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. At height 2 for the prime 3, the power operations arise from the universal degree-3 isogeny of elliptic curves associated to the E-theory.

1 Introduction

The study of cohomology operations has been central to algebraic topology since the 1950s, with applications to solving problems such as the number of independent vector fields on spheres, and the non-existence of maps of Hopf invariant one. Perhaps internally cohomology operations are primarily used to cure the blindness of cohomology theories [Gre88], that is, to cure their varied degrees of inability to detect the fact that a map of spaces is essential. In other words, 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 mth extended power of the d-fold suspension of E

$$\mathbb{P}_E^m(\Sigma^d E) = \big((\Sigma^d E)^{\wedge_E m}\big)_{h\Sigma_m},$$

where $(-)_{h\Sigma_m}$ denotes taking homotopy orbits of the action by the symmetric group on m letters (on the m-fold smash product over E). 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, Section IX.1]). These power operations are organized into a family, and the $\mathbb{P}_E^m(-)$'s assemble together to give the *free commutative E-algebra functor*

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

which passes to a functor of homotopy categories (cf. [BMMS86, Section I.2] and [Rez09, 3.15]).

Under the action of power operations, A_* is an algebra over some operad on 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 A is $K(n)$-local and E is a Morava E-theory. 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 ([Rez09, Theorem B]). This connects the structure of Γ to the geometry underlying E, moving one step forward from a workable object Γ to something computable. Based on this geometric description, 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 $K(1)$-local power operations.

Outline of the paper

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

In Section 2, by doing calculations with a specific elliptic curve associated to our Morava E-theory E, we give formulas of the total power operation ψ^3 on E_0 and the ring S_3 parametrizing the corresponding moduli problem ($\mathrm{Spec} S_3$ as the incidence scheme in the sense of [KM85]).

In Section 3, based on calculations of $E_*B\Sigma_m$ in [ST97] and [Str98], we define individual power operations, and derive the relations they satisfy. Thus in view of the general structures described in [Rez09], we 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 operation. We then derive formulas of the latter from calculations in Section 2.

Remark 1 The parametrization ring S_3 mentioned above turns out to be an algebra on one generator over the base ring where our elliptic curve is defined (cf. Proposition 4). This generator appears as a parameter in the formulas of the total power operation ψ^3, and is responsible for how the individual power operations are defined and how their formulas look like. Different choices of this parameter results in different bases of the Dyer–Lashof algebra Γ.

The parameter in this paper will be derived differently from the one used in [Rezb]; it comes intrinsically from the relative cotangent space of the elliptic curve. This choice of parameter is important for writing down Adem relations in Section 3, and it fits naturally into the treatment of gradings in [Rez09].

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 to work with. Somewhat surprisingly, though it appears to be derived from different considerations, our choice has an analog at the prime 2 which coincides with the parameter used in [Rezb]. Our calculations follow a recipe in hope of generalizing to larger primes; we hope to address these matters and recognize more of the general patterns based on further computational evidence. □

Acknowledgements

I would like to thank Charles Rezk for encouragement on this work, and for his observation in a correspondence which leads to Lemma 7. I would also like to thank Tyler Lawson for the sustained support from him I received as a student.

Conventions

Throughout this paper, we use the symbols

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

to denote a field with q elements, the ring of p-typical Witt vectors over $\mathbb{F}_q$ (if $q = p^n$ with p a prime), and the additive group of integers modulo n, respectively.

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

2 Total power operations

The universal elliptic curve C with a choice of 4-torsion point has equation

$$Y^2Z + aXYZ + acYZ^2 = X^3 + cX^2Z,$$

over the graded ring $\mathbb{Z}[\frac{1}{4}][a,c]$ with $|a| = 1$ and $|c| = 2$. This equation is computed from a general affine Weierstrass equation in xy-coordinates, by requiring that the 4-torsion point P be $(0,0)$, $2P$ be on the x-axis, and $4P$ be the identity of C at the infinity.

In the affine coordinate chart $c = 1$ of the moduli stack $\mathcal{M}\big(\Gamma_1(4)\big)$, C is given by the affine Weierstrass equation

$$y^2 + axy + ay = x^3 + x^2,$$

over the ring $\mathbb{Z}[\frac{1}{4}][a]$, with discriminant $\Delta = a^2(a+4)(a-4)$. Let $S = \mathbb{Z}[\frac{1}{4}][a, \Delta^{-1}]$. Over a field of characteristic 3, this elliptic curve is supersingular precisely when the quantity $h = a^2 + 4$ vanishes (cf. [Sil09, V.4.1a]), and its minimal field of definition is then $\mathbb{F}_9$.

By Serre–Tate theory, 3-adically the deformation theory of C is equivalent to the deformation theory of its 3-divisible group. Let $\widehat{S} = \mathbb{Z}_9[\![h]\!]$; by Hensel's Lemma, both

a and Δ lie in $\widehat{S}$, and both are invertible. In fact, let i be an element generating $\mathbb{Z}_9$ over $\mathbb{Z}_3$ with $i^2 = -1$; then since $h = a^2 + 4$,

$$a \equiv i \mod (3,h) \qquad \text{and} \qquad \Delta = (h-4)(h-20) \equiv -1 \mod (3,h),$$

where $(3,h)$ is the maximal ideal of the complete local ring $\widehat{S} = \mathbb{Z}_9[\![h]\!]$. Thus $\widehat{S}$ is the completion of S with respect to $(3,h)$. Let $\widehat{C}$ denote the formal completion of C at the identity; this defines a formal group over $\widehat{S}$. It is a universal deformation for its reduction to $\mathbb{F}_9 = \widehat{S}/(3,h)$ which is a formal group of height 2. Let E denote the Morava E-theory associated to this height 2 formal group, so that $E_* \cong \mathbb{Z}_9[\![h]\!][u^{\pm 1}]$ with $|u| = 2$, where u corresponds to a local uniformizer at the identity of C.

To study C at the formal neighborhood of its 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 O of C is now $(u,v) = (0,0)$, and u is a local uniformizer at O. The above Weierstrass equation of C becomes

$$v + auv + av^2 = u^3 + u^2 v. \tag{1}$$

Proposition 2 *On the elliptic curve C over S, the uv-coordinates (d,e) of any nonzero 3-torsion point satisfy the identities*

$$f(d) = 0,$$

and

$$e = g(d),$$

where the polynomials $f(u)$ and $g(u)$ are given by

$f(u) = u^8 + 3au^7 + 3a^2u^6 + (a^3+7a)u^5 + (6a^2-6)u^4 + 9au^3 + (-a^2+8)u^2 - 3au - 3,$

$g(u) = -\frac{1}{a(a+4)(a-4)}\big(au^7 + (3a^2-2)u^6 + (3a^3-6a)u^5 + (a^4+a^2+2)u^4 + (4a^3 - 15a)u^3 + 18u^2 - 12au - 18\big).$

Proof Given the elliptic curve

$$C\colon\ y^2 + axy + ay = x^3 + x^2,$$

a nonzero point Q of C is a 3-torsion point if and only if the division polynomial

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

vanishes at Q (cf. [Sil09, Exercise 3.7f]). Substituting x by u/v and clearing the denominators, we have

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

so that $\widetilde{\psi}_3(d,e) = 0$.

We can rewrite the equation (1) of C as a quadratic equation in v:

$$av^2 + (-u^2 + au + 1)v - u^3 = 0$$

(a is invertible in $S = \mathbb{Z}[\frac{1}{4}][a, \Delta^{-1}]$ as $\Delta = a^2(a+4)(a-4)$). Define $\widetilde{f}(u) = \widetilde{\psi}_3(u,v)\widetilde{\psi}_3(u,v')$, where v and v' are formally the conjugate roots of the above equation so that we substitute $v+v'$ as $(u^2-au-1)/a$, and vv' as $-u^3/a$. We then compute that

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

where $f(u)$ is as stated. Since $\widetilde{f}(d) = 0$ and $d \neq 0$, we have the first stated identity

$$f(d) = 0.$$

For the polynomial $g(u)$, note that both the quartic polynomial

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

and the quadratic polynomial

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

vanish at e, and thus so does their greatest common divisor (gcd). By the Euclidean algorithm, we have

$$A(v) = Q_1(v)B(v) + R_1(v),$$
$$B(v) = Q_2(v)R_1(v) + R_2,$$

where

$$R_1(v) = S(d)v + T(d)$$

for some polynomials S and T, and $R_2 = 0$ as a result of $f(d) = 0$. Thus $R_1(v)$ is the gcd of $A(v)$ and $B(v)$, and hence

$$S(d)e + T(d) = R_1(e) = 0.$$

In order to write e in terms of d from the above identity, we apply the Euclidean algorithm to the polynomials $f(u)$ and $S(u)$, and find their gcd to be 1. Thus there are polynomials $p(u)$ and $q(u)$ such that

$$p(u)f(u) + q(u)S(u) = 1.$$

Since $f(d)=0$, we then have $q(d)S(d)=1$, and thus

$$e=-q(d)T(d)=g(d),$$

where g is as stated.

$\widetilde{f}(u)=-\frac{u^4(-3-3au+8u^2-a^2u^2+9au^3-6u^4+6a^2u^4+7au^5+a^3u^5+3a^2u^6+3au^7+u^8)}{a^2}$

$Q_1(v)=\frac{1}{a}-d-\frac{2d^2}{a}+ad^2+2d^3+\frac{d^4}{a}+(-1+2ad+d^2)v+av^2$

$R_1(v)=\frac{d^3}{a}+2d^4-\frac{2d^5}{a}+ad^5+2d^6+\frac{d^7}{a}+(-\frac{1}{a}+\frac{3d^2}{a}+2d^3-\frac{3d^4}{a}+ad^4+2d^5+\frac{d^6}{a})v$

$Q_2(v)=-a(1+ad-4d^2-4ad^3+6d^4-a^2d^4+ad^5-4d^6+a^2d^6+2ad^7+d^8+av-3ad^2v-2a^2d^3v+3ad^4v-a^3d^4v-2a^2d^5v-ad^6v)/(-1+3d^2+2ad^3-3d^4+a^2d^4+2ad^5+d^6)^2$

$R_2(v)=-ad^4(-3-3ad+8d^2-a^2d^2+9ad^3-6d^4+6a^2d^4+7ad^5+a^3d^5+3a^2d^6+3ad^7+d^8)/(-1+3d^2+2ad^3-3d^4+a^2d^4+2ad^5+d^6)^2$

$S(d)=\frac{d^3}{a}+2d^4-\frac{2d^5}{a}+ad^5+2d^6+\frac{d^7}{a}$

$T(d)=-\frac{1}{a}+\frac{3d^2}{a}+2d^3-\frac{3d^4}{a}+ad^4+2d^5+\frac{d^6}{a}$

$p(u)=(-4096a^6+13568a^8-2672a^{10}+179a^{12}-4a^{14}-98304a^7u+19456a^9u-1280a^{11}u+28a^{13}u+8192a^6u^2-69120a^8u^2+17248a^{10}u^2-1610a^{12}u^2+66a^{14}u^2-a^{16}u^2+77824a^7u^3-41984a^9u^3+6384a^{11}u^3-382a^{13}u^3+8a^{15}u^3-4096a^6u^4-55040a^8u^4+11792a^{10}u^4-825a^{12}u^4+19a^{14}u^4-28672a^7u^5+6144a^9u^5-432a^{11}u^5+10a^{13}u^5)/(65536a^8-16384a^{10}+1536a^{12}-64a^{14}+a^{16})$

$q(u)=a(12288a^6-106240a^8+24400a^{10}-2073a^{12}+76a^{14}-a^{16}+307200a^7u-99072a^9u+11856a^{11}u-621a^{13}u+12a^{15}u-20480a^6u^2+296192a^8u^2-71856a^{10}u^2+6555a^{12}u^2-265a^{14}u^2+4a^{16}u^2-135168a^7u^3+199680a^9u^3-40272a^{11}u^3+3082a^{13}u^3-98a^{15}u^3+a^{17}u^3+4096a^6u^4+213760a^8u^4-22928a^{10}u^4-1435a^{12}u^4+239a^{14}u^4-7a^{16}u^4+12288a^7u^5+78592a^9u^5-16880a^{11}u^5+1177a^{13}u^5-27a^{15}u^5+4096a^6u^6+83712a^8u^6-17936a^{10}u^6+1257a^{12}u^6-29a^{14}u^6+28672a^7u^7-6144a^9u^7+432a^{11}u^7-10a^{13}u^7)/(65536a^8-16384a^{10}+1536a^{12}-64a^{14}+a^{16})$ □

Remark 3 We have

$$f(u)\equiv u^2(u+a)^6 \mod 3,$$

where a is invertible in $S=\mathbb{Z}[\frac{1}{4}][a,\Delta^{-1}]$ as $\Delta=a^2(a+4)(a-4)$. The two roots (counted with multiplicity) of $f(u)$ which reduce to zero modulo 3 correspond to the two nonzero elements of the unique order-3 subgroup of C in the formal neighborhood of the identity. $\square$

Proposition 4 *The universal degree-3 isogeny ψ with domain C is defined over the ring*

$$S_3 := S[\alpha]\big/\big(w(\alpha)\big)$$

where

$$w(\alpha) = \alpha^4 - 6\alpha^2 + (a^2 - 8)\alpha - 3,$$

and has range the elliptic curve

$$C'\colon\ v + r(a)uv + r(a)v^2 = u^3 + u^2 v,$$

where

$$r(a) = a^3 + (\alpha^3 - 6\alpha - 12)a - 4(\alpha+1)^2(\alpha-3)a^{-1}.$$

The kernel of this isogeny is generated by a 3-torsion point with coordinates (d, e) satisfying

$\alpha = -\frac{1}{(a+4)(a-4)}\big(ad^7 + (3a^2-2)d^6 + (3a^3-6a)d^5 + (a^4+a^2+2)d^4 + (4a^3-15a)d^3 + (a^2+2)d^2 - 12ad - 18\big) = ae - d^2.$

The induced map on relative cotangent spaces at the identity sends du to αdu.

Proof Let $P = (u, v)$ be a general point on C, and $Q = (d, e)$ be a nonzero 3-torsion point. Rewriting the equation (1) of C as

$$v = u^3 + u^2 v - auv - av^2,$$

we can express v in terms of a power series in u by recursive substitution. For the purpose of our calculations, we take this power series up to u^9 as an expression of v, and write $e = g(d)$ as in Proposition 2.

Define the isogeny $\psi\colon\ C \to C'$ by

$$u' := u\big(\psi(P)\big) = u(P)\cdot u(P-Q)\cdot u(P+Q),$$
$$v' := v\big(\psi(P)\big) = v(P)\cdot v(P-Q)\cdot v(P+Q),$$

whose kernel is precisely the order-3 subgroup generated by Q. By computing the group law of C, we can write down formal expansions in terms of the local uniformizer u at the identity:

$$\begin{aligned} u' &= \alpha u + \cdots, \\ v' &= \beta u^3 + \cdots, \end{aligned} \tag{2}$$

where the coefficients (α, β, etc.) involve a and d.

We then solve for the Weierstrass equation which u' and v' satisfy. For the equation to be in the form of (1), we adjust the definition of v' as

$$v' = \frac{\alpha^3}{\beta} \cdot v(P) \cdot v(P-Q) \cdot v(P+Q).$$

Using this and (2), we get the stated equation of C'.

The first stated formula of α in terms of a and d is computed above in the process of expressing u' in terms of u. The second shorter expression of α in terms of a, d and e can be checked by comparing the former formula with the formula of $g(u)$ in Proposition 2, as $e = g(d)$. In view of $f(d) = 0$ as in Proposition 2, we further compute that α satisfies

$$w(\alpha) = 0,$$

where w is as stated. The last statement in the proposition follows by definition of α in (2).

$v = u^3 - au^4 + (1+a^2)u^5 - a(3+a^2)u^6 + (1+6a^2+a^4)u^7 - a(6+10a^2+a^4)u^8 + (1+20a^2+15a^4+a^6)u^9 + O(u^{10})$

The group law on C (cf. [Sil09, III.2]) satisfies

- given $P(u,v)$, the coordinates of $-P$ are

$$u_0 = -\frac{v}{u(u+v)} \qquad \text{and} \qquad v_0 = -\frac{v^2}{u^2(u+v)};$$

- given $P_1(u_1,v_1)$ and $P_2(u_2,v_2)$, the coordinates of $-(P_1+P_2)$ are

$$u_3 = ak - \frac{b}{1+k} - u_1 - u_2 \qquad \text{and} \qquad v_3 = ku_3 + b,$$

  where $k = \frac{v_1 - v_2}{u_1 - u_2}$ is the slope and $b = \frac{u_1v_2 - u_2v_1}{u_1 - u_2}$ is the v-intercept of the line through P_1 and P_2.

Thus, given $P(u,v)$ and $Q(d,e)$, in order to compute formulas of u' and v',

- set

$$(u_1,v_1) = \left(-\frac{v}{u(u+v)}, -\frac{v^2}{u^2(u+v)}\right) \qquad \text{and} \qquad (u_2,v_2) = (d,e),$$

  and take

$$P - Q = (u_3, v_3);$$

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

Plugging the coordinates of $P - Q$ and $P + Q$ into (2) and in view of $f(d) = 0$, we have, among coefficients of higher powers of u,

$\alpha = -(-18 - 12ad + 2d^2 + a^2d^2 - 15ad^3 + 4a^3d^3 + 2d^4 + a^2d^4 + a^4d^4 - 6ad^5 + 3a^3d^5 - 2d^6 + 3a^2d^6 + ad^7)/((-4 + a)(4 + a))$

$\beta = -(-12 - 6a^2 - 117ad + 3a^3d + 20d^2 - 153a^2d^2 + 10a^4d^2 + 31ad^3 - 80a^3d^3 + 6a^5d^3 - 4d^4 - 96a^2d^4 - 4a^4d^4 + a^6d^4 - 15ad^5 - 33a^3d^5 + 3a^5d^5 - 4d^6 - 33a^2d^6 + 3a^4d^6 - 11ad^7 + a^3d^7)/((-4 + a)a^2(4 + a))$

$\alpha^3/\beta = -(4 - 4a^2 + 9ad - 3a^3d - 12d^2 + 21a^2d^2 - a^4d^2 - 15ad^3 + 11a^3d^3 + 12d^4 + 6a^2d^4 + 3a^4d^4 - 13ad^5 + 9a^3d^5 - 4d^6 + 9a^2d^6 + 3ad^7)/((-4 + a)(4 + a))$ □

Remark 5 The parameter α is invariant under change of coordinates: if $w := \sum_{i=1}^{\infty} a_i u^i$ and $w' := \sum_{i=1}^{\infty} a_i (u')^i$, where $a_i \in S$ and $a_1 \in S^{\times}$, then $w' = \alpha w + \cdots$.

We also note that the analog of α at the prime 2 coincides with d, the u-coordinate of a nonzero 2-torsion point on the universal elliptic curve with a choice of 3-torsion point (cf. [Rezb, Section 3]). □

Let $\widehat{S}_3 = S_3 \otimes_S \widehat{S}$, where S_3 is the ring parametrizing the moduli problem as in Proposition 4. In [Str98] Strickland proves that
$$\widehat{S}_3 \cong E^0 B\Sigma_3 / I,$$
where $I := \sum_{0<i<3} \mathrm{Image}\big(E^0 B(\Sigma_i \times \Sigma_{3-i}) \xrightarrow{\text{transfer}} E^0 B\Sigma_3\big)$ 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 6 *The total power operation*
$$\psi^3 \colon E^0 \to E^0 B\Sigma_3 / I \cong E^0[\alpha]/\big(w(\alpha)\big)$$
is given by

$\psi^3(h) = h^3 + (\alpha^3 - 6\alpha - 36)h^2 + 3(-8\alpha^3 + \alpha^2 + 48\alpha + 130)h + 4(30\alpha^3 - 9\alpha^2 - 178\alpha - 303)$,

$$\psi^3(a) = a^3 + (\alpha^3 - 6\alpha - 12)a - 4(\alpha+1)^2(\alpha-3)a^{-1}.$$

Proof By [Rez09, Theorem B], there is a correspondence between the universal degree-3 isogeny ψ with domain C and the total power operation ψ^3 with domain E^0. In particular $\psi^3(a)$ is given by $r(a)$. As ψ^3 is a ring homomorphism, we then get the formula of $\psi^3(h) = \psi^3(a^2+4)$. □

3 Individual power operations

To understand the power operation structure on E_0, we need to consider composition of power operations. Correspondingly, we need to consider the composite of two degree-3 isogenies.

By Proposition 4, as the kernel of the degree-3 isogeny ψ, the universal example G of an order-3 subgroup of C is defined over $S_3 = S[\alpha]/\big(w(\alpha)\big)$. Similarly, consider the universal degree-3 isogeny ψ' with domain $C' \cong C/G$, and denote its kernel by G'. Let $S' = \mathbb{Z}[\frac{1}{4}][a', (\Delta')^{-1}]$ with $a' = r(a)$ and $\Delta' = (a')^2(a'+4)(a'-4)$, and let $S'_3 = S'[\alpha']/\big(w'(\alpha')\big)$ with $w'(\alpha') = (\alpha')^4 - 6(\alpha')^2 + \big((a')^2 - 8\big)\alpha' - 3$, analogous to S and S_3.

Let $S_{3,3}$ be the pushout in the diagram

$$\begin{tikzcd} S \arrow[r, "t^*"] \arrow[d, "s^*"'] & S'_3 \arrow[d, "\sigma^*"] \\ S_3 \arrow[r, "\tau^*"'] \arrow[ur, phantom, "\ulcorner" very near end] & S_{3,3}, \end{tikzcd}$$

where s^* is the inclusion, and t^* sends a to a'. Then σ^* is the inclusion, and τ^* sends a to a', and α to α'; they classify the subgroup G of C, and the subgroup G' of C', respectively. Thus, via the evident isomorphism $S'_3 \cong S_3$, $S_{3,3}$ carries the universal example of a chain $G < C[3]$ of subgroups of C, with $|G| = |C[3]/G| = 3$.

By base change we then have a commutative diagram of elliptic curves over $S_{3,3}$:

$$\begin{tikzcd} C \arrow[rr, "\psi"] \arrow[dr, "{[3]}"'] & & C/G \cong C' \arrow[d, "\widehat{\psi} = [-1]\psi'"] \\ & C \cong C/C[3] \cong \frac{C/G}{C[3]/G} \cong \frac{C'}{G'} & \end{tikzcd},$$

where $\widehat{\psi}$ is the isogeny dual to ψ. Note that both ψ and ψ' restrict to the third-power Frobenius endomorphism ψ_0 over the supersingular locus. Since $\psi_0^2 = [-3]$ (cf. [Yui79, 5.11] and [Sil09, V.2.3.1]), we have $\widehat{\psi} = [-1]\psi'$ by uniqueness of the dual isogeny (cf. [Sil09, III.6.1a]).

The isogenies in the above diagram induce maps on relative cotangent spaces at the identity, and by Proposition 4 we have a commutative diagram

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

Lemma 7 *The following relations hold in $S_{3,3}$:*

$$\alpha\alpha' + 3 = 0,$$

and

$$\alpha' = -\alpha^3 + 6\alpha + (-a^2 + 8).$$

Proof The first relation is read off from Diagram (3). From this and $w(\alpha) = 0$, we then get the second relation. □

Remark 8 As is noted in Remark 5, the analog of α at the prime 2 coincides with the parameter d used in [Rezb]. Thus, with notation as in [Rezb], d and d' satisfy an analogous relation $dd' + 2 = 0$ in the ring $S_{2,2}$. □

Let S_9 be the pullback in the diagram

$$\begin{tikzcd} S_9 \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & S_{3,3} \arrow[d, "\pi^*"] \\ S \arrow[r, "s^*"'] & S_3 \end{tikzcd}, \tag{4}$$

where π^* sends a to a, α to α, a' to $r(a)$, and α' to $-\alpha^3+6\alpha+(-a^2+8)$ as in Lemma 7; it classifies the chain of subgroups $G < C[3]$ in C. Thus the universal example of an order-9 subgroup of C is defined over S_9, and the map $S_9 \to S$ classifies $C[3]$.

Let A be a $K(2)$-local commutative E-algebra. From the total power operation on E_0 in Section 2, we have total power operations

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

and

$$\begin{aligned}\psi^3 \circ \psi^3\colon\ A_0 &\to \big(A_0 \otimes_{E_0} (E^0B\Sigma_3/I)\big) \;{}_{\psi^3}\!\otimes_{E_0} (E^0B\Sigma_3/I)\\ &\cong \Big(A_0[\alpha']/\big(w'(\alpha')\big)\Big) \;{}_{\psi^3}\!\otimes_{E_0} \Big(E^0[\alpha]/\big(w(\alpha)\big)\Big),\end{aligned}$$

where $\alpha' = \psi^3(\alpha) = -\alpha^3+6\alpha+(-h+12)$ by Lemma 7.

Define the *individual power operations*

$$Q_i\colon\ A_0 \to A_0,$$

for $i = 0,1,2,3$, by

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

Proposition 9 *The following relations hold among the individual power operations Q_0, Q_1, Q_2, and Q_3:*

(i) Additivity
$Q_i(x+y) = Q_i(x) + Q_i(y)$;

(ii) Action on scalars
$Q_0(1) = 1$,
$Q_1(1) = Q_2(1) = Q_3(1) = 0$,
$Q_0(h) = h^3 - 36h^2 + 390h - 1212$,
$Q_1(h) = -6h^2 + 144h - 712$,
$Q_2(h) = 3h - 36$,
$Q_3(h) = h^2 - 24h + 120$,
$Q_0(a) = a^3 - 12a + 12a^{-1}$,
$Q_1(a) = -6a + 20a^{-1}$,
$Q_2(a) = 4a^{-1}$,
$Q_3(a) = a - 4a^{-1}$;

(iii) *Commutation relations (twists)*
$Q_0(hx) = (h^3 - 36h^2 + 390h - 1212)Q_0(x) + (3h^2 - 72h + 360)Q_1(x) + (9h - 108)Q_2(x) + 24Q_3(x)$,
$Q_1(hx) = (-6h^2 + 144h - 712)Q_0(x) + (-18h + 228)Q_1(x) + (-72)Q_2(x) + (h - 12)Q_3(x)$,
$Q_2(hx) = (3h - 36)Q_0(x) + 8Q_1(x) + 12Q_2(x) + (-24)Q_3(x)$,
$Q_3(hx) = (h^2 - 24h + 120)Q_0(x) + (3h - 36)Q_1(x) + 8Q_2(x) + 12Q_3(x)$,
$Q_0(ax) = (a^3 - 12a + 12a^{-1})Q_0(x) + (3a - 12a^{-1})Q_1(x) + (12a^{-1})Q_2(x) + (-12a^{-1})Q_3(x)$,
$Q_1(ax) = (-6a + 20a^{-1})Q_0(x) + (-20a^{-1})Q_1(x) + (-a + 20a^{-1})Q_2(x) + (4a - 20a^{-1})Q_3(x)$,
$Q_2(ax) = (4a^{-1})Q_0(x) + (-4a^{-1})Q_1(x) + (4a^{-1})Q_2(x) + (-a - 4a^{-1})Q_3(x)$,
$Q_3(ax) = (a - 4a^{-1})Q_0(x) + (4a^{-1})Q_1(x) + (-4a^{-1})Q_2(x) + (4a^{-1})Q_3(x)$;

(iv) *Adem relations (products)*
$Q_1Q_0(x) = (-6)Q_0Q_1(x) + (6h - 72)Q_0Q_2(x) + (-6h^2 + 144h - 747)Q_0Q_3(x) + 18Q_1Q_2(x) + 3Q_2Q_1(x) + (-18h + 216)Q_1Q_3(x) + (-54)Q_2Q_3(x) + (-9)Q_3Q_2(x)$,
$Q_2Q_0(x) = (-3)Q_0Q_2(x) + (3h - 36)Q_0Q_3(x) + 9Q_1Q_3(x) + 3Q_3Q_1(x)$,
$Q_3Q_0(x) = Q_0Q_1(x) + (-h + 12)Q_0Q_2(x) + (h^2 - 24h + 126)Q_0Q_3(x) + (-3)Q_1Q_2(x) + (3h - 36)Q_1Q_3(x) + 9Q_2Q_3(x)$;

(v) *Cartan formulas (coproducts)*
$Q_0(xy) = Q_0(x)Q_0(y) + 3\big(Q_1(x)Q_3(y) + Q_2(x)Q_2(y) + Q_3(x)Q_1(y)\big) + 18Q_3(x)Q_3(y)$,
$Q_1(xy) = \big(Q_0(x)Q_1(y) + Q_1(x)Q_0(y)\big) + (-h + 12)\big(Q_1(x)Q_3(y) + Q_2(x)Q_2(y) + Q_3(x)Q_1(y)\big) + 3\big(Q_2(x)Q_3(y) + Q_3(x)Q_2(y)\big) + (-6h + 72)Q_3(x)Q_3(y)$,
$Q_2(xy) = \big(Q_0(x)Q_2(y) + Q_1(x)Q_1(y) + Q_2(x)Q_0(y)\big) + 6\big(Q_1(x)Q_3(y) + Q_2(x)Q_2(y) + Q_3(x)Q_1(y)\big) + (-h + 12)\big(Q_2(x)Q_3(y) + Q_3(x)Q_2(y)\big) + 39Q_3(x)Q_3(y)$,
$Q_3(xy) = \big(Q_0(x)Q_3(y) + Q_1(x)Q_2(y) + Q_2(x)Q_1(y) + Q_3(x)Q_0(y)\big) + 6\big(Q_2(x)Q_3(y) + Q_3(x)Q_2(y)\big) + (-h + 12)Q_3(x)Q_3(y)$;

(vi) *Frobenius congruence (amplification)*
$Q_0(x) \equiv x^3 \mod 3$,
with $\theta\colon A_0 \to A_0$ *such that* $Q_0(x) = x^3 + 3\theta(x)$.

Proof Except for (iv), all the relations can be derived directly from Corollary 6 and the fact that ψ^3 is a ring homomorphism.

Write $\widehat{S}'$, $\widehat{S}'_3$, $\widehat{S}_{3,3}$, and $\widehat{S}_9$, analogous to $\widehat{S}_3$, to denote the completions of rings. To derive (iv), we note that in view of diagram (4) the composite

$$A_0 \xrightarrow{\psi^3} A_0 \otimes_{\widehat{S}\ s^*} \widehat{S}_3 \xrightarrow{\psi^3} A_0 \otimes_{\widehat{S}'\ s^*} \widehat{S}'_3\ {}_{t^*}\!\otimes_{\widehat{S}\ s^*} \widehat{S}_3 \cong A_0 \otimes_{\widehat{S}\ s^*} \widehat{S}_{3,3}$$

factors through $A_0 \otimes_{\widehat{S}} \widehat{S}_9$. In terms of formulas we have

$$\begin{aligned}\psi^3\big(\psi^3(x)\big) &= \psi^3\big(Q_0(x) + Q_1(x)\alpha + Q_2(x)\alpha^2 + Q_3(x)\alpha^3\big)\\ &= \psi^3\big(Q_0(x)\big) + \psi^3\big(Q_1(x)\big)\alpha' + \psi^3\big(Q_2(x)\big)(\alpha')^2 + \psi^3\big(Q_3(x)\big)(\alpha')^3\\ &= \sum_{i,\,j\,=\,0}^{3} Q_iQ_j(x)\alpha^i\big(-\alpha^3 + 6\alpha + (-h+12)\big)^j;\end{aligned}$$

the factorization means that under the projection $\pi^*\colon\ \widehat{S}_{3,3} \to \widehat{S}_3$ the coefficients of α, α^2, and α^3 in the last expression must be 0 (α satisfies a quartic equation in $\widehat{S}_3$). This gives the three relations in (iv). $\square$

Definition 10 We define an associative ring Γ equipped with a ring homomorphism [1] $\eta\colon\ \widehat{S} \to \Gamma$ as follows. The ring Γ is generated over $\widehat{S}$ by elements Q_0, Q_1, Q_2, and Q_3, subject to *commutation relations* and *Adem relations*. The commutation relations state that the Q_i's commute with elements of $\mathbb{Z}_9 \subset \widehat{S}$, and that

$$Q_0h = (h^3 - 36h^2 + 390h - 1212)Q_0 + (3h^2 - 72h + 360)Q_1 + (9h - 108)Q_2 + 24Q_3,$$

$$Q_1h = (-6h^2 + 144h - 712)Q_0 + (-18h + 228)Q_1 + (-72)Q_2 + (h - 12)Q_3,$$

$$Q_2h = (3h - 36)Q_0 + 8Q_1 + 12Q_2 + (-24)Q_3,$$

$$Q_3h = (h^2 - 24h + 120)Q_0 + (3h - 36)Q_1 + 8Q_2 + 12Q_3.$$

The Adem relations are

$$Q_1Q_0 = (-6)Q_0Q_1 + (6h - 72)Q_0Q_2 + (-6h^2 + 144h - 747)Q_0Q_3 + 18Q_1Q_2 + 3Q_2Q_1 + (-18h + 216)Q_1Q_3 + (-54)Q_2Q_3 + (-9)Q_3Q_2,$$

$$Q_2Q_0 = (-3)Q_0Q_2 + (3h - 36)Q_0Q_3 + 9Q_1Q_3 + 3Q_3Q_1,$$

$$Q_3Q_0 = Q_0Q_1 + (-h + 12)Q_0Q_2 + (h^2 - 24h + 126)Q_0Q_3 + (-3)Q_1Q_2 + (3h - 36)Q_1Q_3 + 9Q_2Q_3.$$ $\square$

Remark 11 Proposition 9 describes explicitly the structure of Γ as a *graded twisted bialgebra* over $E_0 = \widehat{S}$ (cf. [Rez09, Section 5] and [Rezb, 2.1]). In particular it follows that Γ has an *admissible basis*, that is, it is free as a left $\widehat{S}$-module on the elements of the form

$$Q_0^iQ_{k_1}\cdots Q_{k_r},$$

[1] The ring homomorphism η is formally the inclusion: an element $s \in \widehat{S} = E_0$ maps to the multiplication-by-s operation on the E_0-algebra A_0. For precise definition of η, cf. [Rez09, Section 6].

where $i, r \geq 0$, and $k_j = 1, 2$, or 3. Note that if we write $\Gamma[d]$ for the degree-d part of Γ, then $\Gamma[d]$ is of rank $1 + 3 + \cdots + 3^d$. $\square$

Example 12 We have $E^0 S^2 \cong \mathbb{Z}_9[\![h]\!][u]/(u^2)$. By definition of α in (2), the Q_i's act canonically on $E^0 S^2$:

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

Let ω be the kernel of $E^0 S^2 \to E^0$. It is a Γ*-module* (cf. [Rezb, 2.2]) on one generator u, and its Γ-module structure is canonical. $\square$

Following terminology in [Rez09, Section 2] and [Rezb, 2.5 and 2.6], we can now describe the power operation structure on $K(2)$-local commutative E-algebras.

Theorem 13 *Let A be a $K(2)$-local commutative E-algebra. Let Γ be the graded twisted bialgebra over E_0 given in Definition 10, and let ω be the Γ-module given in Example 12. Then A_* is an* ω-twisted $\mathbb{Z}/2$-graded amplified Γ-ring. *In particular,*

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

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

Formulas of Γ aside, this result is essentially due to Rezk [Rez09, Rezb].

Proof Let $\widetilde{\Gamma}$ be the graded twisted bialgebra of power operations on E described in [Rez09, Section 6]. It suffices to identify $\widetilde{\Gamma}$ with Γ. There is a direct sum decomposition $\widetilde{\Gamma} = \bigoplus_{d \geq 0} \widetilde{\Gamma}[d]$, where the pieces come from the E-homology of $B\Sigma_{3^d}$ (cf. [Rez09, 6.2]). There is a degree-preserving ring homomorphism $\phi\colon \Gamma \to \widetilde{\Gamma}$ which is an isomorphism in degrees 0 and 1 (cf. Corollary 6). As $\widetilde{\Gamma}$ is generated in degree 1 (by transfer argument), ϕ is surjective. By rank calculations (cf. [ST97, Section 6] and Remark 11), ϕ is also injective. $\square$

4 $K(1)$-local power operations

Let $F = L_{K(1)} E$. The general pattern of the relationship between $K(1)$-local power operations (cf. [Hop]) and the power operations in Section 2 is as follows:

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

Recall Proposition 4 and Corollary 6 that ψ^3 arises from the universal degree-3 isogeny which is parametrized by the ring S_3 with $\widehat{S}_3 \cong E^0 B\Sigma_3/I$. 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 (so that the resulting formal group is of height at most 1) and completing at the ideal (3), i.e. $E_* = \mathbb{Z}_9[\![h]\!][u^{\pm 1}]$ and $F_* = \mathbb{Z}_9[\![h]\!][h^{-1}]^\wedge_3[u^{\pm 1}]$. Explicitly,

$$F_0 = \mathbb{Z}_9(\!(h)\!)^\wedge_3 = \varprojlim_k \mathbb{Z}_9(\!(h)\!)/(3^k) = \left\{ \sum_{n=-\infty}^{\infty} c_n h^n \;\middle|\; c_n \in \mathbb{Z}_9, \lim_{n\to-\infty} c_n = 0 \right\}.$$

The formal group $\widehat{C}$ over E^0 has a unique order-3 subgroup after being pulled back to F^0 (cf. Remark 3), and the composite map $E^0 B\Sigma_3/I \to F^0 B\Sigma_3/I \cong F^0$ classifies this subgroup. The localization $E^0 B\Sigma_3/I \to F^0 B\Sigma_3/I$ factors through $F^0 \otimes_{E^0} E^0 B\Sigma_3/I$. Along the base change $E^0 B\Sigma_3/I \to F^0 \otimes_{E^0} E^0 B\Sigma_3/I$, the special fiber of the 3-divisible group $\widehat{C}$ 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 which gives rise to the $K(1)$-local power operation ψ^3_F.

In Proposition 4 the equation

$$w(\alpha) = \alpha^4 - 6\alpha^2 + (h-12)\alpha - 3 = 0$$

which parametrizes order-3 subgroups of C has a unique root in $\mathbb{F}_3(\!(h)\!)$, and Hensel's Lemma implies that this lifts to a root in $F_0 = \mathbb{Z}_9(\!(h)\!)^\wedge_3$. Plugging this specific value of α into the formulas of $\psi^3\colon E^0 \to E^0[\alpha]/\big(w(\alpha)\big)$ given in Corollary 6, we get an endomorphism of the ring F_0, and this endomorphism is ψ^3_F.

Explicitly, with h invertible in F_0, we can solve for α from the equation $w(\alpha) = 0$ by first writing

$$\alpha = \frac{1}{h-12}(3 + 6\alpha^2 - \alpha^4) = (3 + 6\alpha^2 - \alpha^4) \cdot \sum_{n=1}^{\infty} 12^{n-1} h^{-n}$$

and then substituting α recursively. We plug this into $\psi^3(h)$ and get

$$\psi^3_F(h) = h^3 - 36h^2 + 372h - 996 + 186h^{-1} + 2232h^{-2} + \cdots .$$

Similarly we have

$$\psi_F^3(a) = a^3 - 12a - 6a^{-1} - 84a^{-3} - 933a^{-5} - 10956a^{-7} + \cdots .$$

For an application of the analogous calculations at the prime 2, see [LN, Section 8.2].

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)

[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)

[Gre88] J. P. C. Greenlees, *How blind is your favourite cohomology theory?*, Exposition. Math. **6** (1988), no. 3, 193–208. MR949783 (89j:55001)

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

[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)

[LN] Tyler Lawson and Niko Naumann, *Commutativity conditions for truncated Brown-Peterson spectra of height 2*, arXiv:1101.3897.

[Reza] Charles Rezk, *Lectures on power operations*, 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*, 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)

[ST97] Neil P. Strickland and Paul R. Turner, *Rational Morava E-theory and DS^0*, Topology **36** (1997), no. 1, 137–151. MR1410468 (97g:55005)

[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)

[Yui79] Noriko Yui, *Formal groups and some arithmetic properties of elliptic curves*, Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978), Lecture Notes in Math., vol. 732, Springer, Berlin, 1979, pp. 630–658. MR555721 (80m:14027)