The power operation structure on the $K(1)$-localization of E_2

YIFEI ZHU

Dyer-Lashof theories organize power operations in cohomology. We give an overview of the structure of the Dyer-Lashof theories associated to Morava E-theories, and to their $K(1)$-localizations. When the E-theory is an elliptic cohomology theory, this structure enables us to compute power operations by calculation with elliptic curves.

1 Introduction

The study of cohomology operations has become central to algebraic topology since the 1950s, with applications to solving problems such as vector fields on spheres, and the non-existence of elements of Hopf invariant one. This latter problem has impact on the author most recently felt when he tried to answer a question raised by students in a calculus class (the interested reader might see [Mas83, theorem II]).

Among the operations involved in these applications, the Steenrod operations Sq^i in ordinary cohomology, and the Adams operations ψ^k in K-theory are examples of *power operations*. In this paper we study power operations in Morava E-theories. Here is an outline.

In this section we introduce preliminary definitions, in particular, the Dyer-Lashof theory DL_{E_*} associated to a Morava E-theory E_*.

In section 2 we "translate" from DL_{E_*} and related categories, to categories arising from the formal group and its finite flat subgroups associated to E_*. This "bridge" is the foundation of our discussion, so that later we can study the structure of one side by doing calculation on the other side.

In section 3 we describe power operations in the $K(1)$-local setting where the structure is relatively simple.

Section 4 contains calculations of power operations for a specific Morava E-theory spectrum and its $K(1)$-localization, at the prime 3. Thanks to the connection in section

2, we work with elliptic curves as concrete objects, following a recipe in hope of generalizing our computation to larger primes.

1.1 Dyer-Lashof theories

One organizing principle for understanding the structure among cohomology operations is through the *algebraic theories* (due to Lawvere, cf. [Law63] and [Bor94, chapter 3]). We will have to begin with a collection of definitions and simple facts concerning algebraic theories, following precisely the discussion in [Reza, sections 5–9].

Definition 1 An *(algebraic) theory* is a category T with object set $\{T^0, T^1, T^2, ...\}$, together with a canonical map $T^0 \to T^1$, and *projection maps* $\pi_i\colon T^n \to T^1$ for all $n \geq 1$, $1 \leq i \leq n$ such that $T(T^k, T^n) \xrightarrow{\pi_i} \prod_{i=1}^n T(T^k, T^1)$ is a bijection for all k and n, i.e. T^n is isomorphic to the n-fold product of T^1.

A *morphism of theories* is a functor $\phi\colon R \to T$ which preserves the product structure of a theory, i.e. $\phi(R^k) = T^k$ and $\phi(R^k \xrightarrow{\pi_i} R^1) = T^k \xrightarrow{\pi_i} T^1$.

Definition 2 A *model* of T is a functor $A\colon T \to \mathrm{Set}$ which preserves finite products.

It can be thought of as the underlying set $X = A(T^1)$ together with operations $\psi_f\colon X^k \to X^n$ for each $f \in T(T^k, T^n)$. In particular, a *free model* on n generators is the model $F_T(n)$ defined by $F_T(n)(T^m) = T(T^n, T^m)$. We write Model_T for the category of models of T. For example, let R be a commutative ring, and let F be the full subcategory of the category of commutative R-algebras having as objects $\{F_0, F_1, F_2, ...\}$, where $F_0 = R$ and $F_n = R[x_1, ..., x_n]$ for $n \geq 1$. We then have the theory of commutative R-algebras $C_R = F^{\mathrm{op}}$.

Definition 3 A *commutative operation theory* (COT) is a triple (T, R, ϕ) consisting of a theory T, a commutative ring R, and a morphism $\phi\colon C_R \to T$ of theories, such that the induced functor $\phi^*\colon \mathrm{Model}_T \to \mathrm{Model}_{C_R}$ commutes with finite coproducts.

In other words, every T-model has an underlying structure of a commutative R-algebra, and coproducts in Model_T are computed by tensor products over R. We write $R\{x_1, ..., x_n\}$ for a free T-model on n generators, and we have $R\{x_1, ..., x_n\} \cong R\{x_1\} \otimes_R \cdots \otimes_R R\{x_n\}$.

We next introduce grading to a theory.

Definition 4 Let C be a fixed set C of *colors*, and let $\mathbb{N}[C]$ be the free commutative monoid on C. A C-*graded theory* T is a category with object set $\{T^n\}_{n\in\mathbb{N}[C]}$, together with, for each $n = \sum_{c\in C} n_c[c] \in \mathbb{N}[C]$, a specified identification of T^n with the product $\prod_{c\in C}(T^{[c]})^{n_c}$.

In particular, given a $\mathbb{Z}$-graded theory T and a graded-commutative ring R, we can define a graded COT as a triple (T, R_*, ϕ) similarly as above (the theory C_{R_*} of graded-commutative R_*-algebras is equipped with the graded tensor product). Given a T-model A, we write A_c for the piece with grading c of the model.

For a graded COT (T, R_*, ϕ), and free models $R_*\{x\}$ and $R_*\{x_1, x_2\}$ with $|x| = |x_1| = |x_2| = c$, let $\mathcal{A}(c,d)$ be the set of elements $f \in R_*\{x\}_d = T(T^{[c]}, T^{[d]})$ which are primitive under the comultiplication $R_*\{x\} \xrightarrow{x\mapsto x_1+x_2} R_*\{x_1, x_2\}$. Such $f \in \mathcal{A}(c,d)$ give rise to additive functions $A_c \to A_d$ natural in the model A, and in particular the element $x \in R_*\{x\}_c$ corresponds to the identity map on A_c. Thus we obtain a category $\mathcal{A}$ of additive operations, whose object set is $\mathbb{Z}$, the set of colors of our graded COT.

For example, let $T = O_{H\mathbb{F}_p}$ be the graded COT given by

$$T(O_{H\mathbb{F}_p}^{[c_1]+\cdots+[c_m]}, O_{H\mathbb{F}_p}^{[d_1]+\cdots+[d_n]}) = [K(\mathbb{F}_p, c_1)\times\cdots\times K(\mathbb{F}_p, c_m), K(\mathbb{F}_p, d_1)\times\cdots\times K(\mathbb{F}_p, d_n)],$$

where we use homotopy classes of maps, and use the convention that $K(\mathbb{F}_p, c) = *$ for $c < 0$. Then $\mathrm{Model}_{O_{H\mathbb{F}_p}}$ is the category of unstable algebras over the mod-p Steenrod algebra. Moreover, $\mathcal{A}(c,d)$ is the set of additive operations $H^c(-;\mathbb{F}_p) \to H^d(-;\mathbb{F}_p)$; in particular, for $p = 2$, these are linear combinations of monomials which are admissible composites of Steenrod operations having excess no more than c. Cf. [**?**, section 4.L] for details.

Having the COT describing cohomology operations on spaces, we next consider one describing operations on spectra.

Let S be the sphere spectrum, and Alg_S be the category of commutative S-algebras (cf. [EKMM97]). Let $\mathbb{P}$ be the free S-algebra functor defined by

$$\mathbb{P}(X) = \bigvee_{m\geq 0} \mathbb{P}^m(X) = \bigvee_{m\geq 0} X^{\wedge m}/\Sigma_m,$$

and let $\mathbb{P}_R$ be the free R-algebra functor defined similarly using the smash product over R. These functors descend to homotopy categories.

Definition 5 Given a commutative S-algebra R, the *Dyer-Lashof theory* DL_R is the $\mathbb{Z}$-graded theory T defined by

$$T(T^{[c_1]+\cdots+[c_m]}, T^{[d_1]+\cdots+[d_n]}) = h\mathrm{Alg}_R\Big(\mathbb{P}_R\big(R\wedge(S^{d_1}\vee\cdots\vee S^{d_n})\big), \mathbb{P}_R\big(R\wedge(S^{c_1}\vee\cdots\vee S^{c_m})\big)\Big).$$

In the homotopy category, we can identify $\mathbb{P}^m(S^c)$ with $B\Sigma_m^{cV_m}$ which is the Thom spectrum of a virtual bundle ($V_m = \mathbb{R}^m$ is equipped with the Σ_m-action given by permuting coordinates, and $c \in \mathbb{Z}$). The free theories are given by

$$F_T([c_1]+\cdots+[c_m])_{[d]} = \pi_d \mathbb{P}_R\big(R \wedge (S^{c_1} \vee \cdots \vee S^{c_m})\big) = \pi_d\Big(R \wedge \big(\mathbb{P}(S^{c_1}) \vee \cdots \vee \mathbb{P}(S^{c_m})\big)\Big).$$

Moreover, if $\pi_* R \wedge \mathbb{P}(S^c)$ are flat as left $\pi_* R$-modules, DL_R turns out to be a COT (cf. [Reza, lemma 7.5]).

The significance of DL_R is that it describes all homotopy operations on commutative R-algebras:

$$\mathrm{DL}_R([c],[d]) = h\mathrm{Alg}_R\big(\mathbb{P}_R(R \wedge S^d), \mathbb{P}_R(R \wedge S^c)\big) = \{\pi_c(-) \to \pi_d(-)\}.$$

For example, if R is a ring (no longer a spectrum) containing $\mathbb{F}_2$ and HR is the corresponding Eilenberg-Mac Lane spectrum, there is a complete description of the COT DL_{HR}. A DL_{HR}-model is a graded commutative R-algebra A_*, equipped with functions $Q^s\colon A_c \to A_{c+s}$ for all $s, c \in \mathbb{Z}$, satisfying a set of properties, e.g. the Cartan formula and the Adem relations. Cf. [Reza, section 10] for details.

1.2 Dyer-Lashof theories associated to Morava E-theories

One organizing principle for understanding large-scale phenomena in homotopy theory is through the *chromatic filtration* (cf. [Law09] and [Hopb, section 17]) which corresponds to a stratification of the moduli stack of formal groups into layers according to height. For complex oriented cohomology theories, the formal groups come about in terms of formal group laws which express the first Chern class of the tensor product of two line bundles in terms of the first Chern classes of the individual line bundles.

For each formal group law F of height $n < \infty$ over a perfect field k of characteristic $p > 0$, the Lubin-Tate ring $\mathrm{LT}(k,F) = \mathbb{W}k[\![v_1, \ldots, v_{n-1}]\!]$ is universal among complete local rings with residue field k carrying a formal group law whose reduction to k is F. There is an E_∞ ring spectrum $E_n(k,F)$ whose homotopy groups are $\mathrm{LT}(k,F)[v^{\pm 1}]$ with $|v| = 2$. This is the *Morava E-theory* spectrum (associated to k and F). One can study specific layers in the chromatic filtration through Bousfield localization (cf. [Lur, lectures 20–23]). For example, the $K(1)$-localization of E_2 is the localization to height 1 of a certain Morava E-theory of height 2; the open substack of heights less than or equal to 2 is where *elliptic cohomology theories* (cf. [Lur09]) are concentrated.

Given a Morava E-theory E_*, there is an associated Dyer-Lashof theory DL_{E_*} describing all cohomology operations. It is defined similarly as above, except that we need to apply a certain localization to have good values of $E_*B\Sigma_m$ (which is mostly torsion for a general ring spectrum E) (cf. [Str98, section 3] and [HS99, section 8]). In particular the free model on one generator is $E_*\{x_c\} = \bigoplus_{m\geq 0} E_*^\wedge(B\Sigma_m^{cV_m})$, where the completed theory $E_*^\wedge(-)$ reflects the localization.

As is explained at the beginning of [And95], we hope to learn about the conjectural geometry of the theories E_n by examining cohomology operations – in particular, power operations – along the lines of ordinary rational homology or K-theory (which are the initial cases E_0 and E_1).

2 The structure of power operations

Let E_* be the Morava E-theory associated to a formal group Γ of height $n < \infty$ over a perfect field k of characteristic $p > 0$. Based on knowledge of the spectrum E, we study the structure of DL_{E_*}, the $\mathbb{Z}$-graded Dyer-Lashof theory describing all homotopy operations on commutative E-algebras. We restrict our attention to the degree 0 part DL_{E_0}. The main input comes from deformations of Frobenius, which we discuss below. In particular, when the E-theory is an elliptic cohomology theory, deformations of Frobenius are parametrized by finite flat subgroups of the formal group of the associated elliptic curve, and thus we may study the operations by calculation with elliptic curves.

This section is largely a summary of some of the results in [Reza, section 16] and [Rezb, sections 3 and 4]. Cf. [Rezc] for an exposition of related topics.

2.1 Identifications of categories

First we consider additive operations.

Let $\mathcal{A}$ be the set of additive elements in the free DL_{E_0}-model on one generator $E_0\{x\} = \bigoplus_{m\geq 0} E_0^\wedge B\Sigma_m$. Write $\mathcal{A}_{[m]} \subset E_0^\wedge B\Sigma_m$ for the summand, and write $\mathcal{A}_r = \mathcal{A}_{[p^r]}$. It turns out that $\mathcal{A}_{[m]} = 0$ unless $m = p^r$ for some r (cf. [Str98, lemma 8.10]). Thus $\mathcal{A} = \bigoplus_{r\geq 0} \mathcal{A}_r$ is an associative (not necessarily commutative) graded ring with respect to the product given by "composition of operations", with the unit element given by the generator $x \in E_0\{x\}$ representing the identity operation. Moreover, the category $\mathrm{Mod}_{\mathcal{A}}$ of left $\mathcal{A}$-modules naturally admits a tensor product which makes it into a symmetric monoidal category (cf. [Reza, proposition 7.6]).

We formulate a category equivalent to $\mathrm{Mod}_{\mathcal{A}}$, which is specific to Morava E-theories, using deformations of Frobenius.

Let R be a complete local ring containing $\mathbb{F}_p$ with maximal ideal $\mathfrak{m}$. Given an R-algebra A, let $\mathrm{Frob}^*\colon\ \sigma^*A \to A$ be the map of R-algebras which fits into the diagram

$$\begin{tikzcd}
R \arrow[r, "\sigma"] \arrow[d] & R \arrow[d] \arrow[ddr] & \\
A \arrow[r] \arrow[drr, "\sigma"'] & \sigma^*A \arrow[dr, dashed] \arrow[ul, phantom, "\ulcorner", very near start] & \\
& & A,
\end{tikzcd}$$

where σ sends an element to its p'th power. In particular, if G is a formal group over R, there is an isogeny $\mathrm{Frob}\colon\ G \to \sigma^*G$ of formal groups over R defined by $\mathrm{Frob}^*\colon\ \mathcal{O}_{\sigma^*G} = \sigma^*\mathcal{O}_G \to \mathcal{O}_G$, $R[\![y]\!] \to R[\![x]\!]$ sending y to x^p.

A *deformation of* Γ *to* R is a triple (G, i, α) consisting of a formal group G over R, an inclusion $i\colon\ k \to R/\mathfrak{m}$ and an isomorphism $\alpha\colon\ G_0 \to i^*\Gamma$ of formal groups over $R/\mathfrak{m}$. A $\star$*-isomorphism* $(G, i, \alpha) \to (G', i', \alpha')$ is an isomorphism $\phi\colon\ G \to G'$ of formal groups over R such that $i' = i$ and $\alpha' \circ \phi_0 = \alpha$. We define the *category of deformations of Frobenius over R* as follows.

Definition 6 Let $\mathrm{DefFrob}_\Gamma(R)$ be the category whose objects are deformations of Γ to R, and whose morphisms are isogenies which are deformations of Frobenius, i.e. a morphism $(G, i, \alpha) \to (G', i', \alpha')$ is an isogeny $\phi\colon\ G \to G'$ such that $i' = \sigma^r \circ i$ and $\alpha' \circ \phi_0 = \mathrm{Frob}^r \circ \alpha$ for some $r \geq 0$. In particular, when $r = 0$, ϕ is precisely a $\star$-isomorphism.

We then consider the category of sheaves of modules on $\mathrm{DefFrob}_\Gamma = \{\mathrm{DefFrob}_\Gamma(R)\}$.

Definition 7 Define a category $\mathrm{Mod}_{\mathrm{DefFrob}_\Gamma}$ as follows. An object $\mathcal{F}$ of this category consists of

(1) for each complete local ring R containing $\mathbb{F}_p$, a functor

$$\mathcal{F}_R\colon\ \mathrm{DefFrob}_\Gamma(R)^{\mathrm{op}} \to \mathrm{Mod}_R,$$

(2) for each local homomorphism $f\colon\ R \to S$, a natural isomorphism

$$\mathcal{F}_f\colon\ f^*\mathcal{F}_R \to \mathcal{F}_S f^*,$$

where the first f^* is the functor $\mathrm{Mod}_R \to \mathrm{Mod}_S$ of extending scalars along f, and the second $f^*\colon \mathrm{DefFrob}_\Gamma(R)^{\mathrm{op}} \to \mathrm{DefFrob}_\Gamma(S)^{\mathrm{op}}$ is induced by f ($\mathrm{DefFrob}_\Gamma(-)$ is a functor),

together with natural isomorphisms

(a) $\mathcal{F}_{\mathrm{id}} \cong \mathrm{id}$ and $\mathcal{F}_{gf} \cong \mathcal{F}_g(f^*) \circ g^*(\mathcal{F}_f)$.

A morphism $\eta\colon \mathcal{F} \to \mathcal{G}$ in this category is a collection of natural transformations $\eta_R\colon \mathcal{F}_R \to \mathcal{G}_R$ such that $\mathcal{G}_f \circ f^*(\eta_R) = \eta_S(f^*) \circ \mathcal{F}_f$.

Remark 8 This is a symmetric monoidal category with the tensor product $\mathcal{F} \otimes \mathcal{G}$ given by $(\mathcal{F} \otimes \mathcal{G})_R(G) = \mathcal{F}_R(G) \otimes_R \mathcal{G}_R(G)$.

Theorem 9 ([Reza, pre-theorem 16.4]) *The symmetric monoidal categories* $\mathrm{Mod}_{\mathcal{A}}$ *and* $\mathrm{Mod}_{\mathrm{DefFrob}_\Gamma}$ *are equivalent.*

Next we consider $\mathrm{Model}_{\mathrm{DL}_{E_0}}$, the category of models for the theory DL_{E_0}, on which $\mathcal{A}$ acts. By [Reza, proposition 7.6], there is a forgetful functor $\mathrm{Model}_{\mathrm{DL}_{E_0}} \to \mathrm{Mod}_{\mathcal{A}}$ along which the coproduct of DL_{E_0}-models and the tensor product of $\mathrm{Mod}_{\mathcal{A}}$ agree.

Definition 10 Define a category $\mathrm{Alg}_{\mathrm{DefFrob}_\Gamma}$ as follows. An object $\mathcal{B}$ of this category is a ring object in $\mathrm{Mod}_{\mathrm{DefFrob}_\Gamma}$ which satisfies

(b) the *Frobenius congruence*, i.e. the diagram

$$\begin{tikzcd}
\sigma^*\mathcal{B}_R(G) \arrow[r, "\mathrm{Frob}^*"] \arrow[d, "\mathcal{B}_\sigma(G)"', "\wr"] & \mathcal{B}_R(G) \\
\mathcal{B}_R\sigma^*(G) \arrow[ur, "\mathcal{B}_R(\mathrm{Frob})"'] &
\end{tikzcd}$$

commutes for all complete local rings R containing $\mathbb{F}_p$ and deformations G of Γ to R.

Morphisms in this category are maps of ring objects.

An object $\mathcal{B}$ is said to be *torsion free* if $\mathcal{B}_R(G)$ is p-torsion free for every p-torsion free R and every deformation G to R. We denote by $\mathrm{Alg}^{\mathrm{tf}}_{\mathrm{DefFrob}_\Gamma}$ the full subcategory of $\mathrm{Alg}_{\mathrm{DefFrob}_\Gamma}$ consisting of torsion free objects.

Theorem 11 ([Reza, pre-theorem 16.5]) *There is a forgetful functor* $\mathrm{Model}_{\mathrm{DL}_{E_0}} \to \mathrm{Alg}_{\mathrm{DefFrob}_\Gamma}$ *which restricts to an equivalence* $\mathrm{Model}^{\mathrm{tf}}_{\mathrm{DL}_{E_0}} \cong \mathrm{Alg}^{\mathrm{tf}}_{\mathrm{DefFrob}_\Gamma}$ *between the full subcategories of torsion free objects.*

2.2 Deformations of Frobenius are parametrized by subgroups

Having identified the categories, we now analyze the essential data encoded in $\mathrm{Mod}_{\mathrm{DefFrob}_\Gamma}$ and $\mathrm{Alg}^{\mathrm{tf}}_{\mathrm{DefFrob}_\Gamma}$, by studying the structure of the category $\mathrm{DefFrob}_\Gamma(R)$ of deformations of Frobenius. This turns out to be parametrized by finite flat subgroups of the deformations of Γ to R, as we explain below.

Choosing a coordinate of a formal group G over R, a *degree* (or *rank*) d *subgroup* K *of* G is an effective divisor with $\mathcal{O}_K = R[\![x]\!]/\big(f(x)\big)$ for some degree d monic polynomial $f(x)$ such that $f(x_1 +_G x_2) \in \big(f(x_1), f(x_2)\big)$ and $f(x) \in (x)$. In other words, the group law of G restricts to K, and K contains the identity. Given a subgroup K of G, we can define the *quotient group* G/K (cf. [Str97, section 5]) which is again a formal group.

Henceforth by "subgroups" we mean specifically those that are finite and flat.

One can show that the homomorphism $[d]_G\colon G \to G$ restricts to zero on K (cf. [TO70, section 1]). More concretely, this means that $f(x)$ must divide $[d]_G(x)$. As a consequence, subgroups of a formal group over a p-local ring must have degree p^r. In particular, if G is a formal group over a field k of characteristic $p > 0$, there is exactly one subgroup of degree p^r, given by $f(x) = x^{p^r}$, which is the kernel of the r-fold Frobenius isogeny Frob^r (cf. [Reza, proposition 16.8]).

We have seen that in $\mathrm{DefFrob}_\Gamma(R)$ the degree 1 morphisms (when $r = 0$) are precisely the $\star$-isomorphisms of deformations. In general, with morphisms corresponding to all $r \geq 0$, $\mathrm{DefFrob}_\Gamma(R)$ is equivalent to the following category (cf. [Reza, proposition 16.9]). The objects are $\star$-isomorphism classes of deformations $[G]$. The morphisms are $\star$-isomorphism classes of pairs $[G > K]$: the source of $[G > K]$ is $[G]$, and the target of $[G > K]$ is $[G/K]$, where G/K is a deformation of Γ with $i_{G/K} = \sigma^r \circ i_G$ (p^r being the degree of K). Moreover, if $G/K \cong G'$, then $[G' > K'] \circ [G > K] = [G > K'']$, where K'' is the kernel of the composite $G \to G/K \cong G' \to G'/K'$. Thus deformations of Frobenius with source (G, i, α) correspond *exactly* to subgroups of G.

Example 12 Let Γ be the multiplicative formal group over $\mathbb{F}_p$ of height 1. For the multiplicative formal group $\mathbb{G}_m$ over a p-local ring R, since the formal group law is defined by $1 + (x_1 +_{\mathbb{G}_m} x_2) = (1 + x_1)(1 + x_2)$, we have $[p^r](x) = (1 + x)^{p^r} - 1 = x^{p^r}$. Thus the only subgroups of $\mathbb{G}_m$ are $\mathbb{G}_m[p^r]$ with $\mathcal{O}_{\mathbb{G}_m[p^r]} = \mathcal{O}_{\mathbb{G}_m}/(x^{p^r})$. Moreover, by the Lubin-Tate theorem (cf. [LT66, theorem 3.1] and [Rez98, section 4.3]), every object of $\mathrm{DefFrob}_\Gamma(R)$ is $\star$-isomorphic to $\mathbb{G}_m$. In particular, the set of $\star$-isomorphism classes of deformations of Γ to R is classified by the ring $\mathcal{O}_{\mathrm{univ}} = \mathbb{Z}_p$, and we can take the universal deformation G_{univ} to be the multiplicative formal group over $\mathbb{Z}_p$. Thus by functoriality, to describe an object $\mathcal{B} \in \mathrm{Alg}^{\mathrm{tf}}_{\mathrm{DefFrob}_\Gamma}$, it is enough to give

(1) a p-torsion free $\mathbb{Z}_p$-algebra $B = \mathcal{B}_{\mathbb{Z}_p}(\mathbb{G}_m)$,

(2) maps of $\mathbb{Z}_p$-algebras $\psi^{p^r}\colon B \to B$ (corresponding to the isogenies $[p^r]\colon \mathbb{G}_m \to \mathbb{G}_m$) such that

   (a) $\psi^1 = \mathrm{id}_B$ and $\psi^{p^r} \circ \psi^{p^s} = \psi^{p^{r+s}}$,

   (b) $\psi^p(b) \equiv b^p \mod pB$.

(For comparison, the items are labelled as in definitions 7 and 10.)

We note as in [Rez09, example 1.3] that this is a "p-typicalization" of the original theorem of Wilkerson (cf. [Wil82, proposition 1.2]) which characterizes the torsion free λ-rings in terms of congruences on the Adams operations at all primes. More concretely, let K be the complex K-theory spectrum. Then for $B = \pi_0 A$, where A is a p-complete K-algebra (commutative K-algebra such that $A \cong A^\wedge_p$), ψ^p recovers the p'th Adams operation studied by McClure (cf. [BMMS86, chapters VIII and IX]).

In general, consider the functor X_r which associates to a ring R the set of $\star$-isomorphism classes of pairs $[G > K]$ with K a degree p^r subgroup of G. It is represented by the complete local ring $\mathcal{O}_{X_r} = E^0B\Sigma_{p^r}/I$, where $I = \sum_{0<i<p^r} \mathrm{Image}\big(E^0B(\Sigma_i \times \Sigma_{p^r-i}) \xrightarrow{\text{transfer}} E^0B\Sigma_{p^r}\big)$ is the *transfer ideal* (roughly speaking, the corresponding power operation should be additive, so modulo the "mixing terms" in the Cartan formula) (cf. [Str98, theorem 9.2]). This can be viewed as a generalization of the Lubin-Tate theorem for $\mathcal{O}_{\mathrm{univ}} = \mathcal{O}_{X_0}$. Moreover, there are two ring homomorphisms s^*, $t^*\colon \mathcal{O}_{\mathrm{univ}} \to \mathcal{O}_{X_r}$, where s^* represents the source map $[G > K] \mapsto [G]$, and t^* represents the target map $[G > K] \mapsto [G/K]$. (In example 12, $\mathcal{O}_{X_r} \cong \mathcal{O}_{\mathrm{univ}}$ for all r, and $s^* = t^* = \mathrm{id}$.) Thus to describe an object $\mathcal{B} \in \mathrm{Alg}^{\mathrm{tf}}_{\mathrm{DefFrob}_\Gamma}$, it is enough to give

(1) a p-torsion free $\mathcal{O}_{\mathrm{univ}}$-algebra $B = \mathcal{B}_{\mathcal{O}_{\mathrm{univ}}}(G_{\mathrm{univ}})$,

(2) maps of $\mathcal{O}_{\mathrm{univ}}$-algebras $\psi^{p^r}\colon B \to B \otimes^{s^*}_{\mathcal{O}_{\mathrm{univ}}} \mathcal{O}_{X_r}$ as the composite
$$B \xrightarrow{f^*} B \otimes^{t^*}_{\mathcal{O}_{\mathrm{univ}}} \mathcal{O}_{X_r} \overset{\mathcal{B}_f}{\cong} \mathcal{B}_{\mathcal{O}_{X_r}}(t^* G_{\mathrm{univ}}) \xrightarrow{\mathcal{B}_{\mathcal{O}_{X_r}}(\psi)} \mathcal{B}_{\mathcal{O}_{X_r}}(s^* G_{\mathrm{univ}}) \overset{\mathcal{B}_g}{\cong} B \otimes^{s^*}_{\mathcal{O}_{\mathrm{univ}}} \mathcal{O}_{X_r},$$
where $f = t^*$ and $g = s^*$ are local homomorphisms, and $\psi\colon s^* G_{\mathrm{univ}} \to t^* G_{\mathrm{univ}}$ is the universal deformation of Frob^r (cf. [Str97, section 13]),

satisfying a set of formal properties. In particular, if we denote by u^* the map $\mathcal{O}_{X_1} \to \mathcal{O}_{\mathrm{univ}}/(p)$ which represents the universal Frobenius isogeny, the Frobenius congruence (b) amounts to requiring that
$$B \xrightarrow{\psi^p} B \otimes^{s^*}_{\mathcal{O}_{\mathrm{univ}}} \mathcal{O}_{X_1} \xrightarrow{\mathrm{id} \otimes u^*} B \otimes_{\mathcal{O}_{\mathrm{univ}}} \mathcal{O}_{\mathrm{univ}}/(p) = B/pB$$

be the p'th power map $B \to B/pB \xrightarrow{\sigma} B/pB$ which sends x to $\bar{x}^p$.

Example 13 Consider the elliptic curve $C_0 \subset \mathbb{P}^2_{\mathbb{F}_2}$ defined by

$$Y^2Z + YZ^2 = X^3,$$

which is supersingular so that its formal group $\widehat{C_0}$ is of height 2. It has a universal deformation C over the Lubin-Tate ring $\mathbb{W}\mathbb{F}_2[\![v_1]\!] \cong \mathbb{Z}_2[\![a]\!]$ given by

$$Y^2Z + aXYZ + YZ^2 = X^3,$$

where a is the Hasse invariant so that setting $a = 0$ we recover the supersingular elliptic curve C_0 (cf. [KM85, 2.2.10] and [MR09, proposition 3.2]). Let E be the Morava E-theory spectrum associated to this universal deformation, so that $\pi_*E = \mathbb{Z}_2[\![a]\!][v^{\pm 1}]$ with $|v| = 2$. The power operations on E are constructed in [And95, section 3], with explicit formulas computed in [Rezb, sections 3 and 4]. What follows is directly from the latter reference.

By studying degree 2 subgroups, i.e. subgroups of 2-torsion points on C, we can identify $\mathcal{O}_{X_1} \cong \mathbb{Z}_2[\![a,d]\!]/(d^3 - ad - 2)$: in the affine chart $u = X/Y$, $v = Z/Y$, degree 2 subgroups are generated by points Q of the form $\big(u(Q), v(Q)\big) = (d, -d^3)$ such that $d^3 - ad - 2 = 0$. Thus we have a power operation

$$\psi^2\colon\ E^0X \to E^0X[\![d]\!]/(d^3 - ad - 2).$$

Moreover, by studying the isogeny $\psi_Q\colon\ C \to C'$ whose kernel is the degree 2 subgroup generated by Q, one computes that

$$t^*(a) = \psi^2(a) = a^2 + 3d - ad^2.$$

There are also formulas for a set of functions $Q_0(x)$, $Q_1(x)$ and $Q_2(x)$ which express

$$\psi^2(x) = Q_0(x) + Q_1(x)d + Q_2(x)d^2.$$

In particular, the Frobenius congruence takes the form $Q_0(x) \equiv x^2 \bmod 2$. We will discuss in detail such calculations for Morava E-theories associated to supersingular elliptic curves in section 4.

3 $K(1)$-local power operations

In this section we discuss how to pass to the $K(1)$-local setting from the power operations at arbitrary height described in the previous section. For general background of $K(1)$-local operations, see [Hopa].

Let F be an even-periodic E_∞ ring spectrum such that F^0 is a p-torsion free complete local ring with maximal ideal $\mathfrak{m}$ containing p, and the mod-$\mathfrak{m}$ reduction of the formal group over F^0 is of height $n < \infty$, and let $E = L_{K(1)}F$ be its $K(1)$-localization. For example, the Morava E-theory spectrum associated to the universal deformation of a supersingular elliptic curve in example 13 is such, and we write $F = E_2$, specifying its height.

The general pattern of the relationship between $K(1)$-local power operations and the power operations in section 2.2 is as follows:

$$\begin{tikzcd}
F^0 \arrow[r, "\psi^p"] \arrow[d] & F^0B\Sigma_p/I \arrow[d, "L"] \\
E^0 \arrow[r, "\psi^p"] & E^0B\Sigma_p/I \cong E^0.
\end{tikzcd}$$

Recall that the top operation arises from the universal deformation of Frobenius which is represented by the ring $\mathcal{O}_{X_1} = F^0B\Sigma_p/I$. The vertical maps are induced by the $K(1)$-localization $F \to E$. In terms of homotopy groups, this is obtained by inverting the generator v_1 (so that the resulting formal group is of height at most 1) and completing at the ideal (p), i.e. $F^0 = \mathbb{W}k[\![v_1, ..., v_{n-1}]\!]$ and $E^0 = \mathbb{W}k[\![v_1, ..., v_{n-1}]\!][v_1^{-1}]_p^\wedge$. For example, $\pi_0 L_{K(1)}E_2 = \varprojlim \mathbb{Z}_2(\!(a)\!)/(2^i) = \{\sum_{n=-\infty}^{\infty} c_n a^n | c_n \in \mathbb{Z}_2, c_n \to 0 \text{ 2-adically as } n \to -\infty\}$ (the Hasse invariant $h = a$ can be taken as the generator v_1). In particular the formal group of F^0 obtains a unique degree p subgroup after being pulled back to E^0, and the map L classifies it. We will explain this uniqueness of subgroup and the isomorphism at the bottom right corner shortly.

In order to do calculation we need to examine L more carefully. For a p-divisible group $\mathbb{G}$ over a base scheme X, the restriction of $\mathbb{G}$ to any geometric point $x \in X$ lives in the natural short exact sequence

$$0 \to \mathbb{G}^{\text{for}} \to \mathbb{G}_x \to \mathbb{G}^{\text{ét}} \to 0,$$

where the subobject (the connected component of the identity) is the *formal* component, and the quotient is the *étale* component. The formal component $\mathbb{G}^{\text{for}}$ is a formal group on X. The localization L factors through $E^0 \otimes_{F^0} F^0B\Sigma_p/I$, and along the base change $F^0B\Sigma_p/I \to E^0 \otimes_{F^0} F^0B\Sigma_p/I$ the p-divisible group consisting solely of formal component may split into formal and étale components. We want to take the formal component so as to keep track of the unique subgroup classified by L which lands in the formal group over $E^0B\Sigma_p/I$.

Example 14 We continue example 13 in the $K(1)$-local setting. After base change to $L_{K(1)}E_2$, the universal elliptic curve C has a unique degree 2 subgroup in its formal component which is the canonical subgroup introduced in [Lub67, theorem 1.4]. The degree 2 subgroup generated by $(d, -d^3)$ is contained in the formal component if and only if $(d, -d^3)$ is in the formal neighborhood of the identity $(0, 0)$. The equation $d^3 - ad - 2 = 0$ which parametrizes degree 2 subgroups has a unique root in $\mathbb{F}_2(\!(a)\!)$, and Hensel's lemma implies that this lifts to a root in $\pi_0 L_{K(1)}E_2 \cong \mathbb{Z}_2(\!(a)\!)^{\wedge}_2$. Plugging this specific value of d into $\psi^2\colon\ \pi_0 E_2 \to \pi_0 E_2[\![d]\!]/(d^3 - ad - 2)$, we get an endomorphism of the ring $\pi_0 L_{K(1)}E_2$, and this endomorphism is the $K(1)$-local power operation. For an application of this calculation, see [LN, section 6].

Lastly we note that the above commutative square describes the pattern for $K(m)$-local operations with $m > 1$ as well, but the isomorphism at the bottom right corner is specific to the height 1 case.

Lemma 15 $E^0 B\Sigma_p / I \cong E^0$.

This generalizes what we have seen in example 12 about the multiplicative formal group. A formal group $\mathbb{G}$ of height 1 has a unique degree p subgroup given by $\mathbb{G}[p]$, and the ring $E^0 B\Sigma_p / I$ classifying subgroups of degree p is isomorphic to E^0. Thus the power operation takes the form $\psi^p\colon\ E^0 \to E^0$ which is a lift of Frobenius. In general a height n formal group has $(p^n - 1)/(p - 1)$ degree p subgroups, as in the example of section 4 where $n = 2$ and $p = 3$. See [And95, section 3.5] for an approach of making power operations of higher height land in E^0.

Proof of the lemma First we identify $E^0 B\Sigma_p$ as the E^0-submodule of $E^0 BC_p$ fixed by the action induced by $\mathrm{Aut} C_p \cong \mathbb{F}_p^\times$. This is a special case of the calculation in [Reza, section 12]. We have

$$B\Sigma_p \xrightarrow{\mathrm{tr}} BC_p \xrightarrow{\mathrm{res}} B\Sigma_p,$$

where tr is the transfer map, and res is the restriction map. Since $[\Sigma_p : C_p]$ is prime to p, the composite is a p-local equivalence, and thus p-locally $B\Sigma_p$ is a retract of BC_p. Moreover, $\mathrm{Aut} C_p$ acts on $\mathrm{Hom}(C_p, \Sigma_p)$ as conjugation (it preserves the "cycle type" of the element generating the image of C_p in Σ_p). Thus two maps $C_p \to \Sigma_p$ that differ by an $\mathrm{Aut} C_p$-action induce homotopic maps $BC_p \to B\Sigma_p$, and hence the same map $E^0 B\Sigma_p \to E^0 BC_p$.

We calculate $E^0 BC_p$ by considering the cofiber sequence associated to the construction of Thom space

$$S(L^{\otimes p}) \to BS^1 \to (BS^1)^{L^{\otimes p}},$$

where L is the tautological complex line bundle over BS^1. E^*BS^1 can be calculated (cf. [Hopb, section 1]) as $E^0[\![u]\!]$ with $|u| = 2$, where u is the first Chern class of L. By the Thom isomorphism and the even-periodicity of E^*, the map on cohomology induced by the right-hand map in the cofiber sequence can be identified as $[p]\colon\ E^*BS^1 \to E^*BS^1$. This map sends u to $[p](u) = pu + \cdots + v_1u^p + \cdots$, where v_1 is invertible in $E^0 \cong \mathbb{W}k[\![v_1, ..., v_{n-1}]\!][v_1^{-1}]^\wedge_p$. Also note that we can identify the sphere bundle $S(L^{\otimes p})$ with BC_p. Thus again as E^* is even-periodic, the long exact sequence induced by the cofiber sequence implies that $E^0BC_p \cong E^0[\![u]\!]/\big([p](u)\big)$.

For any $q \in \mathbb{F}_p^\times$, the induced action on E^0BC_p sends u to $[q](u) = qu + \cdots$. Hence as the E^0-submodule of E^0BC_p fixed by the $\mathrm{Aut}C_p$-action, $E^0B\Sigma_p$ can be identified with $E^0 \oplus \big(E^0 \cdot \prod_{q=1}^{p-1}[q](u)\big) \cong E^0 \oplus \big(E^0 \cdot (u^{p-1} + \cdots)\big)$.

Next we identify the transfer ideal $I = \sum_{0<i<p} \mathrm{Image}\big(E^0B(\Sigma_i \times \Sigma_{p-i}) \xrightarrow{\text{transfer}} E^0B\Sigma_p\big)$ as the second summand in $E^0B\Sigma_p$. Similarly as above, for all $0 < i < p$, the composite

$$E^0B(\Sigma_i \times \Sigma_{p-i}) \xrightarrow{\text{res}} E^0 \xrightarrow{\text{tr}} E^0B(\Sigma_i \times \Sigma_{p-i})$$

is multiplication by an invertible scalar, and thus $E^0B(\Sigma_i \times \Sigma_{p-i}) \cong E^0$. Moreover, by the "double-coset formula" the composite

$$E^0 \xrightarrow{\text{tr}} E^0B\Sigma_p \xhookrightarrow{\text{res}} E^0BC_p$$

has image the same as $E^0 \xrightarrow{\text{tr}} E^0BC_p$. Thus I is generated by $\mathrm{tr}(1)$ as an E^0-module.

Write $\langle p\rangle(u) = p + \cdots + v_1u^{p-1} + \cdots$ so that $E^0BC_p = E^0[\![u]\!]/\big(u \cdot \langle p\rangle(u)\big)$, and write $\mathrm{tr}(1) = f(u) \in E^0[\![u]\!]$ by abuse of notation. Note that the composite

$$E^0 \xrightarrow{\text{tr}} E^0BC_p \xrightarrow{\text{res}} E^0$$

is multiplication-by-p. Since this composite sends 1 to $\mathrm{res}\big(f(u)\big) = f(0)$, we have $f(0) = p$. Moreover since $u \cdot \mathrm{tr}(1) = \mathrm{tr}\big(\mathrm{res}(u)\big)$ and $\mathrm{res}(u) = 0$, $u \cdot f(u)$ is divisible by $[p](u)$. We claim that these two conditions on $f(u)$ forces it to be $\langle p\rangle(u)$. Clearly $\langle p\rangle(0) = p$, and $\langle p\rangle(u)$ is annihilated by u in $E^0[\![u]\!]/\big(u \cdot \langle p\rangle(u)\big)$. Applying the snake lemma to two rows of copies of

$$0 \longrightarrow E^0[\![u]\!] \xrightarrow{\cdot u} E^0[\![u]\!] \longrightarrow E^0 \longrightarrow 0$$

with vertical maps being multiplication by $[p](u)$ on $E^0[\![u]\!]$ and zero on E^0, we see that any element annihilated by u is a multiple of $\langle p\rangle(u)$ by an element of E^0. As p is not a zero-divisor in E^0, the claim follows. Thus $I = E^0 \cdot \langle p\rangle(u)$.

Finally as v_1 is invertible in E^0, $E^0B\Sigma_p/I \cong E^0$. □

We also note that at height 1, as in example 12, the power operation ψ^p determines the other ψ^{p^r} with $r > 1$ by iterated composition. Thus in the $K(1)$-local setting, among the operations ψ^{p^r} it suffices to study only ψ^p as above. Moreover if the $K(1)$-local homotopy groups are *p-torsion free*, it turns out that ψ^p determines *all* the power operations (cf. [Reza, section 3]). For this reason we will simply write ψ for *the* $K(1)$-local power operation. At higher height, the relationship among these operations is more complicated.

4 Power operations at the prime 3

In [Rezb], Rezk gives explicit calculations of the algebraic theory of power operations for a specific Morava E-theory of height 2 at the prime 2 (cf. example 13). We record some calculations mimicking some of the results there, at the prime 3, together with calculations of the corresponding $K(1)$-local power operation.

The Morava E-theory F of height 2 that we consider here is associated to the deformations of a supersingular elliptic curve over a field of characteristic 3. Our calculations break into the following steps:

(1) Find the universal elliptic curve with a choice of 4-torsion point, so that a posteriori the supersingular elliptic curve that we are interested in is the one with the Hasse invariant zero;

(2) Study the degree 3 subgroups of this universal elliptic curve. In particular, we need to compute

- the coordinate ring parametrizing degree 3 subgroups,
- the equation of the quotient curve which is the image of the universal degree 3 isogeny;

(3) $K(1)$-localize.

4.1 The universal elliptic curve with a choice of 4-torsion point

Let k be a field of characteristic 3. First we note that a supersingular elliptic curve over k cannot have a 3-torsion point. Moreover, in order to have a *unique* lift of the elliptic curve together with a choice of N-torsion point along a deformation of k, N must be prime to 3. As the associated moduli stack $\mathcal{M}\big(\Gamma_1(2)\big)$ to a level $\Gamma_1(2)$-structure on the elliptic curve is not representable by a scheme due to the existence of nontrivial automorphism of order 2 (cf. [KM85, corollaries 4.7.2 and 2.7.2]), a natural choice for the universal elliptic curve is one equipped with a level $\Gamma_1(4)$-structure.

The computation for the equation of the universal elliptic curve with a choice of 4-torsion point P is analogous to [KM85, 2.2.10] and [MR09, proposition 3.2], where the universal elliptic curve for the prime 2 case has a choice of 3-torsion point (cf. example 13). In the xy-coordinates, with the constraints that P be at the origin, $2P$ be on the x-axis, and $4P$ be the identity O, we have the affine Weierstrass equation

$$y^2 + axy + acy = x^3 + cx^2$$

over the graded ring $\mathbb{Z}_{(3)}[a,c]$, where $|a| = 1$ and $|c| = 2$. The grading comes from the action of $\mathbb{G}_m = \mathrm{Spec}\mathbb{Z}[\lambda^{\pm 1}]$ given by $a \mapsto \lambda a$ and $c \mapsto \lambda^2 c$. By [Sil09, V.4.1(a)], the Hasse invariant can be computed as $h = a^2 + 4c$, so that over k the curve is supersingular precisely when $h = 0$ (note that the minimal field of definition of this supersingular elliptic curve is $\mathbb{F}_9$). To facilitate calculation, we work in the affine coordinate chart $c = 1$ of $\mathcal{M}\big(\Gamma_1(4)\big)$ so that the elliptic curve is given by

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

with the discriminant of the elliptic curve $\Delta = a^2(a+4)(a-4)$ and the Hasse invariant $h = a^2 + 4$. This reduction is analogous to the one discussed in detail in [LN, section 4]. In the uv-coodinates, with $u = x/y$ and $v = 1/y$, the equation becomes

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

which is the form we will use most often later.

We denote this elliptic curve by $\mathcal{E}$.

Remark 16 We note that the curve $\mathcal{E}$, together with the universal elliptic curve with a choice of 3-torsion point for the prime 2 case, give models for studying power operations at *all* primes.

As a record of notation, we can rewrite the equation of $\mathcal{E}$ as

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

and we denote by $\epsilon(v)$ the left-hand side of the above equation, viewed as a quadratic polynomial in v.

4.2 Degree 3 subgroups

4.2.1 3-torsion points

In order to compute the coordinate ring parametrizing degree 3 subgroups, we need to find an equation characterizing the coodinates of a 3-torsion point.

Given the elliptic curve

$$\mathcal{E}:\ y^2 + axy + ay = x^3 + x^2,$$

(x, y) is a 3-torsion point if and only if the division polynomial

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

equals zero (cf. [Sil09, exercise 3.7(d)]). (This polynomial is exactly what one gets for the characterization, away from the prime 2, of a flex point in terms of the second derivative y'' calculated by implicit differentiation.) We want to translate this into the uv-coordinates which are more convenient to work with in the formal neighborhood of the identity (in the xy-coordinates, the identity is at ∞). In this way we will get a "characteristic" equation comparable to $d^3 - ad - 2 = 0$ in example 13, where d was the u-coordinate of a 2-torsion point.

From the formula of multiplication-by-3 in the xy-coordinates, we have

$$[3](u, v) = \left(\frac{\phi_3(\frac{u}{v})\psi_3(\frac{u}{v})}{\omega_3(\frac{u}{v})}, \frac{\psi_3(\frac{u}{v})^3}{\omega_3(\frac{u}{v})} \right),$$

with notation following [Sil09, exercise 3.7(d)], and thus our preliminary equation is $\psi_3(\frac{u}{v}) = 0$. Clearing the denominators in $\psi_3(\frac{u}{v})$, we get

$$\psi_3'(u, v) = 3u^4 + (a^2 + 4)u^3v + 3a^2u^2v^2 + 3a^2uv^3 + a^2v^4.$$

To eliminate v, we multiply the "conjugate" $\psi_3'(u, v')$, where v and v' are conjugate roots of the quadratic equation $\epsilon(v) = 0$. We get a degree 8 polynomial in u:

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

Thus if we denote by (d, e) the coordinates of a 3-torsion point, d must satisfy $f(d) = 0$.

Remark 17 According to section 3, in particular example 14, we expect that $f(u)$ have a unique root reduced to zero modulo 3 after $h = a^2 + 4$ gets inverted, corresponding to the unique subgroup in the formal neighborhood of the identity. However, as we obtain $f(u)$ out of a conjugation procedure, this is not exactly the case. We have

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

and in view of $a \not\equiv 0$ by the nonsingularity of $\mathcal{E}$ (recall that $\Delta = a^2(a+4)(a-4)$), such a root has multiplicity 2 (corresponding to the two nontrivial elements in the subgroup). $f(u)$ is the best possible polynomial solely about u that we have at this point, and in later steps we will have to "rescale" it back to a degree 4 polynomial.

Next, for the coordinates (d, e) of a 3-torsion point, we want to express e in terms of d. At the prime 2 (cf. example 13), the relation $e = -d^3$ can be obtained by manipulating the division polynomial ψ_2 and its "conjugate" as above, or simply by computing the inversion formula for a 2-torsion point on the elliptic curve as in [Rezb, section 3]. The prime 3 case is a little more involved.

Using the Euclidean algorithm, we compute the gcd of

$$A(v) = \psi_3'(u, v) = 3u^4 + (a^2+4)u^3v + 3a^2u^2v^2 + 3a^2uv^3 + a^2v^4$$

and

$$B(v) = \epsilon(v),$$

both of which vanish at (d, e). We have

$$A(v) = B(v)Q_1(v) + R_1(v)$$

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

and it turns out that $R_2(e) = 0$ as a result of $f(d) = 0$. Thus

$$R_1(d, e) = p(d) + q(d)e = 0$$

is a relation between d and e, linear in e. We have formulas for $p(d)$ and $q(d)$, and we can compute the inverse of $q(d)$ by applying the Euclidean algorithm to find

$$1 = a(d)q(d) + b(d)f(d) = a(d)q(d).$$

In the end we have a degree 7 polynomial $e = g(d)$, comparable to $e = -d^3$ in the prime 2 case.

To summarize, in this subsection we find two polynomials f and g, so that any 3-torsion point with the uv-coordinates (d, e) satisfies $f(d) = 0$ and $e = g(d)$.

4.2.2 The universal degree 3 isogeny

Now we are ready to compute the universal degree 3 isogeny and thus the equation of the quotient curve which is its image. From there we can find a formula for the power operation $\psi^3\colon F^0 \to F^0[\![d]\!]/\big(f(d)\big)$, where $F^0 = \mathbb{Z}_9[\![h]\!]$ with the Hasse invariant h as the generator v_1 (to be precise, the target should actually be a certain improved coordinate ring as promised in remark 17).

To compute the coordinates (u', v') of the isogeny, we follow the "Lubin isogeny" construction (cf. [Lub67, proof of theorem 1.4]). Let $P\big(u, v(u)\big)$ be a general point on $\mathcal{E}$, and $Q\big(d, e(d)\big)$ be a 3-torsion point. For $v(u)$, we solve the quadratic equation $\epsilon(v) = 0$, and take the first few terms (up to at least u^9 for our purpose) in the power series expansion of the root satisfying $v(0) = 0$ (lying in the formal neighborhood of the identity). For $e(d)$, we use the polynomial $g(d)$ computed at the end of section 4.2.1. We set

$$u' = u(P)u(P-Q)u(P+Q),$$

and similarly for v'. By computing the inversion and addition formulas for the curve $\mathcal{E}$, we can write down formulas for $u' = \alpha u + \cdots$ and $v' = \beta u^3 + \cdots$ in terms of the uniformizer u and parameters a and d.

Remark 18 In order to have the equation of the quotient curve in Weierstrass form, we need to include an adjusting constant factor α^3/β into v', comparable to the term -1 appearing in the formula for u' in [Rezb].

We then solve for the Weierstrass equation which u' and v' satisfy. The equation of the quotient curve turns out to be

$$v + ruv + rv^2 = u^3 + u^2 v,$$

where

$r(a,d) = -\frac{1}{(-4+a)(4+a)}(-126a + 28a^3 - a^5 + 120d - 9a^2d + 3a^4d + 258ad^2 - 67a^3d^2 + 3a^5d^2 - 152d^3 + 208a^2d^3 - 40a^4d^3 + a^6d^3 + 198ad^4 - 33a^3d^4 - 3a^5d^4 + 8d^5 + 63a^2d^5 - 15a^4d^5 + 70ad^6 - 17a^3d^6 + 24d^7 - 6a^2d^7)$

(note that $(-4+a)(4+a)$ is invertible as $\Delta = a^2(a+4)(a-4)$). Hence $\psi^3(a) = r(a,d)$ gives the power operation. As $d \equiv 0 \bmod 3$, we check that $\psi(a)$ reduces to a^3 modulo 3 (the Frobenius congruence at height 1 over k).

Lastly we compute the coordinate ring as the target of the power operation ψ^3.

Set $t = g(d)/d$, the reciprocal of the x-coordinate of a 3-torsion point. This is a quantity which is invariant under negation using the group law of $\mathcal{E}$ (as we have $[-1](x) = x$) and is "distinguishable" from the identity in the formal neighborhood (in the xy-coodinates the identity is at ∞). In view of $f(d)=0$, we compute that t is the root of a quartic polynomial

$$w(t)=a^2t^4+3a^2t^3+3a^2t^2+(a^2+4)t+3$$

which has a *unique* root reduced to zero modulo 3. We note that via the relation $t=1/x$ this polynomial recovers the division polynomial $\psi_3(x)$. Thus the eight roots of $f(d)$ together with $d=0$ correspond to the nine 3-torsion points on $\mathcal{E}$, and the four roots of $w(t)$ correspond to the four degree 3 subgroups consisting of 3-torsion points, one of which lies in the formal neighborhood of the identity. In particular, the equation of $\mathcal{E}$ implies that d satisfies a quadratic equation in terms of t:

$$(t+1)d^2-at(t+1)d-t=0.$$

From this equation and $w(t)=0$, we can rewrite $\psi^3(a)=r(a,d)$ above in terms of t.

The above calculations are summarized as follows.

Proposition 19 *The universal degree 3 isogeny with source $\mathcal{E}$ is defined over the ring $F^0[\![t]\!]/\big(a^2t^4+3a^2t^3+3a^2t^2+(a^2+4)t+3\big)$, and has target the elliptic curve*

$$y^2+rxy+ry=x^3+x^2,$$

where $r(a,t)=a^3t^3+3a^3t^2+3a^3t-4at+a^3-3a$. The kernel of this isogeny is generated by the 3-torsion point with x-coordinate $1/t$. Thus the power operation ψ^3 is given by

$\psi^3(h)=(t+1)^3h^3-(22t^3+69t^2+75t+27)h^2+(128t^3+424t^2+512t+201)h-16(14t^3+49t^2+65t+27),$

$\psi^3(a)=(t+1)^3a^3-(4t+3)a.$

Remark 20 Recall that $F^0=\mathbb{Z}_9[\![h]\!]$. In the above we also give the formula for $\psi(a)$ since $a\in F^0$. In fact, we have

$$a^2=h-4\equiv -1 \mod (3,h),$$

where the ideal $(3,h)$ is prime in $\mathbb{Z}[h]$. Thus by Hensel's lemma, $a-i\in\mathbb{Z}_3[\![h]\!]$, where $i^2+1=0$. But i generates $\mathbb{Z}_9$ over $\mathbb{Z}_3$.

4.3 $K(1)$-localize

As in example 14, with $h=a^2+4$ invertible, we can solve for t 3-adically from the equation $w(t)=0$ by first writing

$$t=-\frac{1}{a^2+4}(a^2t^4+3a^2t^3+3a^2t^2+3),$$

and then substituting t recursively. Plugging this uniquely determined value of t into $\psi^3(h,t)$ computed above, we get the $K(1)$-local power operation ψ as an endomorphism of the ring $E^0 = \mathbb{Z}_9(\!(h)\!)_3^\wedge$.

References

[Ada74] J. F. Adams, *Stable homotopy and generalised homology*, University of Chicago Press, Chicago, Ill., 1974, Chicago Lectures in Mathematics.

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

[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.

[Bor94] Francis Borceux, *Handbook of categorical algebra. 2*, Encyclopedia of Mathematics and its Applications, vol. 51, Cambridge University Press, Cambridge, 1994, Categories and structures.

[Bou79] A. K. Bousfield, *The localization of spectra with respect to homology*, Topology **18** (1979), no. 4, 257–281.

[Car54] Henri Cartan, *Sur les groupes d'Eilenberg-Mac Lane. II*, Proc. Nat. Acad. Sci. U. S. A. **40** (1954), 704–707.

[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.

[Frö68] A. Fröhlich, *Formal groups*, Lecture Notes in Mathematics, No. 74, Springer-Verlag, Berlin, 1968.

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

[Hopb] Mike Hopkins, *Complex oriented cohomology theories and the language of stacks*, available at http://www.math.rochester.edu/u/faculty/doug/otherpapers/coctalos.pdf.

[HS99] Mark Hovey and Neil P. Strickland, *Morava K-theories and localisation*, Mem. Amer. Math. Soc. **139** (1999), no. 666, viii+100.

[KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985.

[Law63] F. William Lawvere, *Functorial semantics of algebraic theories*, Proc. Nat. Acad. Sci. U.S.A. **50** (1963), 869–872.

[Law09] Tyler Lawson, *An overview of abelian varieties in homotopy theory*, New topological contexts for Galois theory and algebraic geometry (BIRS 2008), Geom. Topol. Monogr., vol. 16, Geom. Topol. Publ., Coventry, 2009, pp. 179–214.

[LN] Tyler Lawson and Niko Naumann, *Topological modular forms of level 3 and E_∞-structures on truncated Brown-Peterson spectra*, arXiv:1101.3897.

[LT66] Jonathan Lubin and John Tate, *Formal moduli for one-parameter formal Lie groups*, Bull. Soc. Math. France **94** (1966), 49–59.

[Lub67] Jonathan Lubin, *Finite subgroups and isogenies of one-parameter formal Lie groups*, Ann. of Math. (2) **85** (1967), 296–302.

[Lur] Jacob Lurie, *Chromatic homotopy theory*, available at http://www.math.harvard.edu/~lurie/252x.html.

[Lur09] J. Lurie, *A survey of elliptic cohomology*, Algebraic topology, Abel Symp., vol. 4, Springer, Berlin, 2009, pp. 219–277.

[Mas83] W. S. Massey, *Cross products of vectors in higher-dimensional Euclidean spaces*, Amer. Math. Monthly **90** (1983), no. 10, 697–701.

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

[MT68] Robert E. Mosher and Martin C. Tangora, *Cohomology operations and applications in homotopy theory*, Harper & Row Publishers, New York, 1968.

[Rav86] Douglas C. Ravenel, *Complex cobordism and stable homotopy groups of spheres*, Pure and Applied Mathematics, vol. 121, Academic Press Inc., Orlando, FL, 1986.

[Rav92] ______, *Nilpotence and periodicity in stable homotopy theory*, Annals of Mathematics Studies, vol. 128, Princeton University Press, Princeton, NJ, 1992, Appendix C by Jeff Smith.

[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.

[Rezc] ______, *Power operations in Morava E-theory: a survey*, available at http://www.math.uiuc.edu/~rezk/midwest-2009-power-ops-handout.pdf.

[Rez98] ______, *Notes on the Hopkins-Miller theorem*, Homotopy theory via algebraic geometry and group representations (Evanston, IL, 1997), Contemp. Math., vol. 220, Amer. Math. Soc., Providence, RI, 1998, pp. 313–366.

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

[Ser53] Jean-Pierre Serre, *Cohomologie modulo 2 des complexes d'Eilenberg-MacLane*, Comment. Math. Helv. **27** (1953), 198–232.

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[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.

[Str97] Neil P. Strickland, *Finite subgroups of formal groups*, J. Pure Appl. Algebra **121** (1997), no. 2, 161–208.

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

[TO70] John Tate and Frans Oort, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21.

[Wil82] Clarence Wilkerson, *Lambda-rings, binomial domains, and vector bundles over* $\mathbf{C}P(\infty)$, Comm. Algebra **10** (1982), no. 3, 311–328.