Chromatic blueshift conjecture: the simple case and an algebraic analogue

Howard Beck*and Kyle Roke†

Department of Mathematics, Massachusetts Institute of Technology

September 4, 2024

1 Abstract

We inspect the power operation of the complex bordism spectrum MU in order to address a recent conjecture of Robert Burklund, Tomer M. Schlank, and Allen Yuan [BSY22] on chromatic blueshift in the Chromatic Nullstellenstatz. We show that the conjecture holds in the case $k = 1$, and we demonstrate that an algebraic analogue of the conjecture fails for higher values of k.

2 Background

We start with a review of terminology and known results about formal group laws, ring spectra and generalized cohomology theories, and the complex bordism spectrum which we will use throughout the paper. At the end, we introduce the chromatic blueshift conjecture.

2.1 Formal Group Laws

We briefly review the notion of formal group laws, taken from Lurie's Chromatic Homotopy Theory notes [Lur10].

Definition 2.1. *A **formal group law** on a commutative ring R is a power series $F \in R[\![x, y]\!]$ satisfying*

- *F(x,0) = x = F(0,x)*
- *F(x,y) = F(y,x)*
- *F(x, F(y,z)) = F(F(x,y),z).*

As the name "formal group law" suggests, these objects mimic abelian groups in a convenient way. To make this obvious, we can define $x +_F y = F(x, y)$ and rewrite the above identities as:

- $x +_F 0 = x = 0 +_F x$
- $x +_F y = y +_F x$
- $x +_F (y +_F z) = (x +_F y) +_F z.$

[*] hbeck@mit.edu

[†] kroke@mit.edu

In this sense, we can recast the identities above as existence of an identity (0), commutativity, and associativity of the formal group law. It can additionally be shown that inverses exist: in particular, that for each x there is some element y such that $F(x, y) = 0$.

Example. The **additive formal group law** is $F(x, y) = x + y$.

Example. The **multiplicative formal group law** is $F(x, y) = x + y + xy$.

Definition 2.2. *A* ***homomorphism*** *between formal group laws F and G is a power series $h(t) \in tR[\![t]\!]$ such that $F(h(x), h(y)) = h(G(x, y))$.*

As before, we can recast this definition to resemble usual groups: $h(x) +_F h(y) = h(x +_G y)$. We give a result from Lurie of the form of such formal group law homomorphisms modulo a prime p, which we will find useful later:

Proposition 2.3 (Lurie, Lecture 12, Claim 9)**.** *Let R be a commutative ring of prime characteristic p. If $h(t)$ is a homomorphism of formal group laws $F, G \in R[\![x, y]\!]$, then either $h = 0$, or there is some $n \geq 0$ and $h'(t) \in R[\![t]\!]$ such that $h(t) = h'(t^{p^n})$ and $h'(t) = \lambda t + O(t^2), \lambda \neq 0$.*

In fact, we will mainly concern ourselves with one particular formal group law homomorphism, representing the usual group idea of multiplication by an integer.

Definition 2.4. *Let $F(x, y)$ be a formal group law on a ring R. The n-**series** $[n](t)$ is defined to satisfy*

- $[0](t) = 0$
- $[n](t) = F([n-1](t), t) = [n-1](t) +_F t$.

It isn't hard to check that the n-series for a formal group law F is a homomorphism from F to itself. In particular, we can apply Proposition 2.3 to it to gain some insight into its form:

Corollary 2.5. *For any formal group law F on a ring R and prime p, we have that $[p](t) = \lambda t^{p^n} + O(t^{2p^n}) \mod p$.*

Proof. We descend to $R/(p)$, a commutative ring in which $p = 0$. By Proposition 2.3, the p-series takes the form $[p](t) = h'(t^{p^n})$ for $h'(t) = \lambda t + O(t^2)$. So $[p](t) = h'(t^{p^n}) = \lambda t^{p^n} + O(t^{2p^n})$. □

Observe that $[n](t) \in tR[\![t]\!]$. Then it makes sense to divide this by t, as below:

Definition 2.6. *Let $\langle n \rangle(t)$ be the power series in $R[\![t]\!]$ defined as:*

$$\langle n \rangle(t) = \frac{[n](t)}{t} \tag{1}$$

Note that in the proof of Corollary 2.5 we could instead work in $R/(p, \lambda)$ and reduce the p-series further to $\lambda' t^{p^m}$ for some $m > n$. This clues us in to the idea that the most important coefficients of the p-series are those coefficients of t^{p^n}-terms, and we enshrine this realization in a definition.

Definition 2.7. *Let F be a formal group law over a commutative ring R, and let p be a prime number. We define v_n to be the coefficient of t^{p^n} in the p-series $[p](t)$.*

Example. For any formal group law $F(x, y)$, $v_0 = p$. This is because $F(x, y) = x+y+O(x^2, xy, y^2)$, so $t +_F t = 2t + O(t^2)$, and $(n-1)t +_F t = nt + O(t^2)$.

Example. (*Example 16 in Lurie, Lecture 12*) For the multiplicative formal group law $F(x, y) = x + y + xy$, the n-series is $(1 + t)^n - 1$. If $p = 0$, then $[p](t) = (1 + t)^p - 1 = t^p \mod p$.

Example. (Proposition 2.17) For a generalized cohomology theory E, the E-valued cohomology of line bundles ξ_1, ξ_2 satisfy a formal group law relation:

$$c_1^E(\xi_1 \otimes \xi_2) = f(c_1^E(\xi_1), c_2^E(\xi_2))$$

where f is a formal group law over $E^*(*)$.

One may ask the question: what do you need to define a formal group law? Certainly, we must need to select coefficients $c_{i,j} \in R$, $i, j \in \mathbb{N}$, and then we can take

$$F(x, y) = \sum_{i,j \in \mathbb{N}} c_{i,j} x^i y^j.$$

In order for F to be a formal group law, we must make sure it satisfies the conditions of Definition 2.6 above. These amount to

- $c_{i,0} = c_{0,i} = \begin{cases} 1 & \text{if } i = 1 \\ 0 & \text{otherwise} \end{cases}$
- $c_{i,j} = c_{j,i}$
- $\sum_{i,j \in \mathbb{N}} c_{i,j} x^i (\sum_{k,l \in \mathbb{N}} c_{k,l} y^k z^l)^j = \sum_{i,j \in \mathbb{N}} c_{i,j} (\sum_{k,l \in \mathbb{N}} c_{k,l} x^k y^l)^i z^j$.

The last of these cases can be, tediously, translated into a relation on the $c_{i,j}$ at each power $x^i y^j z^k$. What all this means, then, is that defining a formal group law is equivalent to selecting a sequence of $c_{i,j}$ which satisfy the above relations. In other words, every formal group law over a ring R comes from a map $\mathbb{Z}[c_{i,j}]/Q \longrightarrow R$, where Q is the ideal generated by the above relations. This ring $\mathbb{Z}[c_{i,j}]/Q$ is then the universal ring for formal group laws, which we will name here:

Definition 2.8. *The* ***Lazard ring*** *L is the unique ring and formal group law $F \in L[\![x, y]\!]$ with the universal property that for every formal group law $G \in R[\![x, y]\!]$, there is a map $\phi : L \longrightarrow R$ such that G is the image of F under $\phi : L[\![x, y]\!] \longrightarrow R[\![x, y]\!]$. We have that $L = \mathbb{Z}[c_{i,j}]/Q$ and $F = \sum c_{i,j} x^i y^j$.*

It turns out that the Lazard ring L has a much simpler form, although we will omit the (complicated) proof here.

Proposition 2.9 (Lurie, Lecture 2, Theorem 4)**.** *$L \cong \mathbb{Z}[t_1, t_2, \ldots]$, where each t_i has graded degree $2i$.*

2.2 Spectra

We discuss briefly the notion of spectra, taken largely from Zeshen Gu's thesis [Gu22].

Definition 2.10. *A* ***spectrum*** *is a sequence of based spaces $\{E_n\}_{n \in \mathbb{Z}}$ along with* ***structure maps*** *$\sigma_n : \Sigma E_n \longrightarrow E_{n+1}$, where ΣE_n is taken to be the based suspension.*

Example. The **sphere spectrum** $\mathbb{S}$ has $\mathbb{S}_n = S^n$ and $\sigma_n : \Sigma S^n \longrightarrow S^{n+1}$ the usual identity.

Example. In general, we can take the **suspension spectrum** $\Sigma^\infty X$ for any based space X, with $(\Sigma^\infty X)_n = \Sigma^n X$, and structure maps the obvious identities.

Example. For any abelian group G, we define the **Eilenberg-Maclane spectrum** HG to have $HG_n = K(G, n)$, with structure maps $\Sigma K(G, n) \longrightarrow K(G, n + 1)$ coming from the homotopy equivalence $K(G, n) \simeq \Omega K(G, n + 1)$.

It turns out that spectra are extremely important objects, corepresenting generalized cohomology theories.

Theorem 2.11 (Theorem 2.0.3 in Gu)**.** *Let h^* be a generalized cohomology theory which satisfies the wedge and Mayer-Vietoris axioms. Then there is some spectrum E such that $h^*(X) = [X, E_n]$, the homotopy classes of maps $X \longrightarrow E_n$.*

Definition 2.12. *Given a spectrum E, we define the E-**cohomology** $E^n(X) = [X, E_n]$. We define the E-**homology** as $E_n(X) = [\mathbb{S}_n, X \wedge E_n]$.*

Definition 2.13. *The* ***homotopy groups*** *of a spectrum E are $\pi_n(E) = E_n(\mathbb{S}) = \lim \pi_{n+k}(E_k)$.*

Note that for a suspension spectrum $E = \Sigma^\infty X$, the homotopy groups of E are the stable homotopy groups of X. Observe also that the Eilenberg-Maclane spectrum corepresents usual cohomology: $HG^*(X) = H^*(X; G)$. This explains how the cohomology groups arise, but not how the usual ring structure comes from it.

Definition 2.14. *A* ***ring spectrum*** *is a spectrum E, along with a unit map $\eta : \mathbb{S} \longrightarrow E$ and a multiplication map $\mu : E \wedge E \longrightarrow E$.*

The multiplication map endows E^* with a multiplication from $E^* \otimes E^* \longrightarrow E^*E \longrightarrow E$. From ring spectra, we can define another important class of spectra, those with complex orientations:

Definition 2.15. *Let E be a ring spectrum. A* ***complex orientation*** *of E is a selection of an element $x \in E^2(\mathbb{CP}^\infty)$ which restricts to $1 \in E^2(\mathbb{CP}^1) = E^2(S^2) = \pi_0(E)$ under the usual inclusion $\mathbb{CP}^1 \longrightarrow \mathbb{CP}^\infty$.*

Proposition 2.16 (Theorem 5.1.2 in Gu)**.** *If E is complex oriented, then $E^*(\mathbb{CP}^\infty) = E^*(*)[\![t]\!]$, and $E^*(\mathbb{CP}^\infty \times \mathbb{CP}^\infty) = E^*(*)[\![x, y]\!]$.*

We will usually write $E^*(*) = E^*$ for brevity.

As Lurie explains, this identification of the cohomology rings of $\mathbb{CP}^\infty$ gives us a connection between spectra and formal group laws. Because maps to $\mathbb{CP}^\infty$ classify line bundles, we can pull back our complex orientation to obtain analogues of Chern classes for generalized cohomology theories. To be specific, if $f : X \longrightarrow \mathbb{CP}^\infty$ classifies a line bundle $\xi \longrightarrow X$, we obtain a map $f^* : E^*[\![t]\!] = E^*(\mathbb{CP}^\infty) \longrightarrow E^*(X)$. Then, we can take $c_1^E(\xi) = f^*(t) \in E^2(X)$. Moreover, there is a map $m : \mathbb{CP}^\infty \times \mathbb{CP}^\infty \longrightarrow \mathbb{CP}^\infty$ which classifies the tensor product $\xi \otimes \xi$ of the tautological bundle $\xi \longrightarrow \mathbb{CP}^\infty$ with itself. We can obtain three Chern classes from this map: $x \in E^*(\mathbb{CP}^\infty \times \mathbb{CP}^\infty) = E^*[\![x, y]\!]$ from the first ξ, y from the second ξ, and some $f(x, y) \in E^*[\![x, y]\!]$ as $c_1^E(\xi \otimes \xi)$.

Proposition 2.17 (Lurie, Lecture 1)**.** *We can deduce that $c_1^E(\xi_1 \otimes \xi_2) = f(c_1^E(\xi_1), c_1^E(\xi_2))$ for some function f and any two line bundles $\xi_1, \xi_2 \longrightarrow X$. Moreover, we can conclude from associativity and commutativity of the tensor product of line bundles, that f must satisfy exactly the same axioms that define formal group laws. Therefore, f induces a formal group law over E^*.*

In this way, each complex orientable spectrum gives a formal group law.

2.3 The Complex Bordism Spectrum MU

Definition 2.18. *We may define a cohomology theory which considers not just maps of simplices $\Delta^n \longrightarrow X$, but all oriented manifolds $Z \longrightarrow X$. Oriented cobordism classes of these maps give the MU-**cohomology** of a space X, written $MU^*(X)$.*

One can check that MU^* is a legitimate cohomology theory. With this conclusion, MU^* must come from a spectrum, which we will call MU. It turns out that there is another construction of MU, which gives a more clear view of its properties. We will not show these are equivalent, but we give the construction here, adapted from Gu:

We take the tautological bundle $\xi_n \longrightarrow BU(n)$ and 'Thomify' it, to get the bundle $Th(\xi_n) \longrightarrow BU(n)$. We will take $MU_{2n} = Th(\xi_n)$ and $MU_{2n+1} = \Sigma MU_{2n}$. The structure maps $\Sigma MU_{2n} \longrightarrow MU_{2n+1}$ are obvious. Recalling that $X \wedge S^n \cong \Sigma^n X$, we take

$$\sigma_{2n+1} : \Sigma^2 Th(\xi_n) \cong Th(\xi_n) \wedge S^2 \cong Th(\xi_n \oplus \mathbb{C}) \longrightarrow Th(\xi_{n+1}).$$

From this second definition, we obtain a ring spectrum structure on MU: we can take the square

$$\begin{tikzcd}
\xi_n \times \xi_m \arrow[r] \arrow[d] & \xi_{n+m} \arrow[d] \\
BU(n) \times BU(m) \arrow[r, "\hat{P}"] & BU(n+m)
\end{tikzcd}$$

and get a map $Th(\xi_n) \wedge Th(\xi_m) \longrightarrow Th(\xi_{n+m})$. This map induces the multiplication. In fact, MU is a so-called $\mathbb{E}_\infty$ ring spectrum, a commutative algebra object in spectra.

A natural question, now, is to ask whether this ring spectrum has a complex orientation, and therefore whether we obtain a formal group law on MU_*. The answer, it turns out, is that yes,

MU has a canonical orientation (and in fact, this is a universal complex orientation). We have that $MU^2(\mathbb{CP}^\infty) = [\mathbb{CP}^\infty, Th(\xi_1)]$. Because $\mathbb{CP}^\infty$ is, in fact, $BU(1)$, we observe there is a natural map

$$\mathbb{CP}^\infty \cong BU(1) \simeq D(\xi_1) \longrightarrow D(\xi_1)/S(\xi_1) \cong Th(\xi_1).$$

Moreover, as Gu explains, this map is actually a homotopy equivalence. In particular, as we observed earlier, this complex orientation gives rise to a canonical formal group law F on MU_*. This formal group law is induced by a map $\phi : L \longrightarrow MU_*$. Remarkably, this map is an isomorphism:

Proposition 2.19 (Gu, Theorem 5.1.4, from Quillen)**.** *The classifying map $\phi : L \longrightarrow MU_*$ for the formal group law on MU (from Proposition 2.17) is an isomorphism.*

Note that this gives us an isomorphism $MU_* \cong L \cong \mathbb{Z}[t_1, t_2, \dots]$. It isn't clear what each of these generators means, however, and so we will seek to find a different set of generators. Our first thought would be taking the classes $c_n = [\mathbb{CP}^n] \in MU_{2n}(*)$. These classes do generate MU_* rationally, but unfortunately they fail to do so integrally. Luckily, we can compute **Hazewinkel generators** from the classes c_n:

Proposition 2.20 (6.2.1 in Gu, from Hazewinkel)**.** *$MU_* \cong \mathbb{Z}[x_1, x_2, \dots]$, where the x_i are given from the formula*

$$\frac{1}{m} v(m) c_{m-1} = x_{m-1} + \sum_{d \,|\, m, d \neq 1, m} \frac{\mu(m,d) v(m)}{v(d)} l_{\frac{m}{d}-1} x_{d-1}^{\frac{m}{d}},$$

where

$$v(m) = \begin{cases} q & \text{if } m = q^r, r \geq 1 \\ 1 & \text{otherwise} \end{cases}$$

and

$$\mu(m,d) = \prod_{q \,|\, m} c(q,d)$$

is a product ranging over primes q, with $c(q,d) = 1$ if $v(d) = 1$ or q, and otherwise $c(q,d)$ is some integer $\equiv 1 \mod q$ and $\equiv 0 \mod v(d)$.

Recall that earlier we mentioned MU is an $\mathbb{E}_\infty$ ring spectrum. In general, we would like to study **genera**: $\mathbb{E}_\infty$ maps $MU \longrightarrow R$. These maps are usually quite difficult to understand, but we can make sense of some of their properties with the **power operations**. The usual pth power operation is a ring map

$$R_* \longrightarrow R_*[\![\alpha]\!]/\langle p \rangle(\alpha)$$

which is induced by the $\mathbb{E}_\infty$ properties of R. The power operation is natural in the sense that if $MU \longrightarrow R$ is an $\mathbb{E}_\infty$ ring spectra map, we obtain a commutative square

$$\begin{tikzcd} MU_* \arrow[r, "P"] \arrow[d, "f"'] & MU_*[\![\alpha]\!]/\langle 2 \rangle(\alpha) \arrow[d] \\ R_* \arrow[r] & R_*[\![\alpha]\!]/\langle 2 \rangle(\alpha) \end{tikzcd}$$

Using this square, then, it is possible to study what sort of coefficient rings these $\mathbb{E}_\infty$ ring spectra can have. In general, the power operation is quite complex, but fortunately, we know what it does to the classes $c_n = [\mathbb{CP}^n]$.

Proposition 2.21 (Gu, Theorem 6.1.3, from Johnson and Noel)**.** *Let q_* be the quotient $MU_*[\![\alpha]\!]/[p](\alpha) \longrightarrow MU_*[\![\alpha]\!]/\langle p \rangle(\alpha)$. We have*

$$q_* \chi^{2m} P(c_m) = \chi^{2m+1} \sum_{k=0}^{m} c_{m-k} \operatorname{coeff}((\sum_{i \geq 0} a_i z^i)^{-(m+1)}, z^k),$$

where

$$\chi = \prod_{i=1}^{p-1} [i](\alpha) \in MU^*[\![\alpha]\!]/[p](\alpha)$$

$$x \sum_{i \geq 0} a_i x^i = \prod_{i=0}^{p-1} (x +_F [i](\alpha)).$$

At this point, we have the tools to computationally approach the central conjecture of this paper.

2.4 Chromatic Blueshift Conjecture

Burklund, Schlank, and Yuan make a very general conjecture, outlined in Conjecture 9.9 of [BSY22]. We investigate a subcase, specifically restricting to $A = C_p$ for a prime p, $\mathcal{F} = \emptyset$, and arbitrary $n \geq 1$.

Definition 2.22. *The C_p-Tate fixed points R is the ring*

$$R^{tC_p} = \alpha^{-1} R[\![\alpha]\!]/[p](\alpha) \tag{2}$$

Conjecture 2.23 (case of Chromatic Blueshift Conjecture)**.** *If $f : MU \longrightarrow R$ is an $\mathbb{E}_\infty$ map between ring spectra such that*

$$f(v_n)^k = 0 \mod (p, v_1, \ldots, v_{n-1})$$

then we have that

$$v_{n-1}^{-1} R^{tC_p}/(p, \ldots, v_{n-2}) = 0$$

That is, it is the trivial ring.

For example, at $n = 1$, this says that if $f(v_1)^k = 0 \bmod p$, then $p^{-1}R^{tC_p}$ is the trivial ring (note that $v_0 = p$).

Note that we do not attempt to tackle the conjecture in the case of other finite abelian groups A or other families of subgroups $\mathcal{F}$, and rather restrict to the simplest nontrivial case of $A = C_p$. We will show in the following sections that this conjecture holds in the case $k = 1$, but an algebraic analogue fails in general for higher values of k. Namely, we demonstrate the following two results:

Theorem 2.24. *If $f : MU \longrightarrow R$ is an $\mathbb{E}_\infty$ map between ring spectra and $f(v_n) = 0 \mod (p, v_1, \ldots, v_{n-1})$, then $v_{n-1}^{-1} R^{tC_p}/(v_0, \ldots, v_{n-2})$ is the trivial ring.*

Note that this directly addresses and establishes subcase of the conjecture. The next result we show is about a purely algebraic analogue of the conjecture, and shows that it fails to hold in general for higher k.

Theorem 2.25. *At $p = 2$, there exists a ring R, a ring map $f : MU \longrightarrow R$, and an induced ring map $\hat{P} : R \longrightarrow R[\![\alpha]\!]/\langle 2 \rangle(\alpha)$ fitting into the commutative diagram:*

$$\begin{tikzcd} MU_* \arrow[r, "P"] \arrow[d, "f"'] & MU_*[\![\alpha]\!]/\langle 2 \rangle(\alpha) \arrow[d] \\ R \arrow[r, "\hat{P}"] & R[\![\alpha]\!]/\langle 2 \rangle(\alpha) \end{tikzcd} \tag{3}$$

which satisfies $f(v_1)^2 = 0 \mod 2$, and yet $2^{-1}R^{tC_p}$ is not the trivial ring.

Note that if R can be realized as the homotopy of a ring spectrum getting its complex orientation from the prescribed classifying map $f : MU_* \longrightarrow R$, then this would disprove the conjecture by means of a counterexample at $p = 2, k = 2$.

3 The Case $k = 1$

We show that the conjecture is true in the simplest cases, where the exponent is 1.

Theorem 3.1. *If $f : MU \longrightarrow R$ is an $\mathbb{E}_\infty$ map and $f(v_n) = 0 \mod (p, v_1, \ldots, v_{n-1})$, then $v_{n-1}^{-1} R^{tC_p}/(v_0, \ldots, v_{n-2})$ is the trivial ring.*

Why would we expect this to be true? Based on Gu's computations, we observe the following pattern, for $p = 2$:

$$\begin{aligned} P(x_1) &= x_1^2 + x_3\alpha + (x_1^4 + x_1^2 x_2 + x_1 x_3)\alpha^2 + \cdots \\ P(x_3) &= x_3^2 + (x_1^4 x_3 + x_1 x_3^2 + x_7)\alpha + \cdots \\ &= x_3^2 + x_7\alpha + \cdots \mod x_1 \\ &\vdots \end{aligned}$$

It turns out that $P(x_7) = x_7^2 + x_{15}\alpha + \cdots \mod (x_1, x_3)$, and we will show that this pattern continues. There is an analogue for higher primes p, which we will state and prove in Lemma 3.7, from which we can readily prove the Theorem. We'll start by building up a series of Lemmas.

Lemma 3.2. *We have that $[p](\alpha) = v_n\alpha^{p^n} + O(\alpha^{2p^n}) \mod (p, v_1, \ldots, v_{n-1})$.*

Proof. We make use of Proposition 2.3. In $R/(p, v_1, v_2, \ldots, v_{n-1})$, we have $p = 0$, so Proposition 2.3 applies to $[p](\alpha)$. Because v_n is the smallest v_i which may not be zero, Proposition 2.3 asserts that $[p](\alpha) = h'(\alpha^{p^m})$ for $m \geq n$, $h'(t) = \lambda t + O(t^2)$. Hence it must be the case that $[p](\alpha) = v_m\alpha^{p^m} + O(\alpha^{2p^m}) = v_n\alpha^{p^n} + O(\alpha^{2p^n}) \mod (p, v_1, \ldots, v_{n-1})$. □

Lemma 3.3. $c_{p^n-1} = p^{n-1}v_n \mod v_1, \ldots, v_{n-1}$.

Proof. Recall that Proposition 2.20 states that

$$\frac{1}{m} v(m) c_{m-1} = x_{m-1} + \sum_{d \,|\, m, d \neq 1, m} \frac{\mu(m,d) v(m)}{v(d)} l_{\frac{m}{d}-1} x_{d-1}^{\frac{m}{d}},$$

where

$$v(m) = \begin{cases} q & \text{if } m = q^r, r \geq 1 \\ 1 & \text{otherwise} \end{cases}$$

and

$$\mu(m,d) = \prod_{q \,|\, m} c(q,d)$$

is a product ranging over primes q, with $c(q,d) = 1$ if $v(d) = 1$ or q, and otherwise $c(q,d)$ is some integer $\equiv 1 \mod q$ and $\equiv 0 \mod v(d)$.

For $m = p$, the sum vanishes, and $v(p) = p$, so we conclude that $c_{p-1} = x_{p-1} = v_1$. Taking $m = p^n$, observe that the sum goes through $d = p, p^2, p^3, \ldots, p^{n-1}$, and so each term of the sum will have a factor of $x_{d-1}^{\frac{m}{d}} = v_i^{p^{n-i}}$, where i ranges over $1, 2, \ldots, n-1$. Operating mod each of $v_1, v_2, \ldots, v_{n-1}$, we see that the sum again vanishes, and so we are left with

$$\frac{1}{p^n} p \cdot c_{p^n-1} = v_n \mod (v_1, \ldots, v_{n-1}).$$

Multiplying by p^{n-1} gives the desired result. □

Lemma 3.4. *If $p^r \mid k$ for $r \geq 1$, then $c_{k-1} = 0 \mod (p^r, v_1, \ldots, v_r)$.*

Proof. We start with $r = 1$. If $k = p$, then Lemma 3.3 tells us that $c_{p-1} = v_1 = 0 \mod (p, v_1)$. We induct on k: if $k > p$, assume that the statement holds for all $l < k$. Then Proposition 2.20, with $m = k$, gives

$$\frac{1}{k}v(k)c_{k-1} = x_{k-1} + \sum_{d \,|\, k, d \neq 1, k} \frac{\mu(k,d)v(k)c_{\frac{k}{d}-1}}{v(d)\frac{k}{d}} x_{d-1}^{\frac{k}{d}}.$$

We multiply through by $\frac{k}{v(k)}$ and get

$$c_{k-1} = \frac{k \cdot x_{k-1}}{v(k)} + \sum_{d \,|\, k, d \neq 1, k} \frac{d \cdot \mu(k,d)c_{\frac{k}{d}-1}}{v(d)} x_{d-1}^{\frac{k}{d}}.$$

Consider possible values of d on the sum in the right-hand side. If $p \,|\, \frac{k}{d}$, then $c_{\frac{k}{d}-1} = 0 \mod (p, v_1)$ by our inductive hypothesis, and $v(d) \,|\, d$, so this coefficient is an integer and

$$\frac{d \cdot \mu(k,d)c_{\frac{k}{d}-1}}{v(d)} x_{d-1}^{\frac{k}{d}} = 0 \mod (p, v_1).$$

Otherwise, d is the maximal power of p dividing k. Note that $d \neq k$, since the sum forbids this, so we can safely say that k is not itself a prime power. In this case, k has another prime factor p', and Gu tells us that $\mu(k,d)$ is divisible by p in this case. Then $v(d) = p \,|\, d$, so the coefficient $\frac{d \cdot \mu(k,d)}{v(d)}$ is an integer. So we see that $p \,|\, \frac{d \cdot \mu(k,d)}{v(d)}$, and hence the entire sum vanishes mod (p, v_1). Then in fact, $c_{k-1} = x_{k-1} \cdot \frac{k}{v(k)}$ mod (p, v_1). But we know that $k > p$, so either (1) k is a prime power p^s, in which case $\frac{k}{v(k)} = p^{s-1}$; or (2) k is not a prime power, in which case $\frac{k}{v(k)} = k$. Either way, $p \,|\, \frac{k}{v(k)}$, and so it vanishes mod (p, v_1).

We now turn our attention to the inductive step. Assume that the statement holds for all $s < r$, and suppose $r > 1$. If $k = p^r$, then Lemma 3.3 tells us that

$$\begin{aligned} c_{k-1} = c_{p^r-1} &= p^{r-1}v_r \quad \mod (v_1, \ldots, v_{r-1}) \\ &= 0 \qquad\qquad \mod (p^r, v_1, \ldots, v_{r-1}, v_r). \end{aligned}$$

We will use this as an inductive base case. If $k > p^r$, assume that the statement holds for all $l < k$.As before, we first consider values of d in the right-hand sum. If $p^r \,|\, \frac{k}{d}$, then $c_{\frac{k}{d}-1} = 0 \mod (p^r, v_1, \ldots, v_r)$ by our inductive hypothesis. If this is not the case, then some maximal power p^s divides $\frac{k}{d}$, where $s < r$. If $s = 0$, then $p^r \,|\, d$, whence it follows that $\frac{d}{v(d)} = p^{r-1}$. Moreover, since $d \neq k$, k has another prime divisor p', and the formula for $\mu(k,d)$ tells us this means $p \,|\, \mu(k,d)$. So in total, $p^r = p^{r-1} \cdot p \,|\, \frac{d \cdot \mu(k,d)}{v(d)}$, and so the term in the sum vanishes mod p^r.

Finally, if $0 < s < r$, our inductive hypothesis tells us that $c_{\frac{k}{d}-1} = 0 \mod (p^s, v_1, \ldots, v_s)$. If d is not a prime power, then $p^{r-s} \,|\, \frac{d}{v(d)}$ and so p^r divides the entire coefficient. But if d is a prime power p^t, then $\frac{d}{v(d)} = p^{t-1}$. If k itself is a prime power p^q, then our assumption $k > p^r$ implies $q > r$, and thus $t > n - s$, so $(t-1) + s \geq n$, in which case p^r again divides the entire coefficient. And at last, if k is not a prime power, then $p \,|\, \mu(k,d)$, so once more p^r divides the whole coefficient. So indeed, the sum on the right-hand side vanishes mod $(p^r, v_1, \ldots, v_r)$.

Now $c_{k-1} = x_{k-1} \cdot \frac{k}{v(k)} \mod (p^r, v_1, \ldots, v_r)$. Again, $k > p^r$, so either (1) k is a prime power p^s for $s > r$, in which case $\frac{k}{v(k)} = p^{s-1}$; or (2) k is not a prime power, in which case $\frac{k}{v(k)} = k$. Either way, $p^r \,|\, \frac{k}{v(k)}$, and so it vanishes mod $(p^r, v_1, \ldots, v_r)$, as required. □

Lemma 3.5. *If $p \nmid q'$, where p is a prime, and if $r \geq s$, then $\binom{p^r q}{p^s q'}$ is divisible by p^{r-s}.*

Proof. We use the formula $\binom{p^r q}{p^s q'} = \frac{p^r q}{p^s q'}\binom{p^r q - 1}{p^s q' - 1}$. The right-hand side simplifies to $\frac{p^{r-s} q}{q'}\binom{p^r q-1}{p^s q'-1}$. Because $p \nmid q'$, $p^{r-s} \,|\, \frac{p^{r-s} q}{q'}\binom{p^r q-1}{p^s q'-1}$, and hence $p^{r-s} \,|\, \binom{p^r q}{p^s q'}$. □

Each of these facts builds up to the following technical Lemma. This is an important result, but the proof is highly combinatorial, and not at all enlightening. The reader should proceed at her own risk.

Lemma 3.6. $\chi^{2(p^n-1)}P(c_{p^n-1}) = p^{n-1}v_n\chi^{p^n-1} \mod (p^n, v_1, \dots, v_{n-1}, \langle p\rangle(\alpha))$.

Proof. We begin with a computation from Proposition 2.21, which we recall states that

$$q_*\chi^{2m}P(c_m) = \chi^{2m+1}\sum_{k=0}^{m} c_{m-k}\,\mathrm{coeff}((\sum_{i\geq 0} a_i z^i)^{-(m+1)}, z^k),$$

where

$$\chi = \prod_{i=1}^{p-1}[i](\alpha) \in MU^*[\![\alpha]\!]/[p](\alpha)$$

$$x\sum_{i\geq 0} a_i x^i = \prod_{i=0}^{p-1}(x +_F [i](\alpha)).$$

At $m = p^n - 1$, this evaluates to

$$\chi^{2(p^n-1)}P(c_{p^n-1}) = \chi^{2p^n-1}\sum_{k=0}^{p^n-1} c_{p^n-k-1}\,\mathrm{coeff}((\sum_{i\geq 0} a_i z^i)^{-p^n}, z^k).$$

First, write

$$h := \left(\sum_{i\geq 0} a_i z^i\right)^{-1} = \frac{1}{a_0} + \sum_{i\geq 1} w_i z^i$$

for appropriate coefficients w_i. For $0 \leq k < p^n$, take any term $z^k \prod w_i^{b_i}$, for $\sum b_i = p^n$ and $\sum ib_i = k$. Then we must have

$$\mathrm{coeff}(h^{p^n}, z^k \prod w_i^{b_i}) = \binom{p^n}{b_0}\binom{p^n - b_0}{b_1}\cdots\binom{b_k}{b_k}.$$

Write each $b_i = p^{r_i}q_i$ for $p \nmid q_i$. Without loss of generality, we assume each b_i is nonzero (if some $b_j = 0$ then we can just ignore it, since $\binom{m}{0} = 1$). Since r_0 is not divisible by p, we can apply Lemma 3.5 to learn that $p^{n-r_0} \mid \binom{p^n}{b_0}$. In fact, at each index i, we know that $\min(r_0, r_1, \dots, r_{i-1}) \mid (p^n - b_0 - b_1 - \cdots - b_{i-1})$. So

$$p^{\max(0, \min(r_0, r_1, \dots, r_{i-1}) - r_i)} \mid \binom{p^n - b_0 - b_1 - \cdots - b_{i-1}}{b_i}.$$

In total, this means that the power p^M of p dividing $\mathrm{coeff}(h^{p^n}, z^k \prod w_i^{b_i})$ is at least

$$M \geq n - r_0 + \sum_{i>0}^{k} \max(0, \min(r_0, r_1, \dots, r_{i-1}) - r_i).$$

We'd like to ignore the indices i where $\min(r_0, r_1, \dots, r_{i-1}) - r_i \leq 0$, so we index these as $r_0 = r_{j_0}, r_{j_1}, \dots, r_{j_N}$. In particular, if some r_i is not among these, then $r_i \geq \min(r_0, r_1, \dots, r_{i-1})$, so that $\min(r_0, r_1, \dots, r_{i-1}) = \min(r_0, r_1, \dots, r_{i-1}, r_i)$. In other words, at each j_i, $\min(r_0, r_1, \dots, r_{j_i - 1}) = \min(r_{j_0}, r_{j_1}, \dots, r_{j_{i-1}})$. Moreover, because $r_{j_i} < \min(r_0, r_1, \dots, r_{j_i-1})$, it must be the case that $\min(r_{j_0}, r_{j_1}, \dots, r_{j_{i-1}}) = r_{j_{i-1}}$. We can thus rewrite the power of p dividing $\mathrm{coeff}(h^{p^n}, z^k \prod w_i^{b_i})$ as at least

$$\begin{aligned}
M &\geq n - r_{j_0} + \sum_{i>0}^{N} \max(0, \min(r_{j_0}, r_{j_1}, \dots, r_{j_{i-1}}) - r_{j_i}) \\
&= n - r_{j_0} + \sum_{i>0}^{N} \min(r_{j_0}, r_{j_1}, \dots, r_{j_{i-1}}) - r_{j_i} \\
&= n - r_{j_0} + \sum_{i>0}^{N} r_{j_{i-1}} - r_{j_i} \\
&= n - r_{j_N}.
\end{aligned}$$

Unraveling the definitions, we have that r_{j_N} is the smallest power of p dividing any of the b_i's. So in fact, $p^{r_{j_N}}$ divides each b_i. This implies that $k = \sum i \cdot b_i$ is divisible by $p^{r_{j_N}}$, and then that $\mathrm{coeff}(h^{p^n}, z^k \prod w_i^{b_i})$ is divisible by $p^{n-r_{j_N}}$. If $p^r \mid k$, then in any way we decompose $k = \sum i \cdot b_i$ with $r_{j_N} \leq r$, we get that $p^{n-r_{j_N}}$ divides the z^k-coefficient, and $p^{n-r} \mid p^{n-r_{j_N}}$. So in fact, we have p^{n-r} always divides the z^k-coefficient.

Then, by Lemma 3.4, the term $c_{p^n-k-1} = 0 \mod (p^r, v_1, \ldots, v_r)$. If $k \neq 0$, then we conclude the z^k-term vanishes mod $(p^n, v_1, \ldots, v_{n-1})$. So the only term that remains in the entire sum is at $k = 0$. By Lemma 3.3, this reduces to $\frac{1}{a_0^{p^n}} p^{n-1} v_n \mod (p^n, v_1, \ldots, v_{n-1})$. We have shown that $\chi = a_0$, so the desired result follows:

$$\chi^{2(p^n-1)} P(c_{p^n-1}) = p^{n-1} v_n \chi^{p^n-1} \mod (p^n, v_1, \ldots, v_{n-1}, \langle p \rangle(\alpha)).$$

□

With these tools in hand, we can proceed with the proof of a strong Lemma.

Lemma 3.7.

$$\frac{\chi^{2(p^n-1)}}{\alpha^{2(p^n-1)}} P(v_n) = \frac{v_n \chi^{p^n-1} - \frac{\chi^{p^n-1}}{\alpha^{p^n-1}} \langle p \rangle(\alpha)}{\alpha^{2p^n-2}} \mod \left(p, v_1, \ldots, v_{n-1}, \frac{[p](\alpha)}{\alpha^{p^n}}\right)$$

Proof. By Lemma 3.6, write

$$\chi^{2(p^n-1)} P(c_{p^n-1}) = p^{n-1} v_n \chi^{p^n-1} \mod (p^n, v_1, \ldots, v_{n-1}, \langle p \rangle(\alpha)).$$

We first inspect the left-hand side. By Lemma 3.3, $c_{p^n-1} = p^{n-1} v_n \mod v_1, \ldots, v_{n-1}$. Then we can expand

$$\chi^{2(p^n-1)} P(c_{p^n-1}) = \chi^{2(p^n-1)} P(p^{n-1} v_n) + \chi^{2(p^n-1)} P(\sum b_{i_1, i_2, \ldots, i_n} v_1^{i_1} v_2^{i_2} \cdots v_n^{i_n}).$$

Assuming inductively that each $P(v_i) = \frac{v_i \chi^{p^i-1} - \frac{\chi^{p^i-1}}{\alpha^{p^i-1}} \langle p \rangle(\alpha)}{\alpha^{2p^i-2}} \mod (p, v_1, \ldots, v_{i-1}, \frac{[p](\alpha)}{\alpha^{p^i}})$ for $i = 1, \ldots, n-1$, the denominator powers of the α cancel with the factor $\alpha^{2(p^n-1)}$ of $\chi^{2(p^n-1)}$, and so

$$\chi^{2(p^n-1)} P(c_{p^n-1}) = \chi^{2(p^n-1)} P(p^{n-1} v_n) + \sum b_{i_1, i_2, \ldots, i_{n-1}} \prod_{i=1}^{n-1} \left(v_i \chi^{p^i-1} - \frac{\chi^{p^i-1}}{\alpha^{p^i-1}} \langle p \rangle(\alpha)\right)^{i_i}.$$

Hence, modulo $v_1, \ldots, v_{n-1}$, we see that

$$\begin{aligned}\chi^{2(p^n-1)} P(c_{p^n-1}) &= \chi^{2(p^n-1)} P(p^{n-1} v_n) + \sum b_{i_1, i_2, \ldots, i_{n-1}} \prod_{i=1}^{n-1} \left(v_i \chi^{p^i-1} - \frac{\chi^{p^i-1}}{\alpha^{p^i-1}} \langle p \rangle(\alpha)\right)^{i_i} \\ &= \chi^{2(p^n-1)} P(p^{n-1} v_n) + \sum b_{i_1, i_2, \ldots, i_{n-1}} \prod_{i=1}^{n-1} \left(-\frac{\chi^{p^i-1}}{\alpha^{p^i-1}} \langle p \rangle(\alpha)\right)^{i_i} \\ &= \chi^{2(p^n-1)} P(p^{n-1} v_n) \mod \langle p \rangle(\alpha).\end{aligned}$$

So we can write

$$p^{n-1} \chi^{2(p^n-1)} P(v_n) = p^{n-1} v_n \chi^{p^n-1} \mod (p^n, v_1, \ldots, v_{n-1}, \langle p \rangle(\alpha)),$$

and dividing by p^{n-1} we see that

$$\chi^{2(p^n-1)} P(v_n) = v_n \chi^{p^n-1} \mod (p, v_1, \ldots, v_{n-1}, \langle p \rangle(\alpha)). \tag{4}$$

We also know, by Lemma 3.2, that

$$[p](\alpha) = v_n \alpha^{p^n} + O(\alpha^{2p^n}) \mod (p, v_1, \ldots, v_{n-1}),$$

so dividing by α we have

$$\langle p\rangle(\alpha) = v_n\alpha^{p^n-1} + O(\alpha^{2p^n-1}) \mod (p, v_1, \ldots, v_{n-1}). \tag{5}$$

Subtracting a multiple of the second equation from the first, we obtain that

$$\chi^{2(p^n-1)}P(v_n) = v_n\chi^{p^n-1} - \frac{\chi^{p^n-1}}{\alpha^{p^n-1}}\langle p\rangle(\alpha) = O(\alpha^{2p^n-1}) \mod (p, v_1, \ldots, v_{n-1}, \langle p\rangle(\alpha)).$$

Then indeed, because we've shown the right-hand side to be divisible by $\alpha^{2(p^n-1)}$, we can take this to be modulo $\frac{[p](\alpha)}{\alpha^{p^n}}$, which has a nonzero constant term, making α a non-zero divisor. So we divide by $\alpha^{2(p^n-1)}$:

$$\frac{\chi^{2(p^n-1)}}{\alpha^{2(p^n-1)}}P(v_n) = \frac{v_n\chi^{p^n-1} - \frac{\chi^{p^n-1}}{\alpha^{p^n-1}}\langle p\rangle(\alpha)}{\alpha^{2p^n-2}} \mod (p, v_1, \ldots, v_{n-1}, \frac{[p](\alpha)}{\alpha^{p^n}}).$$

□

Corollary 3.8. *At $p = 2$, $P(v_n) = v_{n+1}\alpha + O(\alpha^2) \mod (2, v_1, \ldots, v_{n-1}, \frac{[2](\alpha)}{\alpha^{2^n}})$.*

Corollary 3.9. *If $f(v_n) = 0 \mod p$, then for $i = n+1, n+2, \ldots,$ $f(v_i) = 0 \mod (p, v_1, \ldots, v_{n-1})$.*

Proof. We abuse notation and set $v_n = 0$. By Lemma 3.7, we see that

$$\begin{aligned}\frac{\chi^{2(p^n-1)}}{\alpha^{2(p^n-1)}}P(v_n) &= \frac{v_n\chi^{p^n-1} - \frac{\chi^{p^n-1}}{\alpha^{p^n-1}}\langle p\rangle(\alpha)}{\alpha^{2p^n-2}} \mod (p, v_1, \ldots, v_{n-1}, \frac{[p](\alpha)}{\alpha^{p^n}}) \\ 0 &= \frac{\chi^{p^n-1}\langle p\rangle(\alpha)}{\alpha^{3p^n-3}} \mod (p, v_1, \ldots, v_{n-1}, \frac{[p](\alpha)}{\alpha^{p^n}}).\end{aligned}$$

We know that

$$\chi = \prod_{i=1}^{p-1}[i](\alpha) \in MU^*[\![\alpha]\!]/[p](\alpha).$$

Also, $[i](\alpha) = i\alpha + O(\alpha^2)$, so $\chi = (p-1)!\alpha^{p-1} + O(\alpha^p)$. This means that in Lemma 3.7, we could have divided out further by powers of α: not only does $\chi^{2(p^n-1)}$ have a factor of $\alpha^{2(p^n-1)}$, but it is actually divisible by $\alpha^{2(p^n-1)(p-1)}$. Then our equation becomes

$$0 = \frac{\chi^{p^n-1}\langle p\rangle(\alpha)}{\alpha^{2(p^n-1)(p-1)+p^n-1}} \mod (p, v_1, \ldots, v_{n-1}, \frac{[p](\alpha)}{\alpha^{p^n}}).$$

We additionally know $\langle p\rangle(\alpha) = v_{n+1}\alpha^{p^{n+1}-1} + O(\alpha^{p^{n+1}})$. Now, the previous equation says that mod $(p, v_1, \ldots, v_{n-1})$,

$$\frac{\chi^{p^n-1}\langle p\rangle(\alpha)}{\alpha^{2(p^n-1)(p-1)+p^n-1}} = g\frac{[p](\alpha)}{\alpha^{p^n}}$$

for some power series g. The left hand side reduces to

$$\begin{aligned}\frac{\chi^{p^n-1}\langle p\rangle(\alpha)}{\alpha^{2p^{n+1}-p^n-2p+1}} &= \frac{1}{\alpha^{2p^{n+1}-p^n-2p+1}}\left((p-1)!\alpha^{p-1} + O(\alpha^p)\right)^{p^n-1}(v_{n+1}\alpha^{p^{n+1}-1} + O(\alpha^{p^{n+1}})) \\ &= \frac{1}{\alpha^{2p^{n+1}-p^n-2p+1}}\left(v_{n+1}(p-1)!^{p^n-1}\alpha^{(p^n-1)(p-1)+p^{n+1}-1} + O(\alpha^{(p^n-1)(p-1)+p^{n+1}})\right) \\ &= v_{n+1}(p-1)!^{p^n-1}\alpha^{p-1} + O(\alpha^p).\end{aligned}$$

However, we know that

$$\frac{[p](\alpha)}{\alpha^{p^n}} = v_{n+1}\alpha^{p^{n+1}-p^n} + O(\alpha^{p^{n+1}-p^n+1}),$$

and the lowest-degree terms don't match at all. At α^{p-1}, the left-hand side has a coefficient of $(p-1)!^{p^n-1}v_{n+1}$, but the right-hand side is zero! So indeed, v_{n+1} must be zero, or else $(p-1)! = p-1$ mod p would be a zero-divisor, which is absurd.

We can continue this argument inductively: after having shown that $v_{n+1}, \dots, v_{n+m-1} = 0$, the left-hand side becomes

$$\frac{\chi^{p^n-1}\langle p\rangle(\alpha)}{\alpha^{2p^{n+1}-p^n-2p+1}} = v_{n+m}(p-1)!^{p^n-1}\alpha^{p^{n+m}-p^{n+1}+p-1} + O(\alpha^{p^{n+m}-p^{n+1}+p}),$$

and the p-series is

$$\frac{[p](\alpha)}{\alpha^{p^n}} = v_{n+1}\alpha^{p^{n+m}-p^n} + O(\alpha^{p^{n+m}-p^n+1}).$$

As before, we consult the $\alpha^{p^{n+m}-p^{n+1}+p-1}$-term. We end up with the equality $v_{n+m}(p-1)!^{p^n-1} = 0$, and therefore $v_{n+m} = 0$. So indeed, each of $v_{n+1}, v_{n+1}, \dots = 0 \mod (p, v_1, \dots, v_{n-1})$. □

We finally have enough machinery to catch a much bigger fish, and we prove Theorem 3.1. With all the work we have done thus far, Theorem 3.1 becomes relatively easy.

Proof of Theorem 3.1. Assume that $v_n = 0 \mod p$. As in the $n = 1$ case, our aim is to show that $[p](\alpha)$ is a unit in $v_{n-1}^{-1}R^{tC_p}/(p, \dots, v_{n-2}) = v_{n-1}^{-1}\alpha^{-1}R[\![\alpha]\!]/([p](\alpha), p, \dots, v_{n-2})$. In $R[\![\alpha]\!]/(p, \dots, v_{n-2})$, we have

$$[p](\alpha) = v_{n-1}\alpha^{p^{n-1}} + O(\alpha^{p^{n-1}+1}).$$

Then once we invert v_{n-1} and α, we note

$$v_{n-1}^{-1}\alpha^{-p^{n-1}}[p](\alpha) = 1 + O(\alpha),$$

and so we can try to invert it in the usual way. As in the $n = 1$ case, our only barrier is powers of v_{n-1} growing without bound in the denominator. But again, this turns out to be a non-issue: if we have any term $c\alpha^n$ in $[p](\alpha) \in R[\![\alpha]\!]/(p, \dots, v_{n-2})$, then for some m, $p^m > n$, and so $c = 0 \mod p, v_1, \dots, v_{m-1}$. So c is some linear combination of $p, v_1, \dots, v_{m-1}$ in $R[\![\alpha]\!]$, and hence c is a linear combination of $v_{n-1}, \dots, v_{m-1}$ in $R[\![\alpha]\!]/(p, \dots, v_{n-2})$. But in fact, by Lemma 2, each of $v_n, v_{n+1}, \dots, v_{m-1} = 0 \mod (p, v_1, \dots, v_{n-1})$. In other words, in $R[\![\alpha]\!]/(p, \dots, v_{n-2})$, each of $v_n, v_{n+1}, \dots, v_{m-1} = 0 \mod v_{n-1}$. So indeed, c is divisible by v_{n-1} in $R[\![\alpha]\!]/(p, \dots, v_{n-2})$. We conclude, then, that the p-series is divisible by v_{n-1} and hence $v_{n-1}^{-1}\alpha^{-p^{n-1}}[p](\alpha)$ is a unit in $R[\![\alpha]\!]/(p, \dots, v_{n-2})$. It follows that $[p](\alpha) \in v_{n-1}^{-1}\alpha^{-1}R[\![\alpha]\!]/(p, v_1, \dots, v_{n-2})$ is a unit, and hence $v_{n-1}^{-1}R^{tC_p}/(v_0, \dots, v_{n-2})$ is the trivial ring. □

4 Higher Values of k

It turns out that if we want to invert the p-series, it is generally necessary to have the ideal $(v_1, v_2, \dots)^N$ vanish modulo p^N. We show that it is possible for a ring R, endowed with a coherent "power operation" $\hat{P}$, to satisfy $(v_1, v_2, \dots)^N = 0 \mod p$, but not mod p^N. We then show that $p^{-1}R^{tC_p}$ is nontrivial, and we conclude that if R can be written as the homotopy groups of an $\mathbb{E}_\infty$ ring spectrum E, then E provides a contradiction to Conjecture 2.23.

Construction 4.1.

We take $R = MU[b_{ij}]_{i \geq j \geq 1}/(x_i x_j - 2b_{ij})$. In order to define a power operation $\hat{P}$ on R, though, we need to determine $\hat{P}(b_{ij})$. Proceeding in the obvious way, we will define $\hat{P}(b_{ij}) = \frac{1}{2}(f \circ P)(x_i x_j)$. It is not obvious that $(f \circ P)(x_i x_j)$ is divisible by 2, however. But note: if we write

$$P(x_i) = \sum_{k=0}^{\infty} \gamma_k \alpha^k$$

$$P(x_j) = \sum_{k=0}^{\infty} \delta_k \alpha^k$$

we observe that, for grading reasons alone, each γ_k comes from $MU_{2(k+i)}$, and $\delta_k \in MU_{2(k+j)}$. Most importantly, this ensures that $\gamma_k, \delta_k \in (x_1, x_2, \dots)$. Certainly, then, we must have

$$\begin{aligned} 2\hat{P}(b_{ij}) &= P(x_i)P(x_j) \\ &= \left(\sum_{k=0}^{\infty} \gamma_k \alpha^k\right)\left(\sum_{k=0}^{\infty} \delta_k \alpha^k\right) \\ &= \sum_{k=0}^{\infty} \alpha^k \sum_{l=0}^{k} \gamma_l \delta_{k-l}. \end{aligned}$$

Each coefficient $\gamma_l \delta_{k-l}$ must, therefore, come from $(x_1, x_2, \dots)^2$. But by construction, this entire ideal is divisible by 2, so in fact it is no problem to define $\hat{P}(b_{ij})$. It suffices, then, to determine commutativity of the diagram

$$\begin{tikzcd} MU_* \arrow[r, "P"] \arrow[d, "f"'] & MU_*[\![\alpha]\!]/\langle 2\rangle(\alpha) \arrow[d] \\ R \arrow[r, "\hat{P}"] & R[\![\alpha]\!]/\langle 2\rangle(\alpha) \end{tikzcd}$$

which is an immediate consequence of commutativity of the obvious diagram

$$\begin{tikzcd} MU_* \arrow[r, "P"] \arrow[d, "1"'] & MU_*[\![\alpha]\!]/\langle 2\rangle(\alpha) \arrow[d] \\ MU_* \arrow[r] & MU_*[\![\alpha]\!]/\langle 2\rangle(\alpha) \end{tikzcd}$$

since MU injects into R.

Theorem 4.2. *At $p = 2$, R defined in Construction 4.1 gives a diagram of the following form:*

$$\begin{tikzcd} MU_* \arrow[r, "P"] \arrow[d, "f"'] & MU_*[\![\alpha]\!]/\langle 2\rangle(\alpha) \arrow[d] \\ R \arrow[r, "\hat{P}"] & R[\![\alpha]\!]/\langle 2\rangle(\alpha) \end{tikzcd} \tag{6}$$

and has $f(v_1)^2 = 0$ mod 2, but $2^{-1}R^{tC_p}$ is not the trivial ring.

Proof. We will show first that the 2-series is not a unit in $2^{-1}\alpha^{-1}R[\![\alpha]\!]$. So suppose for the sake of contradiction that some $\alpha^{-n}2^{-m}\sum h_i\alpha^i$ is a multiplicative inverse for $[2](\alpha)$. Because the 2-series has a constant term of 2 and MU_* has no 2-torsion, we can confidently say $[2](\alpha)$ is not a zero divisor. What this means is that $[2](\alpha)$ must have a unique multiplicative inverse. The multiplicative inverse of a power series comes from

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + \cdots$$

and so it satisfies:

$$\left(1 + \sum_{i\geq 1} g_i\alpha^i\right)^{-1} = 1 - \left(\sum_{i\geq 1} g_i\alpha^i\right) + \left(\sum_{i\geq 1} g_i\alpha^i\right)^2 - \left(\sum_{i\geq 1} g_i\alpha^i\right)^3 + \cdots$$

Then, it must be that the inverse of the 2-series is

$$\alpha^{-n}2^{-m}\sum h_i\alpha^i = \alpha^{-1}2^{-1}\sum_{i\geq 0}(-1)^i\left(\frac{1}{2\alpha}[2](\alpha) - 1\right)^i.$$

But then we claim the sum on the right-hand side has arbitrarily high powers of 2 in the denominator. To show this, we look at the sum modulo $(v_2, v_3, \dots)$, the term $\left(\frac{1}{2\alpha}[2](\alpha) - 1\right)^i$ becomes

$$\left(\frac{1}{2}(-v_1\alpha + 2v_1^2\alpha + \cdots)\right)^i.$$

So the α^j-term of the right-hand side is of the form

$$\left(\frac{v_1^j}{2^j} + \frac{\lambda_1 v_1^j}{2^{j-1}} + \cdots + \frac{\lambda_{j-1} v_1^j}{2}\right)\alpha^j,$$

for some integers λ_i, which we simplify to

$$\left(\frac{1 + 2\lambda_1 + 4\lambda_2 + \cdots + 2^{j-1}\lambda_{j-1}}{2^j}\right) v_1^j \alpha^j.$$

In particular, the numerator is odd and so we cannot cancel any powers of 2 from there. So the only powers of 2 that cancel are from $v_1^2 = 2b_{11}$, which removes at most $\frac{j}{2}$ from the denominator. Thus, there is an inevitable $2^{\frac{j}{2}}$ in the denominator of each h_j, which forces $m \to \infty$. Of course, this is impossible, so such a multiplicative inverse cannot exist. Because of this, it is not the case that $1 \in ([2](\alpha))$, and so 1 and 0 are distinct elements of $2^{-1}\alpha^{-1}R[\![\alpha]\!]/[2](\alpha)$. So indeed, $2^{-1}R^{tC_p}$ is not the trivial ring. □

On the level of algebra, all E_∞ ring maps out of MU must induce a diagram of the form (6) at $p = 2$. The counterexample produced only has the structure of a pure ring map equipped with a map $\hat{P} : R \to R[\![\alpha]\!]/\langle 2\rangle(\alpha)$. In order for this to be a true counterexample to Conjecture 2.23, we would need R to be the homotopy groups of some ring spectrum E, the map f to descend from an E_∞ ring spectrum map between MU and E, and $\hat{P}$ to be the power operation on the associated cohomology theory.

Therefore, while the case of $k = 2$ is still open, there is now a significant barrier to it being true. That is, any proof of the conjecture would have to also show that the map we constructed can never come from an E_∞ ring map, and that there are additional topological requirements constraining the kind of algebraic maps allowed in these power operation diagrams in a very subtle way.

5 Further Work

One direction we could take from here would be to construct a counterexample for higher k and different primes p. In principle, for $k \geq 2$ and any prime p, we could inspect the ring $R_{(k,p)} = MU_*[b_I]_{I\in\mathbb{Z}^k}/(pb_I - x_{i_1}x_{i_2}\cdots x_{i_k})$. We can again define a coherent power operation, since the ideal $(x_1, x_2, \ldots)^k = 0 \mod p$, and the p-series will again fail to invert because we won't be able to cancel enough factors of p. Note, though, that this proof fails for $k = 1$; each power v_i^j would be divisible by p^j, and so we could cancel enough powers of p.

Another direction would be to consider what a "minimal counterexample" might look like. What we mean by this is whether we can shrink the set of relations on R. Particularly, it seems likely that in order to define a power operation on $b_{11} = \frac{x_1^2}{2}$, for instance, we only need to guarantee that $(v_1, v_2, \ldots)^2 = 0$ mod 2. Moreover, for any $b_{p^i-1,p^j-1} = \frac{v_i v_j}{2}$, we claim that we need only $(v_1, v_2, \ldots)^2 = 0 \mod 2$. This is actually a consequence of Theorem 9, which states at $p = 2$ that

$$P(v_n) = \frac{v_n\alpha^{2^n-1} - \langle 2\rangle(\alpha)}{\alpha^{2(2^n-2)}} \mod (2, v_1, \ldots, v_{n-1}, \frac{[2](\alpha)}{\alpha^{2^n}}).$$

If we denote the 2-series modulo $2, v_1, \ldots, v_{n-1}$ as $\langle 2\rangle_n(\alpha)$, we can in fact write

$$P(v_n) = \frac{v_n\alpha^{2^n-1} - \langle 2\rangle_n(\alpha)}{\alpha^{2(2^n-2)}} + 2\eta_0 + v_1\eta_1 + \cdots + v_{n-1}\eta_{n-1} \mod \frac{[2](\alpha)}{\alpha^{2^n}}.$$

From here, constructing $P(b_{p^i-1,p^j-1})$ is straightforward. Recall that every term of the 2-series has a factor of some v_i; so in fact we can write

$$P(v_n) = \sum_{i=0}^{\infty} v_i\eta_{n,i}$$

for some appropriate $\eta_{n,i}$. So in particular, each coefficient of $P(v_n)$ is an element of $(v_0, v_1, \dots)$. So every coefficient of $P(v_i)P(v_j)$ is an element of $(v_0, v_1, \dots)^2$. Therefore, it is possible to define a coherent power operation on $MU_*[b_{ij}]/(v_iv_j - 2b_{ij})$, and this would provide just as effective a counterexample.

But it's worth asking, is this the smallest set of relations we need? For example, could we dispose of the cross-terms $(v_iv_j, i \neq j)$ and just keep b_{11}, b_{22}, and so on?

It would also be of great interest to determine if the counterexample produced earlier can truly come from an E_∞ ring map, as if it did, that would complete a counterexample to the original conjecture in its most general form.

6 Acknowledgments

This project was done as part of the UROP+ program of the Mathematics department at the Massachusetts Institute of Technology. We would like to thank our mentor, Tristan Yang, for his ceaseless assistance and explanation throughout this project. We would also like to thank Professor Jeremy Hahn for his guidance, direction, and tremendous help.

We are indebted to the John Reed Fund for the funding for our project through the Undergraduate Research Opportunities Program (UROP) at MIT, which has allowed us to pursue research and make an impact.

7 Bibliography

References

[BSY22] Robert Burklund, Tomer M Schlank, and Allen Yuan. The chromatic nullstellensatz. *arXiv preprint arXiv:2207.09929*, 2022.

[Gu22] Zeshen Gu. *On the Power Operations of Mu.* PhD thesis, University of Minnesota, 2022.

[Lur10] Jacob Lurie. Chromatic homotopy theory (252x). Lecture notes, 2010.