The power operation structure on Morava E-theory of height 2 at the prime 3

YIFEI ZHU

We give explicit calculations of the algebraic theory of power operations for a specific Morava E-theory spectrum and its $K(1)$-localization. These power operations arise from the universal degree-3 isogeny of elliptic curves associated to the E-theory.

1 Introduction

Suppose E is a commutative S-algebra, in the sense of [EKMM97], and A is a commutative E-algebra. We want to capture the properties and underlying structure of the homotopy groups $\pi_* A = A_*$ of A, by studying operations associated to the cohomology theory that E represents.

An important family of cohomology operations, called *power operations*, is constructed via the extended powers. Specifically, consider the *m'th extended power* functor

$$\mathbb{P}_E^m(-) := (-)^{\wedge_E m}/\Sigma_m \colon \operatorname{Mod}_E \to \operatorname{Mod}_E$$

on the category of E-modules which sends an E-module to its m-fold smash product over E modulo the action by the symmetric group on m letters. The $\mathbb{P}_E^m(-)$'s assemble together to give the *free commutative E-algebra* functor

$$\mathbb{P}_E(-) := \bigvee_{m \geq 0} \mathbb{P}_E^m(-) \colon \operatorname{Mod}_E \to \operatorname{Alg}_E$$

from the category of E-modules to the category of commutative E-algebras. These functors descend to homotopy categories. In particular, each $\alpha \in \pi_{d+i}\, \mathbb{P}_E^m(\Sigma^d E)$ gives rise to a power operation

$$Q_\alpha \colon A_d \to A_{d+i}$$

(cf. [BMMS86, Sections I.2 and IX.1] and [Rez09, Section 3]).

Under the action of power operations, A_* is an algebra over some operad in E_*-modules involving the structure of $E_*B\Sigma_m$ for all m. This operad is traditionally called a *Dyer–Lashof algebra*, or more precisely, a Dyer–Lashof *theory* as the *algebraic theory* of power operations acting on the homotopy groups of commutative E-algebras (cf. [BMMS86, Chapters III, VIII, and IX] and [Reza, Section 9]).

A specific case is when E represents a Morava E-theory of height n and A is $K(n)$-local. Morava E-theory spectra are of crucial importance in modern stable homotopy theory, particularly in the work of Ando, Hopkins, and Strickland [AHS01]. Much of the $K(n)$-local E-Dyer–Lashof theory has been worked out by those authors (cf. [Rez09, 1.5] for a description of the history). In [Rez09] Rezk gives a unified treatment of this Dyer–Lashof theory. He works out a congruence criterion that must hold in an algebra over the Dyer–Lashof theory ([Rez09, Theorem A]). This enables one to study the Dyer–Lashof *theory*, which models all the algebraic structure naturally adhering to A_*, by working with a certain associative ring Γ as the Dyer–Lashof *algebra*. Moreover, Rezk provides a geometric description of this congruence criterion, in terms of sheaves on the moduli problem of deformations of formal groups and Frobenius isogenies (cf. [Rez09, Theorem B]). This connects the structure of Γ to the geometry underlying E, moving one step forward from a workable object Γ to things that are computable. Based on these, in a companion paper [Rezb], Rezk gives explicit calculations of the Dyer–Lashof theory for a specific Morava E-theory of height $n = 2$ at the prime 2.

The purpose of this paper is to make available calculations analogous to some of the results in [Rezb], at the prime 3, together with calculations of the corresponding power operations on the $K(1)$-localization of the Morava E-theory spectrum.

1.1 Outline of the paper

As in [Rezb], the computation of power operations in this paper follows the approach of [Ste62]: one first defines a total power operation, and then uses the computation of the cohomology of the classifying space $B\Sigma_m$ for the symmetric group to obtain individual power operations. These two steps are carried out in Sections 2 and 3 respectively.

In Section 2, by doing calculations with elliptic curves associated to our Morava E-theory E, we give formulas for the total power operation ψ^3 on E_0 and the ring S_3 which represents the corresponding moduli problem.

In Section 3, based on calculations of $E^*B\Sigma_m$ in [Str98] as reflected in the formula for S_3, we define individual power operations, and derive the relations they satisfy. In view of the general structures studied in [Rez09], we then get an explicit description of the Dyer–Lashof algebra Γ for $K(2)$-local commutative E-algebras.

In Section 4, we describe the relationship between the total power operation ψ^3, at height 2, and the corresponding $K(1)$-local power operations. We then derive formulas for the latter from the calculations in Section 2.

Remark 1 In Section 2, we do calculations with a universal elliptic curve over *all* of the moduli stack which is an affine open subscheme of a weighted projective space (cf. Proposition 3). At the prime 3, the supersingular locus consists of a single closed point, and the corresponding Morava E-theory arises *locally* in an affine coordinate chart of this weighted projective space containing the supersingular locus. In this paper we choose a particular affine coordinate chart for computing the homotopy groups of the E-theory spectrum and the power operations; we hope that the generality of the calculations in Section 2 makes it easier to work with other coordinate charts as well.

Remark 2 The ring S_3 turns out to be an algebra with one generator over the base ring where our elliptic curve is defined (cf. Proposition 6 (i) and (18)). This generator appears as a parameter in the formulas for the total power operation ψ^3, and is responsible for how the individual power operations are defined and how their formulas look. Different choices of this parameter result in different bases of the Dyer–Lashof algebra Γ. The parameter in this paper comes from the relative cotangent space of the elliptic curve at the identity (cf. Proposition 6 (iv), Corollary 11, and Remark 13). This choice is convenient for deriving Adem relations in Proposition 15 (iv), and it fits into the treatment of gradings in [Rez09, Section 2] (cf. Definition 17 (ii) and Theorem 19). We should point out that our choice is by no means canonical. We do not know yet, as part of the structure of the Dyer–Lashof algebra, if there is a canonical basis which is both geometrically interesting and computationally convenient. Somewhat surprisingly, although it appears to come from different considerations, our choice has an analog at the prime 2 which coincides with the parameter used in [Rezb] (cf. Remarks 8 and 12). The calculations follow a recipe in hope of generalizing to other Morava E-theories of height 2; we hope to address these matters and recognize more of the general patterns based on further computational evidence.

1.2 Acknowledgements

I thank Charles Rezk for his encouragement on this work, and for his observation in a correspondence which led to Proposition 10 and Corollary 11.

I thank Kyle Ormsby for helpful discussions on Section 2, and for directing me to places in the literature.

I thank Tyler Lawson for the sustained support from him I received as a student.

1.3 Conventions

Let p be a prime, q a power of p, and n a positive integer. We use the symbols

$$\mathbb{F}_q, \ \overline{\mathbb{F}}_q, \ \mathbb{Z}_q, \ \text{and} \ \mathbb{Z}/n$$

to denote a field with q elements, an algebraic closure of $\mathbb{F}_q$, the ring of p-typical Witt vectors over $\mathbb{F}_q$, and the additive group of integers modulo n, respectively.

If R is a ring, then $R[\![x]\!]$ and $R(\!(x)\!)$ denote the rings of formal power series and formal Laurent series over R in the variable x respectively. If $I \subset R$ is an ideal, then $R_I^\wedge$ denotes the completion of R with respect to I.

If E is an elliptic curve and m is an integer, then $[m]$ denotes the multiplication-by-m map on E, and $E[m]$ denotes the m-torsion subgroup of E.

All formal groups mentioned in this paper will be commutative and one-dimensional.

The terminology for the structure of the Dyer–Lashof theory will follow [Rez09] and [Rezb]; some of the notions there are taken in turn from [BW05] and [Voe03].

2 Total power operations

2.1 A universal elliptic curve and a Morava E-theory spectrum

A Morava E-theory of height 2 at the prime 3 has its formal group as the universal deformation of a height-2 formal group over a perfect field of characteristic 3. Given a supersingular elliptic curve over such a field, its formal completion at the identity produces a formal group of height 2. To study power operations for the corresponding Morava E-theory, we do calculations with the universal deformation of that supersingular elliptic curve which is a family of elliptic curves with a $\Gamma_1(N)$-structure (cf. [KM85, Section 3.2]) where N is not divisible by 3. Here is a specific model (cf. [Hus04, 4(4.6a)]).

Proposition 3 *Over $\mathbb{Z}[1/4]$, the moduli problem of nonsingular elliptic curves with a choice of a point of exact order 4 and a nowhere-vanishing invariant one-form is represented by*

$$C\colon\ y^2 + axy + aby = x^3 + bx^2 \tag{1}$$

with chosen point $(0,0)$ and one-form $dx/(2y+ax+ab) = dy/(3x^2+2bx-ay)$ over the graded ring

$$S^\bullet := \mathbb{Z}[1/4][a,b,\Delta^{-1}]$$

where $|a| = 1$, $|b| = 2$, and $\Delta = a^2b^4(a^2-16b)$.

Proof Let P be the chosen point of exact order 4. Since $2P$ is 2-torsion, the tangent line of the elliptic curve at P passes through $2P$, and the tangent line at $2P$ passes through the identity at the infinity. With this observation, the rest of the proof is analogous to that of [MR09, Proposition 3.2]. □

Over a finite field of characteristic 3, C is supersingular precisely when the quantity

$$H := a^2 + b \tag{2}$$

vanishes (cf. [Sil09, V.4.1a]). As $(3,H)$ is a maximal ideal of $S^\bullet$ corresponding to the closed subscheme $\operatorname{Spec}\mathbb{F}_3$, the supersingular locus consists of a single closed point, and C restricts to $\mathbb{F}_3$ as

$$C_0\colon\ y^2 + xy - y = x^3 - x^2.$$

From the above universal deformation C of C_0, we next produce a Morava E-theory spectrum which is 2-periodic. We follow the convention that elements in algebraic degree n lie in topological degree $2n$, and work in an affine étale coordinate chart of the weighted projective space $\operatorname{Proj}\mathbb{Z}[1/4][a,b]$ (cf. Remark 1). Define elements u and c such that

$$a = uc \qquad \text{and} \qquad b = u^2.$$

Consider the graded ring

$$S^\bullet[u^{-1}] \cong \mathbb{Z}[1/4][a,\Delta^{-1}][u^{\pm 1}]$$

where $|u| = 1$, and denote by S its subring of elements in degree 0 so that

$$S \cong \mathbb{Z}[1/4][c,\delta^{-1}] \tag{3}$$

where $\delta = u^{-12}\Delta = c^2(c^2-16)$. Write

$$\widehat{S} = \mathbb{Z}_9[\![h]\!]$$

where

$$h := u^{-2}H = c^2 + 1. \tag{4}$$

Let i be an element generating $\mathbb{Z}_9$ over $\mathbb{Z}_3$ with $i^2 = -1$. We may choose

$$c \equiv i \mod (3, h)$$

and we have

$$\delta \equiv -1 \mod (3, h)$$

where $(3, h)$ is the maximal ideal of the complete local ring $\widehat{S}$. Then by Hensel's lemma, both c and δ lie in $\widehat{S}$, and both are invertible. Thus

$$\widehat{S} \cong S^{\wedge}_{(3,h)}.$$

Now C restricts to S as

$$y^2 + cxy + cy = x^3 + x^2. \tag{5}$$

Let $\widehat{C}$ be the formal completion of C over S at the identity. It is a formal group over $\widehat{S}$, and its reduction to $\mathbb{F}_9 = \widehat{S}/(3, h)$ is a formal group $\mathbb{G}$ of height 2 in view of (4) and (2). By the Serre–Tate theorem (cf. [KM85, 2.9.1]), 3-adically the deformation theory of an elliptic curve is equivalent to the deformation theory of its 3-divisible group, and thus $\widehat{C}$ is the universal deformation of $\mathbb{G}$ in view of Proposition 3. Let E be the E_∞-ring spectrum which represents the Morava E-theory associated to $\mathbb{G}$ (cf. [GH04, Corollary 7.6]). Then

$$E_* \cong \mathbb{Z}_9[\![h]\!][u^{\pm 1}]$$

where u is in topological degree 2, and it corresponds to a local uniformizer at the identity of C.

2.2 Points of exact order 3

To study C in a formal neighborhood of the identity, it is convenient to make a change of variables. Let

$$u = \frac{x}{y} \quad \text{and} \quad v = \frac{1}{y}, \qquad \text{so} \qquad x = \frac{u}{v} \quad \text{and} \quad y = \frac{1}{v}.$$

The identity of C is then $(u, v) = (0, 0)$, with u a local uniformizer. The equation (1) of C becomes

$$v + auv + abv^2 = u^3 + bu^2v. \tag{6}$$

Proposition 4 *On the elliptic curve C over $S^\bullet$, the uv-coordinates (d,e) of any nonzero 3-torsion point satisfy the identities*

$$f(d) = 0 \tag{7}$$

and

$$e = g(d) \tag{8}$$

where $f, g \in S^\bullet[u]$ are given by

$$\begin{aligned} f(u) = {} & b^4u^8 + 3ab^3u^7 + 3a^2b^2u^6 + (a^3b + 7ab^2)u^5 + (6a^2b - 6b^2)u^4 + 9abu^3 \\ & + (-a^2 + 8b)u^2 - 3au - 3, \\ g(u) = {} & -\frac{1}{a(a^2-16b)}\big(ab^3u^7 + (3a^2b^2 - 2b^3)u^6 + (3a^3b - 6ab^2)u^5 + (a^4 + a^2b \\ & + 2b^2)u^4 + (4a^3 - 15ab)u^3 + 18bu^2 - 12au - 18\big). \end{aligned}$$

Proof [1] Given the elliptic curve C with equation (1), a nonzero point Q is 3-torsion if and only if the polynomial

$$\psi_3(x) := 3x^4 + (a^2 + 4b)x^3 + 3a^2bx^2 + 3a^2b^2x + a^2b^3$$

vanishes at Q (cf. [Sil09, Exercise 3.7f]). Substituting $x = u/v$ and clearing the denominators, we get a homogeneous polynomial

$$\widetilde{\psi}_3(u,v) := 3u^4 + (a^2 + 4b)u^3v + 3a^2bu^2v^2 + 3a^2b^2uv^3 + a^2b^3v^4.$$

As $Q = (d,e)$ in uv-coordinates, we then have

$$\widetilde{\psi}_3(d,e) = 0. \tag{9}$$

To get the polynomial f, we take v as variable and rewrite (6) as a quadratic equation

$$abv^2 + (-bu^2 + au + 1)v - u^3 = 0 \tag{10}$$

where the leading coefficient ab is invertible in $S^\bullet = \mathbb{Z}[1/4][a,b,\Delta^{-1}]$ as $\Delta = a^2b^4(a^2 - 16b)$. Define

$$\widetilde{f}(u) := \widetilde{\psi}_3(u,v)\widetilde{\psi}_3(u,\bar{v}) \tag{11}$$

where v and $\bar{v}$ are formally the conjugate roots of (10) so that we compute $\widetilde{f}$ in terms of u by substituting

$$v + \bar{v} = \frac{bu^2 - au - 1}{ab} \qquad \text{and} \qquad v\bar{v} = -\frac{u^3}{ab}.$$

[1] See Appendix A for formulas for the polynomials $\widetilde{f}$, Q_1, R_1, Q_2, R_2, K, L, M, and N that appear in the proof.

We then factor $\widetilde{f}$ over $S^\bullet$ as

$$\widetilde{f}(u) = -\frac{u^4 f(u)}{a^2 b} \tag{12}$$

with f the stated degree-8 polynomial. We check that f is irreducible by applying Eisenstein's criterion to the maximal ideal $(3, H)$ of $S^\bullet$.

We have $\widetilde{f}(d) = 0$ by (11) and (9). To see $f(d) = 0$, consider the closed subscheme $C[3]^\times \subset C$ of points of exact order 3. By [KM85, 2.3.1] it is finite locally free of rank 8 over S. By the Cayley–Hamilton theorem, as a global section of $C[3]^\times$, u locally satisfies a monic degree-8 equation, and this equation then locally defines the rank-8 scheme $C[3]^\times$. Since $C[3]^\times$ does not contain the identity, it is affine, and is thus globally defined by a monic degree-8 equation in u. In view of $\widetilde{f}(d) = 0$ and (12), we then determine this equation, and (up to a unit in $S^\bullet$) get the first stated identity (7).

To get the polynomial g, we note that both the quartic polynomial

$$A(v) := \widetilde{\psi}_3(d, v)$$

and the quadratic polynomial

$$B(v) := abv^2 + (-bd^2 + ad + 1)v - d^3$$

vanish at e, and thus so does their greatest common divisor (gcd). Applying the Euclidean algorithm (cf. Appendix A for explicit expressions), we have

$$\begin{aligned} A(v) &= Q_1(v)B(v) + R_1(v), \\ B(v) &= Q_2(v)R_1(v) + R_2, \end{aligned}$$

where

$$R_1(v) = K(d)v + L(d)$$

for some polynomials K and L, and $R_2 = 0$ in view of (7). Thus $R_1(v)$ is the gcd of $A(v)$ and $B(v)$, and hence

$$K(d)e + L(d) = R_1(e) = 0.$$

To write e in terms of d from the above identity, we apply the Euclidean algorithm to f and K. Their gcd turns out to be 1, and thus there are polynomials M and N with

$$M(u)f(u) + N(u)K(u) = 1.$$

By (7) we then have $N(d)K(d) = 1$, and thus

$$e = -N(d)L(d) = g(d)$$

where g is as stated. □

Remark 5 We have

$$f(u) \equiv u^2(b^4u^6 + abHu^3 - H) \mod 3.$$

The two roots (counted with multiplicity) of $f(u)$ which reduce to zero modulo 3 correspond to the two nonzero points in the unique order-3 subgroup of C in a formal neighborhood of the identity.

2.3 A universal isogeny and a total power operation

Proposition 6

(i) *The universal degree-3 isogeny ψ with source C is defined over the graded ring*

$$S_3^\bullet := S^\bullet[\kappa]/\big(W(\kappa)\big)$$

where $|\kappa| = -2$ and

$$W(\kappa) = \kappa^4 - \frac{6}{b^2}\,\kappa^2 + \frac{a^2 - 8b}{b^4}\,\kappa - \frac{3}{b^4}, \tag{13}$$

and has target the elliptic curve

$$C'\colon\ v + a'uv + a'b'v^2 = u^3 + b'u^2v$$

where

$$\begin{aligned} a' &= \frac{1}{a}\big((a^2b^4 - 4b^5)\kappa^3 + 4b^4\kappa^2 + (-6a^2b^2 + 20b^3)\kappa + a^4 - 12a^2b + 12b^2\big),\\ b' &= b^3. \end{aligned}$$

(ii) *The kernel of ψ is generated by a point Q of exact order 3 with coordinates (d, e) satisfying*

$$\begin{aligned} \kappa &= -\frac{1}{a^2 - 16b}\big(ab^3d^7 + (3a^2b^2 - 2b^3)d^6 + (3a^3b - 6ab^2)d^5 + (a^4\\ &\qquad + a^2b + 2b^2)d^4 + (4a^3 - 15ab)d^3 + (a^2 + 2b)d^2 - 12ad - 18\big)\\ &= ae - d^2. \end{aligned} \tag{14}$$

(iii) *The restriction of ψ to the supersingular locus at the prime 3 is the 3-power Frobenius endomorphism.*

(iv) *The induced map ψ^* on the relative cotangent space of C' at the identity sends du to κdu.*

Proof [2] Let $P=(u,v)$ be a general point on C, and $Q=(d,e)$ be a nonzero 3-torsion point. Rewriting (6) as
$$v=u^3+bu^2v-auv-abv^2,$$
we express v as a power series in u by substituting this equation into itself recursively. For the purpose of our calculations, we take this power series up to u^{12} as an expression for v, and write $e=g(d)$ as in (8).

Define functions u' and v' by

$$\begin{aligned} u' &:= u(P)\cdot u(P-Q)\cdot u(P+Q),\\ v' &:= v(P)\cdot v(P-Q)\cdot v(P+Q), \end{aligned} \tag{15}$$

where $u(-)$ and $v(-)$ denote the u-coordinate and v-coordinate of a point respectively. By computing the group law on C, we express u' and v' as power series in u:

$$\begin{aligned} u' &= \kappa u + (\text{higher-degree terms}),\\ v' &= \lambda u^3 + (\text{higher-degree terms}), \end{aligned} \tag{16}$$

where the coefficients (κ, λ, etc.) involve a, b, and d. In particular, in view of (7), we compute that κ satisfies $W(\kappa)=0$ with $|\kappa|=-2$ as stated in (i).

Now define the isogeny $\psi\colon\ C\to C'$ by

$$u\big(\psi(P)\big):=u' \qquad \text{and} \qquad v\big(\psi(P)\big):=\frac{\kappa^3}{\lambda}\cdot v' \tag{17}$$

where we introduce the factor κ^3/λ so that the equation of C' will be in the Weierstrass form. Using (16) (cf. Appendix B for explicit expressions), we then determine the coefficients in a general Weierstrass equation and get the stated equation of C'.

We next check the statement of (ii). In view of (17) and (15), the kernel of ψ is the order-3 subgroup generated by Q. In (14), the first identity is computed in (16); we then compare it with the formula for g in Proposition 4 and get the second identity.

For (iii), recall from Section 2.1 that the supersingular locus at the prime 3 is $\operatorname{Spec}\mathbb{F}_3$. Over $\mathbb{F}_3$, since $C[3]=0$ by [Sil09, V.3.1a], Q coincides with the identity, and thus
$$u\big(\psi(P)\big)=u(P)\cdot u(P-Q)\cdot u(P+Q)=\big(u(P)\big)^3.$$
As the u-coordinate is a local uniformizer at the identity, ψ then restricts to $\mathbb{F}_3$ as the 3-power Frobenius endomorphism.

The statement of (iv) follows by definition of κ in (16). □

[2] See Appendix B for the power series expansion of v and details of the calculations involving the group law on C that appear in the proof.

Remark 7 In view of Proposition 6 (iii), the formal completion of $\psi\colon\ C \to C'$ at the identity of C is a *deformation of Frobenius* in the sense of [Rez09, 11.3]. When it is clear from the context, we will simply call ψ itself a deformation of Frobenius.

Remark 8 The analog of κ at the prime 2 coincides with d as studied in [Rezb, Section 3]. It is the u-coordinate of a nonzero 2-torsion point on (the restriction to an affine coordinate chart of) the universal elliptic curve in [MR09, Proposition 3.2].

Recall from Section 2.1 that

$$E^0 \cong \mathbb{Z}_9[\![h]\!] = \widehat{S} \cong S^{\wedge}_{(3,h)}$$

in which c and i are elements with $c^2+1=h$ and $i^2=-1$. Given the graded ring $S_3^\bullet$ in Proposition 6 (i), define

$$S_3 := S[\alpha]/\big(w(\alpha)\big) \tag{18}$$

where

$$w(\alpha) = \alpha^4 - 6\alpha^2 + (c^2-8)\alpha - 3 \tag{19}$$

(cf. the definition of S from $S^\bullet$ in (3)). By [Str98, Theorem 1.1] we have

$$E^0B\Sigma_3/I \cong \big(S_3\big)^{\wedge}_{(3,h)}$$

where

$$I := \bigoplus_{0<i<3} \operatorname{image}\big(E^0B(\Sigma_i \times \Sigma_{3-i}) \xrightarrow{\text{transfer}} E^0B\Sigma_3\big) \tag{20}$$

is the *transfer ideal*. In view of this and the construction of *total power operations* for Morava E-theories in [Rez09, 3.23], we have the following corollary.

Corollary 9 *The total power operation*

$$\psi^3\colon\ E^0 \to E^0B\Sigma_3/I \cong E^0[\alpha]/\big(w(\alpha)\big)$$

is given by

$$\begin{aligned}
\psi^3(h) &= h^3 + (\alpha^3 - 6\alpha - 27)h^2 + 3(-6\alpha^3 + \alpha^2 + 36\alpha + 67)h \\
&\qquad + 57\alpha^3 - 27\alpha^2 - 334\alpha - 342,\\
\psi^3(c) &= c^3 + (\alpha^3 - 6\alpha - 12)c - 4(\alpha+1)^2(\alpha-3)c^{-1},\\
\psi^3(i) &= -\,i,
\end{aligned}$$

where

$$\alpha \equiv 0 \mod 3. \tag{21}$$

Proof By Proposition 6 (i), in xy-coordinates, C' restricts to S_3 as

$$y^2 + c'xy + c'y = x^3 + x^2$$

where

$$c' = \frac{1}{c}\big((c^2-4)\alpha^3 + 4\alpha^2 + (-6c^2+20)\alpha + c^4 - 12c^2 + 12\big).$$

By [Rez09, Theorem B], since the above equation is in the form of (5), there is a correspondence between the restriction to S_3 of the universal isogeny ψ, which is a deformation of Frobenius, and the total power operation ψ^3. In particular $\psi^3(c)$ is given by c'. As ψ^3 is a ring homomorphism, we then get the formula for $\psi^3(h) = \psi^3(c^2+1)$. We also have

$$\big(\psi^3(i)\big)^2 = \psi^3(-1) = -1,$$

and thus $\psi^3(i) = i$ or $-i$. We exclude the former possibility in view of the congruence

$$\psi^3(i) \equiv i^3 \mod 3$$

by [Rez09, Propositions 3.25 and 10.5].

The congruence (21) follows from Remark 5 and (14). □

3 Individual power operations

3.1 A composite of deformations of Frobenius

Recall from Proposition 6 that over $S_3^\bullet$ we have the universal degree-3 isogeny $\psi\colon\ C \to C' = C/G$ where G is an order-3 subgroup of C; in particular, ψ is a deformation of the 3-power Frobenius endomorphism over the supersingular locus. We want to construct a similar isogeny ψ' with source C' so that the composite $\psi' \circ \psi$ will correspond to a composite of total power operations via [Rez09, Theorem B].

Let $G' := C[3]/G$ which is an order-3 subgroup of C'. If G is the unique order-3 subgroup of C in a formal neighborhood of the identity, G' is then the unique subgroup of C' with the same property, as any formal group of height 1 has a unique order-3 subgroup given by the kernel of the multiplication-by-3 map. We define $\psi'\colon\ C' \to C'/G'$ using a nonzero point in G' as in (15) and (17). As in the proof of Proposition 6 (iii), we see that ψ' is a deformation of Frobenius.

Proposition 10 *The following diagram of elliptic curves over $S_3^\bullet$ commutes:*

$$
\begin{tikzcd}
C \arrow[r, "\psi"] \arrow[dr, "{[-3]}"'] & C/G = C' \arrow[d, "\psi'"] \\
& C/C[3] \cong \frac{C/G}{C[3]/G} = \frac{C'}{G'} .
\end{tikzcd}
\tag{22}
$$

Proof By [KM85, 2.4.2], since Proj $S_3^\bullet$ is connected, we need only show that the locus over which $\psi' \circ \psi = [-3]$ is not empty, where by abuse of notation $[-3]$ denotes the map $[-3]$ on C composed with the canonical isomorphism from $C/C[3]$ to C'/G'.

Recall from Section 2.1 that C restricts to the supersingular locus $\mathbb{F}_3$ as

$$C_0\colon\ y^2 + xy - y = x^3 - x^2.$$

By Proposition 6 (iii) both ψ and ψ' restrict as the 3-power Frobenius endomorphism ψ_0. By [KM85, 2.6.3], in the endomorphism ring of C_0, ψ_0 is a root of the polynomial

$$X^2 - \mathrm{trace}(\psi_0) \cdot X + 3 \tag{23}$$

with $\mathrm{trace}(\psi_0)$ an integer satisfying

$$\big(\mathrm{trace}(\psi_0)\big)^2 \leq 4 \cdot 3.$$

Moreover by [Sil09, Exercise 5.10a], since C_0 is supersingular, we have

$$\mathrm{trace}(\psi_0) \equiv 0 \mod 3.$$

Thus $\mathrm{trace}(\psi_0) = 0$, 3, or -3. We exclude the latter two possibilities by checking the action of ψ_0 at the 2-torsion point $(1,0)$. It then follows from (23) that $\psi_0 \circ \psi_0$ agrees with $[-3]$ on C_0 over $\mathbb{F}_3$. □

Analogous to Proposition 6 (iv), let κ' be the element in $S_3^\bullet$ such that $(\psi')^*$ sends du to $\kappa' du$. Note that $|\kappa'| = -6$.

Corollary 11 *The following relations hold in $S_3^\bullet$:*

$$b^4 \kappa\kappa' + 3 = 0$$

and

$$\kappa' = -\kappa^3 + \frac{6}{b^2}\,\kappa - \frac{a^2 - 8b}{b^4}.$$

Proof The isogenies in (22) induce maps on relative cotangent spaces at the identity. By Proposition 6 (iv) we then have a commutative diagram

$$\begin{tikzcd} \kappa\kappa' du & & \kappa' du \arrow[ll, mapsto, "\psi^*"'] \\ & du \arrow[ul, mapsto, "{[-3]^*}"] \arrow[r, equal] & du\,. \arrow[u, mapsto, "(\psi')^*"'] \end{tikzcd}$$

Thus for the first stated relation we need only show that $[3]^*$ sends du to $3du/b^4$.

For $i = 1, 2, 3$, and 4, let Q_i be a generator for each of the four order-3 subgroups of C. Each Q_i can be chosen as Q in (15), and we denote the corresponding quantity κ in (16) by κ_i. Since $[3]$ has the same kernel as the isogeny Ψ defined by

$$u\big(\Psi(P)\big) := u(P) \prod_{i=1}^{4} \big(u(P - Q_i) \cdot u(P + Q_i)\big),$$
$$v\big(\Psi(P)\big) := v(P) \prod_{i=1}^{4} \big(v(P - Q_i) \cdot v(P + Q_i)\big),$$

we have

$$[3]^*(du) = s \cdot \kappa_1\kappa_2\kappa_3\kappa_4 \cdot du \tag{24}$$

where s is a degree-0 unit in $S^\bullet$ coming from an automorphism of C over $S^\bullet$. In view of (13) we have

$$\kappa_1\kappa_2\kappa_3\kappa_4 = -\frac{3}{b^4}.$$

We compute that $s = -1$ by comparing the restrictions of the two sides of (24) to S (cf. (3)): $[3]^*$ becomes the multiplication-by-3 map, and $-3/b^4$ becomes -3 (cf. (19)). Thus $[3]^*$ sends du to $3du/b^4$.

The second stated relation follows by a computation from the first relation and $W(\kappa) = 0$ as in Proposition 6 (i). □

Remark 12 As noted in Remark 8, the (local) analog of κ at the prime 2 coincides with the parameter d in [Rezb, Section 3]. In particular, with the notations there and the equation in [MR09, Proposition 3.2], d and d' satisfy an analogous relation $bdd' + 2 = 0$ which locally reduces to $dd' + 2 = 0$ (the analog of the factor s in the proof of Corollary 11 equals 1; cf. [And95, Theorem 2.5.7]). These arise as examples of the following fact: for any prime p, given a supersingular elliptic curve E over $\overline{\mathbb{F}}_p$, there exists an elliptic curve E' over $\mathbb{F}_{p^2}$ such that it is isomorphic to E over $\overline{\mathbb{F}}_p$ and the p^2-power Frobenius endomorphism of E' equals $[-p]$ ([BGJGP05, Lemma 3.21]).

Remark 13 In view of (22), $-\psi'$ (composed with the canonical isomorphism on the target) turns out to be the dual isogeny of ψ (cf. the proof of [KM85, 2.9.4]). If G is the unique order-3 subgroup of C in a formal neighborhood of the identity, then $\kappa \equiv 0 \mod 3$ by Remark 5 and (14). Thus in view of Corollary 11 we have

$$-\kappa' = \kappa^3 - \frac{6}{b^2}\kappa + \frac{a^2 - 8b}{b^4} \equiv \frac{H}{b^4} \mod 3.$$

Locally this congruence agrees with the interpretation of H as defined by the tangent map of the Verschiebung isogeny over $\mathbb{F}_3$ (cf. [KM85, 12.4.1]).

3.2 Individual power operations

Let A be a $K(2)$-local commutative E-algebra. By [Rez09, 3.23] and Corollary 9, we have a total power operation

$$\psi^3\colon\ A_0 \to A_0 \otimes_{E_0} (E^0 B\Sigma_3/I) \cong A_0[\alpha]/\big(w(\alpha)\big).$$

We also have a composite of total power operations

$$\begin{aligned} A_0 \xrightarrow{\psi^3} A_0 \otimes_{E_0} (E^0 B\Sigma_3/I) &\xrightarrow{\psi^3} \big(A_0 \otimes_{E_0} (E^0 B\Sigma_3/I)\big) \ {}^{\psi^3}\!\otimes_{E_0[\alpha]} (E^0 B\Sigma_3/I) \\ &\cong \Big(A_0[\alpha]/\big(w(\alpha)\big)\Big) \ {}^{\psi^3}\!\otimes_{E_0[\alpha]} \Big(E^0[\alpha]/\big(w(\alpha)\big)\Big) \end{aligned} \tag{25}$$

where the elements in the target $M \ {}^{\psi^3}\!\otimes_R N$ are subject to the equivalence relation (as well as other ones in a usual tensor product)

$$m \otimes (r \cdot n) \sim \big(m \cdot \psi^3(r)\big) \otimes n$$

for $m \in M$, $n \in N$, and $r \in R$ with

$$\psi^3(\alpha) = -\alpha^3 + 6\alpha - h + 9$$

by Corollary 11.

Definition 14 Define the *individual power operations*

$$Q_k\colon\ A_0 \to A_0$$

for $k = 0, 1, 2$, and 3 by

$$\psi^3(x) = Q_0(x) + Q_1(x)\alpha + Q_2(x)\alpha^2 + Q_3(x)\alpha^3. \tag{26}$$

Proposition 15 *The following relations hold among the individual power operations Q_0, Q_1, Q_2, and Q_3:*

(i) $Q_0(1) = 1, \quad Q_1(1) = Q_2(1) = Q_3(1) = 0$;

(ii) $Q_k(x+y) = Q_k(x) + Q_k(y)$ *for all* k;

(iii) Commutation relations

$$\begin{aligned}
Q_0(hx) &= (h^3 - 27h^2 + 201h - 342)Q_0(x) + (3h^2 - 54h + 171)Q_1(x) \\
&\quad + (9h - 81)Q_2(x) + 24Q_3(x), \\
Q_1(hx) &= (-6h^2 + 108h - 334)Q_0(x) + (-18h + 171)Q_1(x) + (-72)Q_2(x) \\
&\quad + (h - 9)Q_3(x), \\
Q_2(hx) &= (3h - 27)Q_0(x) + 8Q_1(x) + 9Q_2(x) + (-24)Q_3(x), \\
Q_3(hx) &= (h^2 - 18h + 57)Q_0(x) + (3h - 27)Q_1(x) + 8Q_2(x) + 9Q_3(x), \\
Q_0(cx) &= (c^3 - 12c + 12c^{-1})Q_0(x) + (3c - 12c^{-1})Q_1(x) + (12c^{-1})Q_2(x) \\
&\quad + (-12c^{-1})Q_3(x), \\
Q_1(cx) &= (-6c + 20c^{-1})Q_0(x) + (-20c^{-1})Q_1(x) + (-c + 20c^{-1})Q_2(x) \\
&\quad + (4c - 20c^{-1})Q_3(x), \\
Q_2(cx) &= (4c^{-1})Q_0(x) + (-4c^{-1})Q_1(x) + (4c^{-1})Q_2(x) + (-c - 4c^{-1})Q_3(x), \\
Q_3(cx) &= (c - 4c^{-1})Q_0(x) + (4c^{-1})Q_1(x) + (-4c^{-1})Q_2(x) + (4c^{-1})Q_3(x),
\end{aligned}$$

$Q_k(ix) = (-i)Q_k(x)$ *for all* k;

(iv) Adem relations

$$\begin{aligned}
Q_1Q_0(x) &= (-6)Q_0Q_1(x) + 3Q_2Q_1(x) + (6h - 54)Q_0Q_2(x) + 18Q_1Q_2(x) \\
&\quad + (-9)Q_3Q_2(x) + (-6h^2 + 108h - 369)Q_0Q_3(x) \\
&\quad + (-18h + 162)Q_1Q_3(x) + (-54)Q_2Q_3(x), \\
Q_2Q_0(x) &= 3Q_3Q_1(x) + (-3)Q_0Q_2(x) + (3h - 27)Q_0Q_3(x) + 9Q_1Q_3(x), \\
Q_3Q_0(x) &= Q_0Q_1(x) + (-h + 9)Q_0Q_2(x) + (-3)Q_1Q_2(x) \\
&\quad + (h^2 - 18h + 63)Q_0Q_3(x) + (3h - 27)Q_1Q_3(x) + 9Q_2Q_3(x);
\end{aligned}$$

(v) Cartan formulas

$$\begin{aligned}
Q_0(xy) &= Q_0(x)Q_0(y) + 3\big(Q_3(x)Q_1(y) + Q_2(x)Q_2(y) + Q_1(x)Q_3(y)\big) \\
&\quad + 18Q_3(x)Q_3(y), \\
Q_1(xy) &= \big(Q_1(x)Q_0(y) + Q_0(x)Q_1(y)\big) \\
&\quad + (-h + 9)\big(Q_3(x)Q_1(y) + Q_2(x)Q_2(y) + Q_1(x)Q_3(y)\big) \\
&\quad + 3\big(Q_3(x)Q_2(y) + Q_2(x)Q_3(y)\big) + (-6h + 54)Q_3(x)Q_3(y),
\end{aligned}$$

$$\begin{aligned}
Q_2(xy) &= \big(Q_2(x)Q_0(y) + Q_1(x)Q_1(y) + Q_0(x)Q_2(y)\big) \\
&\quad + 6\big(Q_3(x)Q_1(y) + Q_2(x)Q_2(y) + Q_1(x)Q_3(y)\big) \\
&\quad + (-h+9)\big(Q_3(x)Q_2(y) + Q_2(x)Q_3(y)\big) + 39Q_3(x)Q_3(y), \\
Q_3(xy) &= \big(Q_3(x)Q_0(y) + Q_2(x)Q_1(y) + Q_1(x)Q_2(y) + Q_0(x)Q_3(y)\big) \\
&\quad + 6\big(Q_3(x)Q_2(y) + Q_2(x)Q_3(y)\big) + (-h+9)Q_3(x)Q_3(y);
\end{aligned}$$

(vi) Frobenius congruence

$$Q_0(x) \equiv x^3 \mod 3.$$

Proof The relations in (i), (ii), (iii), and (v) follow computationally from the fact that ψ^3 is a ring homomorphism together with the formulas in Corollary 9.

For (iv), there is a canonical isomorphism $C/C[3] \cong C$ of elliptic curves. Given the correspondence between deformations of Frobenius and power operations in [Rez09, Theorem B], the commutativity of (22) then implies that the composite (25) lands in A_0. In terms of formulas, we have

$$\begin{aligned}
\psi^3\big(\psi^3(x)\big) &= \psi^3\big(Q_0(x) + Q_1(x)\alpha + Q_2(x)\alpha^2 + Q_3(x)\alpha^3\big) \\
&= \sum_{k=0}^{3} \psi^3\big(Q_k(x)\big)\big(\psi^3(\alpha)\big)^k \\
&= \sum_{k=0}^{3}\sum_{j=0}^{3} Q_jQ_k(x)\alpha^j(-\alpha^3 + 6\alpha - h + 9)^k \\
&\equiv \Psi_0(x) + \Psi_1(x)\alpha + \Psi_2(x)\alpha^2 + \Psi_3(x)\alpha^3 \mod \big(w(\alpha)\big)
\end{aligned}$$

where each Ψ_i is an E_0-linear combination of the Q_jQ_k's. The vanishing of $\Psi_1(x)$, $\Psi_2(x)$, and $\Psi_3(x)$ gives the three relations in (iv).

For (vi), by [Rez09, Propositions 3.25 and 10.5] we have

$$\psi^3(x) \equiv x^3 \mod 3.$$

In view of (21), the congruence in (vi) then follows from (26). □

Example 16 We have $E^0S^2 \cong \mathbb{Z}_9[\![h]\!][u]/(u^2)$. By definition of κ in (16), the Q_k's act canonically on $u \in E^0S^2$:

$$Q_k(u) = \begin{cases} u, & \text{if } k = 1, \\ 0, & \text{if } k \neq 1. \end{cases}$$

We then get the values of the Q_k's on elements in E^0S^2 from Proposition 15 (i)–(iii).

3.3 The Dyer–Lashof algebra

Definition 17

(i) Let i be an element generating $\mathbb{Z}_9$ over $\mathbb{Z}_3$ with $i^2 = -1$. Define γ to be the associative ring generated over $\mathbb{Z}_9[\![h]\!]$ by elements q_0, q_1, q_2, and q_3 subject to the following relations: the q_k's commute with elements in $\mathbb{Z}_3 \subset \mathbb{Z}_9[\![h]\!]$, and satisfy *commutation relations*

$$\begin{aligned} q_0 h &= (h^3 - 27h^2 + 201h - 342)q_0 + (3h^2 - 54h + 171)q_1 + (9h - 81)q_2 \\ &\quad + 24q_3, \\ q_1 h &= (-6h^2 + 108h - 334)q_0 + (-18h + 171)q_1 + (-72)q_2 + (h - 9)q_3, \\ q_2 h &= (3h - 27)q_0 + 8q_1 + 9q_2 + (-24)q_3, \\ q_3 h &= (h^2 - 18h + 57)q_0 + (3h - 27)q_1 + 8q_2 + 9q_3, \\ q_k i &= (-i)q_k \text{ for all } k, \end{aligned}$$

and *Adem relations*

$$\begin{aligned} q_1 q_0 &= (-6)q_0 q_1 + 3q_2 q_1 + (6h - 54)q_0 q_2 + 18q_1 q_2 + (-9)q_3 q_2 \\ &\quad + (-6h^2 + 108h - 369)q_0 q_3 + (-18h + 162)q_1 q_3 + (-54)q_2 q_3, \\ q_2 q_0 &= 3q_3 q_1 + (-3)q_0 q_2 + (3h - 27)q_0 q_3 + 9q_1 q_3, \\ q_3 q_0 &= q_0 q_1 + (-h + 9)q_0 q_2 + (-3)q_1 q_2 + (h^2 - 18h + 63)q_0 q_3 \\ &\quad + (3h - 27)q_1 q_3 + 9q_2 q_3. \end{aligned}$$

(ii) Write $\omega := \pi_2 E$ which is the kernel of $E^0 S^2 \to E^0$ with $E^0 S^2 \cong \mathbb{Z}_9[\![h]\!][u]/(u^2)$. Define ω as a γ-module in the sense of [Rezb, 2.2] with one generator u by

$$q_k \cdot u = \begin{cases} u, & \text{if } k = 1, \\ 0, & \text{if } k \neq 1. \end{cases}$$

Remark 18 In Definition 17 (i), an element $r \in \mathbb{Z}_9[\![h]\!] \cong E_0$ corresponds to the multiplication-by-r operation (cf. [Rez09, Proposition 6.4]), and each q_k corresponds to the individual power operation Q_k (also compare Definition 17 (ii) and Example 16). Under this correspondence, the relations in Proposition 15 (ii)–(v) describe explicitly the structure of γ as that of a *graded twisted bialgebra over* E_0 in the sense of [Rez09, Section 5]. The grading of γ comes from the number of the q_k's in a monomial: for example, commutation relations are in degree 1, and Adem relations are in degree 2. Under these relations, γ has an *admissible basis*: it is free as a left E_0-module on the elements of the form

$$q_0^m q_{k_1} \cdots q_{k_n}$$

where $m, n \geq 0$ ($n = 0$ gives q_0^m), and $k_i = 1$, 2, or 3. If we write $\gamma[d]$ for the degree-d part of γ, then $\gamma[d]$ is of rank $1 + 3 + \cdots + 3^d$.

We now identify γ with the Dyer–Lashof algebra of power operations on $K(2)$-local commutative E-algebras.

Theorem 19 *Let A be a $K(2)$-local commutative E-algebra. Let γ be the graded twisted bialgebra over E_0, and ω be the γ-module in Definition 17. Then A_* is an* ω-twisted $\mathbb{Z}/2$-graded amplified γ-ring *in the sense of [Rez09, Section 2] and [Rezb, 2.5 and 2.6]. In particular,*

$$\pi_* L_{K(2)} \mathbb{P}_E(\Sigma^d E) \cong \big(F_d\big)^{\wedge}_{(3,h)}$$

where F_d is the free ω-twisted $\mathbb{Z}/2$-graded amplified γ-ring with one generator in degree d.

Formulas for γ aside, this result is essentially due to Rezk [Rez09, Rezb].

Proof Let Γ be the graded twisted bialgebra of power operations on E_0 in [Rez09, Section 6]. We need only identify Γ with γ.

There is a direct sum decomposition $\Gamma = \bigoplus_{d \geq 0} \Gamma[d]$ where the summands come from the completed E-homology of $B\Sigma_{3^d}$ (cf. [Rez09, 6.2]). As in Remark 18, we have a degree-preserving ring homomorphism

$$\phi\colon\ \gamma \to \Gamma, \qquad q_k \mapsto Q_k$$

which is an isomorphism in degrees 0 and 1. We need to show that ϕ is both surjective and injective in all degrees.

For the surjectivity of ϕ, we use a transfer argument. We have

$$\nu_3(|\Sigma_3^{\wr d}|) = \nu_3(|\Sigma_{3^d}|) = (3^d - 1)/2$$

where $\nu_3(-)$ is the 3-adic valuation, and $(-)^{\wr d}$ is the d-fold wreath product. Thus following the proof of [Rez09, Proposition 3.17], we see that Γ is generated in degree 1, and hence ϕ is surjective.

By Remark 18 and (the E_0-linear dual of) [Str98, Theorem 1.1], $\gamma[d]$ and $\Gamma[d]$ are of the same rank $1+3+\cdots+3^d$ as free modules over E_0. Hence ϕ is also injective. □

4 $K(1)$-local power operations

Let $F := L_{K(1)}E$ be the $K(1)$-localization of E. The relationship between the power operation on E^0 in Corollary 9 and $K(1)$-local power operations on F^0 (cf. [Hop, Section 3] and [BMMS86, Section IX.3]) is as follows:

$$\begin{tikzcd} E^0 \arrow[r, "\psi^3"] \arrow[d] & E^0B\Sigma_3/I \arrow[d] \\ F^0 \arrow[r, "\psi_F^3"] & F^0B\Sigma_3/J \cong F^0. \end{tikzcd}$$

Here ψ_F^3 is the $K(1)$-local power operation induced by ψ^3, and $J \cong F^0 \otimes_{E^0} I$ is the transfer ideal (cf. (20)). Recall from Proposition 6 (i), (18), and Corollary 9 that ψ^3 arises from the universal degree-3 isogeny which is parametrized by the ring $S_3^\bullet$ with

$$(S_3)^\wedge_{(3,h)} \cong E^0B\Sigma_3/I.$$

The vertical maps are induced by the $K(1)$-localization $E \to F$. In terms of homotopy groups, this is obtained by inverting the generator h and completing at the prime 3 (cf. [Hov97, Corollary 1.5.5]):

$$E_* = \mathbb{Z}_9[\![h]\!][u^{\pm 1}] \qquad \text{and} \qquad F_* = \mathbb{Z}_9[\![h]\!][h^{-1}]^\wedge_3[u^{\pm 1}]$$

with

$$F_0 = \mathbb{Z}_9(\!(h)\!)^\wedge_3 = \left\{ \sum_{n=-\infty}^{\infty} k_n h^n \;\middle|\; k_n \in \mathbb{Z}_9, \lim_{n \to -\infty} k_n = 0 \right\}.$$

The formal group $\widehat{C}$ over E^0 has a unique order-3 subgroup after being pulled back to F^0 (cf. Remark 5), and the map

$$E^0B\Sigma_3/I \to F^0B\Sigma_3/J \cong F^0$$

classifies this subgroup. Along the base change

$$E^0B\Sigma_3/I \to F^0 \otimes_{E^0} (E^0B\Sigma_3/I) \cong (F^0 \otimes_{E^0} E^0B\Sigma_3)/J \cong F^0B\Sigma_3/J,$$

the special fiber of the 3-divisible group of $\widehat{C}$ which consists solely of a formal component may split into formal and étale components. We want to take the formal component so as to keep track of the unique order-3 subgroup of the formal group over F^0. This subgroup gives rise to the $K(1)$-local power operation ψ_F^3.

Recall from (18) that $S_3 = S[\alpha]\big/\big(w(\alpha)\big)$. Since

$$w(\alpha) = \alpha^4 - 6\alpha^2 + (h-9)\alpha - 3 \equiv \alpha(\alpha^3 + h) \mod 3,$$

the equation $w(\alpha) = 0$ has a unique root $\alpha = 0$ in $\mathbb{F}_9(\!(h)\!)$ (cf. (21)). By Hensel's lemma this unique root lifts to a root in $\mathbb{Z}_9(\!(h)\!)_3^\wedge$; it corresponds to the unique order-3 subgroup of $\widehat{C}$ over F^0. Plugging this specific value of α into the formulas for ψ^3 in Corollary 9, we then get an endomorphism of the ring F^0. This endomorphism is the $K(1)$-local power operation ψ^3_F.

Explicitly, with h invertible in F^0, we solve for α from $w(\alpha) = 0$ by first writing

$$\alpha = (3 + 6\alpha^2 - \alpha^4)/(h-9) = (3 + 6\alpha^2 - \alpha^4)\sum_{n=1}^{\infty} 9^{n-1}h^{-n}$$

and then substituting this equation into itself recursively. We plug the power series expansion for α into $\psi^3(h)$ and get

$$\psi^3_F(h) = h^3 - 27h^2 + 183h - 180 + 186h^{-1} + 1674h^{-2} + (\text{lower-degree terms}).$$

Similarly, writing h as $c^2 + 1$ in $w(\alpha) = 0$, we solve for α in terms of c and get

$$\psi^3_F(c) = c^3 - 12c - 6c^{-1} - 84c^{-3} - 933c^{-5} - 10956c^{-7} + (\text{lower-degree terms}).$$

Appendices

Here we list long formulas whose appearance in the main body might affect readability. The calculations involve power series expansions and manipulations of long polynomials with large coefficients (division, factorization, and finding greatest common divisors). They are done using the software *Wolfram Mathematica 8*. The commands `Reduce` and `Solve` are used to extract relations out of given identities.

A Formulas in the proof of Proposition 4

$$\begin{aligned}
\widetilde{f}(u) = -\frac{u^4}{a^2b}\big(&b^4u^8 + 3ab^3u^7 + 3a^2b^2u^6 + (a^3b + 7ab^2)u^5 + (6a^2b - 6b^2)u^4 \\
&+ 9abu^3 + (-a^2 + 8b)u^2 - 3au - 3\big),
\end{aligned}$$

$$Q_1(v) = ab^2v^2 + (b^2d^2 + 2abd - b)v + \frac{b^2d^4}{a} + 2bd^3 + ad^2 - \frac{2bd^2}{a} - d + \frac{1}{a},$$

$$
\begin{aligned}
R_1(v) = {} & \Big(\frac{b^3d^6}{a} + 2b^2d^5 + abd^4 - \frac{3b^2d^4}{a} + 2bd^3 + \frac{3bd^2}{a} - \frac{1}{a}\Big)v + \frac{b^2d^7}{a} + 2bd^6 \\
& + ad^5 - \frac{2bd^5}{a} + 2d^4 + \frac{d^3}{a}, \\
Q_2(v) = {} & \frac{a}{(b^3d^6 + 2ab^2d^5 + a^2bd^4 - 3b^2d^4 + 2abd^3 + 3bd^2 - 1)^2}\big((ab^4d^6 + 2a^2b^3d^5 \\
& + a^3b^2d^4 - 3ab^3d^4 + 2a^2b^2d^3 + 3ab^2d^2 - ab)v - b^4d^8 - 2ab^3d^7 - a^2b^2d^6 \\
& + 4b^3d^6 - ab^2d^5 + a^2bd^4 - 6b^2d^4 + 4abd^3 + 4bd^2 - ad - 1\big), \\
R_2 = {} & -\frac{ad^4}{(b^3d^6 + 2ab^2d^5 + a^2bd^4 - 3b^2d^4 + 2abd^3 + 3bd^2 - 1)^2}(b^4d^8 + 3ab^3d^7 \\
& + 3a^2b^2d^6 + a^3bd^5 + 7ab^2d^5 + 6a^2bd^4 - 6b^2d^4 + 9abd^3 - a^2d^2 + 8bd^2 \\
& - 3ad - 3), \\
K(u) = {} & \frac{b^3u^6}{a} + 2b^2u^5 + \Big(ab - \frac{3b^2}{a}\Big)u^4 + 2bu^3 + \frac{3bu^2}{a} - \frac{1}{a}, \\
L(u) = {} & \frac{b^2u^7}{a} + 2bu^6 + \Big(a - \frac{2b}{a}\Big)u^5 + 2u^4 + \frac{u^3}{a}, \\
M(u) = {} & \frac{b}{a^2(a^2-16b)^2}\big((10a^3b^3 - 112ab^4)u^5 + (19a^4b^2 - 217a^2b^3 - 16b^4)u^4 \\
& + (8a^5b - 126a^3b^2 + 304ab^3)u^3 + (-a^6 + 34a^4b - 266a^2b^2 + 32b^3)u^2 \\
& + (28a^3b - 384ab^2)u - 4a^4 + 51a^2b - 16b^2\big), \\
N(u) = {} & -\frac{1}{a(a^2-16b)^2}\big((10a^3b^5 - 112ab^6)u^7 + (29a^4b^4 - 329a^2b^5 - 16b^6)u^6 \\
& + (27a^5b^3 - 313a^3b^4 - 48ab^5)u^5 + (7a^6b^2 - 15a^4b^3 - 837a^2b^4 - 16b^5)u^4 \\
& + (-a^7b + 66a^5b^2 - 714a^3b^3 + 528ab^4)u^3 + (-4a^6b + 137a^4b^2 \\
& - 1147a^2b^3 + 80b^4)u^2 + (-12a^5b + 237a^3b^2 - 1200ab^3)u + a^6 - 44a^4b \\
& + 409a^2b^2 - 48b^3\big).
\end{aligned}
$$

B Formulas in the proof of Proposition 6

The power series expansion of v in terms of u up to u^{12} is

$$
\begin{aligned}
v = {} & u^3 - au^4 + (a^2 + b)u^5 + (-a^3 - 3ab)u^6 + (a^4 + 6a^2b + b^2)u^7 + (-a^5 - 10a^3b \\
& - 6ab^2)u^8 + (a^6 + 15a^4b + 20a^2b^2 + b^3)u^9 + (-a^7 - 21a^5b - 50a^3b^2 \\
& - 10ab^3)u^{10} + (a^8 + 28a^6b + 105a^4b^2 + 50a^2b^3 + b^4)u^{11} + (-a^9 - 36a^7b \\
& - 196a^5b^2 - 175a^3b^3 - 15ab^4)u^{12}.
\end{aligned}
$$

The group law on C satisfies:

- given $P(u,v)$, the coordinates of $-P$ are
$$\left(-\frac{v}{u(u+bv)}, -\frac{v^2}{u^2(u+bv)}\right);$$
- given $P_1(u_1,v_1)$ and $P_2(u_2,v_2)$, the coordinates of $-(P_1+P_2)$ are
$$u_3 := ak - \frac{bm}{1+bk} - u_1 - u_2 \qquad \text{and} \qquad v_3 := ku_3 + m$$
where
$$k = \frac{v_1 - v_2}{u_1 - u_2} \qquad \text{and} \qquad m = \frac{u_1v_2 - u_2v_1}{u_1 - u_2}.$$

Given $P(u,v)$ and $Q(d,e)$, with the above notations and formulas,

- set
$$(u_1,v_1) = \left(-\frac{v}{u(u+bv)}, -\frac{v^2}{u^2(u+bv)}\right) \qquad \text{and} \qquad (u_2,v_2) = (d,e)$$
so that
$$P - Q = (u_3,v_3);$$
- set
$$(u_1,v_1) = (u,v) \qquad \text{and} \qquad (u_2,v_2) = (d,e)$$
so that
$$P + Q = \left(-\frac{v_3}{u_3(u_3+bv_3)}, -\frac{v_3^2}{u_3^2(u_3+bv_3)}\right).$$

Plugging the coordinates of $P-Q$ and $P+Q$ into (15), and in view of (7), we then have in (16)
$$\begin{aligned}\kappa = &-\frac{1}{a^2-16b}\big(ab^3d^7 + (3a^2b^2-2b^3)d^6 + (3a^3b-6ab^2)d^5 + (a^4+a^2b+2b^2)d^4 \\ &+ (4a^3-15ab)d^3 + (a^2+2b)d^2 - 12ad - 18\big),\\ \lambda = &-\frac{1}{a^2b^2(a^2-16b)}\big((a^3b^3-11ab^4)d^7 + (3a^4b^2-33a^2b^3-4b^4)d^6 + (3a^5b \\ &- 33a^3b^2 - 15ab^3)d^5 + (a^6-4a^4b-96a^2b^2-4b^3)d^4 + (6a^5-80a^3b \\ &+ 31ab^2)d^3 + (10a^4-153a^2b+20b^2)d^2 + (3a^3-117ab)d - 6a^2 - 12b\big),\end{aligned}$$
and we have in (17)
$$\begin{aligned}\frac{\kappa^3}{\lambda} = &-\frac{1}{a^2-16b}\big(3ab^4d^7 + (9a^2b^3-4b^4)d^6 + (9a^3b^2-13ab^3)d^5 + (3a^4b+6a^2b^2 \\ &+ 12b^3)d^4 + (11a^3b-15ab^2)d^3 + (-a^4+21a^2b-12b^2)d^2 + (-3a^3+9ab)d \\ &- 4a^2 + 4b\big).\end{aligned}$$

More extended power series expansions in u for u' (up to u^6) and v' (up to u^9) are needed in (16) to determine the coefficients in the equation of C':

$$\begin{aligned}
u' = &-\frac{1}{a^2-16b}\big((ab^3d^7+3a^2b^2d^6-2b^3d^6+3a^3bd^5-6ab^2d^5+a^4d^4+a^2bd^4\\
&+2b^2d^4+4a^3d^3-15abd^3+a^2d^2+2bd^2-12ad-18)u+(-a^2b^3d^7\\
&+12b^4d^7-3a^3b^2d^6+36ab^3d^6-3a^4bd^5+36a^2b^2d^5+4b^3d^5-a^5d^4\\
&+5a^3bd^4+94ab^2d^4-6a^4d^3+85a^2bd^3-76b^2d^3-9a^3d^2+136abd^2+60bd\\
&+6a)u^2+(a^3b^3d^7-17ab^4d^7+3a^4b^2d^6-50a^2b^3d^6-8b^4d^6+3a^5bd^5\\
&-48a^3b^2d^5-27ab^3d^5+a^6d^4-7a^4bd^4-150a^2b^2d^4-16b^3d^4+7a^5d^3\\
&-113a^3bd^3+9ab^2d^3+16a^4d^2-258a^2bd^2+56b^2d^2+15a^3d-237abd\\
&+2a^2-32b)u^3+(-a^4b^3d^7+16a^2b^4d^7+12b^5d^7-3a^5b^2d^6+46a^3b^3d^6\\
&+64ab^4d^6-3a^6bd^5+42a^4b^2d^5+121a^2b^3d^5+4b^4d^5-a^7d^4+3a^5bd^4\\
&+209a^3b^2d^4+122ab^3d^4-8a^6d^3+114a^4bd^3+248a^2b^2d^3-76b^3d^3\\
&-24a^5d^2+384a^3bd^2-4ab^2d^2-33a^4d+519a^2bd+60b^2d-18a^3\\
&+282ab)u^4+(a^5b^3d^7-9a^3b^4d^7-117ab^5d^7+3a^6b^2d^6-24a^4b^3d^6\\
&-396a^2b^4d^6-24b^5d^6+3a^7bd^5-18a^5b^2d^5-484a^3b^3d^5-111ab^4d^5+a^8d^4\\
&+7a^6bd^4-307a^4b^2d^4-1038a^2b^3d^4+9a^7d^3-73a^5bd^3-1181a^3b^2d^3\\
&+573ab^3d^3+33a^6d^2-451a^4bd^2-1236a^2b^2d^2+72b^3d^2+54a^5d\\
&-807a^3bd-873ab^2d+36a^4-570a^2b-48b^2)u^5+(-a^6b^3d^7-5a^4b^4d^7\\
&+337a^2b^5d^7+12b^6d^7-3a^7b^2d^6-19a^5b^3d^6+1064a^3b^4d^6+204ab^5d^6\\
&-3a^8bd^5-27a^6b^2d^5+1164a^4b^3d^5+638a^2b^4d^5+4b^5d^5-a^9d^4-24a^7bd^4\\
&+441a^5b^2d^4+3195a^3b^3d^4+182ab^4d^4-10a^8d^3-22a^6bd^3+2956a^4b^2d^3\\
&-645a^2b^3d^3-76b^4d^3-43a^7d^2+403a^5bd^2+4594a^3b^2d^2-544ab^3d^2\\
&-78a^6d+996a^4bd+4014a^2b^2d+60b^3d-57a^5+852a^3b+942ab^2)u^6\big),\\
v' = &-\frac{1}{a^2b^2(a^2-16b)}\big((a^3b^3d^7-11ab^4d^7+3a^4b^2d^6-33a^2b^3d^6-4b^4d^6\\
&+3a^5bd^5-33a^3b^2d^5-15ab^3d^5+a^6d^4-4a^4bd^4-96a^2b^2d^4-4b^3d^4\\
&+6a^5d^3-80a^3bd^3+31ab^2d^3+10a^4d^2-153a^2bd^2+20b^2d^2+3a^3d\\
&-117abd-6a^2-12b)u^3+(-2a^4b^3d^7+28a^2b^4d^7-6a^5b^2d^6+82a^3b^3d^6\\
&+28ab^4d^6-6a^6bd^5+78a^4b^2d^5+90a^2b^3d^5-2a^7d^4+8a^5bd^4+294a^3b^2d^4\\
&+20ab^3d^4-14a^6d^3+202a^4bd^3+72a^2b^2d^3-32a^5d^2+510a^3bd^2
\end{aligned}$$

$$
\begin{aligned}
&- 124ab^2d^2 - 30a^4d + 546a^2bd - 6a^3 + 204ab)u^4 + (3a^5b^3d^7 - 38a^3b^4d^7 \\
&- 107ab^5d^7 + 9a^6b^2d^6 - 108a^4b^3d^6 - 409a^2b^4d^6 - 4b^5d^6 + 9a^7bd^5 \\
&- 96a^5b^2d^5 - 590a^3b^3d^5 - 47ab^4d^5 + 3a^8d^4 + a^6bd^4 - 646a^4b^2d^4 \\
&- 912a^2b^3d^4 - 4b^4d^4 + 24a^7d^3 - 292a^5bd^3 - 1249a^3b^2d^3 + 639ab^3d^3 \\
&+ 70a^6d^2 - 1057a^4bd^2 - 849a^2b^2d^2 + 20b^3d^2 + 93a^5d - 1512a^3bd \\
&- 597ab^2d + 48a^4 - 870a^2b - 12b^2)u^5 + (-4a^6b^3d^7 + 24a^4b^4d^7 + 583a^2b^5d^7 \\
&- 12a^7b^2d^6 + 60a^5b^3d^6 + 1923a^3b^4d^6 + 156ab^5d^6 - 12a^8bd^5 + 36a^6b^2d^5 \\
&+ 2268a^4b^3d^5 + 639a^2b^4d^5 - 4a^9d^4 - 40a^7bd^4 + 1256a^5b^2d^4 + 5128a^3b^3d^4 \\
&+ 140ab^4d^4 - 36a^8d^3 + 229a^6bd^3 + 5409a^4b^2d^3 - 2227a^2b^3d^3 - 127a^7d^2 \\
&+ 1597a^5bd^2 + 6835a^3b^2d^2 - 748ab^3d^2 - 201a^6d + 2952a^4bd + 5277a^2b^2d \\
&- 129a^5 + 2130a^3b + 708ab^2)u^6 + (5a^7b^3d^7 + 35a^5b^4d^7 - 1754a^3b^5d^7 \\
&- 275ab^6d^7 + 15a^8b^2d^6 + 125a^6b^3d^6 - 5511a^4b^4d^6 - 1833a^2b^5d^6 - 4b^6d^6 \\
&+ 15a^9bd^5 + 165a^7b^2d^5 - 5988a^5b^3d^5 - 4312a^3b^4d^5 - 103ab^5d^5 + 5a^{10}d^4 \\
&+ 130a^8bd^4 - 2183a^6b^2d^4 - 17022a^4b^3d^4 - 2940a^2b^4d^4 - 4b^5d^4 + 50a^9d^3 \\
&+ 159a^7bd^3 - 15035a^5b^2d^3 + 179a^3b^3d^3 + 1703ab^4d^3 + 206a^8d^2 \\
&- 1708a^6bd^2 - 25304a^4b^2d^2 + 1431a^2b^3d^2 + 20b^4d^2 + 363a^7d - 4398a^5bd \\
&- 23694a^3b^2d - 1437ab^3d + 258a^6 - 3816a^4b - 7026a^2b^2 - 12b^3)u^7 \\
&+ (-6a^8b^3d^7 - 164a^6b^4d^7 + 3864a^4b^5d^7 + 3365a^2b^6d^7 - 18a^9b^2d^6 \\
&- 522a^7b^3d^6 + 11837a^5b^4d^6 + 13701a^3b^5d^6 + 448ab^6d^6 - 18a^{10}bd^5 \\
&- 582a^8b^2d^5 + 12275a^6b^3d^5 + 21828a^4b^4d^5 + 2395a^2b^5d^5 - 6a^{11}d^4 \\
&- 296a^9bd^4 + 3283a^7b^2d^4 + 43960a^5b^3d^4 + 30290a^3b^4d^4 + 424ab^5d^4 \\
&- 66a^{10}d^3 - 1099a^8bd^3 + 32246a^6b^2d^3 + 30529a^4b^3d^3 - 17045a^2b^4d^3 \\
&- 310a^9d^2 + 679a^7bd^2 + 66726a^5b^2d^2 + 24833a^3b^3d^2 - 2192ab^4d^2 - 588a^8d \\
&+ 4809a^6bd + 73578a^4b^2d + 23685a^2b^3d - 444a^7 + 5316a^5b + 30936a^3b^2 \\
&+ 1704ab^3)u^8 + (7a^9b^3d^7 + 392a^7b^4d^7 - 6863a^5b^5d^7 - 17458a^3b^6d^7 \\
&- 515ab^7d^7 + 21a^{10}b^2d^6 + 1218a^8b^3d^6 - 20647a^6b^4d^6 - 61745a^4b^5d^6 \\
&- 6709a^2b^6d^6 - 4b^7d^6 + 21a^{11}bd^5 + 1302a^9b^2d^5 - 20664a^7b^3d^5 \\
&- 81924a^5b^4d^5 - 22146a^3b^5d^5 - 183ab^6d^5 + 7a^{12}d^4 + 567a^{10}bd^4 \\
&- 3982a^8b^2d^4 - 97733a^6b^3d^4 - 158644a^4b^4d^4 - 8392a^2b^5d^4 - 4b^6d^4 \\
&+ 84a^{11}d^3 + 2878a^9bd^3 - 57242a^7b^2d^3 - 160981a^5b^3d^3 + 59447a^3b^4d^3
\end{aligned}
$$

$$+ 3223ab^5d^3 + 442a^{10}d^2 + 2563a^8bd^2 - 142138a^6b^2d^2 - 189134a^4b^3d^2$$
$$+ 18323a^2b^4d^2 + 20b^5d^2 + 885a^9d - 2382a^7bd - 179958a^5b^2d$$
$$- 164688a^3b^3d - 2637ab^4d + 696a^8 - 5400a^6b - 92938a^4b^2 - 29078a^2b^3$$
$$- 12b^4)u^9\big).$$

References

[AHS01] M. Ando, M. J. Hopkins, and N. P. Strickland, *Elliptic spectra, the Witten genus and the theorem of the cube*, Invent. Math. **146** (2001), no. 3, 595–687. MR1869850 (2002g:55009)

[And95] Matthew Ando, *Isogenies of formal group laws and power operations in the cohomology theories E_n*, Duke Math. J. **79** (1995), no. 2, 423–485. MR1344767 (97a:55006)

[BGJGP05] Matthew H. Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen, *Finiteness results for modular curves of genus at least 2*, Amer. J. Math. **127** (2005), no. 6, 1325–1387. MR2183527 (2006i:11065)

[BMMS86] R. R. Bruner, J. P. May, J. E. McClure, and M. Steinberger, *H_∞ ring spectra and their applications*, Lecture Notes in Mathematics, vol. 1176, Springer-Verlag, Berlin, 1986. MR836132 (88e:55001)

[BW05] James Borger and Ben Wieland, *Plethystic algebra*, Adv. Math. **194** (2005), no. 2, 246–283. MR2139914 (2006i:13044)

[EKMM97] A. D. Elmendorf, I. Kriz, M. A. Mandell, and J. P. May, *Rings, modules, and algebras in stable homotopy theory*, Mathematical Surveys and Monographs, vol. 47, American Mathematical Society, Providence, RI, 1997, With an appendix by M. Cole. MR1417719 (97h:55006)

[GH04] P. G. Goerss and M. J. Hopkins, *Moduli spaces of commutative ring spectra*, Structured ring spectra, London Math. Soc. Lecture Note Ser., vol. 315, Cambridge Univ. Press, Cambridge, 2004, pp. 151–200. MR2125040 (2006b:55010)

[Hop] M. J. Hopkins, *$K(1)$-local E_∞ ring spectra*, unpublished notes, 1998, available at `http://www.math.rochester.edu/u/faculty/doug/otherpapers/knlocal.pdf`.

[Hov97] Mark A. Hovey, *v_n-elements in ring spectra and applications to bordism theory*, Duke Math. J. **88** (1997), no. 2, 327–356. MR1455523 (98d:55017)

[Hus04] Dale Husemöller, *Elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 111, Springer-Verlag, New York, 2004, With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. MR2024529 (2005a:11078)

[KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. MR772569 (86i:11024)

[MR09] Mark Mahowald and Charles Rezk, *Topological modular forms of level 3*, Pure Appl. Math. Q. **5** (2009), no. 2, Special Issue: In honor of Friedrich Hirzebruch. Part 1, 853–872. MR2508904 (2010g:55010)

[Reza] Charles Rezk, *Lectures on power operations*, unpublished notes, available at `http://www.math.uiuc.edu/~rezk/power-operation-lectures.dvi`.

[Rezb] ———, *Power operations for Morava E-theory of height 2 at the prime 2*, preprint, available at arXiv:0812.1320.

[Rez09] ———, *The congruence criterion for power operations in Morava E-theory*, Homology, Homotopy Appl. **11** (2009), no. 2, 327–379. MR2591924 (2011e:55021)

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 (2010i:11005)

[Ste62] N. E. Steenrod, *Cohomology operations*, Lectures by N. E. Steenrod written and revised by D. B. A. Epstein. Annals of Mathematics Studies, No. 50, Princeton University Press, Princeton, N.J., 1962. MR0145525 (26 #3056)

[Str98] N. P. Strickland, *Morava E-theory of symmetric groups*, Topology **37** (1998), no. 4, 757–779. MR1607736 (99e:55008)

[Voe03] Vladimir Voevodsky, *Reduced power operations in motivic cohomology*, Publ. Math. Inst. Hautes Études Sci. (2003), no. 98, 1–57. MR2031198 (2005b:14038a)

Department of Mathematics, University of Minnesota, Minneapolis, MN 55455, USA

`zyf@math.umn.edu`