# 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 non-existence of maps of Hopf invariant one, and the maximum number of linearly independent vector fields on spheres. 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.

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 functor of *the $m$th extended power over $E$* from the category of $E$-modules to the category of commutative $E$-algebras

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

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

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

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 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 $E$ 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 $\Gamma$ 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 $\Gamma$ to the geometry underlying $E$, moving one step forward from a workable object $\Gamma$ 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 $K(1)$-local power operations.

## 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 of the symmetric group $\Sigma_m$ to obtain individual power operations. These two steps are carried out in Sections 2 and 3 respectively.

In Section 2, by doing calculations with elliptic curves associated to our Morava $E$-theory $E$, we give formulas of the total power operation $\psi^3$ on $E_0$ and the ring $S_3$ parametrizing the corresponding moduli problem.

In Section 3, based on calculations of $E^*B\Sigma_m$ in [Str98] as reflected in the formula of $S_3$, 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 $\Gamma$ for $K(2)$-local commutative $E$-algebras.

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

**Remark 1** The ring $S_3$ turns out to be an algebra on one generator over the base ring where our elliptic curve is defined (cf. Proposition 4 (i)). This generator appears as a parameter in the formulas of the total power operation $\psi^3$, 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 $\Gamma$. 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 at the identity (cf. Proposition 4 (iv) and Remark 6). This choice of parameter is important for writing down Adem relations in Proposition 12 (iv), and it fits naturally into the treatment of gradings in [Rez09] (cf. Example 15 and Theorem 16).

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]. Our calculations follow a recipe in hope of generalizing to other Morava $E$-theories at 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 encouragement on this work, and for his observation in a correspondence which led to Proposition 8 and Corollary 9. 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

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

to denote a field with $q$ elements, 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 $R^\times$ denotes the group of invertible elements of $R$, and $R[\![x]\!]$ denotes the ring of formal power series over $R$ in the variable $x$. If $I \subset R$ is an ideal, then $R^\wedge_I$ 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 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

### 2.1 An elliptic curve and the corresponding Morava $E$-theory spectrum

The universal generalized 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 $\mathbb{Z}[1/4][a,c]$ with $|a| = 1$ and $|c| = 2$. This equation is computed from a general affine Weierstrass equation in $xy$-coordinates, by requiring that the chosen point $P$ of $C$ be $(0,0)$, $2P$ be on the $x$-axis, and $4P$ be the identity at the infinity (cf. [Hus04, 4(4.6a)]).

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

$$y^2 + axy + ay = x^3 + x^2 \tag{1}$$

over the ring $\mathbb{Z}[1/4][a]$, with discriminant $\Delta = a^2(a+4)(a-4)$. Let

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

over which $C$ is nonsingular. Over a finite field of characteristic 3, this nonsingular elliptic curve is supersingular precisely when the quantity

$$h := a^2 + 4 \tag{2}$$

vanishes (cf. [Sil09, V.4.1a]), and its minimal field of definition is then $\mathbb{F}_9$. Moreover the supersingular locus in this coordinate chart consists of a single closed point, as $(3,h)$ is a maximal ideal of $S$.

We next write

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

Let $i$ be an element generating $\mathbb{Z}_9$ over $\mathbb{Z}_3$ with $i^2 = -1$; then since $h = a^2 + 4$, we have

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

where $(3,h)$ is the maximal ideal of the complete local ring $\widehat{S} = \mathbb{Z}_9[\![h]\!]$. By Hensel's lemma, both $a$ and $\Delta$ lie in $\widehat{S}$, and both are invertible. Thus $\widehat{S}$ is the completion of $S$ with respect to $(3,h)$.

Let $\widehat{C}$ be the formal completion of $C$ at the identity; it is a formal group over $\widehat{S}$. Its reduction to $\mathbb{F}_9 = \widehat{S}/(3,h)$ is a formal group $\mathbb{G}$ of height 2. By Serre–Tate theory, 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 $\mathbb{G}$. Let $E$ be the commutative $S$-algebra representing the Morava $E$-theory associated to $\mathbb{G}$; then

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

with $|u| = 2$, where $u$ corresponds to a local uniformizer at the identity of $C$.

## 2.2 The 3-torsion points on the elliptic curve

To study $C$ at the 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 $O$ of $C$ is then $(u,v) = (0,0)$, with $u$ a local uniformizer at $O$. The Weierstrass equation (1) of $C$ becomes

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

**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 $f, g \in S[u]$ are given by*

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

**Proof** [1] Given the elliptic curve $C$ with equation (1), a nonzero point $Q$ on $C$ 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 a homogeneous polynomial in $u$ and $v$

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

As $Q = (d, e)$ in $uv$-coordinates, we then have $\widetilde{\psi}_3(d, e) = 0$.

To get the polynomial $f$, we rewrite the equation (3) of $C$ as a quadratic equation in $v$

$$av^2 + (-u^2 + au + 1)v - u^3 = 0, \tag{4}$$

where the leading coefficient $a$ is invertible in $S = \mathbb{Z}[1/4][a, \Delta^{-1}]$, as the discriminant of the elliptic curve $\Delta = a^2(a + 4)(a - 4)$ is invertible. Define

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

where $v$ and $\bar{v}$ are formally the conjugate roots of (4) so that we compute $\widetilde{f}$ in terms of $u$ by substituting $v + \bar{v}$ as $(u^2 - au - 1)/a$, and $v\bar{v}$ as $-u^3/a$. We then factor $\widetilde{f}$ over $S$ as

$$\widetilde{f}(u) = -\frac{u^4 f(u)}{a^2}, \tag{5}$$

[1] See Appendix A.1 for formulas of the polynomials $\widetilde{f}$, $Q_1$, $R_1$, $Q_2$, $R_2$, $S$, $T$, $M$, and $N$ that appear below.

where $f$ is the stated degree-8 polynomial. We check that $f$ is irreducible by applying Eisenstein's criterion to the prime ideal $(3,h)$ of the unique factorization domain $S$; in particular,

$$\begin{aligned} f(u) &\equiv u^2(u^6+ahu^3-h) \mod 3 \\ &\equiv u^8 \mod (3,h). \end{aligned} \tag{6}$$

We have $\widetilde{f}(d)=0$; to see $f(d)=0$, consider the closed subscheme $C[3]^\times$ of points of exact order 3. It is finite over $S$ of rank 8: after suitable base change (say over a geometric point which is not the supersingular locus), its associated effective Cartier divisor is the sum of the 8 degree-1 effective Cartier divisors associated to the 8 nonzero 3-torsion points. By the Cayley–Hamilton theorem, as a global section of $C[3]^\times$, $u$ locally satisfies a degree-8 equation, and this equation then locally defines the rank-8 subscheme $C[3]^\times$. Thus as a closed subscheme of the affine scheme $C$ over $S$, $C[3]^\times$ is globally defined by a degree-8 equation in $u$. In view of $\widetilde{f}(d)=0$ and (5), we then determine this equation and get the first stated identity

$$f(d)=0.$$

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

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

and the quadratic polynomial

$$B(v) \coloneqq av^2+(-d^2+ad+1)v-d^3$$

vanish at $e$, and thus so does their greatest common divisor (gcd). Using the Euclidean algorithm, 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

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

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

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

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

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

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

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

where $g$ is as stated. □

**Remark 3** In (6), 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 the formal neighborhood of the identity.

## 2.3 The universal degree-3 isogeny and the corresponding total power operation

**Proposition 4**

*(i) The universal degree-3 isogeny $\psi$ with source $C$ is defined over the ring*

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

*where*

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

*and has target the elliptic curve*

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

*where*

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

*(ii) The isogeny $\psi$ restricts to the supersingular locus as the third-power Frobenius isogeny.*

*(iii) The kernel of $\psi$ is generated by a 3-torsion point with coordinates $(d, e)$ satisfying*

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

*(iv) The induced map $\psi^*$ on relative cotangent spaces at the identity sends $du$ to $\alpha du$.*

**Proof** [2] Let $P = (u, v)$ be a general point on $C$, and $Q = (d, e)$ be a nonzero 3-torsion point. Rewriting the equation (3) of $C$ as

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

we express $v$ in terms of a formal 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.

We define functions $u'$ and $v'$ by

$$\begin{aligned} u' &= u(P) \cdot u(P - Q) \cdot u(P + Q), \\ v' &= v(P) \cdot v(P - Q) \cdot v(P + Q), \end{aligned} \tag{7}$$

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 $v'$ in terms of formal power series in $u$:

$$\begin{aligned} u' &= \alpha u + \text{higher degree terms}, \\ v' &= \beta u^3 + \text{higher degree terms}, \end{aligned} \tag{8}$$

where the coefficients ($\alpha$, $\beta$, etc.) involve $a$ and $d$.

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

$$u\big(\psi(P)\big) = u' \qquad \text{and} \qquad v\big(\psi(P)\big) = \frac{\alpha^3}{\beta} \cdot v', \tag{9}$$

where we introduce the normalizing factor $\alpha^3/\beta$ so that the equation of $C'$ will be in the form of (3). The kernel of $\psi$ is precisely the order-3 subgroup generated by $Q$. Using (8), we then determine the coefficients of a general Weierstrass equation that $u\big(\psi(P)\big)$ and $v\big(\psi(P)\big)$ satisfy. This is the stated equation of $C'$ in (i).

We next check the statement of (ii). Recall that the ideal $(3, h)$ of $S$ corresponds to the supersingular locus $\mathbb{F}_9 = S/(3, h)$. Since there is no nonzero 3-torsion point over the supersingular locus, we have

$$d \equiv e \equiv 0 \mod (3, h).$$

Using this congruence and the formulas (17) (18) of $u(P-Q)$ and $u(P+Q)$ in Appendix A.2, we compute that

$$u\big(\psi(P)\big) = u(P) \cdot u(P - Q) \cdot u(P + Q) \equiv u^3 \mod (3, h). \tag{10}$$

[2] See Appendix A.2 for formulas of the power series expansion of $v$ and the calculations involving the group law on $C$ that appear below.

As the $u$-coordinate is a local uniformizer at the identity, $\psi$ restricts to the supersingular locus as the third-power Frobenius isogeny.

For the remaining statements of the proposition, in (iii), the first formula of $\alpha$ in terms of $a$ and $d$ is computed in (8). We then check the second formula of $\alpha$ in terms of $a$, $d$, and $e$ by comparing the previous one with the formula of $g$ in Proposition 2. In view of $f(d) = 0$ as in Proposition 2, we further compute that $\alpha$ satisfies $w(\alpha) = 0$ where $w$ is as stated in (i). The statement of (iv) follows by definition of $\alpha$ in (8). □

**Remark 5** In view of Proposition 4 (ii), the formal completion of $\psi\colon C \to C'$ at the identity of $C$ is a *deformation of the third-power Frobenius isogeny*, in the sense of [Rez09, 11.3]. When it is clear from the context, we will simply call $\psi$ itself a deformation of the third-power Frobenius isogeny.

**Remark 6** The parameter $\alpha$ is invariant under change of coordinates: if

$$\widetilde{u} := \sum_{i=1}^{\infty} a_i u^i \qquad \text{and} \qquad \widetilde{u}' := \sum_{i=1}^{\infty} a_i (u')^i,$$

where $a_i \in S$ and $a_1 \in S^\times$, then

$$\widetilde{u}' = \alpha \widetilde{u} + \text{higher degree terms}.$$

We also note that the analog of $\alpha$ at the prime 2 coincides with $d$ which is 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]).

In [Str98] Strickland shows that

$$\widehat{S}_3 \cong E^0 B\Sigma_3 / I,$$

where

$$\widehat{S}_3 := S_3 \otimes_S \widehat{S} = \big(S_3\big)^{\wedge}_{(3,h)},$$

and

$$I := \bigoplus_{0<i<3} \operatorname{image}\big(E^0 B(\Sigma_i \times \Sigma_{3-i}) \xrightarrow{\text{transfer}} E^0 B\Sigma_3\big) \tag{11}$$

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 7** *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*

$$\begin{aligned}\psi^3(h) &= h^3 + (\alpha^3 - 6\alpha - 36)h^2 + 3(-8\alpha^3 + \alpha^2 + 48\alpha + 130)h \\ &\quad + 4(30\alpha^3 - 9\alpha^2 - 178\alpha - 303),\\ \psi^3(a) &= a^3 + (\alpha^3 - 6\alpha - 12)a - 4(\alpha+1)^2(\alpha-3)a^{-1}.\end{aligned}$$

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

# 3 Individual power operations

## 3.1 Composition of deformations of Frobenius isogenies

Recall from Proposition 4 that 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, $\psi$ is a deformation of the third-power Frobenius isogeny over the supersingular locus. We want to construct a similar isogeny $\psi'$ 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 $C'$. We then define $\psi'\colon\ C' \to C'/G'$ using a nonzero point in $G'$ as in the proof of Proposition 4 (cf. (9) and (7)).

As the equation of $C'$ in Proposition 4 (i) is in the form of (3), let $a' = r(a)$, $h' = (a')^2 + 4$, and write

$$S' = \mathbb{Z}[1/4][a', (\Delta')^{-1}] \qquad \text{and} \qquad S'_3 = S'[\alpha']/\big(w'(\alpha')\big), \tag{12}$$

where

$$\Delta' = (a')^2(a'+4)(a'-4) \quad \text{and} \quad w'(\alpha') = (\alpha')^4 - 6(\alpha')^2 + \big((a')^2 - 8\big)\alpha' - 3.$$

We then check as in the proof of Proposition 4 (cf. (10)) that the congruence

$$u\big(\psi'(P)\big) \equiv u^3 \mod (3, h')$$

holds, so that $\psi'$ is also a deformation of the third-power Frobenius isogeny.

**Proposition 8** *The following diagram of elliptic curves over $S_3$ commutes:*

$$\begin{array}{ccc} C & \xrightarrow{\quad\psi\quad} & C/G = C' \\ & \searrow^{[-3]} & \downarrow{\scriptstyle \psi'} \\ & & C \cong C/C[3] \cong \frac{C/G}{C[3]/G} = \frac{C'}{G'}, \end{array} \tag{13}$$

*where the isomorphisms in the bottom row are the canonical ones.*

**Proof** In view of (2), over the supersingular locus $\mathbb{F}_9$ the equation of $C$ is

$$y^2 + ixy + iy = x^3 + x^2,$$

where $i$ is an element generating $\mathbb{F}_9$ over $\mathbb{F}_3$ with $i^2 = -1$. Let $\psi_0$ and $\psi_0'$ be the restrictions of $\psi$ and $\psi'$ over $\mathbb{F}_9$ respectively. As they are the third-power Frobenius isogenies, we have

$$\psi_0 \colon C \to C' \qquad \text{and} \qquad \psi_0' \colon C' \to C,$$

where $C'$ has equation

$$y^2 - ixy - iy = x^3 + x^2.$$

Thus the composite $\psi_0' \circ \psi_0$ is the ninth-power Frobenius endomorphism of $C$ over $\mathbb{F}_9$. We claim that this composite coincides with the endomorphism $[-3]$.

Consider the elliptic curve

$$\widetilde{C} \colon y^2 = x^3 + x - 1 \tag{14}$$

over $\mathbb{F}_3$. It is supersingular by [Sil09, V.4.1a], and over $\mathbb{F}_9$ it is isomorphic to $C$ via

$$x \mapsto x, \qquad y \mapsto y - ix - i.$$

Let $\widetilde{\psi}_0$ be the third-power Frobenius endomorphism of $\widetilde{C}$. By [Sil09, V.2.3.1b], $\widetilde{\psi}_0$ satisfies

$$\widetilde{\psi}_0^2 - A\widetilde{\psi}_0 + 3 = 0$$

in the endomorphism ring of $\widetilde{C}$, where $A = 4 - |\widetilde{C}(\mathbb{F}_3)|$ with $|\widetilde{C}(\mathbb{F}_3)|$ the number of $\mathbb{F}_3$-rational points on $\widetilde{C}$. Since each value of $x$ gives at most two values for $y$ in (14), $|\widetilde{C}(\mathbb{F}_3)| \leq 2 \cdot 3 + 1 = 7$. Moreover since $\widetilde{C}$ is supersingular, $A \equiv 0 \mod 3$ (cf. the proof of [Sil09, V.4.1a]). Thus $A = 0$, 3, or $-3$. We exclude the latter two possibilities by checking the action of $\widetilde{\psi}_0$ at the 2-torsion point $(-1, 0)$. Thus the ninth-power Frobenius endomorphism $\widetilde{\psi}_0^2$ agrees with $[-3]$ on $\widetilde{C}$ over $\mathbb{F}_3$. Since $C$

and $\widetilde{C}$ are isomorphic over $\mathbb{F}_9$, the composite $\psi_0' \circ \psi_0$, as the ninth-power Frobenius endomorphism on $C$, then coincides with $[-3]$ as claimed.

It remains to show that $\psi_0' \circ \psi_0 = [-3]$ over $\mathbb{F}_9$ lifts to

$$\psi' \circ \psi = [-3]\colon\ C \to C'/G'$$

over $S_3$, where by abuse of notation $[-3]$ denotes the endomorphism $[-3]$ of $C$ composed with the canonical isomorphisms from $C$ to $C'/G'$. This is done by a rigidity argument, as $\psi' \circ \psi$ and $[-3]$ are morphisms of abelian schemes over a connected base scheme (cf. [MFK94, Proposition 6.1 and Corollary 6.2], and see Appendix B for details). □

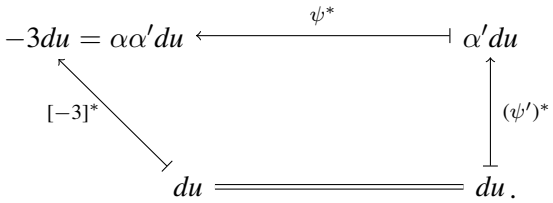
**Corollary 9** *The following relations hold in $S_3$:*

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

*and*

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

**Proof** The isogenies in (13) induce maps on relative cotangent spaces at the identity, so that by Proposition 4 (iv) we have a commutative diagram




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

**Remark 10** As noted in Remark 6, the analog of $\alpha$ at the prime 2 coincides with the parameter $d$ used in [Rezb, Section 3]. In particular, with the notations there, $d$ and $d'$ satisfy an analogous relation $dd' + 2 = 0$.

## 3.2 Individual power operations

Let $A$ be a $K(2)$-local commutative $E$-algebra. By [Rez09, 3.23] and Corollary 7, we have a total power operation

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

With the notations in (12), we also have a composite of total power operations

(15)

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

where elements in $M \,{}^{\psi^3}\!\otimes_{E_0} N$ are subject to the equivalence relations

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

for $m \in M$, $n \in N$, and $r \in E_0$, as well as

$$1 \otimes \alpha' \sim \psi^3(\alpha) \otimes 1$$

with $\psi^3(\alpha) = -\alpha^3 + 6\alpha + (-h+12)$ by Corollary 9.

**Definition 11** 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 12** *The following relations hold among the individual power operations $Q_0$, $Q_1$, $Q_2$, and $Q_3$:*

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

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

*(iii)* *Commutation relations*

$$\begin{aligned}
Q_0(hx) &= (h^3 - 36h^2 + 390h - 1212)Q_0(x) + (3h^2 - 72h + 360)Q_1(x) \\
&\quad + (9h - 108)Q_2(x) + 24Q_3(x), \\
Q_1(hx) &= (-6h^2 + 144h - 712)Q_0(x) + (-18h + 228)Q_1(x) + (-72)Q_2(x) \\
&\quad + (h - 12)Q_3(x), \\
Q_2(hx) &= (3h - 36)Q_0(x) + 8Q_1(x) + 12Q_2(x) + (-24)Q_3(x), \\
Q_3(hx) &= (h^2 - 24h + 120)Q_0(x) + (3h - 36)Q_1(x) + 8Q_2(x) + 12Q_3(x), \\
Q_0(ax) &= (a^3 - 12a + 12a^{-1})Q_0(x) + (3a - 12a^{-1})Q_1(x) + (12a^{-1})Q_2(x) \\
&\quad + (-12a^{-1})Q_3(x), \\
Q_1(ax) &= (-6a + 20a^{-1})Q_0(x) + (-20a^{-1})Q_1(x) + (-a + 20a^{-1})Q_2(x) \\
&\quad + (4a - 20a^{-1})Q_3(x), \\
Q_2(ax) &= (4a^{-1})Q_0(x) + (-4a^{-1})Q_1(x) + (4a^{-1})Q_2(x) + (-a - 4a^{-1})Q_3(x), \\
Q_3(ax) &= (a - 4a^{-1})Q_0(x) + (4a^{-1})Q_1(x) + (-4a^{-1})Q_2(x) + (4a^{-1})Q_3(x);
\end{aligned}$$

*(iv) Adem relations*

$$\begin{aligned}
Q_1Q_0(x) &= (-6)Q_0Q_1(x) + (6h-72)Q_0Q_2(x)\\
&\quad + (-6h^2+144h-747)Q_0Q_3(x) + 18Q_1Q_2(x) + 3Q_2Q_1(x)\\
&\quad + (-18h+216)Q_1Q_3(x) + (-54)Q_2Q_3(x) + (-9)Q_3Q_2(x),\\
Q_2Q_0(x) &= (-3)Q_0Q_2(x) + (3h-36)Q_0Q_3(x) + 9Q_1Q_3(x) + 3Q_3Q_1(x),\\
Q_3Q_0(x) &= Q_0Q_1(x) + (-h+12)Q_0Q_2(x) + (h^2-24h+126)Q_0Q_3(x)\\
&\quad + (-3)Q_1Q_2(x) + (3h-36)Q_1Q_3(x) + 9Q_2Q_3(x);
\end{aligned}$$

*(v) Cartan formulas*

$$\begin{aligned}
Q_0(xy) &= Q_0(x)Q_0(y) + 3\big(Q_1(x)Q_3(y) + Q_2(x)Q_2(y) + Q_3(x)Q_1(y)\big)\\
&\quad + 18Q_3(x)Q_3(y),\\
Q_1(xy) &= \big(Q_0(x)Q_1(y) + Q_1(x)Q_0(y)\big)\\
&\quad + (-h+12)\big(Q_1(x)Q_3(y) + Q_2(x)Q_2(y) + Q_3(x)Q_1(y)\big)\\
&\quad + 3\big(Q_2(x)Q_3(y) + Q_3(x)Q_2(y)\big) + (-6h+72)Q_3(x)Q_3(y),\\
Q_2(xy) &= \big(Q_0(x)Q_2(y) + Q_1(x)Q_1(y) + Q_2(x)Q_0(y)\big)\\
&\quad + 6\big(Q_1(x)Q_3(y) + Q_2(x)Q_2(y) + Q_3(x)Q_1(y)\big)\\
&\quad + (-h+12)\big(Q_2(x)Q_3(y) + Q_3(x)Q_2(y)\big) + 39Q_3(x)Q_3(y),\\
Q_3(xy) &= \big(Q_0(x)Q_3(y) + Q_1(x)Q_2(y) + Q_2(x)Q_1(y) + Q_3(x)Q_0(y)\big)\\
&\quad + 6\big(Q_2(x)Q_3(y) + Q_3(x)Q_2(y)\big) + (-h+12)Q_3(x)Q_3(y);
\end{aligned}$$

*(vi) Frobenius congruence*

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

**Proof** The relations in (i), (ii), (iii), and (v) follow from the fact that $\psi^3$ is a ring homomorphism together with the formulas in Corollary 7.

For (iv), given the correspondence between power operations and deformations of Frobenius isogenies in [Rez09, Theorem B], (13) implies that the composite (15) lands in $A_0$. In terms of formulas, we have

$$\begin{aligned}
\psi^3\big(\psi^3(x)\big) &= \psi^3\big(Q_0(x) + Q_1(x)\alpha + Q_2(x)\alpha^2 + Q_3(x)\alpha^3\big)\\
&= \psi^3\big(Q_0(x)\big) + \psi^3\big(Q_1(x)\big)\alpha' + \psi^3\big(Q_2(x)\big)(\alpha')^2 + \psi^3\big(Q_3(x)\big)(\alpha')^3\\
&= \sum_{i,\,j\,=\,0}^{3} Q_iQ_j(x)\alpha^i\big(-\alpha^3 + 6\alpha + (-h+12)\big)^j\\
&\equiv \Psi_0(x) + \Psi_1(x)\alpha + \Psi_2(x)\alpha^2 + \Psi_3(x)\alpha^3 \mod \big(w(\alpha)\big),
\end{aligned}$$

where each $\Psi_k$ is a linear combination of the $Q_iQ_j$'s. The vanishing of $\Psi_1(x)$, $\Psi_2(x)$, and $\Psi_3(x)$ then gives the three relations in (iv).

For (vi), note that in Definition 11, we have

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

by [Rez09, Propositions 3.25 and 10.5], and

$$\alpha \equiv 0 \mod 3$$

by Remark 3 and Proposition 4 (iii). The congruence in (vi) then follows by definition of $Q_0$. □

### 3.3 The Dyer–Lashof algebra of power operations

**Definition 13** Define $\gamma$ to be the associative ring generated over $\mathbb{Z}_9[\![h]\!]$ 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 $\mathbb{Z}_9 \subset \mathbb{Z}_9[\![h]\!]$, and that

$$\begin{aligned}
q_0h &= (h^3 - 36h^2 + 390h - 1212)q_0 + (3h^2 - 72h + 360)q_1 + (9h - 108)q_2 + 24q_3,\\
q_1h &= (-6h^2 + 144h - 712)q_0 + (-18h + 228)q_1 + (-72)q_2 + (h - 12)q_3,\\
q_2h &= (3h - 36)q_0 + 8q_1 + 12q_2 + (-24)q_3,\\
q_3h &= (h^2 - 24h + 120)q_0 + (3h - 36)q_1 + 8q_2 + 12q_3.
\end{aligned}$$

The Adem relations are

$$\begin{aligned}
q_1q_0 &= (-6)q_0q_1 + (6h - 72)q_0q_2 + (-6h^2 + 144h - 747)q_0q_3 + 18q_1q_2 + 3q_2q_1\\
&\quad + (-18h + 216)q_1q_3 + (-54)q_2q_3 + (-9)q_3q_2,\\
q_2q_0 &= (-3)q_0q_2 + (3h - 36)q_0q_3 + 9q_1q_3 + 3q_3q_1,\\
q_3q_0 &= q_0q_1 + (-h + 12)q_0q_2 + (h^2 - 24h + 126)q_0q_3 + (-3)q_1q_2 + (3h - 36)q_1q_3\\
&\quad + 9q_2q_3.
\end{aligned}$$

**Remark 14** In the above definition of $\gamma$, an element $r \in \mathbb{Z}_9[\![h]\!] = E_0$ corresponds to the multiplication-by-$r$ operation (cf. [Rez09, Proposition 6.4]), and each $q_i$ corresponds to the individual power operation $Q_i$. Under this correspondence, the relations in Proposition 12 (i)(iii)(iv)(v) describe explicitly the structure of $\gamma$ as that of a *graded twisted bialgebra over* $E_0$ in the sense of [Rez09, Section 5]. The grading of $\gamma$ comes from the number of the $q_i$'s in a monomial: for example, commutation relations are in degree 1, and Adem relations are in degree 2. In particular it follows using these

relations that $\gamma$ has an *admissible basis*: it is free as a left $E_0$-module on the elements of the form

$$q_0^s q_{k_1} \cdots q_{k_t},$$

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

**Example 15** We have $E^0 S^2 \cong \mathbb{Z}_9[\![h]\!][u]/(u^2)$. By definition of $\alpha$ in (8), 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 $\omega$ be the kernel of $E^0 S^2 \to E^0$. It is a *$\gamma$-module* on one generator $u$ in the sense of [Rezb, 2.2], and its $\gamma$-module structure is canonical as above via the correspondence between $q_i$ and $Q_i$.

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

**Theorem 16** *Let $A$ be a $K(2)$-local commutative $E$-algebra. Let $\gamma$ be the graded twisted bialgebra over $E_0$ given in Definition 13, and let $\omega$ be the $\gamma$-module given in Example 15. Then $A_*$ is an $\omega$-twisted $\mathbb{Z}/2$-graded amplified $\gamma$-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 $\omega$-twisted $\mathbb{Z}/2$-graded amplified $\gamma$-ring on one generator in degree $d$.*

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

**Proof** Let $\Gamma$ be the graded twisted bialgebra of power operations on $E_0$ described in [Rez09, Section 6]. It suffices to identify $\Gamma$ with $\gamma$. 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]). There is a degree-preserving ring homomorphism $\phi\colon\ \gamma \to \Gamma$ which is an isomorphism in degrees 0 and 1 (cf. Remark 14). 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 by a transfer argument (cf. [Reza, Propositions 10.5 and 10.9]), $\Gamma$ is generated in degree 1, and hence $\phi$ is surjective. Since $\gamma[d]$ and $\Gamma[d]$ are of the same rank $1 + 3 + \cdots + 3^d$ as free modules over $E_0$ by Remark 14 and [Str98, Theorem 1.1]) respectively, $\phi$ is also injective. □

# 4 $K(1)$-local power operations

Let $F = L_{K(1)}E$. The general pattern of the relationship between $K(1)$-local power operations and the power operations in Section 2.3 is as follows:

$$\begin{array}{ccccc} E^0 & \xrightarrow{\psi^3} & E^0B\Sigma_3/I & & \\ \downarrow & & \downarrow & & \\ F^0 & \xrightarrow{\psi^3_F} & F^0B\Sigma_3/J & \xleftarrow{\cong} & F^0, \end{array}$$

where $\psi^3_F$ is the $K(1)$-local power operation induced by $\psi^3$, and $J \cong F^0 \otimes_{E^0} I$ is the transfer ideal (cf. (11)). Recall from Proposition 4 (i) and Corollary 7 that $\psi^3$ arises from the universal degree-3 isogeny which is parametrized by the ring $S_3$ with

$$\widehat{S}_3 = \big(S_3\big)^{\wedge}_{(3,h)} \cong E^0B\Sigma_3/I.$$

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 $h$ (so that the resulting formal group is of height at most 1) and completing at the prime 3 (cf. [Hov97, Corollary 1.5.5]):

$$E_* = \mathbb{Z}_9[\![h]\!][u^{\pm 1}] \qquad \text{and} \qquad F_* = \mathbb{Z}_9[\![h]\!][h^{-1}]^{\wedge}_3[u^{\pm 1}];$$

more explicitly,

$$F_0 = \mathbb{Z}_9(\!(h)\!)^{\wedge}_3 = \varprojlim_k \mathbb{Z}_9(\!(h)\!)/(3^k) = \left\{ \sum_{n=-\infty}^{\infty} c_n h^n \;\middle|\; c_n \in \mathbb{Z}_9, \lim_{n\to-\infty} c_n = 0 \right\}. \tag{16}$$

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

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

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 $\widehat{C}$ 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 $\psi^3_F$.

As in Proposition 4 (i), the ring

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

parametrizes order-3 subgroups of $C$. Since

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

the equation $w(\alpha) = 0$ has a unique root $\alpha = 0$ in $\mathbb{F}_3(\!(h)\!)$ (in view of (16), $\alpha^3 + h$ cannot be zero). By Hensel's lemma this unique root lifts to a root in $\mathbb{Z}_9(\!(h)\!)^\wedge_3$; it corresponds to the unique order-3 subgroup of $\widehat{C}$ over $F^0 = \mathbb{Z}_9(\!(h)\!)^\wedge_3$. Plugging this specific value of $\alpha$ into the formulas of $\psi^3$ in Corollary 7, we then get an endomorphism of the ring $F^0$. This endomorphism is the $K(1)$-local power operation $\psi^3_F$.

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

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

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

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

Similarly, substituting $h$ by $a^2 + 4$ in $w(\alpha) = 0$, we solve for $\alpha$ in terms of $a$ and get

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

# Appendices

# A Lists of long formulas

The calculations in this paper involve power series expansions and basic 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.1 Formulas in the proof of Proposition 2

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

$$
\begin{aligned}
Q_1(v) &= av^2 + (d^2 + 2ad - 1)v + \frac{d^4}{a} + 2d^3 + ad^2 - \frac{2d^2}{a} - d + \frac{1}{a},\\
R_1(v) &= (\frac{d^6}{a} + 2d^5 + ad^4 - \frac{3d^4}{a} + 2d^3 + \frac{3d^2}{a} - \frac{1}{a})v + \frac{d^7}{a} + 2d^6 + ad^5 - \frac{2d^5}{a}\\
&\quad + 2d^4 + \frac{d^3}{a},\\
Q_2(v) &= \frac{a}{(d^6 + 2ad^5 + a^2d^4 - 3d^4 + 2ad^3 + 3d^2 - 1)^2}\big((ad^6 + 2a^2d^5 + a^3d^4 - 3ad^4\\
&\quad + 2a^2d^3 + 3ad^2 - a)v - d^8 - 2ad^7 - a^2d^6 + 4d^6 - ad^5 + a^2d^4 - 6d^4\\
&\quad + 4ad^3 + 4d^2 - ad - 1\big),\\
R_2 &= -\frac{ad^4}{(d^6 + 2ad^5 + a^2d^4 - 3d^4 + 2ad^3 + 3d^2 - 1)^2}(d^8 + 3ad^7 + 3a^2d^6 + a^3d^5\\
&\quad + 7ad^5 + 6a^2d^4 - 6d^4 + 9ad^3 - a^2d^2 + 8d^2 - 3ad - 3),\\
S(d) &= \frac{d^6}{a} + 2d^5 + ad^4 - \frac{3d^4}{a} + 2d^3 + \frac{3d^2}{a} - \frac{1}{a},\\
T(d) &= \frac{d^7}{a} + 2d^6 + ad^5 - \frac{2d^5}{a} + 2d^4 + \frac{d^3}{a},\\
M(u) &= \frac{1}{a^{16} - 64a^{14} + 1536a^{12} - 16384a^{10} + 65536a^8}\big((10a^{13} - 432a^{11} + 6144a^9\\
&\quad - 28672a^7)u^5 + (19a^{14} - 825a^{12} + 11792a^{10} - 55040a^8 - 4096a^6)u^4\\
&\quad + (8a^{15} - 382a^{13} + 6384a^{11} - 41984a^9 + 77824a^7)u^3 + (-a^{16} + 66a^{14}\\
&\quad - 1610a^{12} + 17248a^{10} - 69120a^8 + 8192a^6)u^2 + (28a^{13} - 1280a^{11}\\
&\quad + 19456a^9 - 98304a^7)u - 4a^{14} + 179a^{12} - 2672a^{10} + 13568a^8 - 4096a^6\big),\\
N(u) &= -\frac{a}{a^{16} - 64a^{14} + 1536a^{12} - 16384a^{10} + 65536a^8}\big((10a^{13} - 432a^{11}\\
&\quad + 6144a^9 - 28672a^7)u^7 + (29a^{14} - 1257a^{12} + 17936a^{10} - 83712a^8\\
&\quad - 4096a^6)u^6 + (27a^{15} - 1177a^{13} + 16880a^{11} - 78592a^9 - 12288a^7)u^5\\
&\quad + (7a^{16} - 239a^{14} + 1435a^{12} + 22928a^{10} - 213760a^8 - 4096a^6)u^4 + (-a^{17}\\
&\quad + 98a^{15} - 3082a^{13} + 40272a^{11} - 199680a^9 + 135168a^7)u^3 + (-4a^{16}\\
&\quad + 265a^{14} - 6555a^{12} + 71856a^{10} - 296192a^8 + 20480a^6)u^2 + (-12a^{15}\\
&\quad + 621a^{13} - 11856a^{11} + 99072a^9 - 307200a^7)u + a^{16} - 76a^{14} + 2073a^{12}\\
&\quad - 24400a^{10} + 106240a^8 - 12288a^6\big).
\end{aligned}
$$

## A.2 Formulas in the proof of Proposition 4

$$v = u^3 - au^4 + (a^2+1)u^5 + (-a^3-3a)u^6 + (a^4+6a^2+1)u^7 + (-a^5-10a^3 - 6a)u^8 + (a^6+15a^4+20a^2+1)u^9 + \text{higher degree terms.}$$

The group law on $C$ 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
$$k = \frac{v_1 - v_2}{u_1 - u_2} \qquad \text{and} \qquad b = \frac{u_1v_2 - u_2v_1}{u_1 - u_2}.$$

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

- set
$$(u_1,v_1) = \left(-\frac{v}{u(u+v)}, -\frac{v^2}{u^2(u+v)}\right) \qquad \text{and} \qquad (u_2,v_2) = (d,e),$$
so that
$$P - Q = (u_3, v_3); \tag{17}$$
- set
$$(u_1,v_1) = (u,v) \qquad \text{and} \qquad (u_2,v_2) = (d,e),$$
so that
$$P + Q = \left(-\frac{v_3}{u_3(u_3+v_3)}, -\frac{v_3^2}{u_3^2(u_3+v_3)}\right). \tag{18}$$

Plugging the coordinates of $P-Q$ and $P+Q$ into (7), and in view of $f(d)=0$ as in Proposition 2, we then have in (8)

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

$$\beta = -\frac{1}{a^2(a+4)(a-4)}\big((a^3-11a)d^7 + (3a^4-33a^2-4)d^6 + (3a^5-33a^3 - 15a)d^5 + (a^6-4a^4-96a^2-4)d^4 + (6a^5-80a^3+31a)d^3 + (10a^4 - 153a^2+20)d^2 + (3a^3-117a)d - 6a^2 - 12\big).$$

We have the normalizing factor

$$\frac{\alpha^3}{\beta} = -\frac{1}{(a+4)(a-4)}\big(3ad^7 + (9a^2-4)d^6 + (9a^3-13a)d^5 + (3a^4+6a^2+12)d^4 + (11a^3-15a)d^3 + (-a^4+21a^2-12)d^2 + (-3a^3+9a)d - 4a^2 + 4\big).$$

More extended formulas for $u'$ and $v'$ in (8) are needed to determine the coefficients in the Weierstrass equation of $C'$:

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

$$
\begin{aligned}
&- 124ad^2 - 30a^4d + 546a^2d - 6a^3 + 204a)u^4 + (3a^5d^7 - 38a^3d^7 - 107ad^7\\
&+ 9a^6d^6 - 108a^4d^6 - 409a^2d^6 - 4d^6 + 9a^7d^5 - 96a^5d^5 - 590a^3d^5 - 47ad^5\\
&+ 3a^8d^4 + a^6d^4 - 646a^4d^4 - 912a^2d^4 - 4d^4 + 24a^7d^3 - 292a^5d^3 - 1249a^3d^3\\
&+ 639ad^3 + 70a^6d^2 - 1057a^4d^2 - 849a^2d^2 + 20d^2 + 93a^5d - 1512a^3d\\
&- 597ad + 48a^4 - 870a^2 - 12)u^5 + (-4a^6d^7 + 24a^4d^7 + 583a^2d^7 - 12a^7d^6\\
&+ 60a^5d^6 + 1923a^3d^6 + 156ad^6 - 12a^8d^5 + 36a^6d^5 + 2268a^4d^5 + 639a^2d^5\\
&- 4a^9d^4 - 40a^7d^4 + 1256a^5d^4 + 5128a^3d^4 + 140ad^4 - 36a^8d^3 + 229a^6d^3\\
&+ 5409a^4d^3 - 2227a^2d^3 - 127a^7d^2 + 1597a^5d^2 + 6835a^3d^2 - 748ad^2\\
&- 201a^6d + 2952a^4d + 5277a^2d - 129a^5 + 2130a^3 + 708a)u^6 + (5a^7d^7\\
&+ 35a^5d^7 - 1754a^3d^7 - 275ad^7 + 15a^8d^6 + 125a^6d^6 - 5511a^4d^6 - 1833a^2d^6\\
&- 4d^6 + 15a^9d^5 + 165a^7d^5 - 5988a^5d^5 - 4312a^3d^5 - 103ad^5 + 5a^{10}d^4\\
&+ 130a^8d^4 - 2183a^6d^4 - 17022a^4d^4 - 2940a^2d^4 - 4d^4 + 50a^9d^3 + 159a^7d^3\\
&- 15035a^5d^3 + 179a^3d^3 + 1703ad^3 + 206a^8d^2 - 1708a^6d^2 - 25304a^4d^2\\
&+ 1431a^2d^2 + 20d^2 + 363a^7d - 4398a^5d - 23694a^3d - 1437ad + 258a^6\\
&- 3816a^4 - 7026a^2 - 12)u^7 + (-6a^8d^7 - 164a^6d^7 + 3864a^4d^7 + 3365a^2d^7\\
&- 18a^9d^6 - 522a^7d^6 + 11837a^5d^6 + 13701a^3d^6 + 448ad^6 - 18a^{10}d^5\\
&- 582a^8d^5 + 12275a^6d^5 + 21828a^4d^5 + 2395a^2d^5 - 6a^{11}d^4 - 296a^9d^4\\
&+ 3283a^7d^4 + 43960a^5d^4 + 30290a^3d^4 + 424ad^4 - 66a^{10}d^3 - 1099a^8d^3\\
&+ 32246a^6d^3 + 30529a^4d^3 - 17045a^2d^3 - 310a^9d^2 + 679a^7d^2 + 66726a^5d^2\\
&+ 24833a^3d^2 - 2192ad^2 - 588a^8d + 4809a^6d + 73578a^4d + 23685a^2d\\
&- 444a^7 + 5316a^5 + 30936a^3 + 1704a)u^8 + (7a^9d^7 + 392a^7d^7 - 6863a^5d^7\\
&- 17458a^3d^7 - 515ad^7 + 21a^{10}d^6 + 1218a^8d^6 - 20647a^6d^6 - 61745a^4d^6\\
&- 6709a^2d^6 - 4d^6 + 21a^{11}d^5 + 1302a^9d^5 - 20664a^7d^5 - 81924a^5d^5\\
&- 22146a^3d^5 - 183ad^5 + 7a^{12}d^4 + 567a^{10}d^4 - 3982a^8d^4 - 97733a^6d^4\\
&- 158644a^4d^4 - 8392a^2d^4 - 4d^4 + 84a^{11}d^3 + 2878a^9d^3 - 57242a^7d^3\\
&- 160981a^5d^3 + 59447a^3d^3 + 3223ad^3 + 442a^{10}d^2 + 2563a^8d^2 - 142138a^6d^2\\
&- 189134a^4d^2 + 18323a^2d^2 + 20d^2 + 885a^9d - 2382a^7d - 179958a^5d\\
&- 164688a^3d - 2637ad + 696a^8 - 5400a^6 - 92938a^4 - 29078a^2 - 12)u^9\\
&+ \text{higher degree terms}\big).
\end{aligned}
$$

# B A rigidity argument

Details of the rigidity argument at the end of the proof of Proposition 8 are given in Section B.1, where a statement on cohomology and base change is needed. Section B.2 gives the proof of this statement.

## B.1 The proof

We continue the notations in Proposition 8. Consider the commutative diagram

$$\begin{array}{ccc} C & \xrightarrow{F} & C'/G' \\ & {\scriptstyle\pi}\searrow \quad \swarrow & \\ & \operatorname{Spec} S_3, & \end{array}$$

where $F$ denotes $\psi' \circ \psi - [-3]$, and $\pi$ is the structure morphism of $C$ over $S_3$. Let

$$Z = \{s \in \operatorname{Spec} S_3 \mid F_s \colon C_s \to (C'/G')_s \text{ is zero}\},$$

where $(-)_s$ denotes the fiber of the structure morphism over $s$ (and we will similarly use $(-)_U$ to denote the restriction over an open subscheme $U$ of the base scheme $\operatorname{Spec} S_3$). By considering the supersingular locus, we have seen that $Z$ is nonempty, and we want to show that $Z = \operatorname{Spec} S_3$. Since $\operatorname{Spec} S_3$ is connected, we need only show that $Z$ is both open and closed.

To see that $Z$ is open, we take $s \in Z$ and show that $F_U = 0$ for some open neighborhood $U$ of $s$. Let $V$ be an affine open neighborhood of the identity of $C'/G'$, disjoint from the closed subscheme $(C'/G')[2]^\times$ of points of exact order 2. Then $F^{-1}(V)$ is an open subscheme of $C$ containing $C_s$. Since $\pi$ is proper, it is closed, and thus $F^{-1}(V)$ contains $\pi^{-1}(U)$ for some affine open neighborhood $U$ of $s$ in $\operatorname{Spec} S_3$. Now $F_U \colon C_U \to C'/G'$ factors through $V$, and we want to show that $F_U = 0$. Since $V$ is affine, $F_U \colon C_U \to V$ factors through $\operatorname{Spec} \Gamma(C_U, \mathscr{O}_{C_U})$. Since $\pi$ is proper, smooth and surjective with geometrically connected fibers, by Corollary 20 of Section B.2 there is an isomorphism

$$\mathscr{O}_{\operatorname{Spec} S_3} \xrightarrow{\cong} \pi_* \mathscr{O}_C$$

of formation compatible with arbitrary base change. In particular, by base change to the affine open subscheme $U$ of $\operatorname{Spec} S_3$, we have $U \cong \operatorname{Spec} \Gamma(C_U, \mathscr{O}_{C_U})$. Thus $F_U$

factors as

$$C_U \xrightarrow{\pi} U \xrightarrow{\sigma} V \subset (C'/G'),$$

where $\sigma$ is a section of $(C'/G')_U$. Since $F_U$ is a morphism of group schemes, $\sigma$ is fixed by $[-1]$, and is hence the identity, as $V$ is disjoint from $(C'/G')[2]^\times$. Thus $F_U = 0$.

To see that $Z$ is closed, note that the inverse image in $C$ of the identity of $C'/G'$ is a closed subscheme of $C$, since $C'/G'$ is separated. Thus its complement $W \subset C$ is open. Since $\pi$ is flat and locally of finite presentation, it is open, and thus $\pi(W)$ is open in $\operatorname{Spec} S_3$. As its complement, $Z$ is then closed.

## B.2 Cohomology and base change

We record two consequences of the theorem on cohomology and base change. They lead to Corollary 20 which is needed in Section B.1. Corollaries 18 and 19 and their proofs are reproduced from a course handout by Brian Conrad.

Recall the following theorem of Grothendieck:

**Theorem 17** [3] *Let $f\colon X \to Y$ be a proper morphism of schemes with $Y$ locally noetherian. Let $\mathscr{F}$ be a coherent sheaf on $X$, flat over $Y$. For $i \geq 0$ and $y \in Y$, assume that the natural map*

$$\phi_y^{(i)}\colon (\mathrm{R}^i f_* \mathscr{F})_y \otimes_{\mathscr{O}_{Y,y}} \kappa(y) \to \mathrm{H}^i(X_y, \mathscr{F}_y)$$

*is surjective. Then $\phi_\eta^{(i)}$ is an isomorphism for all $\eta$ in a neighborhood of $y$, and the following are equivalent:*

*(i) $\phi_y^{(i-1)}$ is surjective;*

*(ii) the finite $\mathscr{O}_{Y,y}$-module $(\mathrm{R}^i f_* \mathscr{F})_y$ is free.*

**Corollary 18** *Let $f\colon X \to Y$ be a proper morphism of schemes with $Y$ locally noetherian. If $f$ is flat, surjective and its geometric fibers are reduced and connected, then the natural map*

$$\mathscr{O}_Y \to f_* \mathscr{O}_X$$

*is an isomorphism.*

[3] Cf. [Har77, III.12.11]. The projectivity assumption there needed for coherence of higher pushforwards can be relaxed as properness by [EGA III$_1$, 3.2.1] (cf. [Har77, III.12.2 and III.8.8.1]).

**Proof** Since $f$ is proper, $f_*\mathscr{O}_X$ is a coherent $\mathscr{O}_Y$-module by [EGA III$_1$, 3.2.1]. We want to show that $f_*\mathscr{O}_X$ is locally free of rank 1 using Theorem 17.

For any $y \in Y$, since $X_y$ is non-empty and proper, $\mathrm{H}^0(X_y, \mathscr{O}_{X_y})$ is a nonzero finite-dimensional $\kappa(y)$-algebra, and its formation is compatible with arbitrary extension of $\kappa(y)$ as field extensions are flat. In particular, by passing to a geometric fiber which by assumption is reduced and connected over an algebraically closed field, we see that $\mathrm{H}^0(X_y, \mathscr{O}_{X_y})$ is 1-dimensional over $\kappa(y)$, so that the natural injective map

$$\kappa(y) \to \mathrm{H}^0(X_y, \mathscr{O}_{X_y})$$

is an isomorphism.

As $f$ is flat, we can then apply Theorem 17 with $\mathscr{F} = \mathscr{O}_X$. Since the map

$$\phi_y^{(0)} \colon (f_*\mathscr{O}_X)_y \otimes_{\mathscr{O}_{Y,y}} \kappa(y) \to \mathrm{H}^0(X_y, \mathscr{O}_{X_y}) \cong \kappa(y) \tag{19}$$

is nonzero (1 maps to 1), it is surjective and hence an isomorphism by Theorem 17. Moreover, since $\phi_y^{(-1)}$ is trivially surjective, $(f_*\mathscr{O}_X)_y$ is a free $\mathscr{O}_{Y,y}$-module, and it is of rank 1 in view of the isomorphism $\phi_y^{(0)}$. The isomorphism $\left(\phi_y^{(0)}\right)^{-1}$ then lifts to an isomorphism

$$\mathscr{O}_{Y,y} \xrightarrow{\cong} (f_*\mathscr{O}_X)_y$$

by the freeness of $(f_*\mathscr{O}_X)_y$, for all $y \in Y$. Hence the natural map $\mathscr{O}_Y \to f_*\mathscr{O}_X$ is an isomorphism. □

**Corollary 19** *Let $f \colon X \to Y$ be a proper morphism of schemes with $Y$ locally noetherian. Let $\mathscr{F}$ be a coherent sheaf on $X$, flat over $Y$. Fix $i \geq 0$, and assume that the natural maps $\phi_y^{(i)}$ and $\phi_y^{(i-1)}$ in Theorem 17 are isomorphisms for all $y \in Y$. Consider a locally noetherian $Y$-scheme $Y'$, and the corresponding pullback diagram*

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle f} \\ Y' & \xrightarrow[g]{} & Y. \end{array} \tag{20}$$

*Let $\mathscr{F}'$ be the coherent sheaf $(g')^*\mathscr{F}$ on $X'$, flat over $Y'$. Then the natural map*

$$g^*(\mathrm{R}^i f_*\mathscr{F}) \to \mathrm{R}^i f'_*\mathscr{F}'$$

*is an isomorphism.*

**Proof** We want to apply Theorem 17 to $f'$ and $\mathscr{F}'$, and then use the local freeness of $\mathrm{R}^i f'_* \mathscr{F}'$ to get the desired isomorphism similarly as in the proof of Corollary 18. Let us write $\phi^{(i)}_{\mathscr{F},y}$ for $\phi^{(i)}_y$. For $y' \in Y'$ with $g(y') = y$, we need to show that

$$\phi^{(i)}_{\mathscr{F}',y'} \colon (\mathrm{R}^i f'_* \mathscr{F}')_{y'} \otimes_{\mathscr{O}_{Y',y'}} \kappa(y') \to \mathrm{H}^i(X'_{y'}, \mathscr{F}'_{y'}) \tag{21}$$

is surjective.

By flatness of field extensions, the natural base change map

$$\mathrm{H}^i(X_y, \mathscr{F}_y) \otimes_{\kappa(y)} \kappa(y') \to \mathrm{H}^i(X'_{y'}, \mathscr{F}'_{y'}) \tag{22}$$

is an isomorphism. Thus to show the surjectivity of (21), we need only show that the image contains the $\kappa(y)$-subspace $\mathrm{H}^i(X_y, \mathscr{F}_y)$. Since $\phi^{(i)}_{\mathscr{F},y}$ is surjective, this follows from the commutative diagram of $\kappa(y)$-algebras

$$\begin{array}{ccc}
(\mathrm{R}^i f_* \mathscr{F})_y \otimes_{\mathscr{O}_{Y,y}} \kappa(y) & \xrightarrow{\phi^{(i)}_{\mathscr{F},y}} & \mathrm{H}^i(X_y, \mathscr{F}_y) \\
\downarrow & & \downarrow \\
(\mathrm{R}^i f_* \mathscr{F})_y \otimes_{\mathscr{O}_{Y,y}} \mathscr{O}_{Y',y'} \otimes_{\mathscr{O}_{Y',y'}} \kappa(y') & & \mathrm{H}^i(X_y, \mathscr{F}_y) \otimes_{\kappa(y)} \kappa(y') \\
\downarrow & & \downarrow \wr \\
(\mathrm{R}^i f'_* \mathscr{F}')_{y'} \otimes_{\mathscr{O}_{Y',y'}} \kappa(y') & \xrightarrow{\phi^{(i)}_{\mathscr{F}',y'}} & \mathrm{H}^i(X'_{y'}, \mathscr{F}'_{y'}).
\end{array}$$

Now since $\phi^{(i)}_{\mathscr{F}',y'}$ is surjective for all $y' \in Y'$, and similarly so is $\phi^{(i-1)}_{\mathscr{F}',y'}$, Theorem 17 then implies that $\mathrm{R}^i f'_* \mathscr{F}'$ is locally free on $Y'$. Thus by the freeness of $(\mathrm{R}^i f_* \mathscr{F})_y$ and $(\mathrm{R}^i f'_* \mathscr{F}')_{y'}$, the isomorphism (22) over the residue field $\kappa(y')$ lifts to an isomorphism

$$(\mathrm{R}^i f_* \mathscr{F})_y \otimes_{\mathscr{O}_{Y,y}} \mathscr{O}_{Y',y'} \xrightarrow{\cong} (\mathrm{R}^i f'_* \mathscr{F}')_{y'}$$

over the local ring $\mathscr{O}_{Y',y'}$, for all $y' \in Y'$. Since the left-hand side is isomorphic to $g^*(\mathrm{R}^i f_* \mathscr{F})_{y'}$, the natural map $g^*(\mathrm{R}^i f_* \mathscr{F}) \to \mathrm{R}^i f'_* \mathscr{F}'$ is then an isomorphism. □

**Corollary 20** *Let $f \colon X \to Y$ be a proper smooth surjective morphism of schemes whose geometric fibers are connected. Then the natural map*

$$\mathscr{O}_Y \to f_* \mathscr{O}_X$$

*is an isomorphism. Moreover the formation of this isomorphism is compatible with arbitrary base change: for any $Y$-scheme $Y'$ along with the corresponding pullback diagram (20), the natural map*

$$\mathscr{O}_{Y'} \to f'_* \mathscr{O}_{X'}$$

*is again an isomorphism.*

**Proof** Since $f$ is smooth, it is locally of finite presentation, and thus by [EGA IV$_3$, 8.9.1 and 11.2.6.1] we are reduced to the case when $Y$ is locally noetherian. As smoothness is preserved by arbitrary base change, we may also assume that $Y'$ is locally noetherian. Now since $f$ is smooth, it is flat with reduced geometric fibers. Thus by Corollary 18 the natural map $\mathscr{O}_Y \to f_*\mathscr{O}_X$ is an isomorphism.

We then apply Corollary 19 with $\mathscr{F} = \mathscr{O}_X$ and $i = 0$. For all $y \in Y$, $\phi_y^{(0)}$ is an isomorphism as in the proof of Corollary 18 (cf. (19)), and trivially so is $\phi_y^{(-1)}$. Thus the natural map

$$g^*(f_*\mathscr{O}_X) \to f'_*\mathscr{O}_{X'}$$

is an isomorphism. Together with

$$\mathscr{O}_{Y'} \cong g^*\mathscr{O}_Y \xrightarrow{\cong} g^*(f_*\mathscr{O}_X),$$

we then have that the natural map $\mathscr{O}_{Y'} \to f'_*\mathscr{O}_{X'}$ is an isomorphism. □

## 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, $H_\infty$ *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)

[EGA III$_1$] A. Grothendieck, and J. Dieudonné, *Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. I*, Inst. Hautes Études Sci. Publ. Math. (1961), no. 11, 167.

[EGA IV$_3$] A. Grothendieck, and J. Dieudonné, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III*, Inst. Hautes Études Sci. Publ. Math. (1966), no. 28, 255.

[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)

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52. MR0463157 (57 #3116)

[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)

[MFK94] D. Mumford, J. Fogarty, and F. Kirwan, *Geometric invariant theory*, third ed., Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)], vol. 34, Springer-Verlag, Berlin, 1994. MR1304906 (95m:14012)

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

[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