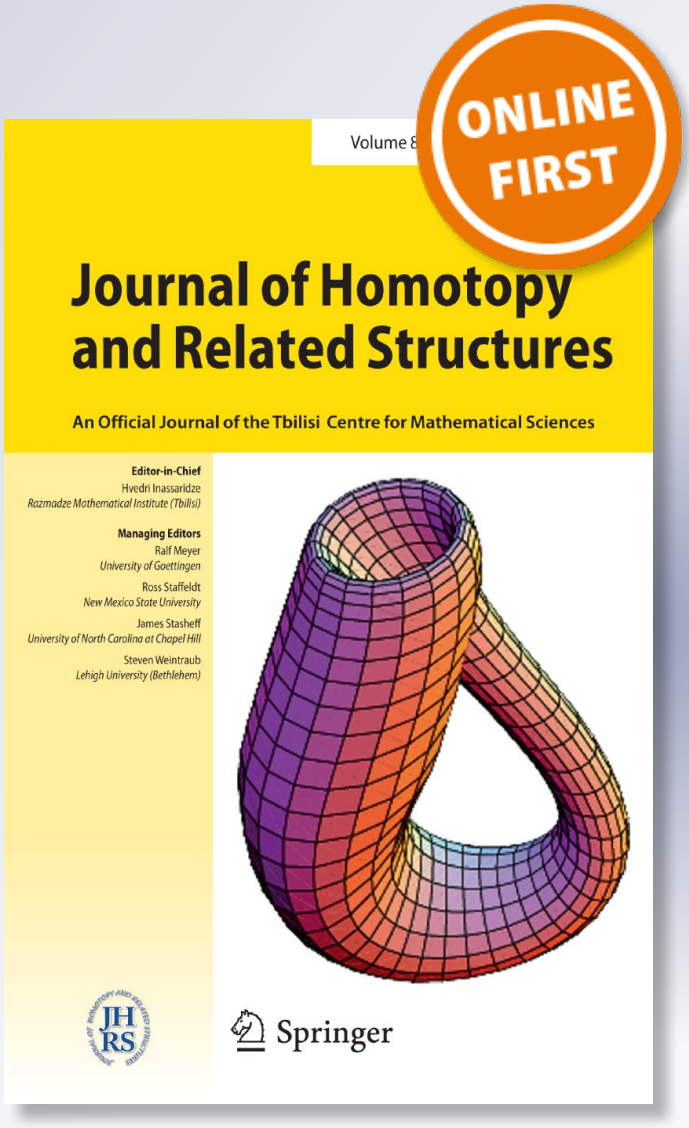
Computations of orbits for the Lubin–Tate ring

Agnès Beaudry, Naiche Downey, Connor McCranie, Luke Meszar, Andy Riddle & Peter Rock

Journal of Homotopy and Related Structures

ISSN 2193-8407

J. Homotopy Relat. Struct.
DOI 10.1007/s40062-018-00228-7



Springer

Journal of Homotopy and Related Structures
https://doi.org/10.1007/s40062-018-00228-7

Computations of orbits for the Lubin–Tate ring

Agnès Beaudry[1] · Naiche Downey[1] · Connor McCranie[1] · Luke Meszar[1] · Andy Riddle[1] · Peter Rock[1]

Received: 24 May 2018 / Accepted: 18 November 2018

Abstract
We take a direct approach to computing the orbits for the action of the automorphism group $\mathbb{G}_2$ of the Honda formal group law of height 2 on the associated Lubin–Tate rings R_2. We prove that $(R_2/p)_{\mathbb{G}_2} \cong \mathbb{F}_p$. The result is new for $p = 2$ and $p = 3$. For primes $p \geq 5$, the result is a consequence of computations of Shimomura and Yabe and has been reproduced by Kohlhaase using different methods.

Keywords Honda formal group law · Lubin-Tate ring · Morava E-theory · Morava stabilizer group · Chromatic Vanishing Conjecture

Contents

Communicated by Craig Westerland.

This material is based on work supported by the CU Boulder Department of Mathematics in the context of its internal Research For Undergraduates program. This material is also based upon work supported by the National Science Foundation under Grant no. DMS-1725563.

✉ Agnès Beaudry
agnes.beaudry@colorado.edu

[1] Department of Mathematics, University of Colorado at Boulder, Campus Box 395, Boulder, CO 80309, USA

Published online: 18 December 2018

1 Introduction

In this paper, we consider a direct approach to computing orbits for the action of the automorphism group of the Honda formal group law of height 2 on the reduction modulo (p) of the associated Lubin–Tate ring. The results are new for $p = 2$ and $p = 3$ and they follow from the work of Shimomura and Yabe [14] if $p \geq 5$, also reproduced by Kohlhaase in [10]. We also use this as an opportunity to highlight some of the results on the action of the automorphism group which appeared in French in the doctoral thesis of Lader [11]. See Sect. 3.

These results are meant to lend weight to a conjecture, which for lack of a better name we will call the Chromatic Vanishing Conjecture. This conjecture plays a key role in the analysis of Hopkins' Chromatic Splitting Conjecture (as stated by Hovey in [9]) at the prime $p = 3$ in [6] and at the prime $p = 2$ in [2]. See Remark 1.3 below. The importance this statement plays at height $n = 2$ was originally highlighted to the last author by Hans-Werner Henn. To state it, consider the Honda formal group law of height n over $\mathbb{F}_{p^n}$. The associated Lubin–Tate ring R_n satisfies $R_n \cong \mathbb{W}[\![u_1, \ldots, u_{n-1}]\!]$ where $\mathbb{W}$ are the Witt vectors on $\mathbb{F}_{p^n}$. Let $\mathbb{H}_n$ be the Honda formal group law of height n and $\mathbb{S}_n$ be the group of automorphisms of $\mathbb{H}_n$ over $\mathbb{F}_{p^n}$. Since $\mathbb{H}_n$ has coefficients in $\mathbb{F}_p$, the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ acts on $\mathbb{S}_n$. We let $\mathbb{G}_n$ be the extension of $\mathbb{S}_n$ by the Galois group.

Conjecture 1.1 (Chromatic Vanishing Conjecture) *Let $\mathbb{W} \to R_n$ and $\mathbb{F}_{p^n} \to R_n/p$ be the natural maps.*

(1) (*Integral*) *The continuous cohomology and homology of $R_n/\mathbb{W}$ vanish in all degrees so that*

$$H^*(\mathbb{G}_n, R_n) \cong H^*(\mathbb{G}_n, \mathbb{W}) \quad H_*(\mathbb{G}_n, R_n) \cong H_*(\mathbb{G}_n, \mathbb{W}).$$

(2) (*Reduced*) *The continuous cohomology and homology of $(R_n/p)/\mathbb{F}_{p^n}$ vanish in all degrees so that*

$$H^*(\mathbb{G}_n, R_n/p) \cong H^*(\mathbb{G}_n, \mathbb{F}_{p^n}) \quad H_*(\mathbb{G}_n, R_n/p) \cong H_*(\mathbb{G}_n, \mathbb{F}_{p^n})$$

When $p \gg n$, the groups $\mathbb{G}_n$ are oriented Poincaré duality groups and the statements for cohomology and homology are equivalent. Further, the reduced conjectures imply their integral versions. Indeed, using the five lemma, (2) implies the vanishing of the continuous cohomology and homology with coefficients in $(R_n/p^k)/(\mathbb{W}/p^k)$ for all $k \geq 1$. A $\lim^1$ exact sequence then gives the desired implication.

The conjecture is a tautology at height $n = 1$. At height $n = 2$, the statements about cohomology are known to hold for all primes. They are due to Shimomura–Yabe if $p \geq 5$ [14], to Henn–Karamanov–Mahowald and Goerss–Henn–Mahowald–Rezk for $p = 3$ [6,8] and to Beaudry–Goerss–Henn for $p = 2$ [1,2]. Kohlhaase has reproduced the results for $p \geq 5$ in [10, Theorem 3.20] using different methods. For $p \geq 5$, Poincaré duality then gives the homological results. Finally, that $H^0(\mathbb{G}_n, R_n) \cong H^0(\mathbb{G}_n, \mathbb{W}) \cong \mathbb{Z}_p$ at all heights and primes is a folklore result of Hopkins See [3, Lemma 1.33].

For $p = 2$ and $p = 3$, similar methods to those used to prove the cohomological results should give a proof of the conjecture for homology. As in the cohomological cases, this would probably be a tedious computation. However, in this paper, we prove the homological result modulo (p) in degree zero via a direct argument for all primes, including $p = 2$ and $p = 3$. Our main theorem is:

Theorem 1.2 *Let p be any prime. The natural map $\mathbb{F}_{p^2} \to R_2/p$ induces an isomorphism*

$$H_0(\mathbb{G}_2, R_2/p) \cong H_0(\mathbb{G}_2, \mathbb{F}_{p^2}).$$

Remark 1.3 We briefly explain the relationship of Conjecture 1.1 with the Chromatic Splitting Conjecture (CSC) as discussed in Section 4 of [9]. Let $K(n)$ be the Morava K-theory spectrum and $E_n = E(\mathbb{F}_{p^n}, \mathbb{H}_n)$ be the Lubin-Tate spectrum, so that $(E_n)_0 \cong R_n$. By the Goerss–Hopkins–Miller Theorem [5], the group $\mathbb{G}_n$ acts on E_n by maps of $\mathcal{E}_\infty$ ring spectra and a well-known result of Devinatz and Hopkins states that $L_{K(n)}S^0 \simeq E_n^{h\mathbb{G}_n}$ [4]. Further, the $K(n)$-local E_n-based Adams–Novikov Spectral Sequence can be identified with the homotopy fixed point spectral sequence

$$E_2^{s,t} = H^s(\mathbb{G}_n, (E_n)_t) \Longrightarrow \pi_{t-s}E_n^{h\mathbb{G}_n} \cong \pi_{t-s}L_{K(n)}S^0.$$

The CSC predicts that the chromatic reassembly process is governed by elements of $\pi_* L_{K(n)}S^0$ which are detected in $E_2^{*,0} \cong H^*(\mathbb{G}_n, R_n)$ by classes in the image of the map from $H^*(\mathbb{G}_n, \mathbb{W})$. Based on a computation of Lazard and Morava [13, Remark 2.2.5], the cohomological version of Conjecture 1.1 would immediately imply that the CSC holds rationally. Integrally, it would at the very least imply that the reassembly classes are present on the E_2-page. At large primes where the spectral sequence collapses, these classes would then exist in homotopy. Proving the cohomological version of Conjecture 1.1 is among the hardest computations in both [6] and [2].

At this time, a computational proof of the Chromatic Vanishing Conjecture at higher heights seems out of reach. One could hope for a computational proof in homological degree zero at general heights. However, the precision of the information on the action of $\mathbb{G}_2$ needed to carry out our direct argument suggests that even in this case, a computational proof may not be feasible. Further, if it is true in general, it should not be a computational accident and there ought to be a compelling conceptual explanation.

Organization of the paper

In Sect. 2, we give the proof of the main result. In Sect. 3, we review the formulas for the action of $\mathbb{G}_2$ needed for the computations.

2 Orbits modulo (p)

In this section, we prove our main result which is a direct computation of the orbits for the action of $\mathbb{G}_2$ at height 2.

2.1 Background and results

We begin by recalling a few facts in order to state our results. We refer the reader to Hazewinkel [7] for more background on formal group laws.

We let $\mathbb{H}_2$ be the Honda formal group law of height 2. The p-series of $\mathbb{H}_2$ has the form

$$[p]_{\mathbb{H}_2}(x) = x^{p^2}.$$

The coefficients of $\mathbb{H}_2$ are in $\mathbb{F}_p$. We let $\mathcal{O}_2$ be the endomorphism ring of $\mathbb{H}_2$ over $\mathbb{F}_{p^2}$. Then $\mathcal{O}_2$ is a module over the p-adic integers $\mathbb{Z}_p$, generated by the automorphisms

$$[1](x) = x \quad S(x) = x^p \quad \zeta(x) = \zeta x$$

where $\zeta \in \mathbb{F}_{p^2}$ is a primitive $p^2 - 1$th root of unity. In fact, letting $\mathbb{W} = \mathbb{Z}_p(\zeta)$ be the ring of integers of the unramified field extension $\mathbb{Q}_p(\zeta)$ of degree 2 over $\mathbb{Q}_p$, an explicit presentation of $\mathcal{O}_2$ is given by

$$\mathcal{O}_2 \cong \mathbb{W}\langle S\rangle/(S^2 = p, Sa = a^\sigma S)$$

where $a \in \mathbb{W}$ and σ is the Frobenius automorphism in

$$\mathrm{Gal} = \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p) \cong \mathbb{Z}/2.$$

The group of automorphisms of $\mathbb{H}_2$ is $\mathbb{S}_2 = \mathcal{O}_2^\times$. Since Gal acts on $\mathcal{O}_2$ via its natural action on $\mathbb{W}$ (and fixing S), we can define

$$\mathbb{G}_2 = \mathbb{S}_2 \rtimes \mathrm{Gal}.$$

Now, we turn to the description of the Lubin–Tate ring R_2. See Lubin–Tate [12] for more details. Let $R_2 = \mathbb{W}[\![u_1]\!]$ and $F(x, y) = x +_F y$ be a deformation of $\mathbb{H}_2$ defined over R_2, chosen so that

$$[p]_F(x) = px +_F u_1 x^p +_F x^{p^2}.$$

It follows from Lubin–Tate theory that the deformations of $\mathbb{H}_2$ to complete local rings are co-represented by continuous homomorphisms from the ring R_2. The group $\mathbb{S}_2$ naturally acts on R_2. The Galois group acts on R_2 via the action on $\mathbb{W}$, fixing u_1, and this extends the action of $\mathbb{S}_2$ to an action of $\mathbb{G}_2$.

To describe the action of $\mathbb{S}_2$, note that any element $g \in \mathbb{S}_2$ can be expressed uniquely as a power series

$$g = \sum_{i=0}^{\infty} g_i S^i$$

where $g_i^{p^2} - g_i = 0$. In other words, a coefficient g_i is either zero or a Teichmüller lift of $\mathbb{F}_{p^2}^{\times}$ in $\mathbb{W}^{\times}$. As we will see in Sect. 3 below,

$$g_*(u_1) = t_0^{p-1} u_1 + t_0^{-1} t_1 (p - p^p) \tag{2.1}$$

for a unit t_0 in $\mathbb{W}[\![u_1]\!]$ such that $t_0 = g_0$ modulo (p, u_1) and an element $t_1 \in \mathbb{W}[\![u_1]\!]$ such that $t_1 = g_1$ modulo (p, u_1). If $g = \zeta$ is a primitive $p^2 - 1$th root of unity in $\mathbb{W}^{\times} \subseteq \mathbb{S}_2$, one can show that $t_0 = \zeta$ and $t_1 = 0$, so that

$$\zeta_*(u_1) = \zeta^{p-1} u_1. \tag{2.2}$$

For more general elements $g \in \mathbb{S}_2$, t_0 is tedious to compute and Sect. 3 is dedicated to this task.

The goal of this paper is to compute the orbits for the action of $\mathbb{G}_2$ on R_2/p, that is, the coinvariants $(R_2/p)_{\mathbb{G}_2}$. We recall the definition of the coinvariants for the action of a profinite group on a profinite module. Let $G = \varprojlim_i G/G_i$ for finite quotients G/G_i. Define

$$\mathbb{Z}_p[\![G]\!] = \varprojlim_{i,j} \mathbb{Z}/p^j[G/G_i]$$

and $\mathbb{F}_p[\![G]\!] = \mathbb{Z}_p[\![G]\!]/(p)$. Then, for any profinite module $M = \varprojlim_k M_k$ where M_k are finite discrete $\mathbb{Z}_p[\![G]\!]$-modules, we have

$$M_G = \varprojlim_{k,j} M_k \otimes_{\mathbb{Z}_p[\![G]\!]} \mathbb{Z}/p^j$$

for the trivial action of G on the right factor $\mathbb{Z}/p^j$. Note that if M is an $\mathbb{F}_p$-vector space, then

$$M_G \cong \varprojlim_k M_k \otimes_{\mathbb{F}_p[\![G]\!]} \mathbb{F}_p.$$

When $G = \mathbb{G}_2$ or $\mathbb{S}_2$, we can choose G_i to be the subgroup consisting of those elements of $\mathbb{S}_2$ which are congruent to 1 modulo (S^i). For $M = R_2/p$, we can choose M_k to be the discrete finite module $R_2/(p, u_1^k)$ and we have

$$(R_2/p)_G = \varprojlim_k R_2/(p, u_1^k) \otimes_{\mathbb{F}_p[\![G]\!]} \mathbb{F}_p. \tag{2.3}$$

We now state the main result.

Theorem 2.1 *There is an isomorphism* $(R_2/p)_{\mathbb{G}_2} \cong \mathbb{F}_p$ *for all primes* p.

The proof of Theorem 2.1 uses formulas for the action of $\mathbb{G}_2$. We begin with a summary of the results which are covered in detail in Sect. 3.

2.2 Summary of the action

The action of $\mathbb{G}_2$ on

$$R_2/p = \mathbb{F}_{p^2}[\![u_1]\!]$$

is given by (2.1), modulo a computation of the unit t_0. The following result, which is [11, Corollary 3.4] for $p \geq 5$ and [8, Section 4.1] for $p = 3$, is sufficient for our purposes when p is odd. We will review the proof of this result in Sect. 3 below and generalize it to include the case $p = 2$.

Theorem 2.2 *Let* p *be any prime. Let* $g \in \mathbb{S}_2$ *be such that* $g = 1 + g_1 S + g_2 S^2$ *modulo* (S^3). *Then*

$$t_0 = 1 + g_1^p u_1 - g_1 u_1^p + \left(g_2 - g_2^p\right) u_1^{p+1} + \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} g_1^{pi} u_1^{p+1+i} + g_1^2 u_1^{2p} + g_1^p u_1^{p^2} \mod (p, u_1^{2p+1}).$$

When $p = 2$, we will need more information about the action of g. We give a computer assisted proof of the following result in Sect. 3.[1]

Theorem 2.3 *Let* $p = 2$. *If* $g = 1 + g_2 S^2 + g_3 S^3 + g_4 S^4 + \cdots$, *then*

$$t_0 = 1 + (g_2 + g_2^2)u_1^3 + g_3 u_1^5 + g_3 u_1^8 + (g_4 + g_4^2)u_1^9 \mod (2, u_1^{10}).$$

2.3 Prime independent arguments

The bulk of the proof of Proposition 2.5 will be in proving the following proposition. We abbreviate $\mathbb{S} = \mathbb{S}_2$ and $R = R_2$ and let $[x]$ denote the image of an element x under the natural map $\mathbb{F}_{p^2}[u_1]/(u_1^k) \to (\mathbb{F}_{p^2}[u_1]/(u_1^k))_{\mathbb{S}}$.

Proposition 2.4 *For* $k \geq 2$, $[u_1^{k-1}] = 0$ *in* $(\mathbb{F}_{p^2}[u_1]/(u_1^k))_{\mathbb{S}}$.

Assuming Proposition 2.4, we prove the following result, which immediately implies Theorem 2.1 by taking Galois coinvariants since $(\mathbb{F}_{p^2})_{\mathrm{Gal}} \cong \mathbb{F}_p$.

[1] If one is willing to work with the formal group law of a super-singular elliptic curve rather than the Honda formal group law, an analogue of Theorem 2.3 follows from Section 6 of [1] where the results were obtained directly. The analogue of Theorem 2.1 also holds in this case, the proof being completely analogous to the one provided below.

Proposition 2.5 *The quotient map $\mathbb{F}_{p^2}[\![u_1]\!] \to \mathbb{F}_{p^2}$ induces an isomorphism*

$$(\mathbb{F}_{p^2}[\![u_1]\!])_{\mathbb{S}} \cong \mathbb{F}_{p^2}.$$

Proof Since taking coinvariants is a right exact functor, the maps in the inverse system (2.3) fit into an exact sequence

$$((u_1^{k-1})/(u_1^k))_{\mathbb{S}} \longrightarrow (\mathbb{F}_{p^2}[u_1]/(u_1^k))_{\mathbb{S}} \longrightarrow (\mathbb{F}_{p^2}[u_1]/(u_1^{k-1}))_{\mathbb{S}} \longrightarrow 0$$

and Proposition 2.4 implies that the left map is trivial. Therefore, (2.3) is a constant inverse system whose first term is $\mathbb{F}_{p^2}$. □

We turn to the proof of Proposition 2.4. We begin with a simple result.

Proposition 2.6 *If n is not of the form $(p+1)\alpha$, then for all $k \geq 0$, $[u_1^n] = 0$ in $(\mathbb{F}_{p^2}[u_1]/(u_1^k))_{\mathbb{S}}$.*

Proof By (2.2),

$$\zeta_*(u_1^n) = \zeta^{n(p-1)} u_1^n = u_1^n + (\zeta^{n(p-1)} - 1)u_1^n.$$

Therefore, $(\zeta^{n(p-1)} - 1)[u_1^n] = 0$. Since ζ is a primitive $p^2 - 1$th root of unity, then $\zeta^{n(p-1)} - 1$ is a unit in $\mathbb{F}_{p^2}$ provided that $p+1$ does not divide n. It follows that, in this case, $[u_1^n] = 0$. □

Remark 2.7 Note that this result is stronger than Proposition 2.4 in the case $n = k-1$. It will be used in its full strength in our proof of Proposition 2.4.

The technique for showing that $[u_1^k] = 0$ in $(\mathbb{F}_{p^2}[u_1]/(u_1^{k+1}))_{\mathbb{S}}$ for $k = (p+1)\alpha$ varies on the p-adic expansion of α.

Proposition 2.8 *If $k = (p+1)\alpha$ for α non trivial such that $\alpha \neq 1$ modulo (p), then $[u_1^k] = 0$ in $(\mathbb{F}_{p^2}[u_1]/(u_1^{k+1}))_{\mathbb{S}}$.*

Proof Let $g = 1 + S$. It follows from Theorem 2.2 that

$$t_0 = 1 + u_1 \mod (p, u_1^p).$$

Therefore by (2.1)

$$\begin{aligned} g_*(u_1^{k-1}) &= u_1^{k-1}(1+u_1)^{(p-1)(k-1)} \mod (p, u_1^{p+k-1}) \\ &= u_1^{k-1} + (p-1)(k-1)u_1^k \mod (p, u_1^{k+1}). \end{aligned}$$

So long as $k \neq 1$ modulo (p), we can conclude that $[u_1^k] = 0$ in $(\mathbb{F}_{p^2}[u_1]/(u_1^{k+1}))_{\mathbb{S}}$. Since $k = \alpha$ modulo (p), this proves the claim. □

2.4 The remainder of the argument for odd primes

Now, we fix p odd. The case $p = 2$ will be treated below. We let

$$k = (p+1)(1 + p + p^2 + \cdots + p^{\ell-1} + p^\ell \eta) \tag{2.4}$$

for $\ell \geq 0$ and η a non-negative integer such that $\eta \neq 1$ modulo (p). The complexity of the problem depends on ℓ. The case when $\ell = 0$ was Proposition 2.8, so we now turn to the case when $\ell \geq 1$ in (2.4). Let

$$k_r = \begin{cases} k & r = 0 \\ k_{r-1} - (p+1)p^{r-1} & 1 \leq r < \ell - 1 \end{cases} \tag{2.5}$$

for $0 \leq r < \ell - 1$.

We prove that $[u_1^{k_r}] = -[u_1^{k_{r+1}}]$ for $0 \leq r < \ell - 1$ (Proposition 2.9) and $[u_1^{k_{\ell-1}}] = 0$ (Proposition 2.10) in $(\mathbb{F}_{p^2}[u_1]/(u_1^{k+1}))_{\mathbb{S}}$. Together, these results finish the proof of Proposition 2.4.

Proposition 2.9 *Let k_r be as in (2.5). For $0 \leq r < \ell - 1$,*

$$[u_1^{k_r}] = -[u_1^{k_{r+1}}]$$

in $(\mathbb{F}_{p^2}[u_1]/(u_1^{k+1}))_{\mathbb{S}}$.

Proof From Theorem 2.2, we deduce that for $g = 1 + S$,

$$t_0 = 1 + u_1 - u_1^p + \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} u_1^{p+1+i} + u_1^{2p} \qquad \text{mod } (u_1^{2p+1}).$$

We use (2.1), the fact that $a^p = a$ for $a \in \mathbb{F}_p$, $(x+y)^p = x^p + y^p$ modulo (p) and the fact that

$$k_{r+1} - p^r = p^r \alpha_r$$

where $\alpha_r = (p+1)(p + \cdots + p^{\ell-1-r} + p^{\ell-r}\eta) - 1$. With this, we deduce that

$$g_*(u_1^{k_{r+1}-p^r}) = u_1^{k_{r+1}-p^r} \left(1 + u_1^{p^r} - u_1^{p^{r+1}} + \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} u_1^{p^{r+1}+(1+i)p^r} + u_1^{2p^{r+1}}\right)^{(p-1)\alpha_r}$$

modulo $(u_1^{k_{r+1}+2p^{r+1}})$. We now simplify this equation. We compute modulo (u_1^{k+1}) and note that

$$\begin{aligned} k + 1 &= k_{r+1} + (p+1)(1 + \cdots + p^r) + 1 \\ &= k_{r+1} + 2(1 + \cdots + p^r) + p^{r+1} < k_{r+1} + 3p^r + p^{r+1}. \end{aligned}$$

Therefore, we immediately get rid of all terms of the form u_1^n for $n \geq k_{r+1}+3p^r+p^{r+1}$. Next, we use the fact that $\alpha_r = p-1$ modulo (p^2) so that $(p-1)\alpha_r = 1+p(p-2)$ modulo (p^2). For $i = i_0 + pi_1 < p^2$ with $0 \leq i_0, i_1 \leq p-1$, we then have

$$\binom{(p-1)\alpha_r}{i} = \binom{(p-1)^2}{i} = \binom{1}{i_0}\binom{p-2}{i_1} \mod (p),$$

where $\binom{m}{n} = 0$ if $m < n$. In particular, $\binom{(p-1)^2}{2} = 0$ modulo (p). Combining these facts, we obtain:

$$\begin{aligned}
g_*(u_1^{k_{r+1}-p^r}) &= u_1^{k_{r+1}-p^r}\left(1+u_1^{p^r}-u_1^{p^{r+1}}+u_1^{p^{r+1}+2p^r}+\frac{p-1}{2}u_1^{p^{r+1}+3p^r}+u_1^{2p^{r+1}}\right)^{(p-1)\alpha_r}\\
&= u_1^{k_{r+1}-p^r}\left(1+\sum_{i=1}^{p+3}\binom{(p-1)\alpha_r}{i}\left(u_1^{p^r}-u_1^{p^{r+1}}+u_1^{p^{r+1}+2p^r}\right.\right.\\
&\quad \left.\left.+\frac{p-1}{2}u_1^{p^{r+1}+3p^r}+u_1^{2p^{r+1}}\right)^i\right)\\
&= u_1^{k_{r+1}-p^r}\left(1+\sum_{i=1}^{p+3}\binom{(p-1)^2}{i}\left(u_1^{p^r}-u_1^{p^{r+1}}+u_1^{p^{r+1}+2p^r}\right.\right.\\
&\quad \left.\left.+\frac{p-1}{2}u_1^{p^{r+1}+3p^r}+u_1^{2p^{r+1}}\right)^i\right)\\
&= u_1^{k_{r+1}-p^r}+\left(u_1^{k_{r+1}}-u_1^{k_{r+1}+p^{r+1}-p^r}+u_1^{k_{r+1}+p^{r+1}+p^r}+\frac{p-1}{2}u_1^{k_{r+1}+p^{r+1}+2p^r}\right.\\
&\quad \left.+u_1^{k_{r+1}+2p^{r+1}-p^r}\right)\\
&\quad +\binom{(p-1)^2}{3}\left(u_1^{k_{r+1}+2p^r}-3u_1^{k_{r+1}+p^{r+1}+p^r}\right)\\
&\quad +\binom{(p-1)^2}{4}\left(u_1^{k_{r+1}+3p^r}-4u_1^{k_{r+1}+p^{r+1}+2p^r}\right)\\
&\quad +\sum_{i=5}^{p+3}\binom{(p-1)^2}{i}u_1^{k_{r+1}+p^r(i-1)}.
\end{aligned}$$

Note further that, if $p \neq 3$, then $\binom{(p-1)^2}{3} = 0$ modulo (p). So $3\binom{(p-1)^2}{3} = 0$ modulo (p) for all primes. The above computation then gives the following relation in the coinvariants

$$\begin{aligned}
0 &= \left[u_1^{k_{r+1}}\right]+\left[u_1^{k_{r+1}+p^{r+1}+p^r}\right]\\
&\quad -\left[u_1^{k_{r+1}+p^{r+1}-p^r}\right]+\left[u_1^{k_{r+1}+2p^{r+1}-p^r}\right]\\
&\quad +\left(\frac{p-1}{2}-4\binom{(p-1)^2}{4}\right)\left[u_1^{k_{r+1}+p^{r+1}+2p^r}\right]+\sum_{i=3}^{p+3}\binom{(p-1)^2}{i}\left[u_1^{k_{r+1}+p^r(i-1)}\right].
\end{aligned}$$

Recall that $[u_1^n] = 0$ if n is not a multiple of $p+1$. Since k_{r+1} is a multiple of $p+1$, it follows that $[u_1^{k_{r+1}+p^{r+1}-p^r}] = [u_1^{k_{r+1}+p^{r+1}+2p^r}] = [u_1^{k_{r+1}+2p^{r+1}-p^r}] = 0$ modulo (p). Similarly, the only term that can remain in the summation after taking this into account is the case $i = p+2$. However, $\binom{(p-1)^2}{p+2} = 0$ modulo (p), so the summation is also zero. Therefore, the second and third lines of the equation are zero in the coinvariants. We conclude that

$$0 = \left[u_1^{k_{r+1}}\right] + \left[u_1^{k_{r+1}+p^{r+1}+p^r}\right].$$

□

Proposition 2.10 *Let $k_{\ell-1} = (p+1)(p^{\ell-1} + p^\ell \eta)$ for a non-negative integer η such that $\eta \neq 1$ modulo (p) as in (2.5). Then*

$$\left[u_1^{k_{\ell-1}}\right] = 0$$

in $(\mathbb{F}_{p^2}[u_1]/(u_1^{k+1}))_{\mathbb{S}}$.

Proof Note that

$$k_{\ell-1} - p^\ell = p^{\ell-1}\alpha_\ell$$

where $\alpha_\ell = 1 + (p+p^2)\eta$. Therefore,

$$g_*\left(u_1^{k_{\ell-1}-p^\ell}\right) = u_1^{k_{\ell-1}-p^\ell} \left(1 + u_1^{p^{\ell-1}} - u_1^{p^\ell} + \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} u_1^{p^\ell+(1+i)p^{\ell-1}} + u_1^{2p^\ell}\right)^{(p-1)\alpha_\ell}$$

modulo $(u_1^{k_{\ell-1}+p^\ell+p^{\ell-1}})$ and note that

$$\begin{aligned} k+1 &= k_{\ell-1} + p^{\ell-1} + 2(1+\cdots+p^{\ell-2}) \\ &< k_{\ell-1} + p^{\ell-1} + 3p^{\ell-2} \leq k_{\ell-1} + 2p^{\ell-1}. \end{aligned}$$

So, using the fact that $(p-1)\alpha_\ell = (p-1) + p(p-\eta)$ modulo (p^2), we simplify as before to obtain

$$\begin{aligned} g_*\left(u_1^{k_{\ell-1}-p^\ell}\right) &= u_1^{k_{\ell-1}-p^\ell}\left(1 + u_1^{p^{\ell-1}} - u_1^{p^\ell} + u_1^{p^\ell+2p^{\ell-1}}\right)^{(p-1)\alpha_\ell} \\ &= u_1^{k_{\ell-1}-p^\ell}\left(1 + (p-1)\alpha_\ell\left(u_1^{p^{\ell-1}} - u_1^{p^\ell} + u_1^{p^\ell+2p^{\ell-1}}\right)\right. \\ &\quad \left. + \binom{(p-1)\alpha_\ell}{2}\left(u_1^{p^{\ell-1}} - u_1^{p^\ell}\right)^2\right) \end{aligned}$$

$$
\begin{aligned}
&= u_1^{k_{\ell-1}-p^\ell}\left(1-u_1^{p^{\ell-1}}+u_1^{p^\ell}-u_1^{p^\ell+2p^{\ell-1}}+\binom{p-1}{2}\left(u_1^{2p^{\ell-1}}-2u_1^{p^\ell+p^{\ell-1}}\right)\right.\\
&\left.+\sum_{i=3}^{p+1}\binom{(p-1)+p(p-\eta)}{i}u_1^{ip^{\ell-1}}\right)\\
&= u_1^{k_{\ell-1}-p^\ell}-u_1^{k_{\ell-1}-p^\ell+p^{\ell-1}}+u_1^{k_{\ell-1}}-u_1^{k_{\ell-1}+2p^{\ell-1}}\\
&\quad+\binom{p-1}{2}\left(u_1^{k_{\ell-1}-p^\ell+2p^{\ell-1}}-2u_1^{k_{\ell-1}+p^{\ell-1}}\right)\\
&\quad+\sum_{i=3}^{p-1}\binom{p-1}{i}u_1^{k_{\ell-1}-p^\ell+ip^{\ell-1}}+\sum_{j=0}^{1}\binom{p-1}{j}\binom{p-\eta}{1}u_1^{k_{\ell-1}+jp^{\ell-1}}.
\end{aligned}
$$

As before, noting that $[u_1^\eta]=0$ if $p+1$ does not divide n, while $p+1$ does divide $k_{\ell-1}$, we obtain the following relation in the coinvariants:

$$
\begin{aligned}
0 &= -\left[u_1^{k_{\ell-1}-p^\ell+p^{\ell-1}}\right]+\left[u_1^{k_{\ell-1}}\right]-\left[u_1^{k_{\ell-1}+2p^{\ell-1}}\right]\\
&\quad+\binom{p-1}{2}\left(\left[u_1^{k_{\ell-1}-p^\ell+2p^{\ell-1}}\right]-2\left[u_1^{k_{\ell-1}+p^{\ell-1}}\right]\right)\\
&\quad+\sum_{i=3}^{p-1}\binom{p-1}{i}\left[u_1^{k_{\ell-1}-p^\ell+ip^{\ell-1}}\right]-\eta\sum_{j=0}^{1}\binom{p-1}{j}\left[u_1^{k_{\ell-1}+jp^{\ell-1}}\right]\\
&= \left[u_1^{k_{\ell-1}}\right]-\eta\left[u_1^{k_{\ell-1}}\right].
\end{aligned}
$$

Since $\eta\neq 1$ modulo (p), we can conclude that $[u_1^{k_{\ell-1}}]=0$. □

2.5 The remainder of the argument for the prime two

We follow steps similar to those taken at odd primes.

Proposition 2.11 *Let $k=3\alpha$ where α is an integer congruent to* 1 *modulo* (4). *Then* $[u_1^k]=0$ *in* $(\mathbb{F}_4[u_1]/(u_1^{k+1}))_{\mathbb{S}}$.

Proof Choose $g=1+S$ and consider $g_*(u_1^{k-2})$. We have

$$
\begin{aligned}
g_*(u_1^{k-2}) &= t_0^{k-2}u_1^{k-2}\\
&= u_1^{k-2}(1+u_1+u_1^2)^{k-2} \mod (2,u_1^{k+1})\\
&= u_1^{k-2}+u_1^{k-1}+\left(1+\binom{k-2}{2}\right)u_1^k \mod (2,u_1^{k+1}).
\end{aligned}
$$

Since $k-2=1$ modulo (4), we have

$$\binom{k-2}{2} = \binom{1}{0}\binom{0}{1}\cdots = 0 \mod (2).$$

So, $[u_1^{k-1}] = [u_1^k]$ in $(\mathbb{F}_4[u_1]/(u_1^{k+1}))_{\mathbb{S}}$. Since $k-1 \neq 0$ modulo (3), $[u_1^{k-1}]$ is zero in $(\mathbb{F}_4[u_1]/(u_1^{k+1}))_{\mathbb{S}}$ by Proposition 2.6 and the claim follows. □

Now, we let $k = 3(1+2+2^2+\cdots+2^{\ell-1}+2^{\ell+1}\eta)$ for η any non-negative integer and $\ell \geq 2$, we write

$$k_r = \begin{cases} k & r = 0 \\ k_{r-1} - 3\cdot 2^{r-1} & 1 \leq r \leq \ell - 2. \end{cases} \tag{2.6}$$

We prove that $[u_1^{k_r}] = [u_1^{k_{r+1}}]$ for $0 \leq r < \ell-2$ (Proposition 2.12) and that $[u_1^{k_{\ell-2}}] = 0$ (Proposition 2.13) in $(\mathbb{F}_4[u_1]/(u_1^{k+1}))_{\mathbb{S}}$. Together, these results finish the proof of Proposition 2.4.

Proposition 2.12 *Let k_r be as in (2.6). For $0 \leq r < \ell - 2$,*

$$\left[u_1^{k_r}\right] = \left[u_1^{k_{r+1}}\right]$$

in $(\mathbb{F}_4[u_1]/(u_1^{k+1}))_{\mathbb{S}}$.

Proof Take $g = 1+\zeta S^2+\zeta S^4$. Note that $\zeta+\zeta^2 = 1$ modulo (2), so by Theorem 2.3,

$$g_*\left(u_1^{k_{r+1}-3\cdot 2^r}\right) = u_1^{k_{r+1}-3\cdot 2^r}\left(1+u_1^3+u_1^9\right)^{k_{r+1}-3\cdot 2^r} \mod \left(2, u_1^{2^{r+3}+k_{r+1}-2^r}\right)$$

Note that since

$$k+1-k_{r+1} = 3(1+2+\cdots+2^r)+1 = 3\cdot 2^{r+1}-2$$

and $2^{r+3}-2^r > 3\cdot 2^{r+1}-2$, we have that $2^{r+3}+k_{r+1}-2^r \geq k+1$. So modulo (u_1^{k+1}),

$$\begin{aligned} g_*\left(u_1^{k_{r+1}-3\cdot 2^r}\right) &= u_1^{k_{r+1}-3\cdot 2^r}\left(1+u_1^{3\cdot 2^r}+u_1^{9\cdot 2^r}\right)^{2^{-r}k_{r+1}-3} \\ &= \sum_{i=0}^{2^{-r}k_{r+1}-3}\binom{2^{-r}k_{r+1}-3}{i}u_1^{k_{r+1}-3\cdot 2^r}\left(u_1^{3\cdot 2^r}+u_1^{9\cdot 2^r}\right)^i \\ &= \sum_{i=0}^{2^{-r}k_{r+1}-3}\sum_{j=0}^{i}\binom{2^{-r}k_{r+1}-3}{i}\binom{i}{j}u_1^{k_{r+1}+3\cdot 2^{r+1}j+3\cdot 2^r(i-1)}. \end{aligned}$$

Modulo (u_1^{k+1}), only terms with $j = 0$ and $i < 3$ contribute to the sum. So

$$\begin{aligned}
&= \binom{2^{-r}k_{r+1} - 3}{0} u_1^{k_{r+1}-3\cdot 2^r} + \binom{2^{-r}k_{r+1} - 3}{1} u_1^{k_{r+1}} + \binom{2^{-r}k_{r+1} - 3}{2} u_1^{k_{r+1}+3\cdot 2^r} \\
&= u_1^{k_{r+1}-3\cdot 2^r} + u_1^{k_{r+1}} + \binom{2^{-r}k_{r+1} - 3}{2} u_1^{k_r}.
\end{aligned}$$

Finally, since $2^{-r}k_{r+1} - 3 = 3$ modulo (4), then $\binom{2^{-r}k_{r+1}-3}{2} = 1$ modulo (2). So we conclude that

$$g_*\left(u_1^{k_{r+1}-3\cdot 2^r}\right) = u_1^{k_{r+1}-3\cdot 2^r} + u_1^{k_{r+1}} + u_1^{k_r} \mod \left(2, u_1^{k+1}\right).$$

Therefore, $[u_1^{k_{r+1}}] = [u_1^{k_r}]$ as desired. □

Proposition 2.13 *Let $k_{\ell-2}$ be as in (2.6). Then $[u_1^{k_{\ell-2}}] = 0$ in $(\mathbb{F}_4[u_1]/(u_1^{k+1}))_{\mathbb{S}}$.*

Proof Choose $g = 1 + S$ and consider $g_*(u_1^{2^{\ell-1}+3\cdot 2^{\ell+1}\eta})$. We have

$$\begin{aligned}
g_*\left(u_1^{2^{\ell-1}+3\cdot 2^{\ell+1}\eta}\right) &= u_1^{2^{\ell-1}+3\cdot 2^{\ell+1}\eta} \\
&\left(1 + u_1 + u_1^2 + u_1^4\right)^{2^{\ell-1}+3\cdot 2^{\ell+1}\eta} \mod \left(2, u_1^{3(2^\ell+2^{\ell+1}\eta)}\right)
\end{aligned}$$

noting that $3(2^\ell + 2^{\ell+1}\eta) \geq k + 1$. Therefore, modulo (u_1^{k+1}), we have

$$\begin{aligned}
g_*\left(u_1^{2^{\ell-1}+3\cdot 2^{\ell+1}\eta}\right) &= u_1^{2^{\ell-1}+3\cdot 2^{\ell+1}\eta}\left(1 + u_1^{2^{\ell-1}} + u_1^{2^\ell} + u_1^{2^{\ell+1}}\right)^{1+3\cdot 2^2\eta} \\
&= u_1^{2^{\ell-1}+3\cdot 2^{\ell+1}\eta} \sum_{s=0}^{1+3\cdot 2^2\eta} \sum_{i=0}^{s} \sum_{j=0}^{i} \binom{1+3\cdot 2^2\eta}{s} \binom{s}{i} \binom{i}{j} u_1^{2^{\ell-1}(s-i)} u_1^{2^\ell(i-j)} u_1^{2^{\ell+1}j} \\
&= \sum_{s=0}^{1+3\cdot 2^2\eta} \sum_{i=0}^{s} \sum_{j=0}^{i} \binom{1+3\cdot 2^2\eta}{s} \binom{s}{i} \binom{i}{j} u_1^{2^{\ell-1}(1+s+i+2j)+3\cdot 2^{\ell+1}\eta}.
\end{aligned}$$

Note that if $s + i + 2j \geq 5$, the terms vanish for degree reasons. Hence, $s \leq 4$, $i \leq 4 - s$, and $j \leq 2 - (s + i)/2$, so that

$$\begin{aligned}
&g_*\left(u_1^{2^{\ell-1}+3\cdot 2^{\ell+1}\eta}\right) \\
&= \sum_{s=0}^{4} \sum_{i=0}^{\max(s,4-s)} \sum_{j=0}^{\max(i,2-(s+i)/2)} \binom{1+3\cdot 2^2\eta}{s} \binom{s}{i} \binom{i}{j} u_1^{2^{\ell-1}(1+s+i+2j)+3\cdot 2^{\ell+1}\eta}.
\end{aligned}$$

Since $1 + 3 \cdot 2^2\eta = 1$ modulo (4), $\binom{1+3\cdot 2^2\eta}{2} = \binom{1+3\cdot 2^2\eta}{3} = 0$ modulo (2). Further, $\binom{1+3\cdot 2^2\eta}{4} = \eta$ modulo (2). Enumerating the remaining possibilities gives

$$g_*\left(u_1^{2^{\ell-1}+3\cdot 2^{\ell+1}\eta}\right) = u_1^{2^{\ell-1}+3\cdot 2^{\ell+1}\eta} + u_1^{2^\ell+3\cdot 2^{\ell+1}\eta} + u_1^{3(2^{\ell-1}+2^{\ell+1}\eta)} + (1+\eta)u_1^{3(2^\ell+2^{\ell+1}\eta)-2^{\ell-1}}$$

and this holds modulo $(2, u_1^{k+1})$. Therefore, since $k_{\ell-2} = 3(2^{\ell-1} + 2^{\ell+1}\eta)$, we have

$$\left[u_1^{k_{\ell-2}}\right] = \left[u_1^{2^\ell+3\cdot 2^{\ell+1}\eta}\right] + (1+\eta)\left[u_1^{3(2^\ell+2^{\ell+1}\eta)-2^{\ell-1}}\right]$$

in $(\mathbb{F}_4[u_1]/(u_1^{k+1}))_{\mathbb{S}}$. However, the right hand terms are zero by Proposition 2.6, which proves the claim. □

3 The action of the Morava stabilizer group

In this section, we continue to abbreviate $R = R_2$ and $\mathbb{S} = \mathbb{S}_2$. Here, we follow the derivation of the formula for the universal deformation $F(x, y)$ and the resulting formulas for the action of $\mathbb{S}$ on R as outlined in the doctoral thesis of Lader [11]. Note that the methods of [11] are a generalization of the techniques of [8, Section 4.1] at primes $p \geq 5$. We claim no originality, but include the computations we need here. One reason for this is that the doctoral thesis is only available in French. We have also decided to add more details to the proofs and have taken the opportunity to note that, with one minor adjustment (Theorem 3.4), the results generalize to the case $p = 2$.

3.1 The universal deformation

We start by fixing a prime p. Let

$$V \cong \mathbb{Z}_{(p)}[v_1, v_2, \ldots]$$

and $G(x, y)$ be the universal p-typical formal group law defined over V. We choose to work with the Araki generators, which can be described as follows. Let $\ell_0 = 1$,

$$\log_G(x) = \sum_{i\geq 0} \ell_i x^{p^i}$$

and $\exp_G(x)$ be the formal power series inverse of $\log_G(x)$ under composition. The Araki generators v_i's are then determined by the recursive formula

$$p\ell_n = \sum_{0\leq i\leq n} \ell_i v_{n-i}^{p^i}$$

where by convention $v_0 = p$. The universal p-typical formal group law is computed as

$$G(x, y) = \exp_G(\log_G(x) + \log_G(y))$$

and the Araki generators have the property that

$$[p]_G(x) = \sum_{i \geq 0}{}^{G} v_i x^{p^i}$$

where $[p]_G(x)$ is the p-series for $G(x, y)$.

The formal group law $F(x, y)$ over R is obtained from $G(x, y)$ as follows. Consider the ring homomorphism

$$\varphi \colon V \to R$$

determined by $\varphi(v_1) = u_1$, $\varphi(v_2) = 1$ and $\varphi(v_n) = 0$ for $n > 2$. The formal group law $F(x, y)$ is defined by

$$F(x, y) = \varphi_* G(x, y).$$

It follows that

$$\log_F(x) = \sum_{i \geq 0} L_i x^{p^i}$$

for $L_i = \varphi(\ell_i)$ and that

$$[p]_F(x) = px +_F u_1 x^p +_F x^{p^2}.$$

We record that

$$L_1 = \frac{u_1}{p - p^p}, \quad L_2 = \frac{\left(1 + \frac{u_1^{p+1}}{p-p^p}\right)}{p - p^{p^2}}, \quad L_3 = \frac{\frac{u_1}{p-p^p} + \frac{u_1^{p^2}}{p-p^{p^2}} + \frac{u_1^{p^2+p+1}}{(p-p^p)\left(p-p^{p^2}\right)}}{p - p^{p^3}}. \tag{3.1}$$

The goal of this section is to approximate $F(x, y)$. From now on, we let $\log(x) = \log_F(x)$ and $\exp(x) = \exp_F(x)$ so that

$$F(x, y) = \exp(\log(x) + \log(y)).$$

We will prove the following result, which is [11, Lemma 3.1].

Theorem 3.1 (Lader) *Let p be any prime. Modulo $(x, y)^{p^2+1}$, the formal group law $F(x, y)$ satisfies*

$$F(x,y) = x + y - \frac{u_1}{1-p^{p-1}} C_p(x,y) - \sum_{i=1}^{p} u_1^{i+1} P_{p+i(p-1)}(x,y) - \frac{1}{1-p^{p^2-1}} \left(1 + \frac{u_1^{p+1}}{p-p^p}\right) C_{p^2}(x,y),$$

where

$$C_{p^k}(x,y) = \frac{1}{p}\left((x+y)^{p^k} - x^{p^k} - y^{p^k}\right)$$

and

$$P_{p+i(p-1)}(x,y) = \frac{1}{(p-p^p)^{i+1}} \sum_{j=0}^{i} \frac{(-1)^j}{j+1} \binom{p(j+1)}{j} \binom{j(p-1)+p}{i-j} (x^p + y^p)^{i-j} (x+y)^{p+pj-i}.$$

We begin with some preliminary results.

Theorem 3.2 *Let p be any prime. Given*

$$\log(x) = x + L_1 x^p + L_2 x^{p^2} \mod (x^{p^3})$$

the inverse series is given by

$$\exp(x) = x - L_1 x^p \left(\sum_{j=0}^{p} \frac{(-1)^j}{j+1} \binom{p(j+1)}{j} \left(L_1 x^{p-1}\right)^j \right) - L_2 x^{p^2} \mod (x^{p^2+1})$$

Proof First, we recall the Lagrange inversion formula for the inverse of a formal power series. The formula states that given a formal power series

$$f(x) = a_1 x + a_2 x^2 + a_3 x^3 + \cdots$$

the inverse series is given by

$$f^{-1}(x) = b_1 x + b_2 x^2 + b_3 x^3 + \cdots$$

where $b_1 = \frac{1}{a_1}$ and for $n > 1$ we have

$$b_n = \frac{1}{n a_1^n} \sum_{c_1, c_2, \ldots} (-1)^{c_1 + c_2 + \cdots} \frac{n(n+1)\cdots(n-1+c_1+c_2+\cdots)}{c_1! c_2! \cdots}$$

$$\left(\frac{a_2}{a_1}\right)^{c_1}\left(\frac{a_3}{a_1}\right)^{c_2}\left(\frac{a_4}{a_1}\right)^{c_3}\cdots,$$

with the sum taken over $c_1, c_2, c_3, \ldots$ such that

$$c_1 + 2c_2 + 3c_3 + \cdots = n - 1.$$

In the current case, $f(x) = \log(x) = x + L_1x^p + L_2x^{p^2}$ modulo (x^{p^3}), so we have coefficients a_n given by

$$a_n = \begin{cases} 1 & \text{if } n = 1 \\ L_1 & \text{if } n = p \\ L_2 & \text{if } n = p^2 \\ 0 & \text{otherwise.} \end{cases}$$

The Lagrange inversion formula for the coefficients of $\exp(x)$ then simplifies to

$$b_n = \frac{1}{n}\sum_{c_1,c_2,c_3,\ldots}(-1)^{c_1+c_2+c_3+\cdots}\frac{n(n+1)\cdots(n-1+c_1+c_2+c_3+\cdots)}{c_1!c_2!c_3!\cdots}a_2^{c_1}a_3^{c_2}a_4^{c_3}\cdots.$$

But since $a_i = 0$ unless $i = 1$, p or p^2, the terms in the sum will vanish if the exponent on any of these terms is nonzero. Hence, the only nonzero c_i that will contribute to the sum are those for which $i = p - 1$ and $i = p^2 - 1$. Hence,

$$b_n = \frac{1}{n}\sum_{c_{p-1},c_{p^2-1}}(-1)^{c_{p-1}+c_{p^2-1}}\frac{n(n+1)\cdots(n-1+c_{p-1}+c_{p^2-1})}{c_{p-1}!c_{p^2-1}!}a_p^{c_{p-1}}a_{p^2}^{c_{p^2-1}}$$

where

$$(p-1)c_{p-1} + (p^2-1)c_{p^2-1} = n - 1.$$

We consider $\exp(x)$ modulo (x^{p^2+1}), so we only need to compute the coefficients b_n up to $n = p^2$. Therefore, the only solutions of $(p-1)c_{p-1} + (p^2-1)c_{p^2-1} = n - 1$ are

$$c_{p-1} = i, \quad c_{p^2-1} = 0 \qquad \text{for } i = 1, 2, \ldots, p+1$$

when $n = i(p-1) + 1$ together with

$$c_{p-1} = 0, \quad c_{p^2-1} = 1$$

when $n = p^2$. Hence,

$$b_n = \begin{cases} \frac{(-1)^i}{i(p-1)+1}\binom{pi}{i}L_1^i & \text{if } n = i(p-1)+1 \text{ for } i = 1, \ldots, p \\ \frac{(-1)^{p+1}}{p^2}\binom{p(p+1)}{(p+1)}L_1^{p+1} - L_2 & \text{if } n = p^2 \\ 0 & \text{otherwise.} \end{cases}$$

It follows that

$$\begin{aligned} \exp(x) &= x + \left(\sum_{i=1}^{p+1} \frac{(-1)^i}{i(p-1)+1}\binom{pi}{i}L_1^i x^{i(p-1)+1}\right) - L_2 x^{p^2} \\ &= x + \left(\sum_{i=1}^{p+1} \frac{(-1)^i}{i}\binom{pi}{i-1}L_1^i x^{i(p-1)+1}\right) - L_2 x^{p^2} \end{aligned}$$

Letting $j = i - 1$ gives the formula. □

Now that we have formulas for both $\log(x)$ and $\exp(x)$ we can apply them to compute $F(x, y) = \exp(\log(x) + \log(y))$ and prove Theorem 3.1.

Proof of Theorem 3.1 First, we consider the middle term $\sum_{j=0}^{p} \frac{(-1)^j}{j+1}\binom{p(j+1)}{j} L_1^{j+1} x^{j(p-1)+p}$ of Theorem 3.2. Evaluating at $\log(x) + \log(y)$, modulo $(x, y)^{p^2+1}$ we have

$$\begin{aligned} &\sum_{j=0}^{p} \frac{(-1)^j}{j+1}\binom{p(j+1)}{j} L_1^{j+1}\big((x+y) + L_1(x^p + y^p)\big)^{j(p-1)+p} \\ &= \sum_{j=0}^{p} \sum_{k=0}^{j(p-1)+p} \frac{(-1)^j}{j+1}\binom{p(j+1)}{j}\binom{j(p-1)+p}{k} \\ &\quad L_1^{k+j+1}(x^p + y^p)^k (x+y)^{j(p-1)+p-k}. \end{aligned}$$

The terms of this polynomial are homogeneous of degree $pk + j(p-1) + p - k = (k+j)(p-1)+p$. So, modulo $(x, y)^{p^2+1}$, the terms in the sum vanish when $k+j > p$. Therefore, we can restrict the upper bound on the inner sum to $p - j$ to obtain

$$\begin{aligned} &= \sum_{j=0}^{p} \sum_{k=0}^{p-j} \frac{(-1)^j}{j+1}\binom{p(j+1)}{j}\binom{j(p-1)+p}{k} L_1^{k+j+1}(x^p+y^p)^k (x+y)^{j(p-1)+p-k} \\ &= \sum_{j=0}^{p} \sum_{i=j}^{p} \frac{(-1)^j}{j+1}\binom{p(j+1)}{j}\binom{j(p-1)+p}{i-j} L_1^{i+1}(x^p + y^p)^{i-j}(x+y)^{p+jp-i} \\ &= \sum_{i=0}^{p} \sum_{j=0}^{i} \frac{(-1)^j}{j+1}\binom{p(j+1)}{j}\binom{j(p-1)+p}{i-j} L_1^{i+1}(x^p + y^p)^{i-j}(x+y)^{p+jp-i}. \end{aligned}$$

Here, we have set $i = k + j$. For the final step, note that the second sum is over i, j such that $0 \le j \le i \le p$. This condition is equivalent to the condition that $0 \le i \le p$ and $0 \le j \le i$; hence, the sums are the same.

Evaluating the final term, $L_2 x^{p^2}$ at $\log(x) + \log(y)$ we have

$$L_2(\log(x) + \log(y))^{p^2} = L_2(x + y)^{p^2} \mod (x, y)^{p^2+1}.$$

So, modulo $(x, y)^{p^2+1}$, and substituting for L_1 and L_2 using (3.1), we have

$$\begin{aligned}
&\exp(\log(x) + \log(y)) \\
&= (x + y) + L_1(x^p + y^p) + L_2(x^{p^2} + y^{p^2}) \\
&\quad -L_1(x + y)^p - \sum_{i=1}^{p} L_1^{i+1} \sum_{j=0}^{i} \frac{(-1)^j}{j+1} \binom{p(j+1)}{j} \binom{j(p-1)+p}{i-j} \\
&\quad (x^p + y^p)^{i-j} (x + y)^{p+pj-i} \\
&= x + y - \frac{u_1}{p - p^p} pC_p(x, y) \\
&\quad - \sum_{i=1}^{p} u_1^{i+1} \frac{1}{(p - p^p)^{i+1}} \sum_{j=0}^{i} \frac{(-1)^j}{j+1} \binom{p(j+1)}{j} \binom{j(p-1)+p}{i-j} \\
&\quad (x^p + y^p)^{i-j} (x + y)^{p+pj-i} \\
&\quad - \frac{1}{p - p^{p^2}} \left(1 + \frac{u_1^{p+1}}{p - p^p}\right) pC_{p^2}(x, y) \\
&= x + y - \frac{u_1}{1 - p^{p-1}} C_p(x, y) - \sum_{i=1}^{p} u_1^{i+1} P_{p+i(p-1)}(x, y) \\
&\quad - \frac{1}{1 - p^{p^2-1}} \left(1 + \frac{u_1^{p+1}}{p - p^p}\right) C_{p^2}(x, y).
\end{aligned}$$

□

3.2 The action

The following is Proposition 3.2 in [11]. To make sense of the statement, recall the following facts. Fix $g = \sum_{i \ge 0} g_i S^i$ in $\mathbb{S}$ with $g_i^{p^2} - g_i = 0$. Let $g_*\colon R \to R$ be ring homomorphism given by the left action of $\mathbb{S}$ on R. Then there is an associated $\star$-isomorphism $h_g\colon g_* F \to F$, and since F is p-typical, it takes the form

$$h_g(x) = \sum_{i \ge 0}^{F} t_i(g) x^{p^i} \tag{3.2}$$

for $t_i(g) \in R$ such that $t_i(g) = g_i$ modulo (p, u_1). In particular, t_0 is a unit. Further, note that $[p]_F(x) = px +_F u_1 x^p +_F x^{p^2}$ and the $t_i(g)$ satisfy the following recursive formula

$$h_g([p]_{g_*F}(x)) = [p]_F(h_g(x)). \tag{3.3}$$

Below, we fix g and abbreviate $t_i = t_i(g)$.

Theorem 3.3 (Lader) *Let p be any prime. Let $g \in \mathbb{S}$. Then*

(a) $g_*(u_1) = t_0^{p-1}u_1 + t_0^{-1}t_1(p - p^p)$,
(b) $t_0 = t_0^{p^2} + u_1 t_1^p - t_0^{p(p-1)} t_1 u_1^p$ *modulo* (p), *and*
(c) $t_1 = t_1^{p^2} + t_2^p u_1 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} u_1^{i+1} t_1^{pi} t_0^{p^2(p-i)}$ *modulo* (p, u_1^{p+1}).

Proof First, studying (3.3) modulo (x^{p+1}) gives

$$t_0 \left(px \underset{g_*F}{+} g_*(u_1)x^p \right) \underset{F}{+} t_1(px)^p = p\left(t_0 x +_F t_1 x^p\right) +_F u_1 (t_0 x)^p.$$

The higher order terms are all of order greater than x^p, so this reduces to

$$t_0 px + t_0 g_*(u_1)x^p + t_1 p^p x^p = pt_0 x + pt_1 x^p + u_1 t_0^p x^p.$$

Comparing the coefficients of x^p gives (a).

Using this result modulo (p), (3.3) gives the following equality:

$$\sum_{i\geq 0}^{F} t_i \left(t_0^{p-1}u_1 x^p \underset{g_*F}{+} x^{p^2} \right)^{p^i} = u_1 \left(\sum_{i\geq 0}^{F} t_i x^{p^i} \right)^p \underset{F}{+} \left(\sum_{i\geq 0}^{F} t_i x^{p^i} \right)^{p^2}. \tag{3.4}$$

This trivially reduces to

$$\begin{aligned} &t_0 \left(t_0^{p-1}u_1 x^p \underset{g_*F}{+} x^{p^2} \right) \underset{F}{+} t_1 \left(t_0^{p-1}u_1 x^p \underset{g_*F}{+} x^{p^2} \right)^p \\ &\quad = u_1 \left(t_0 x \underset{F}{+} t_1 x^p \underset{F}{+} t_2 x^{p^2} \right)^p \underset{F}{+} \left(t_0 x \underset{F}{+} t_1 x^p \underset{F}{+} t_2 x^{p^2} \right)^{p^2}. \end{aligned}$$

The higher order terms are divisible by x^{p^2+1}, so we conclude that

$$t_0^p u_1 x^p + \left(t_0 + t_1 (t_0^{p-1}u_1)^p\right) x^{p^2} = u_1 t_0^p x^p + \left(u_1 t_1^p + t_0^{p^2}\right) x^{p^2}.$$

Part (b) follows by comparing coefficients of x^{p^2}.

The proof of part (c) is more involved: it is proved by comparing the coefficients of x^{p^3}. First, using parts (a) and (b) we compute the following modulo (x^{p^3+1}, u_1^{p+1}), using the fact that $g_*(u_1)x^p \underset{g_*F}{+} x^{p^2} = t_0^{p-1}u_1 x^p + x^{p^2}$ modulo (x^{p^2+p}):

$$\begin{aligned}
&\sum_{i\geq 0}^{F} t_i \left(g_*(u_1)x^p \underset{g_*F}{+} x^{p^2} \right)^{p^i} \\
&= t_0 \left(t_0^{p-1} u_1 x^p \underset{g_*F}{+} x^{p^2} \right) \underset{F}{+} t_1 \left(t_0^{p-1} u_1 x^p + x^{p^2} \right)^p \underset{F}{+} t_2 \left(t_0^{p-1} u_1 x^p \right)^{p^2} \\
&= t_0 \left(t_0^{p-1} u_1 x^p \underset{g_*F}{+} x^{p^2} \right) \underset{F}{+} \left(t_1 t_0^{p(p-1)} u_1^p x^{p^2} + t_1 x^{p^3} \right)
\end{aligned}$$

Therefore, the coefficient of x^{p^3} is $c + t_1$ where c is the coefficient of x^{p^3} in

$$t_0 \left(t_0^{p-1} u_1 x^p \underset{g_*F}{+} x^{p^2} \right) \underset{F}{+} t_1 t_0^{p(p-1)} u_1^p x^{p^2}.$$

To compute this coefficient define

$$X = t_0^{p-1} u_1 x^p, \quad Y = x^{p^2}, \quad Z = t_1 t_0^{p(p-1)} u_1^p x^{p^2}.$$

First, we note that $X^i Z^j = 0$ modulo (u^{p+1}) for $i, j > 0$. Then, letting

$$F(s,t) = s + t + \sum_{i,j>0} a_{i,j} s^i t^j,$$

we have that c is the coefficient of x^{p^3} in the following expression which is computed modulo (u_1^{p+1}, x^{p^3+1}):

$$\begin{aligned}
t_0(X \underset{g_*F}{+} Y) \underset{F}{+} Z &= t_0(X \underset{g_*F}{+} Y) + Z + \sum_{i,j>0} a_{i,j} (t_0 X \underset{g_*F}{+} Y)^i Z^j \\
&= t_0(X \underset{g_*F}{+} Y) + Y + Z + \sum_{i,j>0} a_{i,j} Y^i Z^j - Y \\
&= t_0(X \underset{g_*F}{+} Y) + Y \underset{F}{+} Z - Y.
\end{aligned}$$

From Theorem 3.1, we have that, modulo (x^{p^3+1}),

$$Y \underset{F}{+} Z = Y + Z - \frac{u_1}{1 - p^{p-1}} C_p(Y,Z) - \sum_{i=1}^{p} u_1^{i+1} P_{p+i(p-1)}(Y,Z).$$

We have dropped the term involving $C_{p^2}(Y,Z)$ since it has degree greater than p^3. Each monomial in $C_p(Y,Z)$ is a multiple of Z, so $u_1 C_p(Y,Z)$ vanishes modulo (u_1^{p+1}). The terms of the sum indexed by i are homogeneous of degree $p^3 + i(p^3 - p^2)$ and so vanish modulo (x^{p^3+1}). Therefore, the coefficient of x^{p^3} in $Y \underset{F}{+} Z$ is zero modulo (u_1^{p+1}).

Using Theorem 3.1 again, we have that modulo (x^{p^3+1})

$$X \underset{g_*G}{+} Y = X + Y - \frac{u_1}{1-p^{p-1}} C_p(X,Y) - \sum_{i=1}^{p} u_1^{i+1} P_{p+i(p-1)}(X,Y).$$

Again, the term involving $C_{p^2}(X,Y)$ has degree greater than p^3 and has been omitted. The highest power of x in $C_p(X,Y)$ is $p^3 - p^2 + p$, so this term in the sum cannot contribute to the coefficient of x^{p^3}. This leaves the sum indexed by i. Fix i. Then if $i - j \geq 1$, the monomials of $P_{p+i(p-1)}$ are zero modulo (u_1^{p+1}, x^{p^3+1}). So we only consider the terms such that $i = j$, which gives

$$\sum_{i=1}^{p} u_1^{i+1} \tfrac{1}{(p-p^p)^{i+1}} \tfrac{(-1)^i}{i+1} \binom{p(i+1)}{i} (X+Y)^{p+i(p-1)}.$$

When the power of $Y = x^{p^2}$ in the binomial expansion $(X+Y)^{p+i(p-1)}$ exceeds p, the monomials vanish modulo (x^{p^3+1}). In the remaining monomials, the exponent of $X = t_0^{p-1} u_1 x^p$ is at least $i(p-1)$, so that after multiplying with u_1^{i+1}, these monomials vanish modulo (u_1^{p+1}). Therefore, the coefficient of x^{p^3} in $X +_F Y$ is also zero modulo (u_1^{p+1}). We conclude that $c = 0$ modulo (u_1^{p+1}) which implies that the coefficient of x^{p^3} on the left hand side of (3.4) is t_1 modulo (u_1^{p+1}).

Now, we need to compute the coefficient of x^{p^3} on the right hand side of (3.4). Modulo (u_1^{p+1}, x^{p^3+1}), we have,

$$\begin{aligned}
&u_1 \left(\sum_{i\geq 0}^{F} t_i x^{p^i} \right)^p \underset{F}{+} \left(\sum_{i\geq 0}^{F} t_i x^{p^i} \right)^{p^2} \\
&= u_1 \left(t_0 x \underset{F}{+} t_1 x^p \underset{F}{+} t_2 x^{p^2} \right)^p \underset{F}{+} \left(t_0 x \underset{F}{+} t_1 x^p \underset{F}{+} t_2 x^{p^2} \right)^{p^2} \\
&= u_1 \left(\left(t_0 x \underset{F}{+} t_1 x^p \right)^p + t_2^p x^{p^3} \right) \underset{F}{+} \left(t_0^{p^2} x^{p^2} + t_1^{p^2} x^{p^3} \right) \\
&= \left(u_1 \left(t_0 x \underset{F}{+} t_1 x^p \right)^p \underset{F}{+} t_0^{p^2} x^{p^2} \right) + u_1 t_2^p x^{p^3} + t_1^{p^2} x^{p^3}
\end{aligned}$$

We apply Theorem 3.1. Using the fact that we are working modulo (p), that $C_{p^2}(t_0 x, t_1 x^p)^p = 0$ modulo (x^{p^3+1}), and that, modulo (u_1^{p+1}, x^{p^3+1}),

$$u_1\left(t_0x \underset{F}{+} t_1x^p\right)^p = u_1\left(t_0x + t_1x^p - \frac{u_1}{1-p^{p-1}}C_p(t_0x, t_1x^p) - \sum_{i=1}^{p} u_1^{i+1}P_{p+i(p-1)}(t_0x, t_1x^p)\right)^p$$
$$= u_1\left(t_0^px^p + t_1^px^{p^2}\right)$$

the problem reduces to computing the coefficient of x^{p^3} in

$$\left(u_1t_0^px^p + u_1t_1^px^{p^2}\right) \underset{F}{+} t_0^{p^2}x^{p^2} + \left(u_1t_2^p + t_1^{p^2}\right)x^{p^3}.$$

Let

$$A = u_1t_0^px^p, \quad B = u_1t_1^px^{p^2}, \quad C = t_0^{p^2}x^{p^2}.$$

Then the coefficient of x^{p^3} in the preceding expression is $c + (u_1t_2^p + t_1^{p^2})$ where c is the coefficient of x^{p^3} in

$$(A + B) \underset{F}{+} C.$$

Using Theorem 3.1 once again, we have that modulo (x^{p^3+1})

$$(A + B) \underset{F}{+} C = A + B + C - \frac{u_1}{1-p^{p-1}}C_p(A + B, C) - \sum_{i=1}^{p} u_1^{i+1}P_{p+i(p-1)}(A + B, C)$$

dropping as usual the term involving $C_{p^2}(A+B, C)$ for degree reasons. Since $A+B$ is divisible by u_1x^p and C by x^{p^2}, a slightly tedious but straightforward inspection of the sum indexed by i shows that it vanishes modulo (u_1^{p+1}, x^{p^3+1}). Clearly, $A + B + C$ has no powers of x^{p^3}, so cannot contribute to the coefficient of x^{p^3}. It remains to inspect $C_p(A + B, C)$. We have

$$C_p(A + B, C) = \sum_{k=1}^{p-1}\frac{1}{p}\binom{p}{k}u_1^k\left(t_0^px^p + t_1^px^{p^2}\right)^k t_0^{p^2(p-k)}x^{p^2(p-k)}$$
$$= \sum_{k=1}^{p-1}\frac{1}{p}\binom{p}{k}u_1^k\left(\sum_{\ell=0}^{k}\binom{k}{\ell}t_0^{p\ell}t_1^{p(k-\ell)}x^{p\ell+p^2(k-\ell)}\right)t_0^{p^2(p-k)}x^{p^2(p-k)}$$
$$= \sum_{k=1}^{p-1}\frac{1}{p}\binom{p}{k}u_1^k\left(\sum_{\ell=0}^{k}\binom{k}{\ell}t_0^{p\ell+p^2(p-k)}t_1^{p(k-\ell)}x^{p^3-\ell(p^2-p)}\right).$$

The terms of degree p^3 correspond to those for which $\ell = 0$, which is exactly $C_p(B, C)$. Hence, the coefficient of x^{p^3} in $(A + B) \underset{F}{+} C$ is equal to the coefficient of x^{p^3} in

$$-\frac{u_1}{1-p^{p-1}} C_p(B,C) = -\frac{1}{p-p^p}\left(\sum_{k=1}^{p-1}\binom{p}{k} u_1^{k+1} t_0^{p^2(p-k)} t_1^{pk}\right) x^{p^3}.$$

So, combining this with the above, we get that the coefficient of x^{p^3} on the right hand side of (3.4) is

$$t_1^{p^2} + t_2^p u_1 - \frac{1}{p-p^p}\sum_{i=1}^{p-1}\binom{p}{i} u_1^{i+1} t_1^{pi} t_0^{p^2(p-i)}$$

modulo (u_1^{p+1}). Hence, equating coefficients, we have

$$t_1 = t_1^{p^2} + t_2^p u_1 - \sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i} u_1^{i+1} t_1^{pi} t_0^{p^2(p-i)} \mod (p, u_1^{p+1})$$

as claimed. □

We finish with the following result.

Theorem 3.4 (Lader) *Let p be any prime. Let $g = 1 + g_1 S + g_2 S^2$ modulo (S^3). Then*

$$t_0 = 1 + g_1^p u_1 - g_1 u_1^p + \left(g_2 - g_2^p\right) u_1^{p+1} + \sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i} g_1^{pi} u_1^{p+1+i} + g_1^2 u_1^{2p} + g_1^p u_1^{p^2} \mod \left(p, u_1^{2p+1}\right).$$

Proof Using the fact that, modulo (p, u_1), $t_0 = 1$, $t_1 = g_1$, and $t_2 = g_2$ and the fact that $g_i^{p^2} = g_i$, it follows from part (c) of Theorem 3.3 that

$$t_1 = g_1 + g_2^p u_1 - u_1^2 \sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i} u_1^{i-1} g_1^{pi} \mod (p, u_1^{p+1}).$$

From part (b) of Theorem 3.3, we also conclude that

$$t_0 = 1 + g_1^p u_1 - g_1 u_1^p \mod (p, u_1^{p+1}).$$

Now, re-substituting these results into part (b) of Theorem 3.3 and computing modulo (p, u_1^{2p+1}), we have

$$\begin{aligned}
t_0 &= \left(1+g_1^p u_1\right)^{p^2} + u_1\left(g_1+g_2^p u_1\right)^p \\
&\quad - (1+g_1^p u_1)^{p(p-1)}\left(g_1+g_2^p u_1 - u_1^2\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}u_1^{i-1}g_1^{pi}\right)u_1^p \\
&= 1+g_1^p u_1^{p^2} + u_1 g_1^p + g_2 u_1^{p+1} \\
&\quad - \left(u_1^p - g_1 u_1^{2p}\right)\left(g_1+g_2^p u_1 - u_1^2\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}u_1^{i-1}g_1^{pi}\right) \\
&= 1+g_1^p u_1 - g_1 u_1^p + \left(g_2 - g_2^p\right)u_1^{p+1} + \sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}u_1^{p+i+1}g_1^{pi} \\
&\quad + g_1^2 u_1^{2p} + g_1^p u_1^{p^2}.
\end{aligned}$$

This proves the claim. □

Note that the last term in Theorem 3.4 vanishes modulo (u_1^{2p+1}) when p is odd.

3.3 Formulas for the prime 2

To prove our results when $p = 2$, we need more information on the action of g than what was determined in Theorem 3.4. We gather the information in this section. We note that the computations in this section are computer assisted, but are consistent with the results of [1], which study the action of the group of automorphisms of the formal group law of a super-singular curve on an associated Lubin–Tate ring.

First, we get specific about the results of Theorem 3.3 and Theorem 3.4 in the case at hand.

Corollary 3.5 *Let $p = 2$ and $g \in \mathbb{S}$. Then*

(a) $g_* u_1 = t_0 u_1$ *modulo* (2),
(b) $t_0 = t_0^4 + u_1 t_1^2 + t_0^2 t_1 u_1^2$ *modulo* (2), *and*
(c) $t_1 = t_1^4 + t_2^2 u_1 + u_1^2 t_1^2 t_0^4$ *modulo* $(2, u_1^3)$.

Further, for $g = 1 + g_1 S + g_2 S^2 + \cdots$,

$$\begin{aligned}
t_1 &= g_1 + g_2^2 u_1 + g_1^2 u_1^2 \mod (2, u_1^3). \\
t_0 &= 1 + g_1^2 u_1 + g_1 u_1^2 + (g_2 + g_2^2)u_1^3 + g_1^2 u_1^4 \mod (2, u_1^5).
\end{aligned}$$

The computation of $F(x, y) = \exp(\log(x) + \log(y))$ modulo $(x, y)^{16}$ using the information provided at the beginning of Sect. 3.1 is not expensive for a computer. It would not be enlightening to include the formula here, but the following computations use it, together with the following fact.

Lemma 3.6 *If $F(x, y)$ is known modulo $(x, y)^{16}$ and $x^2|X$ and $x^4|Y$, then $F(X, Y)$ is determined modulo $(x, y)^{34}$.*

Proof The error terms for $F(x, y)$ have the form $xy(x, y)^{14}$. If X, Y are as stated, the monomials $XY(X, Y)^{14}$ have degree at least 34. □

As before, we collect information from the relation

$$\sum_{i\geq 0}^{F} t_i \left(t_0 u_1 x^2 \underset{g_* F}{+} x^4 \right)^{2^i} = u_1 \left(\sum_{i\geq 0}^{F} t_i x^{2^i} \right)^2 \underset{F}{+} \left(\sum_{i\geq 0}^{F} t_i x^{2^i} \right)^4. \tag{3.5}$$

We will study the coefficients in this equation up to that of x^{32} for elements $g \in \mathbb{S}$ of the form $g = 1 + g_2 S^2$ modulo (S^3). Note that $t_1 = g_1$ modulo $(2, u_1)$ and since $g_1 = 0$, we have $t_1 = 0$ modulo $(2, u_1)$. We also note that, modulo $(2, u_1)$, $F(x, y)$ is equivalent to the Honda formal group law whose coefficients are in $\mathbb{F}_2$. So,

$$F(x, y)^2 = F(x^2, y^2) \mod (2, u_1).$$

Proposition 3.7 *Let $g = 1 + g_2 S^2 + g_3 S^3 + g_4 S^4 + \cdots$. Then*

(a) $t_3 = g_3 + g_4^2 u_1$ *modulo* $(2, u_1^2)$,
(b) $t_2 = g_2 + g_3^2 u_1 + g_1 u_1^2 + (g_4 + g_2^2 + g_2^2) u_1^3$ *modulo* $(2, u_1^4)$
(c) $t_1 = g_2^2 u_1 + g_3 u_1^3 + g_3^2 u_1^5 + g_3 u_1^6 + (g_2 + g_2^3 + g_4 + g_4^2) u_1^7$ *modulo* $(2, u_1^8)$
(d) $t_0 = 1 + (g_2 + g_2^2) u_1^3 + g_3 u_1^5 + g_3 u_1^8 + (g_4 + g_4^2) u_1^9$ *modulo* $(2, u_1^{10})$.

Computer Assisted Proof For (a), we compute the coefficients of x^{32} modulo $(2, u_1^2)$ in (3.5). For this, we note using the above observations that (3.5) reduces to the following relation modulo (u_1^2, x^{33}):

$$\begin{aligned} &t_0 \left(t_0 u_1 x^2 +_F x^4 \right) +_F t_1 x^8 +_F t_2 x^{16} + t_3 x^{32} \\ &\quad = u_1 \left(t_0^2 x^2 +_F t_2^2 x^8 +_F t_3^2 x^{16} + t_4^2 x^{32} \right) +_F \left(t_0 x +_F t_2 x^4 + t_3 x^8 \right)^4. \end{aligned}$$

By Lemma 3.6, both sides are determined modulo (x^{34}) by $F(x, y)$ modulo $(x, y)^{16}$. A direct computation comparing both sides gives

$$t_3 = t_3^4 + t_4^2 u_1 \mod (2, u_1^2).$$

Since $t_i = g_i$ modulo $(2, u_1)$, we get (a).

To get (b) we compute the coefficients of x^{16} modulo $(2, u_1^4)$ in (3.5). Modulo $(2, u_1^4, x^{17})$, we have

$$t_0 \left(t_0 u_1 x^2 \underset{g_* F}{+} x^4 \right) +_F t_1 \left(t_0 u_1 x^2 \underset{g_* F}{+} x^4 \right)^2 + t_2 x^{16}$$

$$= u_1 \left(t_0 x +_F t_1 x^2 +_F t_2 x^4 + t_3 x^8\right)^2 \underset{F}{+} \left(t_0 x +_F t_1 x^2 + t_2 x^4\right)^4.$$

A direct computation comparing both sides gives the relation

$$t_2 = t_2^4 + t_3^2 u_1 + t_1 t_0^2 u_1^2 + t_1^4 t_2^2 u_1^2 + t_0^{16} u_1^3 + t_2^2 t_0^8 u_1^3 + t_1^6 t_0^4 u_1^3 + t_0^4 u_1^3 \mod (2, u_1^4).$$

To get the result, we combine this with the fact that $t_i = g_i$ modulo $(2, u_1)$, with (a) and with Corollary 3.5.

To get (c), we compute the coefficient of x^8 modulo $(2, u_1^8)$ in (3.5). Modulo $(2, u_1^8, x^9)$, we have

$$\begin{aligned} t_0 \left(t_0 u_1 x^2 \underset{g_* F}{+} x^4\right) +_F t_1 \left(t_0 u_1 x^2 \underset{g_* F}{+} x^4\right)^2 + t_2 t_0^4 u_1^4 x^8 \\ = u_1 \left(t_0 x +_F t_1 x^2 + t_2 x^4\right)^2 \underset{F}{+} \left(t_0 x + t_1 x^2\right)^4. \end{aligned}$$

A direct computation comparing both sides gives

$$\begin{aligned} t_1 = t_1^4 + t_0^8 u_1^4 + t_1 t_0^6 u_1^6 + t_0^5 u_1^4 + t_1^2 t_0^4 u_1^5 + t_2 t_0^4 u_1^4 + t_1^2 t_0^4 u_1^2 \\ + t_1 t_0^3 u_1^3 + t_2^2 u_1 \mod (2, u_1^8). \end{aligned} \tag{3.6}$$

Now, we do a short recursion. First, we use (a), (b) and Corollary 3.5 to compute that

$$\begin{aligned} t_1 &= g_2^2 u_1 + g_3 u_1^3 + g_3^2 u_1^5 \mod (2, u_1^6) \\ t_0 &= 1 + (g_2 + g_2^2) u_1^3 \mod (2, u_1^5). \end{aligned}$$

We use this again in part (b) of Corollary 3.5 and in (3.6) to finish the proof. □

Acknowledgements We thank some of the usual suspects for useful conversations: Tobias Barthel, Mark Behrens, Paul Goerss, Hans-Werner Henn, Mike Hopkins, Niko Naumann and Vesna Stojanoska. We also thank the referee and the editors their input.

References

1. Beaudry, A.: Towards the homotopy of the $K(2)$-local Moore spectrum at $p = 2$. Adv. Math. **306**, 722–788 (2017). https://doi.org/10.1016/j.aim.2016.10.020
2. Beaudry, A., Goerss, P.G., Henn, H.-W.: Chromatic splitting for the $K(2)$-local sphere at $p = 2$. arXiv e-prints (2017). arXiv:1712.08182
3. Bobkova, I., Goerss, P.G.: Topological resolutions in k(2)-local homotopy theory at the prime 2. Journal of Topology **11**(4), 918–957 (2018). https://doi.org/10.1112/topo.12076
4. Devinatz, E.S., Hopkins, M.J.: Homotopy fixed point spectra for closed subgroups of the Morava stabilizer groups. Topology **43**(1), 1–47 (2004). https://doi.org/10.1016/S0040-9383(03)00029-6
5. Goerss, P.G., Hopkins, M.J.: Moduli spaces of commutative ring spectra. In: Baker, A., Richter, B. (eds.) Structured Ring Spectra. London Mathematical Society Lecture Note series, vol. 315, pp. 151–200. Cambridge University Press, Cambridge (2004). https://doi.org/10.1017/CBO9780511529955.009

6. Goerss, P.G., Henn, H.-W., Mahowald, M.E.: The rational homotopy of the $K(2)$-local sphere and the chromatic splitting conjecture for the prime 3 and level 2. Doc. Math. **19**, 1271–1290 (2014)
7. Hazewinkel, M.: Formal Groups and Applications. Pure and Applied Mathematics, vol. 78. Academic Press, Inc. (Harcourt Brace Jovanovich Publishers), New York (1978)
8. Henn, H.-W., Karamanov, N., Mahowald, M.E.: The homotopy of the $K(2)$-local Moore spectrum at the prime 3 revisited. Math. Z. **275**(3–4), 953–1004 (2013). https://doi.org/10.1007/s00209-013-1167-4
9. Hovey, M.: Bousfield localization functors and Hopkins' chromatic splitting conjecture. In: Cenkl, M., Miller, H. (eds.) The Čech Centennial (Boston, MA, 1993). Contemporary Mathematics, vol. 181, pp. 225–250. American Mathematical Society, Providence, RI (1995). https://doi.org/10.1090/conm/181/02036
10. Kohlhaase, J.: On the Iwasawa theory of the Lubin–Tate moduli space. Compos. Math. **149**(5), 793–839 (2013)
11. Lader, O.: Une résolution projective pour le second groupe de Morava pour $p \geq 5$ et applications. Theses, Université de Strasbourg, October (2013). https://tel.archives-ouvertes.fr/tel-00875761
12. Lubin, J., Tate, J.: Formal moduli for one-parameter formal Lie groups. Bull. Soc. Math. France **94**, 49–59 (1966). http://www.numdam.org/item?id=BSMF_1966__94__49_0
13. Morava, J.: Noetherian localisations of categories of cobordism comodules. Ann. Math. (2) **121**(1), 1–39 (1985). https://doi.org/10.2307/1971192
14. Shimomura, K., Yabe, A.: The homotopy groups $\pi_*(L_2 S^0)$. Topology **34**(2), 261–289 (1995). https://doi.org/10.1016/0040-9383(94)00032-G