot \psi(q^{n-i-1}) + (i+1))/e$. The previous observation shows that all of these are strictly greater than $-\psi(q^n)/e$ except possibly the second when $i = 0$. Thus our problem reduces to that of examining the π-adic valuations of the coefficients of $h_n^q/\pi = \sum b_i x^i$.

For the moment let us write a_i in place of $a_{i,n}$. The coefficient b_i is

$$b_i = \frac{1}{\pi} \sum a_{i_1} \cdots a_{i_q}$$

where the sum is over all q-tuples $I = (i_1 \cdots i_q)$ with

$$|I| = \sum_{i=1}^{q} i_j = i.$$

For $i > q^{n+1}$ at least one of the i_j is greater than q^n and so by induction

$$-\frac{1}{e} + \gamma(\Pi a_{i_j}) > -\left(\frac{1}{e} + \frac{q \cdot \psi(q^{n-1})}{e} \right) = -\frac{\psi(q^n)}{e}.$$

On the other hand, when $i = q^{n+1}$ there is exactly one q-tuple with the property $i \leq q^n$ for all j namely $i_j = q^n$, $j = 1, \ldots, q$.

In this case

$$-\frac{1}{e} + \gamma(\Pi a_{ij}) = -\left(\frac{1}{e} + q\gamma(a_{q^n}) \right) = -\left(\frac{1}{e} + \frac{q\psi(q^{n-1})}{e} \right) = -\frac{\psi(q^n)}{e}.$$

Thus $\gamma(b_{q^{n+1}}) = -\psi(q^n)/e$.

To complete our proof of this proposition we again induct on n. It is clear by direct computation that R_1 is generated by h_1 and h_2. Suppose that R_n is generated by $\{h_i | i = 1, 2, \ldots, n+1\}$ and consider R_{n+1}. The polynomial h_{n+2} has

degree $(q^{n+2} - 1)/(q - 1) < q^{n+2}$ and so, applying the previous lemma and the observation above repeatedly we can find $f \in R_n$ such that $h_{n+2} - f$ is of degree q^{n+1}. Furthermore, the π-adic norm of the leading coefficient of $h_{n+2} - f$ will be $-\psi(q^{n+1})/e$, again by the observation above. Thus

$$\mathrm{Span}\langle R_n, h_{n+2}\rangle = \mathrm{Span}\langle R_n, h_{n+2} - f\rangle = \mathrm{Span}\langle R_n, f_{n+1}\rangle = R_{n+1}. \quad \square$$

We thus have

COROLLARY 11. $\mathrm{Im}(\Phi)_0 = C$.

It only remains for us to establish the injectivity of Φ. The kernel of

$$\Phi\colon E_A T \to E_A T \otimes K = K[u, u^{-1}, v, v^{-1}]$$

will consist of the torsion subgroup of $E_A T$. Since $E_A T$ is a module over the local ring A the injectivity of Φ will follow from that of the induced map

$$\Phi'\colon E_A T/(\pi) \to (C \otimes E_A)/(\pi).$$

PROPOSITION 12. Φ' is an isomorphism.

PROOF. If we let $K_A(1) = F_q[v_1, v_1^{-1}]$ as in [R1], then

$$(E_A T)/(\pi) \simeq K_A(1) \otimes V_A T \otimes K_A(1)$$

which is denoted $\Sigma_A(1)$ in [R1]. It has the presentation

$$\Sigma_A(1) = K_A(1)[t_i | i = 1, 2, \ldots]/(v_1 t_i^q - v_1^{q^i} t_i).$$

Its degree 0 component, which we willl denote $S_A(1)_*$ has the presentation

$$S_A(1)_* = F_q[S_i | i = 1, 2, \ldots]/(s_i^q - s_i).$$

The map (Φ_0') sends s_i to g_i so it will suffice to show that (Φ_0') restricted to the subalgebra of $S_A(1)_*$ generated by $s_1, \ldots, s_n$ maps isomorphically to the subalgebra generated by $g_1, \ldots, g_n$. We first note that the inclusion $B \hookrightarrow C$ induces an isomorphism $B/(\pi) \to C/(\pi)$. This is because $(w - 1)/\pi \in B$ and C, so that $w \equiv 1 \mod(\pi)$.

Now the subalgebra of $S_A(1)_*$ generated by $s_1, \ldots, s_n$ is clearly of rank q^n over F_q. Thus, since Φ' is surjective, we need only compute the rank of the subalgebra of $B/(\pi)$ generated by $g_1, \ldots, g_n$ or, equivalently, that of the subalgebra of $\overline{B}/(\pi)$ generated by $h_1, \ldots, h_n$. This is $R_{n-1}/(\pi)$ which is also generated by $f_0, \ldots, f_{n-1}$. Since $\pi \cdot f_{i+1} = f_i^q - f_i$ we have $f_i^q = f_i$ in $R_{n-1}/(\pi)$ and so $R_{n-1}/(\pi)$ has rank q^n also. $\square$

3. $\mathrm{Ext}_{E_A T}(E_A, E_A)$ and Ravenel's conjecture. The relation between our description of $E_A T$ in §2 and the group $\mathrm{Ext}_{V_A T}(V_A, V_A)$ occurring in the Ravenel conjecture involves three steps. First the computation of $\mathrm{Ext}_{E_A T}(E_A, E_A)$, second the relation of this to the chromatic spectral sequence of [R1], and finally the analysis of the differentials in that spectral sequence. We consider these in order.

The computation of $\mathrm{Ext}_{E_A T}(E_A, E_A)$ proceeds as in [S, Propositions 19.17–19.22], where the special case $K = Q$ is considered. The only property of Q that is used is that it is a field.

PROPOSITION 13. $\operatorname{Ext}_{E_A T}^{1,2k(q-1)}(E_A, E_A) = A/J_{k \cdot (q-1)}$.

PROOF. In general, for any Hopf algebra H over a ring R we have

$$\operatorname{Ext}_H^{1,k}(R, R) = P_k(H)/(\eta_L - \eta_R)(R)$$

where $P_k(\ )$ denotes the degree k primitives. In our case this becomes

$$\operatorname{Ext}_{E_A T}^{1,2k(q-1)}(E_A, E_A) = P_k(E_A T)/(\eta_L - \eta_R)(E_A)$$

and 0 in dimensions not divisible by $2(q-1)$. The denominator is easily identified:

$$(\eta_L - \eta_R)(E_A) = A \cdot (u^k - v^k).$$

For the numerator, first note that

$$P_k(K[u, u^{-1}, v, v^{-1}]) = K \cdot (u^k - v^k).$$

Therefore

$$P_k(E_A T) = A \cdot ((u^k - v^k)/\pi^{d(k)})$$

where $d(k)$ is the largest integer for which $(u^k - v^k)/\pi^{d(k)} \in E_A T$, i.e. $(w^k - 1)/\pi^{d(k)} \in C$. From our description of C in §2 we see that $\pi^{d(k)} \cdot A = J_{k \cdot (q-1)}$. □

We next recall the construction of the chromatic spectral sequence and relate the Ext group constructed above to groups which occur there. Define inductively a pair of sequences of $V_A T$ comodules N_A^i and M_A^i by:

$$N_A^0 = V_A, \quad M_A^i = (v_i^A)^{-1} V_A \otimes N_A^i, \quad N_A^{i+1} = M_A^i/N_A^i.$$

These occur in the short exact sequences

$$0 \to N_A^i \to M_A^i \to N_A^{i+1} \to 0$$

which can be combined to give a resolution of V_A over $V_A T$:

$$0 \to V_A \to M_A^0 \to M_A^1 \to \cdots .$$

If we write

$$D_1^{s,t} = \operatorname{Ext}_{V_A T}^{t,*}(V_A, N_A^s) \quad \text{and} \quad E_1^{s,t} = \operatorname{Ext}_{V_A T}^{t,*}(V_A, M_A^s)$$

then we obtain an exact couple:

$$
\begin{array}{ccc}
D_1 & \longrightarrow & D_1 \\
& \nwarrow \quad \swarrow & \\
& E_1 &
\end{array}
$$

The spectral sequence associated to this couple is the chromatic spectral sequence, which converges to $\operatorname{Ext}_{V_A T}^{*,*}(V_A, V_A)$. Ravenel's conjecture is concerned with $\operatorname{Ext}_{V_A T}^{1,*}(V_A, V_A)$ which occurs as $E_2^{1,0}$ in this spectral sequence (since $E_1^{0,1} = 0$). We therefore concentrate on

$$E_1^{1,0} = \operatorname{Ext}_{V_A T}^{0,*}(V_A, M_A^1), \qquad E_1^{2,0} = \operatorname{Ext}_{V_A T}^{0,*}(V_A, M_A^2)$$

and the differential d_1 between these two groups, whose kernel is $E_2^{1,0}$.

The first of these groups is related to our previous computation by the following v_1 local change of rings theorem which holds for any v_1 local $V_A T$ comodule, but which we state only for the special case which we need.

THEOREM 14. $\mathrm{Ext}_{V_A T}(V_A, M_A^1) \simeq \mathrm{Ext}_{E_A T}(E_A, E_A \otimes_{V_A} M_A^1)$.

The proof of this result is a straightforward generalization of Theorem 3.10 of [M-R].

Based on this theorem we can compute $E_1^{1,0}$.

COROLLARY 15.

$$\mathrm{Ext}_{V_A T}^{0,*}(V_A, M_A^1) \simeq \begin{cases} K/A & \text{if } * = 0, \\ \mathrm{Ext}_{E_A T}^{1,*}(E_A, E_A) & \text{otherwise.} \end{cases}$$

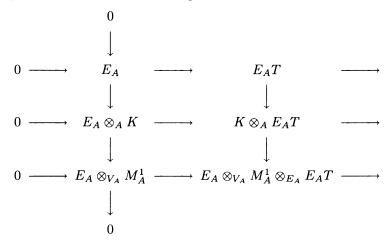PROOF. When the map $d_0 \colon M_A^0 \to M_A^1$ is tensored with E_A it yields the exact sequence

$$0 \to E_A \to E_A \otimes_{V_A} M_A^0 \to E_A \otimes_{V_A} M_A^1 \to 0$$

which has associated to it a long exact sequence of Ext groups. Since the middle term in the short exact sequence is isomorphic to $E_A \otimes_A K$ whose Ext groups are given by

$$\mathrm{Ext}_{E_A T}(E_A, E_A \otimes_A K) = \begin{cases} K & \text{if } (*,*) = (0,0), \\ 0 & \text{otherwise,} \end{cases}$$

the result follows.   □

The proof of this corollary provides us with a convenient representation for elements of $E_1^{1,0}$. If we take the cobar resolution over $E_A T$ of the groups in the short exact sequence, then we obtain the diagram:

$$
\begin{array}{ccccc}
& & 0 & & \\
& & \downarrow & & \\
0 \longrightarrow & E_A & \longrightarrow & E_A T & \longrightarrow \\
& \downarrow & & \downarrow & \\
0 \longrightarrow & E_A \otimes_A K & \longrightarrow & K \otimes_A E_A T & \longrightarrow \\
& \downarrow & & \downarrow & \\
0 \longrightarrow & E_A \otimes_{V_A} M_A^1 & \longrightarrow & E_A \otimes_{V_A} M_A^1 \otimes_{E_A} E_A T & \longrightarrow \\
& \downarrow & & & \\
& 0 & & &
\end{array}
$$

Using Theorem 14 and this diagram we see that we may represent an element of $\mathrm{Ext}_{V_A T}^{0,*}(V_A, M_A^1)$ by an element $x \in E_A \otimes_A K$ with the property that $(\eta_L - \eta_R)(x) \in E_A T$. Such a representative is unique modulo E_A.

The final step in our consideration of Ravenel's conjecture is the study of the differential d_1 and the identification of its kernel. We first describe this kernel in terms of the representation given above for elements of $E_1^{1,0}$ and then do the necessary number theory to determine when this kernel is all of $E_1^{1,0}$.

Using the long exact Ext sequences associated to the short exact sequences

$$0 \to N_A^i \to M_A^i \to N_A^{i+1} \to 0$$

for $i = 1, 2$ and the fact that the differential d_1 is given by the composition

$$\text{Ext}^{0,*}_{V_A T}(V_A, M_A^1) \to \text{Ext}^{0,*}_{V_A T}(V_A, N_A^2) \to \text{Ext}^{0,*}_{V_A T}(V_A, M_A^2)$$

we see that the kernel of d_1 is given by the image of $\text{Ext}^{0,*}_{V_A T}(V_A, N_A^1)$ in $\text{Ext}^{0,*}_{V_A T}(V_A, M_A^1)$. We can relate this to our earlier description of elements in $E_1^{1,0}$ using the following diagram whose rows are exact:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & V_A & \longrightarrow & V_A \otimes K & \longrightarrow & N_A^1 & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & v_1^{-1} V_A & \longrightarrow & v_1^{-1} V_A \otimes_A K & \longrightarrow & M_1 & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E_A & \longrightarrow & E_A \otimes K & \longrightarrow & E_A \otimes M_A^1 & \longrightarrow & 0
\end{array}
$$

Tracing through this diagram we see that an element $x \in E_A \otimes K$ represents an element in the image of $\text{Ext}^{0,*}_{V_A T}(V_A, N_A^1)$ if it is the image under the center vertical composition of an element $y \in V_A \otimes K$ with the property that $(\eta_L - \eta_R)(y) \in V_A T$. The content of Theorem 14 is that any $x \in E_A \otimes K$ representing an element of $E_1^{1,0}$ will be the image of an element $z \in v_1^{-1} V_A \otimes K$ with $(\eta_L - \eta_R)(z) \in v_1^{-1} V_A \otimes V_A T$. It will be the image of an element y as above if the expression of z as a Laurent polynomial in v_1 does not involve any negative powers of v_1 which are nontrivial modulo V_A.

Before we can describe this kernel more explicitly we require a more precise description of the arithmetic function $d(l)$ which determines the ideal J_*.

PROPOSITION 16. *If $(m, p) = 1$ then $d(mp^k) = d(p^k)$.*

PROOF. d is defined so that for any $a \in A$ with $a \equiv 1 \bmod \pi$ we have

$$a^{p^k} \equiv 1 \bmod \pi^{d(p^k)}.$$

Therefore

$$a^{mp^k} = (a^{p^k})^m \equiv 1 \bmod \pi^{d(p^k)}$$

and so $d(mp^k) l \geq d(p^k)$.

On the other hand there exists $a \in A$ with $a \equiv 1 \bmod \pi$ for which

$$a^{p^k} \not\equiv 1 \bmod \pi^{d(p^k)+1}.$$

Using the binomial theorem we see that this implies that, since $(m, p) = 1$,

$$a^{mp^k} = \left(a^{p^k}\right)^m \not\equiv 1 \bmod \pi^{d(p^k)+1}$$

and so $d(mp^k) \leq d(p^k)$ also. $\square$

Thus we can restrict our attention to the value of d at powers of p. For this we will use the following result concerning congruences in A from [**Ha**, p. 228].

LEMMA 17. *If $x \in A$ is such that $x \equiv 1 + a\pi^\nu \bmod \pi^{\nu+1}$ then*

$$
x^p = \begin{cases}
1 + a^p \pi^{p\nu} \bmod \pi^{p\nu+1} & \text{if } \nu < e/(p-1), \\
1 + (a^p - \varepsilon a)\pi^{p\nu} \bmod \pi^{p\nu+1} & \text{if } \nu = e/(p-1), \\
1 - \varepsilon a \pi^{\nu+e} \bmod \pi^{\nu+e+1} & \text{if } \nu > e/(p-1),
\end{cases}
$$

where ε is the unit in A for which $p = -\varepsilon \pi^e$.

This lemma allows us to explicitly describe d if $e/(p-1)$ is not a power of p.

PROPOSITION 18. *If $p^{l-1} < e/(p-1) < p^l$ then*

$$d(p^k) = \begin{cases} p^k & \text{if } k \le l, \\ p^l + (k-1)e & \text{if } k > l. \end{cases}$$

PROOF. The lemma shows that, for $k \le l$ $d(p^k) = p \cdot d(p^{k-1})$ and, for $k > l$ $d(p^k) = e + d(p^{k-1})$. $\square$

If $e/(p-1)$ is a power of p the situation is the same in low dimensions. Just as above we can show

PROPOSITION 19. *If $e/(p-1) = p^l$ and $k \le l$ then $d(p^k) = p^k$.*

The critical level is $k = (l+1)$ where the existence of pth roots of unity becomes important.

PROPOSITION 20. *If $k > l$, then the following equation holds except in the case where $e = p^l(p-1)$, $f = 1$, and A contains pth roots of unity:*

$$d(p^k) = p^l + (k-l) \cdot e.$$

PROOF. The result will follow as above for all $k > l$ if we can establish it for the case $k = l+1$. If $x = 1 + a\pi \bmod \pi^2$ then, by the lemma,

$$x^{p^{l+1}} \equiv 1 + (a^{p^{l+1}} - \varepsilon a^{p^l})\pi^{p^{l+1}} \quad \bmod \pi^{p^{l+1}+1}.$$

Thus it suffices for us to show that there exists $a \in A$ which is not a solution of the congruence $(a^{p^{l+1}} - \varepsilon a^{p^l}) \equiv 0 \bmod \pi$. To do this we count the number of solutions of this congruence and show that there are less than p^f of them modulo π. Since the pth power map is an automorphism of $A/\pi A$ any solution of this congruence is the p^lth power of a (unique modulo π) solution of $a^p - \varepsilon a \equiv 0 \bmod \pi$. This congruence has either p solutions or 1 solution modulo π according to whether A does or does not contain pth roots of unity [**Ha**, p. 224]. $\square$

PROPOSITION 21. *If $e/(p-1) = p^l$, $f = 1$ and A contains pth roots of unity then $p^{l+1} < d(p^{l+1}) \le p^{l+1} + p^l$.*

PROOF. The left hand inequality follows from the previous proof. For the right hand one, note that

$$(1 + \pi^2)^{p^{l+1}} \equiv 1 + \pi^{p^{l+1}+p^l} \quad \bmod \pi^{p^{l+1}+p^l+1}. \quad \square$$

REMARK 22. Using the description of the 1-units (units congruent to $1 \bmod \pi$) in A given in [**Ha**, p. 242] the left-hand inequality above can be improved to $p^{l+1} + p^{\mu-1} \le d(p^{l+1})$ if the group of roots of unity of pth power order in A has order p^μ.

For $k > l+1$ the computation is as before.

PROPOSITION 23. *If $d(p^{l+1}) = p^{l+1} + u$ then, for $k > l+1$, $d(p^k) = p^l + (k-l) \cdot e + u$.*

We can now complete our description of the kernel of d_1. Proposition 13 and the description of $d(l)$ given above give an upper bound for the order of this kernel. To identify cases in which this upper bound is attained we must construct specific elements in $E_1^{1,0}$.

PROPOSITION 24.   (i) *If* $(m,p) = 1$, $p^l \leq e/(p-1) < p^{l+1}$ *and* $k \leq l$ *then*
$(\eta_L - \eta_R)(v_1^{mp^k}/\pi^{p^k}) \in V_A T$.

(ii) *If* $(m,p) = 1$, $p^l \leq e/(p-1) < p^{l+1}$ *and* $k > l$ *then* $(\eta_L - \eta_R)(v_1^{mp^k}/\pi^{p^l+(k-l)e})$
$\in V_A T$.

PROOF. Since $(\eta_R)(v_1) = (v_1 + \pi t_1)$ and so $(\eta_L - \eta_R)(v_1) = (-\pi t_1)$ both
these results follow from computing the π-adic valuations of the coefficients of the
binomial expansion of $(v_1 + \pi t_1)^{mp^k}$.   □

Combining Proposition 20 with the description of elements of $\mathrm{Ker}(d_1)$ following
Corollary 15 we see that we have

COROLLARY 25.   *Except in the case where* $e = p^l(p-1)$, $f = 1$, *and* A *contains*
pth roots of unity the following equation holds:

$$\mathrm{Ext}^{1,n(q-1)}_{V_A T}(V_A, V_A) = A/J_{n(q-1)}.$$

In the case excluded in Corollary 25 we can construct the following element of
$E_1^{1,0}$.

PROPOSITION 26.   *If* $e/(p-1) = p^l$, $f = 1$, A *contains pth roots of unity and*
u *is as in Proposition* 23 *then*

$$(\eta_L - \eta_R)\left(\left(v_1^{p^{l+1}}\right) - \pi^{p^{l+1}}(v_2/v_1)^{p^l}\right)/\pi^{p^{l+1}+u} \in V_A T.$$

PROOF. Since $u \leq p^l$ it is sufficient for us to compute the numerator of this
quotient modulo $\pi^{p^{l+1}+p^l}$. Expanding $(v_1 + \pi t_1)^{p^{l+1}}$ we obtain

$$(\eta_L - \eta_R)(v_1)^{p^{l+1}} \equiv \binom{p^{l+1}}{p^l}\pi^{p^l} t_1^{p^l} v_1^{p^l(p-1)} + \pi^{p^{l+1}} t_1^{p^l}$$

$$\equiv p\pi^{p^l} t_1^{p^l} v_1^{p^l(p-1)} + \pi^{p^{l+1}} t_1^{p^l}$$

$$\equiv \pi^{p^{l+1}}\left(t_1^{p^{l+1}} - \varepsilon t_1^{p^l} v_1^{p^l(p-1)}\right) \quad \bmod \pi^{p^{l+1}+p^l}.$$

On the other hand $\eta_R(v_2/v_1) \equiv (v_2/v_1) + t_1^p - t_1 v_1^{p-1} \bmod \pi$ and so

$$(\eta_L - \eta_R)\left(\pi^{p^{l+1}}(v_2/v_1)^{p^l}\right) \equiv \pi^{p^{l+1}}\left(t_1^{p^{l+1}} - t_1^{p^l} v_1^{p^l(p-1)}\right) \quad \bmod \pi^{p^{l+1}+p^l}.$$

The result now follows from the observation that $\varepsilon \equiv 1 \bmod \pi^u$ which can be
established by expanding $(1 + \pi)^{p^{l+1}}$ and noting that it must be congruent to
$1 \bmod \pi^{p^{l+1}+u}$.   □

Since the element $((v_1^{p^{l+1}}/\pi^{p^{l+1}+1}) - (v_2/v_1)^{p^l}/\pi)$ contains negative powers of
v_1 which are nonzero modulo $V_A T$ we have constructed an element of $E_1^{1,0}$ which
is not in the kernel of d_1. We have, therefore

COROLLARY 27.   *If* $f = 1$, $e/(p-1) = p^l$, *and* A *contains pth roots of unity*
then

$$\mathrm{Ext}^{1,p^{l+1}(p-1)}_{V_A T}(V_A, V_A) = A/(\pi^{p^{l+1}}) \neq A/J_{p^{l+1}(p-1)}.$$

We can also take powers of the elements constructed in Proposition 26 to obtain
elements of $\mathrm{Ext}^{1,n(p-1)}$ if p^{l+1} divides n. These powers do not contain any neg-
ative powers of v_1 which are nontrivial modulo $V_A T$. Thus we can complete our
description of $\mathrm{Ext}^{1,*}_{V_A T}(V_A, V_A)$:

KEITH JOHNSON

COROLLARY 28. *If $f = 1$, $e/(p-1) = p^l$, and A contains pth roots of unity, then except in the case $n = p^{l+1}$,*

$$\mathrm{Ext}^{1,n(p-1)}_{V_A T}(V_A, V_A) = A/J_{n(p-1)}.$$

REFERENCES

[**AHS**] J. F. Adams, A. S. Harris and R. M. Switzer, *Hopf algebras of co-operations for real and complex K-theory*, Proc. London Math. Soc. **23** (1971), 385–408.

[**C**] P. J. Cahen, *Polynomes a valeurs entieres*, Canad. J. Math. **24** (1972), 747–754.

[**CF**] J. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, New York, 1967.

[**Ha**] H. Hasse, *Number theory*, Springer-Verlag, New York, 1980.

[**Hz**] M. Hazewinkel, *Formal groups and applications*, Academic Press, New York, 1973.

[**MR**] H. R. Miller and D. C. Ravenel, *Morava stabilizer algebras and the localization of Novikov's E_2-term*, Duke Math. J. **44** (1977), 433–447.

[**O**] A. Ostrowski, *Über Ganzwertige Polynome in Algebraischen Zahlkorper*, J. Reine Angew. Math. (Crelle) **149** (1919), 117–124.

[**P**] G. Polya, *Über Ganzwertige Polynome in Algebraischen Zahlkörper*, J. Reine Angew. Math. (Crelle) **149** (1919), 97–116.

[**R1**] D. C. Ravenel, *Formal A-modules and the Adams-Novikov spectral sequence*, J. Pure Appl. Math. **32** (1984), 327–345.

[**R2**] _____, *The structure of Morava stabilizer algebras*, Invent. Math **37** (1976), 109–120.

[**S**] R. M. Switzer, *Algebraic topology–homotopy and homology*, Grundlehren Math. Wiss., Band 212, Springer-Verlag, Berlin and New York, 1975.

DEPARTMENT OF MATHEMATICS, STATISTICS AND COMPUTING SCIENCE, DALHOUSIE UNIVERSITY, HALIFAX, NOVA SCOTIA, CANADA