

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

YIFEI ZHU

We give an overview of the structure of the Dyer-Lashof theories associated to Morava E -theories, and to their $K(1)$ -localizations in particular, leading to the connection with explicit calculations of elliptic curves when the E -theory is an elliptic cohomology theory.

1 Introduction

The study of cohomology operations has become central to algebraic topology since the 1950s, with applications to problems such as vector fields on spheres, and the non-existence of elements of Hopf invariant one, the latter of which has impact on the author most recently felt when he tried to answer a question raised by students in a calculus class (interested readers might see [8]).

1.1 Dyer-Lashof theories

One organizing principle for understanding the structure among operations is through the *algebraic theories* of operations. An (*algebraic*) *theory* is a category T with object set $\{T^0, T^1, T^2, \dots\}$, together with *projection maps* $\pi_i: T^n \rightarrow T^1$ 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 , ie T^n is isomorphic to the n -fold product of T^1 . Also there is a canonical map $T^0 \rightarrow T^1$. A *morphism of theories* is a functor $\phi: T \rightarrow T'$ which preserves the product structure of a theory, ie $\phi(T^k) = T'^k$ and $\phi(T^k \xrightarrow{\pi_i} T^1) = T'^k \xrightarrow{\pi'_i} T'^1$.

A *model* of the theory T is a functor $A: T \rightarrow \text{Set}$ which preserves finite products. It can be thought of as the underlying set $X = A(T^1)$ together with operations $\psi_f: X^k \rightarrow X^n$ corresponding to 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 $\{F_0, F_1, F_2, \dots\}$, where $F_0 = R$ and $F_n = R[x_1, \dots, x_n]$ for $n \geq 1$. We then have the theory of commutative R -algebras $C_R = F^{\text{op}}$.

A *commutative operation theory* (COT) is a triple (T, R, ϕ) consisting of a theory T , a commutative ring R , and a morphism $\phi: C_R \rightarrow T$ of theories, such that the induced functor $\phi^*: \text{Model}_T \rightarrow \text{Model}_{C_R}$ 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 will write $R\{x_1, \dots, x_n\}$ for a free T -model on n generators, and we have $R\{x_1, \dots, x_n\} \cong R\{x_1\} \otimes_R \dots \otimes_R R\{x_n\}$.

We next introduce grading to a theory by having a fixed set C of *colors*. Let $\mathbb{N}[C]$ be the free commutative monoid on C . A C -graded theory T is then a category with object set $\{T^d\}_{d \in \mathbb{N}[C]}$, together with, for each $d = \sum_{c \in C} d_c [c] \in \mathbb{N}[C]$, a specified identification of T^d with the product $\prod_{c \in C} (T^{[c]})^{d_c}$. In particular, we can define a graded COT as a triple (T, R_*, ϕ) similarly as above, with T a \mathbb{Z} -graded theory and R_* a graded commutative ring.

For a graded COT (T, R_*, ϕ) , 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 $R_*\{x\} \xrightarrow{x \mapsto x_1 + x_2} R_*\{x_1, x_2\}$, where $|x| = |x_1| = |x_2| = c$. Such $f \in \mathcal{A}(c, d)$ give rise to additive functions $A_c \rightarrow A_d$ 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

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

where we use homotopy classes of maps, and use the convention that $K(\mathbb{F}_p, c) = *$ for $c < 0$. Then $\text{Model}_{O_{H\mathbb{F}_p}}$ is the category of unstable algebras over the mod- p Steenrod algebra, and $\mathcal{A}(c, d)$ is the set of additive operations $H^c(-; \mathbb{F}_p) \rightarrow H^d(-; \mathbb{F}_p)$, which, for $p = 2$, are linear combinations of monomials as admissible composites of Steenrod operations having excess no more than c .

Having the COT describing cohomology operations on spaces, we next consider one describing operations on spectra. Given a commutative S -algebra R (S is the sphere spectrum), the *Dyer-Lashof theory* DL_R is the \mathbb{Z} -graded theory T defined by

$$T(T^{[c_1] + \dots + [c_m]}, T^{[d_1] + \dots + [d_n]}) = h\text{Alg}_R\left(\mathbb{P}_R(R \wedge (S^{d_1} \vee \dots \vee S^{d_n})), \mathbb{P}_R(R \wedge (S^{c_1} \vee \dots \vee S^{c_m}))\right),$$

where \mathbb{P} is the free algebra functor defined by $\mathbb{P}(X) = \bigvee_{m \geq 0} \mathbb{P}^m(X) = \bigvee_{m \geq 0} X^{\wedge m} / \Sigma_m$.

We have the identification $\mathbb{P}^m(S^c) \cong B\Sigma_m^{cV_m}$, where $V_m = \mathbb{R}^m$ equipped with the Σ_m -action given by permuting coordinates, and $c \in \mathbb{Z}$, so that the right-hand side is the Thom spectrum of a virtual bundle. The free theories are given by

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

Moreover, if $\pi_* R \wedge \mathbb{P}(S^c)$ are flat as left $\pi_* R$ -modules, DL_R becomes a COT. The significance of DL_R is that it describes all homotopy operations on commutative R -algebras:

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

For example, if R is a ring (no longer a spectrum) containing \mathbb{F}_2 , there is a complete description of DL_{HR} , which is a COT. A DL_{HR} -model is a graded commutative R -algebra A_* , equipped with functions $Q^s: A_c \rightarrow A_{c+s}$ for all $s, c \in \mathbb{Z}$, satisfying a bunch of properties, eg the Cartan formula and the Adem relations.

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 [4, 2]), which corresponds to a stratification of the moduli stack of formal groups into layers according to height. 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, given any complex oriented cohomology theories. Morava E -theories are universal among cohomology theories at each fixed layer of this filtration. More precisely, for each formal group law F of height $n < \infty$ over a perfect field k of characteristic p , there is an E_∞ ring spectrum $E_n(k, F)$ whose homotopy groups are the Lubin-Tate ring $\mathbb{W}k[[v_1, \dots, v_{n-1}]]$ which is universal among complete local rings with residue field k carrying a formal group law whose reduction to k is F .

Given a Morava E -theory E_* , there is an associated Dyer-Lashof theory DL_{E_*} describing all E -cohomology operations, which 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). 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.

In the following sections we discuss the structure of DL_{E_*} . As is explained right at the beginning of [1], 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 . Based on knowledge of the spectrum E , we study the structure of DL_{E_*} , the \mathbb{Z} -graded Dyer-Lashof theory associated to E_* , which describes 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 E is an elliptic spectrum, these are parametrized by finite subgroups of the formal group of the associated elliptic curve, and thus we may study the operations by doing calculations of elliptic curves.

2.1 Identifications of categories

First we consider the 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 [15]). Thus $\mathcal{A} = \bigoplus_{r \geq 0} \mathcal{A}_r$ is an associative (not necessarily commutative) graded ring with respect to a 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 $\text{Mod}_{\mathcal{A}}$ of left \mathcal{A} -modules naturally admits a tensor product.

We formulate a category equivalent to $\text{Mod}_{\mathcal{A}}$, 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} . If A is an R -algebra, we write $\text{Frob}^*: \sigma^*A \rightarrow A$ for the map of R -algebras which fits into the diagram

$$\begin{array}{ccc}
 R & \xrightarrow{\sigma} & R \\
 \downarrow & & \downarrow \\
 A & \xrightarrow{\quad} & \sigma^*A \\
 & \searrow \sigma & \swarrow \text{Frob}^* \\
 & & A,
 \end{array}$$

where σ sends an element to its p th power. In particular, if G is a formal group over R , there is an isogeny $\text{Frob}: G \rightarrow \sigma^*G$ of formal groups over R defined by $\text{Frob}^*: \mathcal{O}_{\sigma^*G} = \sigma^*\mathcal{O}_G \rightarrow \mathcal{O}_G, R[[y]] \rightarrow R[[x]]$ 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 $i: k \rightarrow R/\mathfrak{m}$ and an isomorphism $\alpha: G_0 \rightarrow i^*\Gamma$ of formal groups over R/\mathfrak{m} . And a \star -isomorphism $(G, i, \alpha) \rightarrow (G', i', \alpha')$ is an isomorphism $\phi: G \rightarrow G'$ of formal groups over R such that $i' = i$ and $\alpha' \circ \phi_0 = \alpha$. We define $\text{DefFrob}_\Gamma(R)$ to be the category whose objects are deformations of Γ to R , and whose morphisms are isogenies which are deformations of Frobenius, ie a morphism $(G, i, \alpha) \rightarrow (G', i', \alpha')$ is an isogeny $\phi: G \rightarrow G'$ such that $i' = \sigma^r \circ i$ and $\alpha' \circ \phi_0 = \text{Frob}^r \circ \alpha$ for some $r \geq 0$. In particular, ϕ is precisely a \star -isomorphism if $r = 0$.

We then define a category $\text{Mod}_{\text{DefFrob}_\Gamma}$ as follows, which is the category of sheaves of modules on $\text{DefFrob}_\Gamma = \{\text{DefFrob}_\Gamma(R)\}$. An object \mathcal{F} consists of

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

$$\mathcal{F}_R: \text{DefFrob}_\Gamma(R)^{\text{op}} \rightarrow \text{Mod}_R,$$

- (2) for each local homomorphism $f: R \rightarrow R'$, a natural isomorphism

$$\mathcal{F}_f: f^*\mathcal{F}_R \rightarrow \mathcal{F}_{R'}f^*,$$

where the first f^* is the functor $\text{Mod}_R \rightarrow \text{Mod}_{R'}$ of extending scalars along f , and the second $f^*: \text{DefFrob}_\Gamma(R)^{\text{op}} \rightarrow \text{DefFrob}_\Gamma(R')^{\text{op}}$ is induced by f (as $\text{DefFrob}_\Gamma(-)$ is a functor),

such that they admit coherent natural isomorphisms

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

And a morphism $\eta: \mathcal{F} \rightarrow \mathcal{G}$ is a collection of natural transformations $\eta_R: \mathcal{F}_R \rightarrow \mathcal{G}_R$ such that $\mathcal{G}_f \circ f^*(\eta_R) = \eta_{R'}(f^*) \circ \mathcal{F}_f$. Moreover, this is a tensor category with $\mathcal{F} \otimes \mathcal{G}$ given by $(\mathcal{F} \otimes \mathcal{G})_R(G) = \mathcal{F}_R(G) \otimes_R \mathcal{G}_R(G)$.

Theorem 1 ([9]) *There is an equivalence of tensor categories $U: \text{Mod}_{\mathcal{A}} \rightarrow \text{Mod}_{\text{DefFrob}_\Gamma}$.*

Next we consider $\text{Model}_{\text{DL}_{E_0}}$, the category of models for the theory DL_{E_0} , on which \mathcal{A} acts so that there is a forgetful functor $\text{Model}_{\text{DL}_{E_0}} \rightarrow \text{Mod}_{\mathcal{A}}$ along which the coproduct of DL_{E_0} -models and the tensor product of $\text{Mod}_{\mathcal{A}}$ agree. We define a category $\text{Alg}_{\text{DefFrob}_\Gamma}$ as follows. An object \mathcal{B} is a ring object in $\text{Mod}_{\text{DefFrob}_\Gamma}$ which satisfies

(b) the *Frobenius congruence*, ie the diagram

$$\begin{array}{ccc}
 \sigma^* \mathcal{B}_R(G) & \xrightarrow{\text{Frob}^*} & \mathcal{B}_R(G) \\
 \mathcal{B}_\sigma(G) \downarrow \wr & \nearrow \mathcal{B}_R(\text{Frob}) & \\
 \mathcal{B}_R \sigma^*(G) & &
 \end{array}$$

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

And morphisms 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 .

Theorem 2 ([9]) *There is a functor $U: \text{Model}_{\text{DL}_{E_0}} \rightarrow \text{Alg}_{\text{DefFrob}_\Gamma}$, and it restricts to an equivalence $U: \text{Model}_{\text{DL}_{E_0}}^{\text{tf}} \rightarrow \text{Alg}_{\text{DefFrob}_\Gamma}^{\text{tf}}$ of 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 $\text{Mod}_{\text{DefFrob}_\Gamma}$ and $\text{Alg}_{\text{DefFrob}_\Gamma}$, by studying the structure of the category $\text{DefFrob}_\Gamma(R)$ of deformations of Frobenius. This turns out to be parametrized by subgroups of the deformations of Γ to R .

Choosing a coordinate of a formal group G over R , a degree (or rank) d subgroup K of G is an effective divisor with $\mathcal{O}_K = R[[x]]/(f(x))$ for some degree d monic polynomial $f(x)$ such that $f(x_1 +_G x_2) \in (f(x_1), f(x_2))$ and $f(x) \in (x)$, ie the group law of G restricts to K and K contains the identity. One can show that the homomorphism $[d]_G: G \rightarrow G$ restricts to zero on K (cf [16]). 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 , there is exactly one subgroup of degree p^r , given by $f(x) = x^{p^r}$, which is the kernel of Frob^r .

We have seen that in $\text{DefFrob}_\Gamma(R)$ the “degree 1” morphisms (when $r = 0$) are precisely the \star -isomorphisms of deformations. In general, including the cases when $r \geq 0$, $\text{DefFrob}_\Gamma(R)$ can be shown to be equivalent to the following category (cf [9]). The objects are \star -isomorphism classes of deformations $[G]$. And 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 $G \rightarrow G/K \cong G' \rightarrow G'/K'$. Thus deformations of Frobenius with source (G, i, α) correspond *exactly* to finite subgroups of G .

Example 3 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 $1 + (x_1 +_{\mathbb{G}_m} x_2) = (1 + x_1)(1 + x_2)$, inductively 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 [7]), every object of $\text{DefFrob}_\Gamma(R)$ 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 $\mathcal{O}_{\text{univ}} = \mathbb{Z}_p$, 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 $\mathcal{B} \in \text{Alg}_{\text{DefFrob}_\Gamma}$, it is enough to give

- (1) a \mathbb{Z}_p -algebra $B = \mathcal{B}_{\mathbb{Z}_p}(\mathbb{G}_m)$,
- (2) maps of \mathbb{Z}_p -algebras $\psi^{p^r} : B \rightarrow B$ (corresponding to the isogenies $[p^r] : \mathbb{G}_m \rightarrow \mathbb{G}_m$) such that
 - (a) $\psi^1 = \text{id}_B$ and $\psi^{p^r} \circ \psi^{p^s} = \psi^{p^{r+s}}$,
 - (b) $\psi^p(b) \equiv b^p \pmod{pB}$.

(For comparison, the items are labelled as in the definitions of $\text{Mod}_{\text{DefFrob}_\Gamma}$ and $\text{Alg}_{\text{DefFrob}_\Gamma}$ above.) We note as in [12] that this is a “ p -typicalization” of the original theorem of Wilkerson (cf [17]), 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 $A \cong A_p^\wedge$), ψ^p recovers the classical p th Adams operation. On the other hand, if B contains \mathbb{F}_p , then $\psi^p(b) = b^p$ is the classical Frobenius map on the ring of Witt vectors $\mathbb{W}B = \text{Hom}_{\text{Alg}_{\mathbb{Z}_p}}(\Lambda, B)$, where $\Lambda = \mathbb{Z}_p[x_k, k \geq 0]$. For more discussions on Lubin’s theory of isogenies and the p -series of the multiplicative formal group, which underlies this example, see [1, example 2.7].

In general, 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 , is represented by the complete local ring $\mathcal{O}_{X_r} = E^0 B \Sigma_{p^r} / I$, where $I = \sum_{0 < i < p^r} \text{Image}(E^0 B(\Sigma_i \times \Sigma_{p^r-i}) \xrightarrow{\text{transfer}} E^0 B \Sigma_{p^r})$ is the *transfer ideal* (roughly speaking, the corresponding power operation should be additive, so modulo the “extra terms” in the Cartan formula). This can be viewed

as a generalization of the Lubin-Tate theorem for $\mathcal{O}_{\text{univ}} = \mathcal{O}_{X_0}$. Moreover, there are two ring homomorphisms $s^*, t^*: \mathcal{O}_{\text{univ}} \rightarrow \mathcal{O}_{X_r}$, where s^* represents the source map $[G > K] \mapsto [G]$, and t^* represents the target map $[G > K] \mapsto [G/K]$. (In the example of multiplicative formal group, $\mathcal{O}_{X_r} \cong \mathcal{O}_{\text{univ}}$ for all r , and $s^* = t^* = \text{id}$.) Thus to describe an object $\mathcal{B} \in \text{Alg}_{\text{DefFrob}_r}$, it is enough to give

- (1) an $\mathcal{O}_{\text{univ}}$ -algebra $B = \mathcal{B}_{\mathcal{O}_{\text{univ}}}(G_{\text{univ}})$,
- (2) maps of $\mathcal{O}_{\text{univ}}$ -algebras $\psi^{p^r}: B \rightarrow B \otimes_{\mathcal{O}_{\text{univ}}}^{s^*} \mathcal{O}_{X_r}$ (as the composite

$$B \xrightarrow{f^*} B \otimes_{\mathcal{O}_{\text{univ}}}^{t^*} \mathcal{O}_{X_r} \xrightarrow{\mathcal{B}_f} \mathcal{B}_{\mathcal{O}_{X_r}}(t^* G_{\text{univ}}) \xrightarrow{\mathcal{B}_{\mathcal{O}_{X_r}}(\psi)} \mathcal{B}_{\mathcal{O}_{X_r}}(s^* G_{\text{univ}}) \xrightarrow{\mathcal{B}_g} B \otimes_{\mathcal{O}_{\text{univ}}}^{s^*} \mathcal{O}_{X_r},$$

where $f = t^*$ and $g = s^*$ are local homomorphisms, and $\psi: s^* G_{\text{univ}} \rightarrow t^* G_{\text{univ}}$ is an isogeny as the universal deformation of Frob^r (cf [15])),

satisfying a bunch of formal properties. In particular, the Frobenius congruence (b) amounts to requiring that

$$B \xrightarrow{\psi^p} B \otimes_{\mathcal{O}_{\text{univ}}}^{s^*} \mathcal{O}_{X_1} \xrightarrow{\text{id} \otimes u^*} B \otimes_{\mathcal{O}_{\text{univ}}} \mathcal{O}_{\text{univ}}/(p) = B/pB$$

factor through the p th power map $\sigma: B/pB \rightarrow B/pB$, where $u^*: \mathcal{O}_{X_1} \rightarrow \mathcal{O}_{\text{univ}}/(p)$ represents the universal Frobenius isogeny.

Example 4 Consider the elliptic curve $C_0 \subset \mathbb{P}_{\mathbb{F}_2}^2$ 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 (with $|a| = 0$) is the Hasse invariant so that setting $a = 0$ we recover the supersingular elliptic curve C_0 . 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 [1], with explicit formulas computed in [10, 11].

By studying degree 2 subgroups, ie subgroups of 2-torsion points on the elliptic curve, 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 C of the form $(u(Q), v(Q)) = (d, -d^3)$ such that $d^3 - ad - 2 = 0$. Thus we have a power operation

$$\psi^2: E^0 X \rightarrow E^0 X[d]/(d^3 - ad - 2).$$

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

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

together with formulas for

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

In particular, the Frobenius congruence takes the form $Q_0(x) \equiv x^2 \pmod{2}$. 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 [3].

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 4 is such, which we now write $F = E_2$, specifying its height.

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

$$\begin{array}{ccc} F^0 & \xrightarrow{\psi^p} & F^0 B\Sigma_p / I \\ \downarrow & & \downarrow L \\ E^0 & \xrightarrow{\psi^p} & E^0 B\Sigma_p / I \cong E^0. \end{array}$$

Recall that the top operation arises from the universal deformation of Frobenius, which is represented by the ring $\mathcal{O}_{X_1} = F^0 B\Sigma_p / I$, where $I = \sum_{0 < i < p} \text{Image}(E^0 B(\Sigma_i \times \Sigma_{p-i}) \xrightarrow{\text{transfer}} E^0 B\Sigma_p)$ is the transfer ideal. The vertical maps are induced by the $K(1)$ -localization $F \rightarrow E$. In terms of homotopy groups, it is obtained by inverting

the height 2 generator v_1 and completing at the ideal (p) , ie $F^0 = \mathbb{W}k[[v_1, \dots, v_{n-1}]]$ and $E^0 = \mathbb{W}k[[v_1, \dots, v_{n-1}]]_p^\wedge$. For example, $\pi_0 L_{K(1)} E_2 = \varprojlim \mathbb{Z}((a))/(2^i) = \{\sum_{n=-\infty}^{\infty} c_n a^n \mid c_n \in \mathbb{Z}_2, c_n \rightarrow 0 \text{ 2-adically as } n \rightarrow -\infty\}$. 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 explicit 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 $0 \rightarrow \mathbb{G}^{\text{for}} \rightarrow \mathbb{G}_x \rightarrow \mathbb{G}^{\text{ét}} \rightarrow 0$ with the subobject (the connected component of the identity) the *formal* component and the quotient the *étale* component. The formal component \mathbb{G}^{for} is a formal group on X . The localization L factors through $E^0 \otimes_{F^0} F^0 B\Sigma_p/I$, and along the base change $F^0 B\Sigma_p/I \rightarrow E^0 \otimes_{F^0} F^0 B\Sigma_p/I$ the p -divisible group consisting solely of formal component may split into formal and étale components. We want to take the formal component so that the unique subgroup classified by L lands in the formal group over $E^0 B\Sigma_p/I$.

Example 5 We continue example 4 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 [6]. To be explicit, 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 $\pi_0 L_{K(1)} E_2 \cong \mathbb{Z}_2((a))$. Plugging this specific value of d into $\psi^2: \pi_0 E_2 \rightarrow \pi_0 E_2[d]/(d^3 - ad - 2)$, 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 [5, 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, namely the uniqueness of the degree p subgroup after localization, is specific to the height 1 case.

Lemma 6 $E^0 B\Sigma_p/I \cong E^0$.

We can interpret this isomorphism as generalizing what we have seen in example 3 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 thus the ring $E^0 B\Sigma_p/I$ classifying subgroup of

degree p is isomorphic to E^0 so that the power operation takes the form $\psi^p: E^0 \rightarrow E^0$ which is a lift of Frobenius. In general a height n formal group has $(p^n - 1)/(p - 1)$ degree p subgroups, as can be seen from the calculations in the proof below, and in the example of section 4 where $n = 2$ and $p = 3$.

Proof First we identify $E^0 B\Sigma_p$ as the subset of $E^0 BC_p$ fixed by the action induced by $\text{Aut} C_p \cong \mathbb{F}_p^\times$. This is a special case of the calculations in [9, section 12]. We have

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

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, $\text{Aut} C_p$ acts on $\text{Hom}(C_p, \Sigma_p)$ by precomposing, which induces homotopic maps $BC_p \rightarrow B\Sigma_p$, and thus the same map $E^0 B\Sigma_p \rightarrow E^0 BC_p$. We can calculate $E^0 BC_p$ by considering the pullback square

$$\begin{array}{ccc} BC_p & \longrightarrow & BS^1 \\ \downarrow \lrcorner & & \downarrow \otimes p \\ * & \longrightarrow & BS^1, \end{array}$$

where the right-hand vertical map sends the tautological line bundle to its p th tensor power. Applying $E^0(-)$ we have a pushout square where the right-hand vertical map becomes $[p]: E^0[u] \rightarrow E^0[u]$ with u the first Chern class of the tautological line bundle and $[p](u)$ the p -series of the formal group law of E . Thus $E^0 BC_p \cong E^0[u]/([p](u))$, where $[p](u) = pu + \dots + v_1 u^p + \dots$ with v_1 invertible in $E^0 \cong \mathbb{W}k[v_1, \dots, v_{n-1}][v_1^{-1}]_p^\wedge$. For $q \in \mathbb{F}_p^\times$, the induced action on $E^0 BC_p$ sends u to $[q](u) = qu + \dots$. Hence $E^0 B\Sigma_p \cong (E^0 BC_p)^{\text{Aut} C_p} \cong E^0 \oplus (E^0 \cdot \prod_{q=1}^{p-1} [q](u)) = E^0 \oplus (E^0 \cdot (u^{p-1} + \dots))$.

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

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

is the identity, and thus $E^0 B(\Sigma_i \times \Sigma_{p-i}) \cong E^0$. Moreover, by the “double-coset formula” the composite

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

has image the same as $E^0 \xrightarrow{\text{tr}} E^0 BC_p$. Thus I is generated by $\text{tr}(1)$ as an E^0 -module. Write $E^0 BC_p = E^0[[u]]/[p](u) = E^0[[u]]/(u \cdot \langle p \rangle(u))$, where $\langle p \rangle(u) = p + \cdots + v_1 u^{p-1} + \cdots$, and write $\text{tr}(1) = f(u) \in E^0[[u]]$ by abuse of notation. Since the composite

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

is multiplication by p , $f(0) = \text{res}(f(u)) = \text{res}(\text{tr}(1)) = p$. Moreover $u \cdot f(u) = u \cdot \text{tr}(1) = \text{tr}(\text{res}(u)) = \text{tr}(0) = 0$, and thus $u \cdot f(u)$ is divisible by $[p](u)$. We claim that $f(u) = \langle p \rangle(u)$. Clearly $\langle p \rangle(u)$ starts with p and is annihilated by u in $E^0[[u]]/(u \cdot \langle p \rangle(u))$. 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 every 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 $I = E^0 \cdot \langle p \rangle(u)$. As v_1 is invertible in E^0 , $E^0 B\Sigma_p / (\langle p \rangle(u)) \cong E^0$. \square

We also note that at height 1, as in example 3, the power operation ψ^p determines the other operations ψ^{p^r} for $r > 1$ by self composition. Thus in the $K(1)$ -local setting it suffices to study only ψ^p as above, and 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 [10], 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 4). 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. Many ideas in carrying out these calculations were suggested by the author's advisor, Tyler Lawson.

The Morava E -theory F of height 2 we consider here is associated to the deformations of a supersingular elliptic curve over \mathbb{F}_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 elliptic curve - in particular, we need to compute
 - the coordinate ring parametrizing degree 3 subgroups,
 - the equation of the quotient curve as the image of the universal degree 3 isogeny;
- (3) $K(1)$ -localize.

We try to make the calculations along a general recipe in hope of adaptability to larger primes.

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

First we note that a supersingular elliptic curve over \mathbb{F}_3 cannot have a 3-torsion point, and in order to have a unique lift of the elliptic curve together with a choice of N -torsion point along a deformation of $k = \mathbb{F}_3$ to a complete local ring R with residue field containing k , N must be prime to 3. As the associated moduli stack $\mathcal{M}(\Gamma_1(2))$ 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, the 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 [13, proposition 3.2], where the universal elliptic curve used for the prime 2 case has a choice of 3-torsion point. 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 $\mathbb{G}_m = \text{Spec} \mathbb{Z}[\lambda^{\pm 1}]$ given by $a \mapsto \lambda a$ and $c \mapsto \lambda^2 c$. By [14, theorem 4.1(a)], the Hasse invariant can be computed as $h = a^2 + 4c$, so that the curve is supersingular precisely when $h = 0$. To facilitate calculation, we work in the affine coordinate chart $c = 1$ of $\mathcal{M}(\Gamma_1(4))$ so that the elliptic curve is given by

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

with $\Delta = a^2(a + 4)(a - 4)$ and $h = a^2 + 4$. This reduction is analogous to the one discussed in detail in [5, section 4]. In uv -coordinates, with $u = x/y$ and $v = 1/y$, this is

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

which is the form we will use most often later. We denote this elliptic curve by \mathcal{E} .

We note that \mathcal{E} , together with the universal elliptic curve with a choice of 3-torsion point studied in [13] and [10], give models for *all* primes.

4.2 Degree 3 subgroups

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

$$\psi_3(x) = 3x^4 + (a^2 + 4)x^3 + 3a^2x^2 + 3a^2x + a^2 = 0$$

(cf [14, 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 explicitly in the formal neighborhood of the identity (in xy -coordinates, the identity is at ∞), and get a “characteristic” equation comparable to $d^3 - ad - 2 = 0$ in example 4, 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 [14, 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

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

coming from the equation of \mathcal{E} . 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 a 3-torsion point (d, e) must satisfy $f(d) = 0$.

We note that according to section 3, in particular example 5, $f(u)$ should have a unique root reduced to zero modulo 3 after $h = a^2 + 4$ gets inverted. We compute that

$$f(u) \equiv u^2(u + a)^6 \pmod{3},$$

and in view of $a \neq 0$ by the nonsingularity of \mathcal{E} (recall that $\Delta = a^2(a+4)(a-4)$), such a root has multiplicity 2. Thus $f(u)$, extracted out of a conjugation procedure, is not ideal in this aspect. This is the best possible polynomial solely about u we have at this point, and in later steps we will have to improve and “rescale” it back to a degree 4 polynomial.

Next we want to express e in terms of d . At the prime 2 (cf example 4), the relation $e = -d^3$ can be obtained, for example, 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 [10]. 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

$$B(v) = av^2 + (1 + au - u^2)v - u^3 \quad (\text{equation of } \mathcal{E}),$$

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 explicit 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 14 polynomial $e = g(d)$, comparable to $e = -d^3$ in the prime 2 case.

Now we are ready to compute the universal degree 3 isogeny and thus the equation of the quotient curve, from which we can find an explicit formula for the power operation $\psi^3: F^0 \rightarrow F^0[d]/(f(d))$, where $F^0 = \mathbb{Z}_3[[h]]$ (to be precise, the target should actually be a certain improved coordinate ring as promised earlier).

We follow the “Lubin isogeny” construction (cf [6, proof of theorem 1.4]) to compute the coordinates (u', v') of the isogeny as follows. Let $P(u, v(u))$ be a general point on \mathcal{E} , and $Q(d, e(d))$ be a 3-torsion point. For $v(u)$, we use an approximation with the first few terms (up to at least degree 9 for our purpose) from the power series expansion of

one of the roots (the one lying in the formal neighborhood of the identity, ie $v(0) = 0$) of the quadratic equation

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

for $e(d)$, we use the polynomial $g(d)$ computed above. 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 explicit formulas for $u' = \alpha u + \dots$ and $v' = \beta u^3 + \dots$ in terms of the uniformizer u and parameters a and d . We note that 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 [10]. We then solve for the Weierstrass equation which u' and v' satisfy so that the equation of the quotient curve turns out to be

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

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, and we check that it reduces to a^3 modulo 3 (the Frobenius congruence at height 1 over \mathbb{F}_3), as $d \equiv 0 \pmod{3}$.

Lastly we compute the coordinate ring as the target of the power operation ψ^3 . Set $t = g(d)/d$, which is the inverse 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 its formal neighborhood (in the xy -coordinates the identity is at ∞). Given that $f(d) = 0$, 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 .

Proposition 7 *The universal degree 3 isogeny with source \mathcal{E} is defined over the ring $F^0[\Delta^{-1}][t]/(a^2t^4 + 3a^2t^3 + 3a^2t^2 + (a^2 + 4)t + 3)$, 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

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

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

4.3 $K(1)$ -localize

As in example 5, 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 $E^0 = \mathbb{Z}_3((h))[\Delta^{-1}]_3^\wedge$.

References

- [1] **M Ando**, *Isogenies of formal group laws and power operations in the cohomology theories E_n* , Duke Math. J. 79 (1995) 423–485
- [2] **MJ Hopkins**, *Complex oriented cohomology theories and the language of stacks*, available at <http://www.math.rochester.edu/u/faculty/doug/otherpapers/coctalos.pdf>
- [3] **MJ Hopkins**, *$K(1)$ -local E_∞ ring spectra*, available at <http://www.math.rochester.edu/u/faculty/doug/otherpapers/knlocal.pdf>

- [4] **T Lawson**, *An overview of abelian varieties in homotopy theory*, from: “New topological contexts for Galois theory and algebraic geometry (BIRS 2008)”, *Geom. Topol. Monogr.* 16, *Geom. Topol. Publ.*, Coventry (2009) 179–214
- [5] **T Lawson**, **N Naumann**, *Topological modular forms of level 3 and E_∞ -structures on truncated Brown-Peterson spectra*, arXiv:1101.3897
- [6] **J Lubin**, *Finite subgroups and isogenies of one-parameter formal Lie groups*, *Ann. of Math.* (2) 85 (1967) 296–302
- [7] **J Lubin**, **J Tate**, *Formal moduli for one-parameter formal Lie groups*, *Bull. Soc. Math. France* 94 (1966) 49–59
- [8] **W S Massey**, *Cross products of vectors in higher dimensional Euclidean spaces*, *Amer. Math. Monthly* 90 (1983) 697–701
- [9] **C Rezk**, *Lectures on power operations*, available at <http://www.math.uiuc.edu/~rezk/power-operation-lectures.dvi>
- [10] **C Rezk**, *Power operations for Morava E -theory of height 2 at the prime 2*, arXiv:0812.1320
- [11] **C Rezk**, *Power operations in Morava E -theory: a survey*, available at <http://www.math.uiuc.edu/~rezk/midwest-2009-power-ops-handout.pdf>
- [12] **C Rezk**, *The congruence criterion for power operations in Morava E -theory*, *Homology, Homotopy Appl.* 11 (2009) 327–379
- [13] **C Rezk**, **M Mahowald**, *Topological modular forms of level 3*, *Pure Appl. Math. Q.* 5 (2009) 853–872
- [14] **J H Silverman**, *The arithmetic of elliptic curves, Second edition*, volume 106 of *Graduate Texts in Mathematics*, Springer, Dordrecht (2009)
- [15] **N P Strickland**, *Morava E -theory of symmetric groups*, *Topology* 37 (1998) 757–779
- [16] **J Tate**, **F Oort**, *Group schemes of prime order*, *Ann. Sci. École Norm. Sup.* (4) 3 (1970) 1–21
- [17] **C Wilkerson**, *Lambda-rings, binomial domains, and vector bundles over $\mathbf{CP}(\infty)$* , *Comm. Algebra* 10 (1982) 311–328