GENERALIZED n-SERIES AND DE RHAM COMPLEXES

S. K. DEVALAPURKAR AND M. L. MISTERKA

ABSTRACT. The goal of this article is to study some basic algebraic and combinatorial properties of "generalized n-series" over a commutative ring R, which are functions $s : \mathbf{Z}_{\geq 0} \to R$ satisfying a mild condition. A special example of generalized n-series is given by the q-integers $\frac{q^n-1}{q-1} \in \mathbf{Z}[q]$. Given a generalized n-series s, one can define s-analogues of factorials (via $n!_s = \prod_{i=1}^n s(n)$) and binomial coefficients. We prove that Pascal's identity, the binomial identity, Lucas' theorem, and the Vandermonde identity admit s-analogues; each of these specialize to their appropriate q-analogue in the case of the q-integer generalized n-series. We also study the growth rates of generalized n-series defined over the integers. Finally, we define an s-analogue of the (q-)derivative, and prove s-analogues of the Poincaré lemma and the Cartier isomorphism for the affine line, as well as a pullback square due to Bhatt-Lurie.

CONTENTS

1. Introduction

1.1. **Summary.** Recent work of Bhatt, Drinfeld, Lurie, Morrow, Scholze, and others (see, e.g., [BMS18, BS19, Sch17, Dri21, Dri22, BL22]) has shown that q-deformations of classical number-theoretic and algebro-geometric concepts play a central role in arithmetic geometry. The basic premise behind the theory of q-deformations is the idea that the q-integers $[n]_q = \frac{q^n-1}{q-1}$ display many similarities to the ordinary integers. This idea has a rich history: the key ideas date back to Euler and Jacobi, and a q-analogue of the derivative originates with Jackson in 1909 (see [Jac09]). We refer the reader to the book [KC02] for a detailed exposition of q-deformed mathematics.

The theory of *formal group laws* supplies a simultaneous generalization of both ordinary integers and q-integers (see Recollection 4.3.1 for a quick summary of the basics of formal group laws, and [Haz78, Rav86] for a detailed treatment). Namely, every formal group law F over a ring R defines a sequence of power series $\langle n\rangle$ over R for every integer $n \in \mathbf{Z}$. In the case of the the additive formal group law $x+y$, we have $\langle n\rangle = n$; and in the case of the multiplicative formal group law $x+y+xy$, one can identify $\langle n\rangle = [n]_q$. The goal of this article is to explore whether certain aspects of q-deformed mathematics (such as q-analogues of basic combinatorial formulae, and properties of the q-de Rham complex of [Sch17]) admit generalizations to arbitrary formal group laws. The primary motivation behind our investigation is the unpublished observation of Arpon Raksit that homotopy-theoretic methods naturally suggest studying "F-analogues" of the q-deformations arising in the aforementioned work of Bhatt-Morrow-Scholze.[1]

Our primary observation is that one does not need the structure of a formal group law to define and study these "F-analogues". Instead, the following significantly weaker structure suffices:

Definition (Definition 2.1.4)**.** *Fix a ring R (always assumed commutative with unit). A generalized n-series (GNS) over R is a function $s : \mathbf{Z}_{\geq 0} \to R$ such that:*

(1) $s(0) = 0$,
(2) $s(n)$ is not a zero-divisor for any $n > 0$,
(3) $s(n-k) \mid s(n) - s(k)$ for all $n > k > 0$.

For instance, the map $s : \mathbf{Z}_{\geq 0} \to \mathbf{Z}[\![q-1]\!]$ sending $n \mapsto [n]_q = \frac{q^n-1}{q-1}$ defines a GNS.

In the body of this article, we show that this simple definition is sufficient for proving several analogues of classical combinatorial identities, and is also enough to study an "s-deformation" of the classical algebraic de Rham complex. The results of this article do not rely on any sophisticated tools: rather, the purpose is to demonstrate the efficiency of Definition 2.1.4. The work done in this article seems closely related to Bhargava's [Bha00], but we have not attempted to make a comparison.

If $n \geq 0$, let $n!_s = \prod_{k=1}^n s(k)$, and let $\binom{n}{j}_s = \frac{n!_s}{j!_s(n-j)!_s}$ denote the s-analogues of the factorial and binomial coefficient, respectively. Our main combinatorial results are the following; for the full statement of some of these results, we refer the reader to the body of the text.

Theorem A. *Fix a GNS s over R. The following hold:*

(1) Pascal's identity (Proposition 2.1.3):

$$\binom{n}{k}_s = \binom{n-1}{k-1}_s + \frac{s(n)-s(k)}{s(n-k)}\binom{n-1}{k}_s.$$

(2) An s-analogue of the binomial and q-binomial theorems; see Theorem 2.3.7.

(3) Lucas' theorem (Proposition 2.4.8): suppose that $s(1) = 1$ and

$$s(a+b) \equiv s(a) + s(b) \pmod{s(a)s(b)}$$

[1] Since the actual homotopy theory does not play any role in this paper, we refer the interested reader to Remark 4.3.25 below for more.

for all $a, b \in \mathbf{Z}_{>0}$. Then, for any prime p and any nonnegative integers n_1, n_0, k_1, k_0 such that $n_0, k_0 < p$, we have

$$\binom{n_1 p + n_0}{k_1 p + k_0}_s \equiv \binom{n_1}{k_1}\binom{n_0}{k_0}_s \pmod{s(p)}.$$

(4) An analogue of the Vandermonde and q-Vandermonde identities; see Theorem 2.5.4.

In Section 3, we study the growth rate of generalized n-series over $\mathbf{Z}$. For instance, we show in Theorem 3.3.1 that if $s(n)$ is a strictly increasing generalized n-series over $\mathbf{Z}$ which is not a scalar multiple of $n \mapsto [n]_q$ for any $q \in \mathbf{Z}_{>0}$, then $s(n) = \Omega_a(a^n)$ for all $a \geq 0$.

As one might expect given our motivation above, one important class of examples of generalized n-series arises via formal group laws. Recall (see Recollection 4.3.1) that a formal group law over a commutative ring R is a two-variable power series $x +_F y \in R[\![x, y]\!]$ such that $(x +_F y) +_F z = x +_F (y +_F z)$ and $x +_F y \equiv x + y \pmod{(x, y)^2}$. If $n \geq 0$ is an integer, the n-series of F is defined via the formula

$$[n]_F(t) = \overbrace{t +_F t +_F \cdots +_F t}^{n} \in tR[\![t]\!].$$

Let $\langle n\rangle_F = \frac{[n]_F(t)}{t}$. Suppose (for simplicity) that R is torsionfree. Then, the function $\mathbf{Z}_{\geq 0} \to R[\![t]\!]$ sending $n \mapsto \langle n\rangle_F$ defines a GNS over $R[\![t]\!]$ (Proposition 4.3.4).

One can define the *F-de Rham complex* of the affine line $\mathbf{A}^1 = \operatorname{Spec} R[x]$ as the cochain complex

$$F\Omega_{\square,\mathbf{A}^1} = \left(R[\![t]\!][x] \xrightarrow{\nabla_F} R[\![t]\!][x]dx\right),\ x^n \mapsto \langle n\rangle_F x^{n-1}dx.$$

This was first defined by Arpon Raksit in unpublished work. Many analytic properties of the usual (q-)derivative continue to hold for the F-derivative: for instance, we show (see Corollary 4.3.15) that there is an explicit power series $F\log(x)$ which recovers the q-logarithm when F is the q-integer GNS, and which satisfies the property that $\nabla_F(F\log(x)) = 1/x$. Using this analogue of the q-logarithm, we prove a generalization of the Cartesian square of [BL22, Lemma 3.5.18] in Theorem 4.4.10.

Our main results regarding the F-de Rham complex can be summarized as follows:

Theorem B (Theorem 4.3.21)**.** *Let R be a torsionfree (say) commutative ring, and let F be a formal group law over R.*

(1) Let $R[\![t]\!]\langle x\rangle_F$ denote the ring $R[\![t]\!][x, \frac{x^n}{[n]_F!}]_{n\geq 0}$. Then the Poincaré lemma holds: the cohomology of the complex $F\Omega_{\square,\mathbf{A}^1} \otimes_{R[\![t]\!][x]} R[\![t]\!]\langle x\rangle_F$ is concentrated in degree zero, where it is isomorphic to $R[\![t]\!]$.

(2) The Cartier isomorphism holds: after setting $\langle p\rangle_F = 0$, the ith cohomology of the complex $F\Omega_{\square,\mathbf{A}^1}$ is isomorphic to the ith term of a Frobenius twist of $F\Omega_{\square,\mathbf{A}^1}$.

(3) There is an analogue of the décalage isomorphism of [BO78, BS19] *for $F\Omega_{\square,\mathbf{A}^1}$.*

This result in fact admits a generalization to arbitary GNS (not just ones which arise from formal group laws), but the statement is slightly more complicated; see Section 4.2. As with the combinatorial results above, Theorem 4.3.21 is not technically involved; however, it is supposed to serve as a blueprint for a more general program that we outline at the end of Section 4.3. In particular, we expect (see Conjecture 4.3.23) that the assignment $R[x_1, \ldots, x_n] \mapsto (F\Omega_{\square,\mathbf{A}^1})^{\otimes_{R[\![t]\!]} n}$ should extend to a functor from the category of commutative R-algebras to the ∞-category of $\mathbf{E}_\infty$-$R[\![t]\!]$-algebras.

1.2. **Table of commonly-used notation.** This article will introduce some notation which will be used heavily throughout. For the reader's convenience, we have summarized the commonly-used ones in the table below.

Symbol	Definition	Location in text
$R[1/s]$	$R[s(1)^{-1}, s(2)^{-1}, \cdots]$	(1)
$c_s(n,k)$	$\frac{s(n)-s(k)}{s(n-k)}$	(2)
$(x+y)_s^n$	Characterized by specific conditions	Definition 2.3.5
$C_s(n,k)$	$\frac{s(n+k)-s(n)-s(k)}{s(n)s(k)}$	Notation 2.4.4
$\left(\begin{smallmatrix} n & \vert & m \\ j & \vert & k \end{smallmatrix}\right)_s$	$\sum_{m<i_1<i_2<\cdots<i_j\leq m+n}\left(\prod_{\ell=1}^{j} c_s(i_\ell, i_\ell-k+j-\ell)\right)$	Definition 2.5.2
$\langle n\rangle_F(t)$	$\frac{[n]_F(t)}{t}$ for a FGL $F(x,y)$	Recollection 4.3.1
$\ell_F(t)$, $\mathcal{E}_F(t)$	Logarithm and exponential of a FGL	Recollection 4.3.1
$F\log(x)$	$\frac{t}{\ell_F(t)}\log(x)$	Corollary 4.3.15
$\mathbf{G}_m^{\sharp,F}$	"F-divided power hull" of zero section of $\mathbf{G}_m$	Definition 4.4.5

1.3. **Acknowledgements.** The first author is grateful to Ben Antieau and (especially) Arpon Raksit for discussions on this topic, as well as Michael Kural for his help in proving the main result of Section 4.4 in the case of the multiplicative formal group law. The first author was supported by the NSF GRFP under grant DGE-2140743. The second author is grateful to Pavel Etingof for suggesting that an s-analogue of the q-binomial theorem might exist. Finally, both authors are grateful to the directors and organizers of PRIMES-USA for the opportunity to collaborate, as well as for comments on this article!

2. THE s-BINOMIAL COEFFICIENTS

2.1. **A generalization of binomial coefficients.** Recall that the binomial coefficient $\binom{n}{k}$ is defined by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

The q-factorial and q-binomial coefficients are defined by

$$[n]!_q = [1]_q \cdot [2]_q \cdot \dots \cdot [n]_q, \qquad \binom{n}{k}_q = \frac{[n]!_q}{[k]!_q[n-k]!_q},$$

where $[n]_q = (q^n - 1)/(q-1) \in \mathbf{Z}[\![q-1]\!]$. The similarity of these two definitions hints that it might be interesting to study a simultaneous generalization of the usual and q-binomial coefficients, where the sequence of elements $n \in \mathbf{Z}$ and $[n]_q \in \mathbf{Z}[\![q-1]\!]$ are replaced by a sequence of elements in a commutative ring satisfying certain conditions.

Definition 2.1.1. Let R be a ring, and let $s : \mathbf{Z}_{\geq 0} \to R$ be a function such that $s(0) = 0$ and for all $n > 0$, $s(n)$ is not a zero-divisor. For integers $n \geq k \geq 0$, we define the *s-factorial* $n!_s$ by

$$0!_s = 1, \quad n!_s = \prod_{k=1}^{n} s(k),$$

and the *s-binomial coefficient* $\binom{n}{k}_s$ by

$$\binom{n}{k}_s = \frac{n!_s}{k!_s(n-k)!_s}.$$

Remark 2.1.2. In general, this quotient is undefined in R; however, it is always defined in the localization

$$R[1/s] := R[s(1)^{-1}, s(2)^{-1}, s(3)^{-1}, \dots]. \tag{1}$$

We will soon restrict to the case where the s-binomial coefficients are elements of R.

The s-binomial coefficient need not satisfy any nice properties, since there are no restrictions placed on s. Our first observation is the following.

Proposition 2.1.3. *Let R be a ring and let $s : \mathbf{Z}_{\geq 0} \to R$ be a function that satisfies the following conditions:*

(1) $s(0) = 0$,
(2) $s(n)$ is not a zero-divisor for any $n > 0$,
(3) $s(n-k) \mid s(n) - s(k)$ for all $n > k > 0$.

Then, for all integers $n \geq k \geq 0$, the s-binomial coefficient $\binom{n}{k}_s$ is an element of R, and the s-binomial coefficients satisfy an "s-Pascal identity": For all $n > k > 0$,

$$\binom{n}{k}_s = \binom{n-1}{k-1}_s + \frac{s(n)-s(k)}{s(n-k)}\binom{n-1}{k}_s.$$

Proof. Indeed, observe that in the localization $R[1/s]$, we have:

$$\begin{aligned}\frac{s(n)-s(k)}{s(n-k)}\binom{n-1}{k}_s &= \frac{s(n)-s(k)}{s(n-k)}\frac{(n-1)!_s}{k!_s(n-k-1)!_s} \\ &= \frac{s(n)\cdot(n-1)!_s}{k!_s(n-k)!_s} - \frac{s(k)\cdot(n-1)!_s}{k!_s(n-k)!_s} \\ &= \frac{n!_s}{k!_s(n-k)!_s} - \frac{(n-1)!_s}{(k-1)!_s(n-k)!_s} \\ &= \binom{n}{k}_s - \binom{n-1}{k-1}_s.\end{aligned}$$

It remains to show that $\binom{n}{k}_s \in R$ for all $n \geq k \geq 0$. We will use induction on n.

The base case is clear, since $\binom{0}{0}_s = 1 \in R$. For the inductive step, assume that for some fixed n and for all k with $n-1 \geq k \geq 0$, $\binom{n-1}{k}_s \in R$. Let k be an integer such that $n \geq k \geq 0$. If $k = 0$, then $\binom{n}{k}_s = 1 \in R$. Otherwise, we can apply the s-Pascal identity:

$$\binom{n}{k}_s = \binom{n-1}{k-1}_s + \frac{s(n)-s(k)}{s(n-k)}\binom{n-1}{k}_s.$$

By the inductive hypothesis, the two s-binomial coefficients on the right-hand side are in R, and by condition (c) in the theorem statement, $\frac{s(n)-s(k)}{s(n-k)} \in R$. Therefore, $\binom{n}{k}_s \in R$. This completes the induction proof. □

Motivated by Proposition 2.1.3, we are led to the following:

Definition 2.1.4. Let R be a ring. A *generalized n-series (GNS) over R* is a function $s : \mathbf{Z}_{\geq 0} \to R$ such that the following conditions are true:

(1) $s(0) = 0$,
(2) $s(n)$ is not a zero-divisor for any $n > 0$,
(3) $s(n-k) \mid s(n) - s(k)$ for all $n > k > 0$.

If s is a generalized n-series, we will define

$$c_s(n,k) := \frac{s(n)-s(k)}{s(n-k)}. \tag{2}$$

Example 2.1.5 (Integers)**.** The inclusion $s : \mathbf{Z}_{\geq 0} \to \mathbf{Z}$ is clearly a GNS over $\mathbf{Z}$.

Example 2.1.6 (q-integers)**.** Consider the function $s : \mathbf{Z}_{\geq 0} \to \mathbf{Z}[\![q-1]\!]$ given by $s(n) = [n]_q$. This defines a GNS: the first two conditions are satisfied, since $[0]_q = 0$, $[n]_q \neq 0$ for $n > 0$, and $\mathbf{Z}[\![q-1]\!]$ is an integral domain. For the third condition, note that

$$\begin{aligned}[n]_q - [k]_q &= \frac{q^n-1}{q-1} - \frac{q^k-1}{q-1} = \frac{q^n-q^k}{q-1} \\ &= q^k\left(\frac{q^{n-k}-1}{q-1}\right) = q^k[n-k]_q.\end{aligned}$$

Therefore, s is a GNS over $\mathbf{Z}[\![q-1]\!]$, and we can apply Proposition 2.1.3 to conclude that $\binom{n}{k}_q \in \mathbf{Z}[\![q-1]\!]$ for all $n \geq k \geq 0$. The s-Pascal identity reduces to the well-known q-Pascal identity:

$$\binom{n}{k}_q = \binom{n-1}{k-1}_q + q^k\binom{n-1}{k}_q.$$

Remark 2.1.7. One can extend the definition of the s-binomial coefficients to allow arbitrary integers k by defining $\binom{n}{k}_s = 0$ when $k < 0$ or $k > n$. Using this extended definition, the s-Pascal identity remains true when $k = 0$:

$$\binom{n-1}{-1}_s + \frac{s(n)-s(0)}{s(n-0)}\binom{n-1}{0}_s = 0 + 1 \cdot 1 = 1 = \binom{n}{0}_s.$$

This relies on the condition $s(0) = 0$. The fact that Pascal's identity fails for $k = 0$ if $s(0) \neq 0$ is one motivation for including condition (1) in the definition of GNS.

2.2. **Number-theoretic properties of generalized n-series.** In this section, we prove some number-theoretic properties of generalized n-series, which will be useful later in this article. The main result of this section is the following:

Theorem 2.2.1. *Let s be a generalized n-series over a ring R. Then, for all $a, b, n \in \mathbf{Z}_{\geq 0}$,*

(1) $a \mid b \implies s(a) \mid s(b)$,
(2) $a \equiv b \pmod{n} \implies s(a) \equiv s(b) \pmod{s(n)}$,
(3) the ideals $(s(a), s(b))$ and $(s(\gcd(a, b)))$ are equal.

If $s(1)$ is a unit in R, then for all $a, n \in \mathbf{Z}_{\geq 0}$,

(4) a is a unit in $\mathbf{Z}/n \implies s(a)$ is a unit in $R/s(n)$.

Remark 2.2.2. In the case $R = \mathbf{Z}$, the equivalence of ideals in Theorem 2.2.1 is equivalent to

$$\gcd(s(a), s(b)) = \pm s(\gcd(a, b)).$$

We will prove Theorem 2.2.1 as a sequence of lemmas. Fix a generalized n-series s over a ring R.

Lemma 2.2.3. *Let $a, b \in \mathbf{Z}_{\geq 0}$. Then, $a \mid b$ implies $s(a) \mid s(b)$.*

Proof. We will use induction. Base case: $s(a) \mid s(0)$ because $s(0) = 0$. Inductive hypothesis: Let $n \in \mathbf{Z}_{>0}$, and assume that $s(a) \mid s(a(n-1))$. Then, by the divisibility condition in the definition of generalized n-series,

$$s(a) \mid s(a(n-1)) = s(an - a) \mid s(an) - s(a),$$

so $s(a) \mid s(an)$. □

Lemma 2.2.4. *Let $a, b, n \in \mathbf{Z}_{\geq 0}$. If $a \equiv b \pmod{n}$ then*

$$s(a) \equiv s(b) \pmod{s(n)}.$$

Another way to state this lemma is that s induces a well-defined function from $\mathbf{Z}/n$ to $R/s(n)$.

Proof. By the definition of congruence, $n \mid a - b$, so $s(n) \mid s(a - b)$ by Lemma 2.2.3. The definition of generalized n-series requires that

$$s(a - b) \mid s(a) - s(b),$$

so $s(n) \mid s(a) - s(b)$, which means that $s(a) \equiv s(b) \pmod{s(n)}$. □

Lemma 2.2.5. *Suppose that $s(1)$ is a unit in R. If $a, n \in \mathbf{Z}_{\geq 0}$ such that a is a unit in $\mathbf{Z}/n$, then $s(a)$ is a unit in $R/s(n)$.*

Proof. Let b be the multiplicative inverse of a modulo n. Then, $ab \equiv 1 \pmod{n}$. By Lemmas 2.2.3 and 2.2.4,

$$s(a) \mid s(ab) \equiv s(1) \pmod{s(n)}.$$

So in the ring $R/s(n)$, $s(a)$ divides $s(1)$, which is a unit (because it is a unit in R). Therefore, $s(a)$ is a unit in $R/s(n)$. □

Lemma 2.2.6. *Let $a, b \in \mathbf{Z}_{\geq 0}$. Then, we have the following equivalence of ideals:*

$$\big(s(\gcd(a, b))\big) = \big(s(a), s(b)\big).$$

Proof. Let $d = \gcd(a, b)$. By Lemma 2.2.3, $s(d) \mid s(a)$ and $s(d) \mid s(b)$, so $s(a), s(b) \in (s(d))$. This means that

$$\big(s(d)\big) \supseteq \big(s(a), s(b)\big).$$

For the other direction, we can use Bézout's identity to write $d = am + bn$ for some $m, n \in \mathbf{Z}$. Taking this equation modulo a gives $d \equiv bn \pmod{a}$. By Lemma 2.2.4, $s(d) \equiv s(bn) \pmod{s(a)}$. Therefore, Lemma 2.2.3 implies that

$$s(d) \in s(bn) + \big(s(a)\big) \subseteq \big(s(a), s(b)\big),$$

and hence $\big(s(d)\big) \subseteq \big(s(a), s(b)\big)$. This shows that the two ideals are equal. □

2.3. The s-binomial theorem.

Recollection 2.3.1. The binomial theorem and the q-binomial theorem are the following two identities:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k,$$

$$(x+y)_q^n = \sum_{k=0}^{n} \binom{n}{k}_q q^{k(k-1)/2} x^{n-k} y^k,$$

where $(x+y)_q^n$ is defined by

$$(x+y)_q^n = \prod_{k=0}^{n-1} (x + q^k y) = (x+y)(x+qy)\cdots(x+q^{n-1}y).$$

Note that the $x + y$ in the parentheses is part of the notation, and cannot be treated as a sum; see [KC02] for this notation.

Remark 2.3.2. For readers who are familiar with the q-Pochhammer symbol, $(x+y)_q^n = x^n(-y/x; q)_n$, and $(a; q)_n = (1 + (-a))_q^n$.

We will now state and prove an analogue of the binomial theorem for the s-binomial coefficients. We begin by defining an analogue of the symbol $(x+y)_q^n$. To motivate the definition, recall that the q-analogue $(x+y)_q^n$ is the unique polynomial in $\mathbf{Z}[\![q-1]\!][x, y]$ such that the following properties hold:

- The q-derivative with respect to x of $(x+y)_q^n$ is $[n]_q(x+y)_q^{n-1}$. This is analogous to the fact that the classical derivative of $(x+y)^n$ with respect to x is $n(x+y)^{n-1}$.
- $(x+y)_q^0 = 1$.
- If $y = -x$, then $(x+y)_q^n$ is 0 for all $n > 0$.

To define an s-analogue $(x+y)_q^n$ in a similar way, we need an s-derivative; we will greatly expand on this notion in Section 4.

Definition 2.3.3. Let $s : \mathbf{Z}_{\geq 0} \to R$ be a GNS. The *s-derivative* is the R-linear map $\nabla_s : R[x] \to R[x]$ given on monomials by $\nabla_s(x^n) = s(n)x^{n-1}$.

Remark 2.3.4. When $n = 0$, we have $\nabla_s(x^0) = s(0)x^{-1}$. This is not defined in $R[x]$ unless $s(0) = 0$, which is always true when s is a GNS. Continuing Remark 2.1.7, this observation is another reason for requiring $s(0) = 0$ in the definition of GNS.

We can now define $(x+y)_s^n$:

Definition 2.3.5. Let s be a GNS over R, so that $R[1/s] = R[s(1)^{-1}, s(2)^{-1}, \dots]$. Define $(x+y)_s^n$ for $n \in \mathbf{Z}_{\geq 0}$ to be the unique polynomial in $R[1/s][x, y]$ such that the following three conditions hold:

(1) $(x+y)_s^0 = 1$,
(2) $(x + (-x))_s^n = 0$ for all $n > 0$,
(3) $\nabla_{s,x}(x+y)_s^n = s(n)(x+y)_s^{n-1}$.

Here, $\nabla_{s,x} : R[1/s][x,y] \to R[1/s][x,y]$ is the operator given by the "s-derivative with respect to x": it is simply the $R[1/s][y]$-linear extension of the s-derivative $\nabla_s : R[x] \to R[x]$ to $R[1/s][x,y]$.

Lemma 2.3.6. *The symbol $(x+y)^n_s$ in Definition 2.3.5 is well-defined: it exists and is unique. Moreover, $(x+y)^n_s$ is a homogeneous polynomial of degree n.*

Proof. We will use induction on n. For the base case $n = 0$, observe that $(x+y)^0_s = 1$ by condition (1).

For the inductive step, fix $n > 0$, and suppose that for all $k < n$, $(x+y)^k_s$ is well-defined and homogeneous of degree k. We can s-antidifferentiate $s(n)(x+y)^{n-1}_s$ using the $R[1/s][y]$-linear operator $I_{s,x} : R[1/s][x,y] \to R[1/s][x,y]$ defined on monomials by $I_{s,x}(x^k) = s(k+1)^{-1}x^{k+1}$. By definition, this operator produces polynomials with no term of x-degree 0. Although the s-antiderivative

$$f(x,y) = I_{s,x}(s(n)(x+y)^{n-1}_s)$$

is homogeneous of degree n (since the operator $I_{s,x}$ increases x-degree by 1) and satisfies condition (3), it might not equal $(x+y)^n_s$ because it does not have to satisfy condition (2). Since $f(x,y)$ is homogeneous of degree n, $f(x,-x)$ is a scalar multiple of x^n, say ax^n. Then, the polynomial

$$g(x,y) = f(x,y) - a(-y)^n$$

satisfies

$$\nabla_{s,x} g(x,y) = \nabla_{s,x} f(x,y) = s(n)(x+y)^{n-1}_s$$

and

$$g(x,-x) = f(x,-x) - a(-(-x))^n = ax^n - ax^n = 0.$$

It follows that $(x+y)^n_s$ exists, and one possible value for it is $g(x,y)$, which is homogeneous of degree n.

It remains to show that $(x+y)^n_s$ is unique. We know that any polynomial $h(x,y)$ that satisfies the conditions of $(x+y)^n_s$ must match $g(x,y)$ in every term with positive x-degree, because their s-derivatives with respect to x are both $s(n)(x+y)^{n-1}_s$. Therefore, $h(x,y) - g(x,y)$ is a scalar multiple of y^n, say by^n. Setting $y = -x$ gives $b(-x)^n = h(x,-x) - g(x,-x)$, which is 0 by condition (2), so $b = 0$. Therefore, $h(x,y) = g(x,y)$. This proves that $(x+y)^n_s$ is unique and is equal to $g(x,y)$. □

Recall from Section 2 that we originally defined the s-binomial coefficients as elements of the ring $R[1/s] = R[s(1)^{-1}, s(2)^{-1}, \dots]$, and later proved (using the s-Pascal identity) that if s is a GNS, then all the s-binomial coefficients are elements of R. We will do something similar for $(x+y)^n_s$ below, and we will use the s-binomial theorem as a lemma in the proof that $(x+y)^n_s \in R[x,y]$. Here is the s-binomial theorem:

Theorem 2.3.7 (s-binomial theorem)**.** *Let s be a GNS over R. Then, as elements of $R[1/s][x,y]$, we have:*

$$(x+y)^n_s = \sum_{k=0}^{n} \binom{n}{k}_s x^{n-k} y^k (0+1)^k_s.$$

Proof. We will use induction on n, and the inductive step will mainly consist of applying the s-antidifferentiation operator $I_{s,x}$ from the proof of Lemma 2.3.6 to both sides. For the base case, observe that if $n = 0$, both sides are 1.

For the inductive step, fix $n > 0$, and assume that the s-binomial theorem is true for $n - 1$:

$$(x+y)^{n-1}_s = \sum_{k=0}^{n-1} \binom{n-1}{k}_s x^{n-k-1} y^k (0+1)^k_s.$$

Multiplying both sides by $s(n)$, applying $I_{s,x}$, and using $R[1/s][y]$-linearity gives:

$$\begin{aligned} I_{s,x}(s(n)(x+y)_s^{n-1}) &= s(n)\sum_{k=0}^{n-1}\binom{n-1}{k}_s I_{s,x}(x^{n-k-1})y^k(0+1)_s^k \\ &= \sum_{k=0}^{n-1}\frac{s(n)}{s(n-k)}\binom{n-1}{k}_s x^{n-k}y^k(0+1)_s^k. \end{aligned}$$

Notice that

$$\frac{s(n)}{s(n-k)}\binom{n-1}{k}_s = \frac{s(n)(n-1)!_s}{s(n-k)k!_s(n-k-1)!_s} = \frac{n!_s}{k!_s(n-k)!_s} = \binom{n}{k}_s.$$

This implies that

$$I_{s,x}(s(n)(x+y)_s^{n-1}) = \sum_{k=0}^{n-1}\binom{n}{k}_s x^{n-k}y^k(0+1)_s^k.$$

The right-hand side almost looks like the right-hand side of the s-binomial theorem that we are trying to prove, but the upper limit of the summation is $n-1$ instead of n. To fix this, add $y^n(0+1)_s^n$ to both sides, giving

$$I_{s,x}(s(n)(x+y)_s^{n-1}) + y^n(0+1)_s^n = \sum_{k=0}^{n}\binom{n}{k}_s x^{n-k}y^k(0+1)_s^k.$$

We just have to show that the left-hand side is equal to $(x+y)_s^n$.

Let $g(x,y)$ be the left-hand side. The s-derivative with respect to x of $g(x,y)$ is $s(n)(x+y)_s^{n-1}$, because $I_{s,x}$ is an s-antiderivative operator (a right inverse of $\nabla_{s,x}$) and $y^n(0+1)_s^n$ is constant with respect to x. This is equal to the s-derivative of $(x+y)_s^n$, so $g(x,y)$ matches $(x+y)_s^n$ in all terms with positive x-degree. Both $g(x,y)$ and $(x+y)_s^n$ are homogeneous of degree n, so the only terms with x-degree 0 are the y^n terms. The coefficient of y^n in $g(x,y)$ is $(0+1)_s^n$ because $I_{s,x}$ never produces terms with x-degree 0. The y^n term of $(x+y)_s^n$ is $(0+y)_s^n$, which is $y^n(0+1)_s^n$ by homogeneity, so the coefficient of y^n in $(x+y)_s^n$ is also $(0+1)_s^n$. Therefore, $g(x,y)=(x+y)_s^n$, so

$$(x+y)_s^n = \sum_{k=0}^{n}\binom{n}{k}_s x^{n-k}y^k(0+1)_s^k.$$

This is what we needed to show for the inductive step. □

To complete this subsection, we will show that the coefficients of $(x+y)_s^n$ are elements of R for all GNS s over R and all $n \in \mathbf{Z}_{\geq 0}$. This means that the s-binomial theorem is really an equivalence of polynomials in $R[x,y]$, and can be stated without using the larger ring $R[1/s][x,y]$.

Proposition 2.3.8. *Let s be a GNS over a ring R. For all nonnegative integers n, we have $(x+y)_s^n \in R[x,y]$.*

Proof. It suffices to show that $(0+1)_s^n \in R$ for all nonnegative integers n, because using the s-binomial theorem, we could conclude that

$$(x+y)_s^n = \sum_{k=0}^{n}\binom{n}{k}_s x^{n-k}y^k(0+1)_s^k \in R[x,y].$$

Setting $x=-1$ and $y=1$ in the s-binomial theorem, we get

$$0 = ((-1)+1)_s^n = \sum_{k=0}^{n}\binom{n}{k}_s (-1)^{n-k}(0+1)_s^k,$$

so

$$(0+1)_s^n = \sum_{k=0}^{n-1} \binom{n}{k}_s (-1)^{n-k-1}(0+1)_s^k. \tag{3}$$

This is a recurrence relation for $(0+1)_s^n$.

To prove that $(0+1)_s^n \in R$, we will use induction on n. For the base case, note that $(0+1)_s^0 = 1$ which is an element of R. For the inductive step, note that if $(0+1)_s^k \in R$ for all $k < n$, then by the recurrence relation 3 and the fact that the s-binomial coefficients are in R (Proposition 2.1.3),

$$(0+1)_s^n = \sum_{k=0}^{n-1} \binom{n}{k}_s (-1)^{n-k-1}(0+1)_s^k \in R.$$

This completes the induction. □

Remark 2.3.9. Using the recurrence relation 3, it can be shown that

$$\frac{(-1)^n(0+1)_s^n}{n!_s} = \sum_{\ell=1}^{n} \left(\sum_{k_1+k_2+\cdots+k_\ell=n} \left(\prod_{j=1}^{\ell} \frac{-1}{k_\ell!_s} \right) \right),$$

where the inner sum is over all ordered ℓ-tuples $(k_1, k_2, \ldots, k_\ell)$ of positive integers that sum to n. Combining the inner and outer sums, the right-hand side can be viewed as a sum over compositions (ordered partitions) of n. Isolating $(0+1)_s^n$ gives

$$(0+1)_s^n = \sum_{\pi \text{ composition of } n} (-1)^{n-|\pi|} \binom{n}{\pi_1, \pi_2, \ldots, \pi_{|\pi|}}_s.$$

The summand is an s-multinomial coefficient, defined by

$$\binom{n}{k_1, k_2, \ldots, k_n}_s = \frac{n!_s}{k_1!_s \cdot k_2!_s \cdot \cdots \cdot k_n!_s},$$

and $|\pi|$ denotes the length of π.

2.4. **The s-Lucas theorem.**

Recollection 2.4.1. Lucas's theorem says that for all primes p and all integers $n_1, n_0, k_1, k_0 \in \mathbf{Z}_{\geq 0}$ such that $n_0, k_0 < p$,

$$\binom{n_1 p + n_0}{k_1 p + k_0} \equiv \binom{n_1}{k_1}\binom{n_0}{k_0} \pmod{p}.$$

There is a q-analogue of this identity, known as the q-Lucas theorem:

$$\binom{n_1 p + n_0}{k_1 p + k_0}_q \equiv \binom{n_1}{k_1}\binom{n_0}{k_0}_q \pmod{[p]_q}.$$

This identity is also true if p is composite, as long as we replace the modulus $[p]_q$ with the cyclotomic polynomial $\Phi_p(q)$. Notice that the first binomial coefficient on the right-hand side of the q-Lucas theorem is *not* a q-binomial coefficient.

Here is an s-analogue of Lucas's theorem:

Theorem 2.4.2 (s-Lucas theorem)**.** *Let s be a GNS over R such that $s(1) = 1$ and*

$$s(a+b) \equiv s(a) + s(b) \pmod{s(a)s(b)} \tag{4}$$

for all $a, b \in \mathbf{Z}_{>0}$. Then, for any prime p and any nonnegative integers n_1, n_0, k_1, k_0 such that $n_0, k_0 < p$, we have

$$\binom{n_1 p + n_0}{k_1 p + k_0}_s \equiv \binom{n_1}{k_1}\binom{n_0}{k_0}_s \pmod{s(p)}.$$

Remark 2.4.3. Define $\Phi_n(s) = \prod_{d|n} s(d)^{\mu(n/d)}$, where μ denotes the Möbius function. Note that Möbius inversion implies the identity $s(n) = \prod_{d|n} \Phi_n(s)$. One can prove a "composite version" of the s-Lucas theorem where $s(p)$ is replaced by $\Phi_n(s)$, but the statement is more complicated.

For the rest of this section, we fix the GNS s over R. To simplify the statement of the s-Lucas theorem, we will use the following:

Notation 2.4.4. For integers $a, b \in \mathbf{Z}_{>0}$, we define

$$C_s(a,b) = \frac{s(a+b) - s(a) - s(b)}{s(a)s(b)} \in R[1/s].$$

The extra condition (4) in Theorem 2.4.2 is therefore equivalent to $C_s(a,b)$ being defined in R for all $a, b \in \mathbf{Z}_{>0}$.

Lemma 2.4.5. *Suppose that $C_s(a,b)$ is defined in R for all $a, b \in \mathbf{Z}_{>0}$. Then, for all integers $m > 0$ and $n > k \geq 0$,*

$$c_s(mn, mk) \equiv 1 \pmod{s(m)}.$$

Proof. By definition,

$$c_s(mn, mk) - 1 = \frac{s(mn) - s(mk) - s(mn-mk)}{s(mn-mk)} = s(mk)C_s(mk, mn-mk).$$

By Lemma 2.2.3, $s(m) \mid s(mk)$, so the right-hand side is divisible by $s(m)$. Therefore, $c_s(mn, mk) - 1 \equiv 0 \pmod{s(m)}$. □

Remark 2.4.6. A consequence of this lemma is the interesting fact that if we define the "rescaled" GNS $s_m(n) = s(mn)$ for each positive integer m, then Pascal's identity for the s_m-binomial coefficients is the same as the usual Pascal's identity when we reduce modulo $s(m)$. This implies the following congruence:

Lemma 2.4.7. *Suppose that $C_s(a,b)$ is defined for all $a, b \in \mathbf{Z}_{>0}$. For all integers $m > 0$ and $0 \leq k \leq n$,*

$$\binom{n}{k}_{s_m} \equiv \binom{n}{k} \pmod{s(m)}.$$

Proof. We will use induction on n. For the base case, observe that if $n = 0$ then $k = 0$, so both sides are 1. For the inductive step, assume that the desired claim is true when n is replaced by $n-1$. Then:

$$\begin{aligned}
\binom{n}{k}_{s_m} &= \binom{n-1}{k-1}_{s_m} + c_{s_m}(n,k)\binom{n-1}{k}_{s_m} && \text{by the } s\text{-Pascal identity (Proposition 2.1.3),}\\
&= \binom{n-1}{k-1}_{s_m} + c_s(mn,mk)\binom{n-1}{k}_{s_m} && \text{by definition of } c_{s_m},\\
&\equiv \binom{n-1}{k-1}_{s_m} + \binom{n-1}{k}_{s_m} && \text{by Lemma 2.4.5,}\\
&\equiv \binom{n-1}{k-1} + \binom{n-1}{k} && \text{by inductive hypothesis,}\\
&= \binom{n}{k} \pmod{s(m)} && \text{by Pascal's identity.}
\end{aligned}$$

Therefore, by induction, this is true for all $m \in \mathbf{Z}_{>0}$. □

Theorem 2.4.2 is a consequence of a slight variant.

Proposition 2.4.8 (Another s-Lucas theorem)**.** *Let s be a GNS such that $s(1) = 1$. Let p be prime and let $n_1, n_0, k_1, k_0 \in \mathbf{Z}_{\geq 0}$ such that $n_0, k_0 < m$. Then,*

$$\binom{n_1 p + n_0}{k_1 p + k_0}_s \equiv \binom{n_1}{k_1}_{s_p} \binom{n_0}{k_0}_s \pmod{s(p)},$$

where s_p is the rescaled GNS from Remark 2.4.6.

Proof of Theorem 2.4.2. This is an immediate consequence of Proposition 2.4.8 and Lemma 2.4.7. □

Remark 2.4.9. Proposition 2.4.8 is just Theorem 2.4.2 but with $\binom{n_1}{k_1}$ replaced by $\binom{n_1}{k_1}_{s_p}$, and no requirement that $C_s(a, b)$ be an element of R.

Before we prove Proposition 2.4.8 in full generality, we will prove the special case where $n_0 = k_0 = 0$. Then, we will use this case as a lemma in the proof of the general result.

Proof of Theorem 2.4.8 in the case $n_0 = k_0 = 0$. Writing out the definition of the s-binomial coefficient $\binom{pn}{pk}_s$, we get

$$\binom{pn}{pk}_s = \frac{s(pn)s(pn-1)\cdots s(pn-pk+1)}{s(pk)s(pk-1)\cdots s(1)}.$$

By Lemma 2.2.5, $s(pn-j)$ is a unit modulo $s(p)$ for all j not divisible by p. Together with Lemma 2.2.4, this implies that we can cancel $s(pn-j)$ with $s(pk-j)$ (since they are congruent units modulo $s(p)$). After all of this cancellation, we are left with

$$\binom{pn}{pk}_s = \frac{s(pn)s(p(n-1))\cdots s(p(n-k+1))}{s(pk)s(p(k-1))\cdots s(p)},$$

which is just $\binom{n}{k}_{s_p}$. This means that

$$\binom{pn}{pk}_s \equiv \binom{n}{k}_{s_p} \pmod{s(p)}.$$

Combining this with the congruence of $\binom{n}{k}_{s_p}$ and $\binom{n}{k}$, we get

$$\binom{pn}{pk}_s \equiv \binom{n}{k} \pmod{s(p)},$$

which is the special case of Theorem 2.4.8 where $n_0 = k_0 = 0$. □

We will now extend this to any value of n_0 in the valid range $0 \leq n_0 < p$.

Proof of Theorem 2.4.8 in the case $k_0 = 0$. We proved Proposition 2.4.8 above for $n_0 = 0$, so let $0 < n_0 < p$. Notice that the definition of s-binomial coefficients implies that

$$s(n-k)\binom{n}{k}_s = \frac{n!_s}{k!_s(n-k-1)!_s} = s(n)\binom{n-1}{k}_s.$$

Therefore,

$$s(p(n_1-k)+n_0)\binom{pn_1+n_0}{pk}_s = s(pn_1+n_0)\binom{pn_1+n_0-1}{pk}_s.$$

Since n_0 is a unit modulo p, we see that $s(p(n_1-k)+n_0)$ is a unit modulo $s(p)$. But $s(p(n_1-k)+n_0)$ is congruent to $s(pn_1+n_0)$ by Lemma 2.2.4. Since both are units, this implies that

$$\binom{pn_1+n_0}{pk}_s \equiv \binom{pn_1+n_0-1}{pk}_s \pmod{s(p)}.$$

A simple induction proof gives

$$\binom{pn_1+n_0}{pk}_s \equiv \binom{pn_1}{pk}_s \pmod{s(p)}.$$

It follows that

$$\binom{pn_1+n_0}{pk}_s \equiv \binom{pn_1}{pk}_s \equiv \binom{n_1}{k} = \binom{n_1}{k}\binom{n_0}{0}_s \pmod{s(p)},$$

which is exactly the s-Lucas theorem where $k_0 = 0$. □

Finally, we will extend this by induction to any value of k_0 between 0 and $p-1$.

Proof of Theorem 2.4.8 in full generality. We will use induction on k_0. We already proved the base case $k_0 = 0$ above. Suppose we have shown that the induction hypothesis

$$\binom{pn_1+n_0}{pk_1+k_0-1}_s \equiv \binom{n_1}{k_1}\binom{n_0}{k_0-1}_s \pmod{s(p)}$$

is true for some k_0-1 between 0 and $p-2$ (or $0 < k_0 < p$). We will show that it is true with k_0-1 replaced by k_0. Notice that for all integers $1 \le k \le n$,

$$s(k)\binom{n}{k}_s = \frac{n!_s}{(k-1)!_s(n-k)!_s} = s(n-k+1)\binom{n}{k-1}_s,$$

so

$$s(pk_1+k_0)\binom{pn_1+n_0}{pk_1+k_0}_s = s(p(n_1-k_1)+n_0-k_0+1)\binom{pn_1+n_0}{pk_1+k_0-1}_s.$$

Reducing modulo $s(p)$ gives

$$s(k_0)\binom{pn_1+n_0}{pk_1+k_0}_s \equiv s(n_0-k_0+1)\binom{pn_1+n_0}{pk_1+k_0-1} \pmod{s(p)}.$$

So

$$\begin{aligned} s(k_0)\binom{pn_1+n_0}{pk_1+k_0}_s &\equiv s(n_0-k_0+1)\binom{pn_1+n_0}{pk_1+k_0-1} \\ &\equiv \binom{n_1}{k_1}s(n_0-k_0+1)\binom{n_0}{k_0-1}_s \\ &= \binom{n_1}{k_1}s(k_0)\binom{n_0}{k_0}_s \pmod{s(p)}. \end{aligned}$$

Since $0 < k_0 < p$, $s(k_0)$ is a unit modulo $s(p)$, so we can cancel it from both sides, and we get the congruence we wanted. Therefore, the induction proof is complete. □

When the ring R is $\mathbf{Z}$, there is a version of the s-Lucas theorem which allows p to be any natural number, not just a prime; see Theorem 3.4.4.

2.5. The s-Vandermonde identity.

Recollection 2.5.1. The classical Vandermonde identity states that

$$\binom{m+n}{k} = \sum_j \binom{m}{k-j}\binom{n}{j};$$

this admits a q-analogue, known as the the q-Vandermonde identity:

$$\binom{m+n}{k}_q = \sum_j \binom{m}{k-j}_q\binom{n}{j}_q q^{j(m-k+j)}.$$

To state an s-analogue of the Vandermonde identity, we need a definition.

Definition 2.5.2. For $m, n, k, j \in \mathbf{Z}$ with $0 \leq j \leq n$ and $0 \leq k - j \leq m$, define

$$\left(\begin{matrix} n \\ j \end{matrix}\middle|\begin{matrix} m \\ k \end{matrix}\right)_s = \sum_{\substack{I \subseteq (m, m+n] \cap \mathbf{Z} \\ |I| = j}} \left(\prod_{\ell=1}^{j} c_s(i_\ell, n - (k - j + \ell)) \right),$$

where $I = \{i_1 < \cdots < i_j\}$. We also set $\left(\begin{smallmatrix} n \\ j \end{smallmatrix}\middle|\begin{smallmatrix} m \\ k \end{smallmatrix}\right)_s = 0$ for $j < 0$ or $j > n$.

Remark 2.5.3. For $s(n) = n$, the product inside the sum in Definition 2.5.2 is 1, so the sum is just the number of subsets of $(m, m+n] \cap \mathbf{Z}$ of size j, which is $\binom{n}{j}$. In that sense, $\left(\begin{smallmatrix} n \\ j \end{smallmatrix}\middle|\begin{smallmatrix} m \\ k \end{smallmatrix}\right)_s$ is an s-analogue of the subset-counting definition of $\binom{n}{j}$ which depends on two extra parameters m and k. The other type of s-binomial coefficient $\binom{n}{j}_s$ is an s-analogue of the algebraic definition of $\binom{n}{j}$.

Theorem 2.5.4 (s-Vandermonde identity)**.** *For all $m, n, k \in \mathbf{Z}_{\geq 0}$ with $k \leq m + n$,*

$$\binom{m+n}{k}_s = \sum_j \binom{m}{k-j}_s \left(\begin{matrix} n \\ j \end{matrix}\middle|\begin{matrix} m \\ k \end{matrix}\right)_s,$$

where the sum is taken over all $j \in \mathbf{Z}$ such that $0 \leq j \leq n$ and $0 \leq k - j \leq m$.

Question 2.5.5. As explained in [Sas18], the q-Vandermonde identity for $\binom{m+n}{k}_q$ can be understood as arising via a motivic cellular decomposition of the Grassmannian $\mathrm{Gr}_k(\mathbf{C}^{m+n})$. Is there a motivic interpretation of Theorem 2.5.4? (A similar question can also be asked for the s-analogues of the other combinatorial identities proved elsewhere in this article.)

The proof of Theorem 2.5.4 requires a preliminary lemma, which can be viewed as an analogue of Pascal's identity for $\left(\begin{smallmatrix} n \\ j \end{smallmatrix}\middle|\begin{smallmatrix} m \\ k \end{smallmatrix}\right)_s$.

Lemma 2.5.6. *For all $m, n, k, j \in \mathbf{Z}$ such that $0 \leq k - j \leq m$,*

$$\left(\begin{matrix} n \\ j \end{matrix}\middle|\begin{matrix} m \\ k \end{matrix}\right)_s = \left(\begin{matrix} n-1 \\ j \end{matrix}\middle|\begin{matrix} m \\ k \end{matrix}\right)_s + c_s(m+n, m+n-k) \left(\begin{matrix} n-1 \\ j-1 \end{matrix}\middle|\begin{matrix} m \\ k-1 \end{matrix}\right)_s.$$

Notice that this includes the cases $j < 0$ and $j > n$.

Proof. We will split up the sum in the definition of $\left(\begin{smallmatrix} n \\ j \end{smallmatrix}\middle|\begin{smallmatrix} m \\ k \end{smallmatrix}\right)_s$ into two sums, based on whether I contains $m+n$ or not. If $m+n \notin I$, then I ranges over all j-element subsets of $(m, m+n-1] \cap \mathbf{Z}$. If $m+n \in I$, then we remove it, and we get a $(j-1)$-element subset of $(m, m+n-1] \cap \mathbf{Z}$. Then, we have to pull out the $\ell = j$ term of the product, since $i_j = m+n$. So we have

$$\begin{aligned}
\left(\begin{matrix} n \\ j \end{matrix}\middle|\begin{matrix} m \\ k \end{matrix}\right)_s &= \sum_{\substack{I \subseteq (m, m+n] \cap \mathbf{Z} \\ |I| = j}} \left(\prod_{\ell=1}^{j} c_s(i_\ell, i_\ell - (k - j + \ell)) \right) \\
&= \sum_{\substack{I \subseteq (m, m+n] \cap \mathbf{Z} \\ |I| = j \\ m+n \in I}} \left(\prod_{\ell=1}^{j} c_s(i_\ell, i_\ell - (k - j + \ell)) \right) + \sum_{\substack{I \subseteq (m, m+n-1] \cap \mathbf{Z} \\ |I| = j}} \left(\prod_{\ell=1}^{j} c_s(i_\ell, i_\ell - (k - j + \ell)) \right) \\
&= \sum_{\substack{I \subseteq (m, m+n-1] \cap \mathbf{Z} \\ |I| = j-1}} c_s(m+n, m+n-(k-j+j)) \left(\prod_{\ell=1}^{j-1} c_s(i_\ell, i_\ell - (k - j + \ell)) \right) + \left(\begin{matrix} n-1 \\ j \end{matrix}\middle|\begin{matrix} m \\ k \end{matrix}\right)_s \\
&= c_s(m+n, m+n-k) \left(\begin{matrix} n-1 \\ j-1 \end{matrix}\middle|\begin{matrix} m \\ k-1 \end{matrix}\right)_s + \left(\begin{matrix} n-1 \\ j \end{matrix}\middle|\begin{matrix} m \\ k \end{matrix}\right)_s.
\end{aligned}$$

Rearranging this completes the proof. □

Proof of Theorem 2.5.4. We will prove this by induction on n. For the base case, observe that if $n = 0$, then all j in the range of summation satisfy $0 \leq j \leq 0$, so either the sum is empty (if $k - 0 > m$) or its only term is $j = 0$ (if $k - 0 \leq m$). The conditions of the theorem force $k \leq m + n = m$, so the sum has exactly one term:

$$\sum_j \binom{m}{k-j}_s \left(\begin{array}{c|c} n & m \\ j & k \end{array}\right)_s = \binom{m}{k}_s \left(\begin{array}{c|c} 0 & m \\ 0 & k \end{array}\right)_s .$$

We want to show that this is $\binom{m}{k}_s$. The definition of $\left(\begin{smallmatrix} 0 & \vert & m \\ 0 & \vert & k \end{smallmatrix}\right)_s$ gives the rather degenerate identity

$$\left(\begin{array}{c|c} 0 & m \\ 0 & k \end{array}\right)_s = \sum_{\substack{I \subseteq (m,m] \cap \mathbf{Z} \\ |I| = 0}} \left(\prod_{\ell=1}^{0} c_s(i_\ell, i_\ell - (k+\ell)) \right) = \sum_{I \subseteq \emptyset} 1 = 1,$$

which completes the base case.

For the inductive step, suppose that the theorem is true with n replaced by $n - 1$. We will first apply a version of the s-Pascal identity to $\binom{m+n}{k}_s$ that has been "flipped" using the identity $\binom{n}{k}_s = \binom{n}{n-k}_s$:

$$\begin{aligned}
\binom{m+n}{k}_s &= \binom{m+n}{m+n-k}_s \\
&= \binom{m+n-1}{m+n-k-1}_s + c_s(m+n, m+n-k) \binom{m+n-1}{m+n-k}_s \\
&= \binom{m+n-1}{k}_s + c_s(m+n, m+n-k) \binom{m+n-1}{k-1}_s .
\end{aligned}$$

The inductive hypothesis gives:

$$\begin{aligned}
&\binom{m+n-1}{k}_s + c_s(m+n, m+n-k) \binom{m+n-1}{k-1}_s \\
&= \sum_j \binom{m}{k-j}_s \left(\begin{array}{c|c} n-1 & m \\ j & k \end{array}\right)_s + c_s(m+n, m+n-k) \sum_j \binom{m}{k-1-j}_s \left(\begin{array}{c|c} n-1 & m \\ j & k-1 \end{array}\right)_s \\
&= \sum_j \binom{m}{k-j}_s \left(\begin{array}{c|c} n-1 & m \\ j & k \end{array}\right)_s + c_s(m+n, m+n-k) \sum_j \binom{m}{k-j}_s \left(\begin{array}{c|c} n-1 & m \\ j-1 & k-1 \end{array}\right)_s \\
&= \sum_j \binom{m}{k-j}_s \left(\left(\begin{array}{c|c} n-1 & m \\ j & k \end{array}\right)_s + c_s(m+n, m+n-k) \left(\begin{array}{c|c} n-1 & m \\ j-1 & k-1 \end{array}\right)_s \right) .
\end{aligned}$$

By Lemma 2.5.6, this is equal to

$$\sum_j \binom{m}{k-j}_s \left(\begin{array}{c|c} n & m \\ j & k \end{array}\right)_s ,$$

which completes the induction. □

3. GENERALIZED n-SERIES OVER $\mathbf{Z}$

3.1. **Lexicographically small nonnegative integer generalized n-series.** When doing computations with generalized n-series, it is useful to have some examples over $\mathbf{Z}$ that are lexicographically small (close to 0 for small values of n). We will restrict to integer GNS that are always nonnegative. We have already seen some examples of relatively small integer generalized n-series: $s(n) = n$ and $s(n) = [n]_q$. Before looking at an algorithm for constructing lexicographically small GNS, we need a definition:

Definition 3.1.1. Let R be a ring, and let $N \in \mathbf{Z}_{\geq 0}$. A *partial generalized n-series* is a function $s : \{0, 1, \ldots, N\} \to R$ such that $s(0) = 0$, $s(n)$ is not a zero-divisor for $0 < n \leq N$, and for all $0 \leq k \leq n \leq N$, $s(n-k) \mid s(n) - s(k)$. An *extension* of a partial GNS s is a GNS which agrees with s on the domain of s.

Given a partial GNS

$$s : \{0, 1, \ldots, N\} \to \mathbf{Z}_{\geq 0}$$

we can use a greedy algorithm to construct the lexicographically smallest nonnegative GNS $\widetilde{s}$ which is an extension of s.

Definition 3.1.2. Suppose we are given a partial GNS $s : \{0, 1, \ldots, N\} \to \mathbf{Z}_{\geq 0}$. Define a function $\widetilde{s} : \mathbf{Z}_{\geq 0} \to \mathbf{Z}_{\geq 0}$ in the following way: $\widetilde{s}(n) = s(n)$ for $0 \leq n \leq N$, and for each $n > N$ we define $\widetilde{s}(n)$ in terms of the previous values of $\widetilde{s}(k)$ to be the smallest positive integer that makes the restriction $\widetilde{s}|_{\{0,1,\ldots,n\}}$ a partial GNS.

The fact that $\widetilde{s}$ is well-defined is nontrivial. We have to show that at each step of the algorithm, $\widetilde{s}(n)$ exists. We will actually prove a stronger theorem:

Theorem 3.1.3. *Consider the following recursive construction of an arbitrary nonnegative GNS over $\mathbf{Z}$: Start with $s(0) = 0$, and for each N starting with 1 in increasing order, choose $s(N)$ to be an* arbitrary *integer such that $s|_{\{0,1,\ldots,N\}}$ is a partial GNS. No matter what choices are made, it is always possible to continue (there are never any contradictions).*

Proof. Suppose we have a partial GNS s with domain $\{0, 1, \ldots, N-1\}$, and we want to choose $s(N)$. We have to show that there exists $s(N)$ such that for all $0 < k < N$, $s(N-k) \mid s(N) - s(k)$. This is equivalent to $s(N) \equiv s(k) \pmod{s(N-k)}$, so we really have a system of linear congruences. This system has a solution by the generalized Chinese Remainder Theorem as long as no two congruences contradict each other. We want to show that if we reduce two of the congruences $s(N) \equiv s(N-k) \pmod{s(k)}$ and $s(N) \equiv s(N-j) \pmod{s(j)}$ modulo $\gcd(s(k), s(j))$, they become the same congruence. That is, we want to show that

$$s(N-k) \equiv s(N-j) \pmod{\gcd(s(k), s(j))}.$$

By Lemma 2.2.6, $\gcd(s(k), s(j)) = \pm s(\gcd(k, j))$. And since

$$N - k \equiv N \equiv N - j \pmod{\gcd(k, j)},$$

the desired congruence must be true by Lemma 2.2.4. □

We have seen that many number-theoretical properties of the positive integers remain true for arbitrary GNS. However, there are some important differences between $s(n) = n$ and other GNS. For example, if $n = p^j m$ with $p \nmid m$, then n/p^j is a unit modulo p. This is generally false for other generalized n-series; using Theorem 3.1.3, we can construct a counterexample.

Example 3.1.4. Let s be an extension of the partial GNS with domain $\{0, 1, \ldots, 6\}$ whose values are $0, 1, 2, 3, 10, 11, 12$. One can check manually that this forms a partial GNS. For this GNS,

$$\frac{s(6)}{s(2)} = \frac{12}{2} = 6 \equiv 0 \pmod{s(2)}.$$

3.2. **An upper bound on lexicographically small nonnegative integer GNS.** In this section, we will write partial generalized n-series as lists of numbers, where the first item in the list is $s(0)$. For example:

Example 3.2.1. Define a partial generalized n-series $0, 1, 3$ via the function $s : \{0, 1, 2\} \to \mathbf{Z}_{\geq 0}$ given by $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 3$. If we apply the algorithm of Definition 3.1.2 to the partial generalized n-series $0, 1, k$ where $k \in \mathbf{Z}_{>0}$, we get a generalized n-series $0, 1, k, 1, k, \ldots$, where the n-th term is 0 if $n = 0$, 1 if n is odd, and k if n is even and nonzero. If we start with a longer partial generalized n-series s, say $0, 1, 3, 4$, then the generalized n-series $\widetilde{s}$ starts with

$$0, 1, 3, 4, 9, 19, 552, 22081,$$

and the next few terms are

$$219440979, 2669857856653708, 6558922971496604200448626056129.$$

This seems to grow very fast when n increases, almost doubling the number of digits each term. As we will see, $\widetilde{s}(n)$ is bounded by

$$\widetilde{s}(n) < 12^{2^{n-4}}, \qquad n \geq 4, \text{ and}$$
$$\widetilde{s}(n) = \Omega_a(a^n), \qquad \forall a \geq 0.$$

The upper bound (a special case of Theorem 3.2.5) is proved below, and the lower bound (a special case of Theorem 3.3.1) is proved in the next subsection.

Let us first show that $\widetilde{s}$ is strictly increasing.

Lemma 3.2.2. *Let $N \geq 3$, and let $s : \{0, 1, \ldots, N\} \to \mathbf{Z}_{\geq 0}$ be a strictly increasing partial generalized n-series. Then, $\widetilde{s}$ is also strictly increasing.*

Remark 3.2.3. The condition $N \geq 3$ is important, because we already saw that if $s = 0, 1, 3$ (so $N = 2$) then $\widetilde{s} = 0, 1, 3, 1, 3, \ldots$, which is not strictly increasing.

Proof. Notice that $s(2) > s(1) \geq 1$. Let $n > N$. We will show that $\widetilde{s}(n) > \widetilde{s}(n-1)$. By Lemma 2.2.4, $\widetilde{s}(n) \equiv s(1) \pmod{s(n-1)}$, so either $\widetilde{s}(n) = s(1)$ or $\widetilde{s}(n) > s(n-1)$. The first case cannot happen because $\widetilde{s}(n) \equiv s(2) \pmod{\widetilde{s}(n-2)}$, and $\widetilde{s}(n-2) \geq s(2) > s(1)$. Therefore, $\widetilde{s}(n) > \widetilde{s}(n-1)$. □

Given the value of $\widetilde{s}(k)$ for all $1 \leq k < n$, there is an upper bound on $\widetilde{s}(n)$, as long as $\widetilde{s}$ is strictly increasing:

Lemma 3.2.4. *Let $s : \{0, 1, \ldots, N\} \to \mathbf{Z}$ be a strictly increasing partial generalized n-series with $N \geq 3$. Then, for all $n > N$,*

$$\widetilde{s}(n) < \operatorname{lcm}\{\widetilde{s}(k) \mid 0 < k < n\}.$$

Proof. Recall that the proof of the existence of $\widetilde{s}$ (Theorem 3.1.3) constructs $\widetilde{s}(n)$ from $\widetilde{s}(k)$ for all $0 < k < n$ using the generalized Chinese Remainder Theorem. The congruences are $x \equiv \widetilde{s}(n-k) \pmod{\widetilde{s}(k)}$ for each $0 < k < n$, so the generalized CRT proves the existence of a unique solution x modulo $L = \operatorname{lcm}\{\widetilde{s}(k) \mid 0 < k < n\}$. Therefore, there exists a solution to the system of congruences with $0 < x \leq L$. The smallest positive solution is $\widetilde{s}(n)$ by Definition 3.1.2, so $\widetilde{s}(n) \leq L$. We just have to show that $\widetilde{s}(n) \neq L$.

Suppose for contradiction that $\widetilde{s}(n) = L$. Then, by Lemma 2.2.4, $L \equiv \widetilde{s}(1) \pmod{\widetilde{s}(n-1)}$. But by the definition of L, L is divisible by $\widetilde{s}(n-1)$, so $\widetilde{s}(1)$ is also divisible by $\widetilde{s}(n-1)$. Since $n - 1 > N - 1 > 1$, $\widetilde{s}(1) < \widetilde{s}(n-1)$ by Lemma 3.2.2, which is a contradiction. □

Using the fact that the LCM of a set is at most its product, we can prove the following upper bound:

Theorem 3.2.5. *Let $s : \{0, 1, \ldots, N\} \to \mathbf{Z}$ be a strictly increasing partial generalized n-series with $N \geq 3$. Then, for all $n > N$,*

$$\widetilde{s}(n) < \Pi^{2^{n-(N+1)}},$$

where $\Pi = \prod_{k=1}^{N} s(k)$.

Proof. We will use strong induction. Suppose that $n > N$ and for all k strictly between N and n,

$$\widetilde{s}(k) < \Pi^{2^{k-(N+1)}}.$$

By Lemma 3.2.4 and the inductive hypothesis,

$$\begin{aligned}\widetilde{s}(n) &< \operatorname{lcm}\{\widetilde{s}(k) \mid 0 < k < n\} \leq \prod_{k=1}^{n-1} \widetilde{s}(k)\\ &\leq \left(\prod_{k=1}^{N} s(k)\right)\left(\prod_{k=N+1}^{n-1} \Pi^{2^{k-(N+1)}}\right)\\ &= \Pi \cdot \prod_{k=0}^{n-(N+2)} \Pi^{2^k} = \Pi \cdot \Pi^{\left(\sum_{k=0}^{n-(N+2)} 2^k\right)}\\ &= \Pi \cdot \Pi^{2^{n-(N+1)}-1} = \Pi^{2^{n-(N+1)}}.\end{aligned}$$

This completes the induction. □

Remark 3.2.6. Another way to think about this theorem is that the recursively defined sequence

$$a_n = \begin{cases} s(n) & \text{if } 0 \leq n \leq N,\\ \prod_{k=1}^{n-1} a_k & \text{if } n > N \end{cases}$$

is exactly equal to $\Pi^{2^{n-(N+1)}}$ for all $n > N$, and we know that $\widetilde{s}(n)$ satisfies this recurrence but with the equality replaced by $<$ whenever $n > N$, so it should be true that $\widetilde{s}(n) < a_n$ for all $n > N$.

3.3. **A lower bound on strictly increasing integer GNS.** We proved an upper bound on the lexicographically smallest extension of the partial GNS $0, 1, 3, 4$ in the previous section, but we also stated a lower bound. The purpose of this subsection is to prove this lower bound by proving a more general result.

Theorem 3.3.1. *Let $s(n)$ be a strictly increasing generalized n-series over $\mathbf{Z}$ that is not a scalar multiple of $n \mapsto [n]_q$ for any $q \in \mathbf{Z}_{>0}$. Then, $s(n) = \Omega_a(a^n)$ for all $a \geq 0$.*

In this theorem statement, we use the convention that $[n]_1 = n$. To prove Theorem 3.3.1, we will use the following lemma:

Lemma 3.3.2. *Let s satisfy the conditions of Theorem 3.3.1, and fix a nonnegative integer a. Then, for all sufficiently large n,*

$$s(n+1) \neq as(n) + s(1).$$

Proof. Let $k \in \mathbf{Z}_{\geq 0}$ such that $s(k+1) \neq as(k) + s(1)$. Such a k must exist, because otherwise $s(n+1) = as(n) + s(1)$ for all $n \in \mathbf{Z}_{\geq 0}$. This would imply by induction that $s(n) = s(1)[n]_q$ with $q = a$ for all n, which contradicts our assumption about s. Next, choose an integer N large enough so that

$$s(N-k) > \max\{s(k+1), as(k) + s(1)\}.$$

This is always possible, because $s : \mathbf{Z}_{\geq 0} \to \mathbf{Z}$ is strictly increasing and therefore unbounded.

To prove the lemma, we will show that for all $n \geq N$, we have $s(n+1) \neq as(n) + s(1)$. Suppose for contradiction that there exists $n \geq N$ with

$$s(n+1) = as(n) + s(1).$$

Taking this equation modulo $s(n-k)$ and using Lemma 2.2.4 gives

$$s(k+1) \equiv as(k) + s(1) \pmod{s(n-k)}.$$

But $n \geq N$, so

$$s(n-k) \geq s(N-k) > \max\{s(k+1), as(k)+s(1)\},$$

so the modulus is greater than both sides of the congruence, which means that it is an equality. This contradicts the fact that $s(k+1) \neq as(k)+s(1)$. □

Proof of Theorem 3.3.1. We want to show that $s(n) = \Omega_a(a^n)$ for all $a \geq 0$. It suffices to prove this for $a \in \mathbf{Z}_{\geq 0}$. For each integer b with $0 < b < a$, apply Lemma 3.3.2 with a replaced by b. This gives an integer N_b such that for all $n \geq N_b$,

$$s(n+1) \neq bs(n)+s(1).$$

Let

$$N = \max\{N_b \mid 0 < b < a\}.$$

We claim that for all $n \geq N$, we have $s(n+1) \geq as(n)+s(1)$.

To see this, let $n \geq N$. By Lemma 2.2.4,

$$s(n+1) \equiv s(1) \pmod{s(n)},$$

so $s(n+1) = bs(n)+s(1)$ for some $b \in \mathbf{Z}$. Since s is strictly increasing, b must be positive. We want to show that $b \geq a$. If $b < a$, then we defined N_b above, and $n \geq N \geq N_b$. So $s(n+1) \neq bs(n)+s(1)$, which is a contradiction. Therefore, $b \geq a$, so

$$s(n+1) \geq as(n)+s(1).$$

To complete the proof, notice that the claim implies (by induction) that for all $n \geq N$, $s(n) \geq a^{n-N}s(N)$, which means that $s(n) = \Omega_a(a^n)$ as $n \to \infty$. □

3.4. **A more general s-Lucas theorem.** The s-Lucas theorem (Proposition 2.4.8) is a congruence modulo $s(p)$, where s is a GNS and p is prime. The q-Lucas theorem has a more general form which allows p to be composite:

$$\binom{n_1p+n_0}{k_1p+k_0}_q \equiv \binom{n_1}{k_1}\binom{n_0}{k_0}_q \pmod{\Phi_p(q)}.$$

In this subsection, we will state and prove an s-analogue of the more general q-Lucas theorem in the case $n_0 = k_0 = 0$.

Recall the s-analogue $\Phi_n(s)$ of the cyclotomic polynomial from Remark 2.4.3.

Theorem 3.4.1. *If s is a GNS over* $\mathbf{Z}$*, then $\Phi_n(s) \in \mathbf{Z}$ for all $n > 0$.*

We will prove that $\Phi_n(s) \in \mathbf{Z}$ by showing that

$$\Phi_n(s) = \frac{s(n)}{\operatorname{lcm}\{s(n/p) \mid p \text{ prime factor of } n\}}.$$

Here is a lemma:

Lemma 3.4.2. *Let S be an arbitrary multiset of positive integers. Then,*

$$\operatorname{lcm}(S) = \prod_{\substack{\text{multiset } A\subseteq S\\ A\neq\emptyset}} \gcd(A)^{(-1)^{|A|-1}}.$$

This lemma can be proved using the tools of elementary number theory. Notice that when s is a two-element multiset $\{a,b\}$, this formula reduces to $\operatorname{lcm}(a,b) = ab/\gcd(a,b)$.

Proof of Lemma 3.4.2. We can decompose the right-hand side into its prime-power factors. Let p be a prime, and let T be the multiset $\{v_p(a) \mid a \in S\}$, where $v_p(a)$ is the exponent of p in the prime factorization of a. The exponent of p in the right-hand side of the equality we are trying to prove is

$$\sum_{\substack{\text{multiset } B \subseteq T \\ B \neq \emptyset}} (-1)^{|B|-1} \min(B),$$

because a GCD of powers of p is p to the power of the minimum exponent. We want to show that this is equal to $v_p(\operatorname{lcm}(S))$, which is $\max(T)$. Write $T = \{a_1, a_2, \ldots, a_k\}$, where $k = |T|$ and $a_1 \leq a_2 \leq \cdots \leq a_n$. We will count the number of times each a_j is counted in the sum. Since $\max(T) = a_n$, we have to show that a_n is counted once and a_j is counted 0 times for all $1 \leq j < n$.

Let $1 \leq j \leq n$ and let $1 \leq k \leq n$. We want to count how many subsets $B \subseteq T$ have minimum j and cardinality n. Such a subset must include a_j, but can have any combination of $k-1$ elements a_ℓ with $\ell > j$. There are $\binom{n-j}{k-1}$ choices for these remaining elements. Therefore, the number of times a_j is counted in the sum is

$$\sum_{k=1}^{n} (-1)^{k-1} \binom{n-j}{k-1} = \sum_{k=0}^{n-1} (-1)^k \binom{n-j}{k}.$$

Since $\binom{n-j}{k}$ is zero for $k > n-j$, this is just the alternating sum of row $n-j$ of Pascal's triangle, which is 0 if $n-j > 0$ and 1 if $n-j = 0$. Therefore, a_j is counted 0 times for $j < n$ and 1 time for $j = n$ in the sum

$$\sum_{\substack{B \subseteq P \\ B \neq \emptyset}} (-1)^{|B|-1} \min(B),$$

so the sum is equal to a_n. This means that the exponents of p in the left-hand and right-hand sides of the equality in the theorem statement are both a_n. Combining this fact for each prime p proves the lemma. □

Proof of Theorem 3.4.1. Let P be the set of prime factors of n, and let

$$r(n) = \frac{s(n)}{\operatorname{lcm}\{s(n/p) \mid p \in P\}}.$$

Notice that $r(n) \in \mathbf{Z}$ because Lemma 2.2.3 implies that $s(n/p) \mid s(n)$ for all prime factors p of n. We want to show that $\Phi_n(s) = r(n)$.

By the definition of $r(n)$,

$$\frac{s(n)}{r(n)} = \operatorname{lcm}\left\{ s\left(\frac{n}{p}\right) \,\middle|\, p \in P \right\}.$$

By Lemma 3.4.2 with $S = \{s(n/p) \mid p \in P\}$, this is equal to

$$\prod_{\substack{A \subseteq P \\ A \neq \emptyset}} \gcd\left\{ s\left(\frac{n}{p}\right) \,\middle|\, p \in A \right\}^{(-1)^{|A|-1}}.$$

Lemma 2.2.6 and the fact that s is nonnegative imply that s preserves GCDs, so

$$\gcd\left\{ s\left(\frac{n}{p}\right) \,\middle|\, p \in A \right\} = s\left(\gcd\left\{ \frac{n}{p} \,\middle|\, p \in A \right\} \right) = s\left(\frac{n}{\operatorname{lcm}(A)} \right).$$

This implies that

$$\frac{s(n)}{r(n)} = \prod_{\substack{A \subseteq P \\ A \neq \emptyset}} s\left(\frac{n}{\operatorname{lcm}(A)} \right)^{(-1)^{|A|-1}}.$$

Dividing both sides by $s(n)$ and taking the reciprocal of both sides gives

$$r(n) = \prod_{A \subseteq P} s\left(\frac{n}{\operatorname{lcm}(A)}\right)^{(-1)^{|A|}}.$$

(On the right-hand side, we removed the condition $A \neq \emptyset$ and multiplied the exponent by -1.)

We have to count how many ways each divisor d of n can be written as $\operatorname{lcm}(A)$ for $A \subseteq P$. Since the elements of A are distinct primes, $\operatorname{lcm}(A)$ is the product of the elements of A. Therefore, $d = \operatorname{lcm}(A)$ is square-free, and given d there is a unique choice of A (the set of prime factors of d). So we get

$$r(d) = \prod_{\substack{d \mid n \\ d \text{ square-free}}} s\left(\frac{n}{d}\right)^{\mu(d)},$$

using the fact that $\mu(d)$ is $(-1)^{|A|}$ if A is the set of prime factors of a square-free number d. Since $\mu(d) = 0$ for d not square-free, we can remove the restriction that d is square-free:

$$r(n) = \prod_{d \mid n} s\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d \mid n} s(d)^{\mu(n/d)} = \Phi_n(s).$$

This is what we wanted to show. □

Before proving the s-Lucas theorem for composite p, we will prove a lemma about $\Phi_n(s)$.

Lemma 3.4.3. *Let s be a nonnegative integer GNS, let $m \in \mathbf{Z}_{>0}$, and let $a, b \in \mathbf{Z}_{\geq 0}$ such that*

$$a \equiv b \not\equiv 0 \pmod{m}.$$

Define

$$d = \gcd(a, m) = \gcd(b, m).$$

Then,

$$\frac{s(a)}{s(d)} \equiv \frac{s(b)}{s(d)} \pmod{\Phi_m(s)}.$$

Additionally, both sides of this congruence are units modulo $\Phi_m(s)$. Equivalently, the function $\mathbf{Z}_{\geq 0} \to \mathbf{Z}_{\geq 0}$ defined by $a \mapsto s(a)/s(\gcd(a, m))$ induces a well-defined function

$$(\mathbf{Z}/m) \setminus \{0\} \to (\mathbf{Z}/\Phi_m(s))^\times.$$

Proof. By Lemma 2.2.4,

$$s(a) \equiv s(b) \pmod{s(m)}.$$

Since $\gcd(s(m), s(d)) = s(d)$, this implies that

$$\frac{s(a)}{s(d)} \equiv \frac{s(b)}{s(d)} \quad \left(\operatorname{mod} \frac{s(m)}{s(d)}\right).$$

Notice that

$$\begin{aligned}
\gcd\left\{\frac{s(m)}{s(d)} \;\middle|\; d \text{ proper divisor of } m\right\} &= \frac{s(m)}{\operatorname{lcm}\{s(d) \mid d \text{ proper divisor of } m\}} \\
&= \frac{s(m)}{\operatorname{lcm}\{s(m/p) \mid p \text{ prime factor of } m\}} \\
&= \Phi_m(s).
\end{aligned}$$

In the second step of this chain of equalities, we used the fact that for every proper divisor d of m there exists a prime factor p of m such that $d \mid m/p$. We also used Lemma 2.2.3. We can conclude that

$\Phi_m(s) \mid s(m)/s(d)$ for all proper divisors d of m. In particular, for $d = \gcd(a, m) = \gcd(b, m)$, we have

$$\frac{s(a)}{s(d)} \equiv \frac{s(b)}{s(d)} \pmod{\Phi_m(s)}.$$

To complete the proof, we just have to show that $s(a)/s(d)$ is a unit modulo $\Phi_m(s)$. This is true because $\Phi_m(s) \mid s(m)/s(d)$ implies that

$$\gcd\left(\Phi_m(s), \frac{s(a)}{s(d)}\right) \mid \gcd\left(\frac{s(m)}{s(d)}, \frac{s(a)}{s(d)}\right) = \frac{\gcd(s(m), s(a))}{s(d)} = \frac{s(d)}{s(d)} = 1. \qquad \square$$

Theorem 3.4.4 ("Composite version" of the s-Lucas theorem)**.** *Let $m \in \mathbf{Z}_{>0}$ and let $n, k \in \mathbf{Z}_{\geq 0}$. Then,*

$$\binom{nm}{km}_s \equiv \binom{n}{k}_{s_m} \pmod{\Phi_m(s)}.$$

Proof. By definition,

$$\binom{nm}{km}_s = \frac{s(nm)s(nm-1)\cdots s(nm-km+1)}{s(km)s(km-1)\cdots s(1)} = \frac{\prod_{j=1}^{km} s(nm-km+j)}{\prod_{j=1}^{km} s(j)}.$$

Our goal will be to cancel each $s(nm - km + j)$ with the corresponding $s(j)$ modulo $\Phi_m(s)$. The problem is that in general, these are not units modulo $\Phi_m(s)$. To fix this, we will divide $s(nm-km+j)$ and $s(j)$ by $s(\gcd(j, m))$:

$$\binom{nm}{km}_s = \frac{\prod_{j=1}^{km} s(nm-km+j)/s(\gcd(j,m))}{\prod_{j=1}^{km} s(j)/s(\gcd(j,m))}.$$

Since $j \equiv nm - km + j \pmod{m}$, we can apply Lemma 3.4.3 for all j not divisible by m, and we get that

$$\frac{s(nm-km+j)}{s(\gcd(j,m))} \quad \text{and} \quad \frac{s(j)}{s(\gcd(j,m))}$$

are congruent units modulo $\Phi_m(s)$.

Therefore, we can cancel $s(nm - km + j)/s(\gcd(j, m))$ with $s(j)/s(\gcd(j, m))$ modulo $\Phi_m(s)$ for every j not divisible by m. We get

$$\begin{aligned}\binom{nm}{km}_s &= \frac{\prod_{j=1}^{km} s(nm-km+j)/s(\gcd(j,m))}{\prod_{j=1}^{km} s(j)/s(\gcd(j,m))} \\ &\equiv \frac{\prod_{\ell=1}^{k} s((n-k+\ell)m)/s(m)}{\prod_{\ell=1}^{k} s(\ell m)/s(m)} \\ &= \frac{\prod_{\ell=1}^{k} s((n-k+\ell)m)}{\prod_{\ell=1}^{k} s(\ell m)} \\ &= \binom{n}{k}_{s_m} \pmod{\Phi_m(s)}.\end{aligned}$$

We changed product indices from j to $\ell = j/m$, because the terms with $m \nmid j$ were canceled in the second step. $\square$

Remark 3.4.5. When m is prime, Theorem 3.4.4 reduces to the case $n_0 = k_0 = 0$ of the s-Lucas theorem (Proposition 2.4.8).

4. Generalized n-Series and de Rham Complexes

4.1. **Basic properties of the s-de Rham complex.** In this subsection, we will define the "s-de Rham complex" using the s-derivative of Definition 2.3.3. Recall that this is the R-linear map $\nabla_s : R[x] \to R[x]$ given on monomials by $\nabla_s(x^n) = s(n)x^{n-1}$. Write $\mathbf{A}^1 = \operatorname{Spec} R[x]$ to denote the affine line over R.

Definition 4.1.1. The s-de Rham complex for $R[x]$ is the 2-term complex

$$s\Omega_{\square,\mathbf{A}^1} := (R[x] \xrightarrow{\nabla_s} R[x]dx).$$

Here, the square indicates the dependence of $s\Omega_{\square,\mathbf{A}^1}$ on the choice of coordinate x.

Remark 4.1.2. It is easy to generalize the s-de Rham complex to several variables (e.g., by defining $s\Omega_{\mathbf{A}^n}$ to be $s\Omega_{\square,\mathbf{A}^1}^{\otimes_R n}$). Since proving multivariable analogues of the results below is straightforward, we will only study the case of a single variable.

Example 4.1.3. Let $s : \mathbf{Z}_{\geq 0} \to \mathbf{Z}[\![q-1]\!]$ denote the q-integer GNS from Example 2.1.6. Then Definition 4.1.1 is precisely the q-de Rham complex of [Sch17].

The s-Pascal identity of Proposition 2.1.3 can be restated in terms of the s-derivative:

Lemma 4.1.4. *There is an equality of operators:*

$$\left[\frac{\nabla_s^k}{k!_s}, x\right] = \frac{\nabla_s^{k-1}}{(k-1)!_s}.$$

Proof. Let $n > k \geq 0$ be integers. Since $\nabla_s(x^n) = s(n)x^{n-1}$, we have

$$\nabla_s^k(x^n) = s(n)s(n-1)\cdots s(n-k+1)x^{n-k} = \frac{n!_s}{(n-k)!_s}x^{n-k}.$$

This implies that

$$\frac{\nabla_s^k}{k!_s}x^n = \binom{n}{k}_s x^{n-k}.$$

The s-Pascal identity can therefore be stated as:

$$\frac{\nabla_s^k}{k!_s}x^n = \frac{\nabla_s^{k-1}}{(k-1)!_s}x^{n-1} + x\frac{\nabla_s^k}{k!_s}x^{n-1}.$$

Rearranging gives

$$\frac{\nabla_s^k}{k!_s}x^n - x\frac{\nabla_s^k}{k!_s}x^{n-1} = \frac{\nabla_s^{k-1}}{(k-1)!_s}x^{n-1}.$$

Recognizing the left side as a commutator of operators, this can be written as

$$\left[\frac{\nabla_s^k}{k!_s}, x\right]x^{n-1} = \frac{\nabla_s^{k-1}}{(k-1)!_s}x^{n-1}.$$

This implies the desired equality of operators. □

Remark 4.1.5. One can similarly restate the s-Lucas theorem (Proposition 2.4.8) via the s-derivative: namely, if the hypotheses of Proposition 2.4.8 are satisfied, then for any prime p and any nonnegative integers n_1, n_0, k_1, k_0 such that $n_0, k_0 < p$, we have

$$\frac{\nabla_s^{k_1p+k_0}}{(k_1p+k_0)!_s}(x^{n_1p+n_0}) \equiv \frac{\partial_{x^p}^{k_1}}{k_1!}(x^{n_1p})\frac{\nabla_s^{k_0}}{k_0!_s}(x^{n_0}) \pmod{s(p)}.$$

Proposition 4.1.6 (s-product rule)**.** *For a GNS s over R, define an R-bilinear operator $\star_s : R[x] \otimes_R R[x] \to R[x]$ on monomials by*

$$x^a \star_s x^b = c_s(a+b+1, a)x^{a+b}$$

for all $a, b \in \mathbf{Z}_{\geq 0}$. Then, for all $f, g \in R[x]$,

$$\nabla_s(fg) = \nabla_s(f)g + f \star_s \nabla_s(g).$$

Proof. Since ∇_s is R-linear and $\star_s$ is R-bilinear, the theorem follows from the case where f and g are monomials x^a and x^b. In this case,

$$\begin{aligned}
\nabla_s(x^a)x^b + x^a \star_s \nabla_s(x^b) &= s(a)x^{a-1}x^b + x^a \star_s s(b)x^{b-1} \\
&= s(a)x^{a+b-1} + s(b)c_s(a+b, a)x^{a+b-1} \\
&= \left(s(a) + s(b) \cdot \frac{s(a+b) - s(a)}{s(b)}\right) x^{a+b-1} \\
&= (s(a) + s(a+b) - s(a))x^{a+b-1} \\
&= s(a+b)x^{a+b-1} \\
&= \nabla_s(x^{a+b}). \qquad \square
\end{aligned}$$

Example 4.1.7. Let $s : \mathbf{Z}_{\geq 0} \to \mathbf{Z}[\![q-1]\!]$ denote the q-integer GNS from Example 2.1.6. Then

$$c_s(a+b+1, a) = \frac{[a+b+1]_q - [a]_q}{[b+1]_q} = \frac{q^{a+b+1} - q^a}{q^{b+1} - 1} = q^a,$$

so that $x^a \star_s x^b = q^a x^{a+b} = (qx)^a x^b$. In particular,

$$f(x) \star_s \nabla_s(g(x)) = f(qx)\nabla_q(g(x)),$$

so that Proposition 4.1.6 reduces to the usual q-Leibniz rule.

Example 4.1.8. One can check that the function $s : \mathbf{Z}_{\geq 0} \to \mathbf{Z}[\![q-1]\!]$ given by

$$s(n) = \frac{1}{q-1}\frac{q^{2n}-1}{q^{2n}+1} \in \mathbf{Z}[\![q-1]\!]$$

defines a GNS; see Example 4.3.2. It follows that

$$c_s(a+b+1, a) = \frac{\frac{q^{2(a+b+1)}-1}{q^{2(a+b+1)}+1} - \frac{q^{2a}-1}{q^{2a}+1}}{\frac{q^{2(b+1)}-1}{q^{2(b+1)}+1}} = \frac{2q^{2a}(q^{2(b+1)}-1)}{(q^{2(a+b+1)}-1)(q^{2a}-1)}.$$

In particular, unlike for the q-integer GNS, there is no simple expression for $f(x) \star_s g(x)$.

Corollary 4.1.9. *Fix a GNS s over R. Then the complex $s\Omega_{\Box,\mathbf{A}^1}$ naturally admits the structure of a (noncommutative) differential graded R-algebra.*

Proof. Define a left and right $s\Omega^0_{\Box,\mathbf{A}^1} = R[x]$-module structure on $s\Omega^1_{\Box,\mathbf{A}^1}$ as follows: the right module structure is the obvious one, and the left module structure is given by $g(x) \cdot f(x)dx = g \star_s f(x)dx$. Then the s-Leibniz rule of Proposition 4.1.6 produces a $s\Omega^0_{\Box,\mathbf{A}^1}$-bimodule structure on $s\Omega^1_{\Box,\mathbf{A}^1}$ such that the s-derivative satisfies the Leibniz rule; this is precisely the structure of a differential graded R-algebra. $\square$

4.2. **s-analogues of the Poincaré lemma and Cartier isomorphism.** The Poincaré lemma says that over a field k of characteristic zero, the cohomology of the de Rham complex is concentrated in degree zero (where it is isomorphic to k). A version of this statement is also true over $\mathbf{Z}$. Namely, if $\mathbf{Z}\langle x\rangle = \mathbf{Z}[x, \frac{x^n}{n!}]_{n\geq 0}$ denotes the divided power envelope of $\mathbf{Z}[x]$, then the cohomology of the complex $\Omega^\bullet_{\mathbf{Z}[x]/\mathbf{Z}} \otimes_{\mathbf{Z}[x]} \mathbf{Z}\langle x\rangle$ is concentrated in degree zero (where it is isomorphic to $\mathbf{Z}$). This admits a straightforward generalization to the s-de Rham complex:

Proposition 4.2.1 (s-Poincaré lemma)**.** *Let s be a GNS over R, and let $R\langle x\rangle_s$ denote the ring $R[x, \frac{x^n}{n!_s}]_{n\geq 0}$. Then the cohomology of the complex $s\Omega_{\square,\mathbf{A}^1} \otimes_{R[x]} R\langle x\rangle_s$ is concentrated in degree zero, where it is isomorphic to R.*

Proof. We need to show that the R-linear map

$$R\langle x\rangle_s \xrightarrow{\nabla_s} R\langle x\rangle_s dx$$

is surjective, and has kernel R. Surjectivity follows from the observation that $\nabla_s \frac{x^n}{n!_s} = \frac{x^{n-1}}{(n-1)!_s}$; this also implies that the kernel of ∇_s is precisely the R-submodule of $R\langle x\rangle_s$ generated by the constants. □

Remark 4.2.2. Note that the ring $R\langle x\rangle_s$ is nonzero, since the elements $n!_s \in R$ are not zero-divisors; in fact, $R\langle x\rangle_s$ is a subring of $R[1/s]$.

The s-de Rham complex also satisfies an analogue of the Cartier isomorphism.

Recollection 4.2.3. The Cartier isomorphism says that if A is a smooth $\mathbf{F}_p$-algebra, there is a canonical isomorphism $\Omega^i_{A/\mathbf{F}_p} \cong \mathrm{H}^i(\Omega^\bullet_{A/\mathbf{F}_p})$. If φ denotes the Frobenius on R, this isomorphism is roughly given by "$\frac{\varphi}{p^i}$". When $A = \mathbf{F}_p[x]$, one can interpret the Cartier isomorphism as giving a canonical isomorphism

$$\Omega^i_{\mathbf{Z}[x^p]/\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{F}_p \cong \mathrm{H}^i(\Omega^\bullet_{\mathbf{Z}[x]/\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{F}_p)$$

sending $d(x^p) \mapsto [x^{p-1}dx]$. In [Sch17, Proposition 3.4], Scholze proves a q-analogue of the Cartier isomorphism. Let $\mathbf{Z}[\zeta_p]$ denote the quotient $\mathbf{Z}[\![q-1]\!]/[p]_q$, so that ζ_p denotes a primitive pth root of unity. Then there is a canonical isomorphism

$$\Omega^i_{\mathbf{Z}[x^p]/\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{Z}[\zeta_p] \cong \mathrm{H}^i(q\Omega^\bullet_{\mathbf{Z}[x]/\mathbf{Z}} \otimes_{\mathbf{Z}[\![q-1]\!]} \mathbf{Z}[\zeta_p]).$$

Both of these results admit an s-analogue.

Proposition 4.2.4. *Let s be a GNS over R such that $s(1)$ is a unit in $R/s(p)$. Then there is a canonical isomorphism*

$$s\Omega^i_{\square,\mathbf{A}^1} \otimes_R R/s(p) \cong \mathrm{H}^i(s\Omega_{\square,\mathbf{A}^1} \otimes_R R/s(p))$$

sending $x^n \mapsto x^{np}$ in degree zero and $x^n dx \mapsto [x^{np}x^{p-1}dx]$.

Proof. Let us first compute $\mathrm{H}^0(s\Omega_{\square,\mathbf{A}^1} \otimes_R R/s(p))$, i.e., the kernel of ∇_s. Observe that if $a \in R$, then $ax^n \mapsto as(n)x^{n-1}dx$. If $p|n$, then $s(p)|s(n)$, so that $\nabla_s(ax^n) = 0 \in R[x]/s(p)$. It follows from Lemma 2.2.5 that $\nabla_s(ax^n) = 0 \in R[x]/s(p)$ if and only if $s(p)|a$. This implies that $\mathrm{H}^0(s\Omega_{\square,\mathbf{A}^1} \otimes_R R/s(p)) \cong R[x^p]$.

To calculate $\mathrm{H}^1(s\Omega_{\square,\mathbf{A}^1} \otimes_R R/s(p))$, i.e., the cokernel of ∇_s, we need to determine the image of ∇_s. If $ax^n dx$ is in the image of ∇_s for some $a \in R$, then there must be some $b \in R$ such that $bs(n+1) = a$. If $p|n+1$, it follows that $a = 0 \in R/s(p)$; if $p \nmid n+1$, then $s(n+1)$ is a unit (by the preceding discussion), so that $b = \frac{a}{s(n+1)}$. It follows that the image of ∇_s is precisely $\bigoplus_{p\nmid n+1} R\{x^n dx\}$, so that

$$\mathrm{coker}(\nabla_s) = \bigoplus_{n\geq 1} R\{x^{np-1}dx\} \cong \bigoplus_{n\geq 1} R\{x^{p(n-1)} \cdot x^{p-1}dx\}.$$

This implies that $\mathrm{H}^1(s\Omega_{\square,\mathbf{A}^1} \otimes_R R/s(p)) \cong R[x^p]d(x^p)$, as desired. □

In fact, the classical and q-Cartier isomorphisms are special cases of a more general result due to Berthelot and Ogus [BO78]. Let us now review this statement; we will then state and prove the analogue for generalized n-series.

Recollection 4.2.5. Let R be a ring, and let $f \in A$ be a non-zero-divisor. If $M^\bullet$ is a cochain complex of R-modules which is termwise f-torsionfree, the *décalage* $\eta_f M^\bullet$ is the subcomplex of $M^\bullet[1/f]$ defined via

$$(\eta_f M)^i = \{x \in f^i M^i | dx \in f^{i+1} M^{i+1}\}.$$

See [BMS18, Section 6] and [BO78]. One basic property of the décalage construction is the following. Let $\mathrm{H}^\bullet(M/f)$ denote the complex whose underlying graded abelian group is $\bigoplus_{i\in\mathbf{Z}} \mathrm{H}^i(M/f)$, and where the differential is given by the f-Bockstein $\beta : \mathrm{H}^i(M/f) \to \mathrm{H}^{i+1}(M/f)$. Then there is a natural isomorphism of complexes

$$\eta_f(M)/f \xrightarrow{\sim} \mathrm{H}^\bullet(M/f). \tag{5}$$

We will only need the case when $M^\bullet$ is termwise f-torsionfree; but let us mention that η_f preserves quasi-isomorphisms, and one can extend η_f to a (non-exact) functor $L\eta_f : D(R) \to D(R)$ on the the derived category of R.

Let k be a perfect field of characteristic $p > 0$. A very special case of a result of Berthelot and Ogus (in [BO78]) says that if $W(k)$ is the ring of Witt vectors of k and A is a $W(k)$-algebra, there is a Frobenius[2] semilinear isomorphism $\Omega_A \xrightarrow{\sim} L\eta_p\Omega_A$. Suppose for simplicity that Ω_A is p-torsionfree; applying (5) with $f = p$ then defines an isomorphism of complexes

$$\eta_p(\Omega_A)/p \xrightarrow{\sim} \mathrm{H}^\bullet(\Omega_A/p). \tag{6}$$

Note that if we write $A_0 = A/p$, then $\Omega_A/p \cong \Omega_{A_0/k}$. The Frobenius semilinear isomorphism $\Omega_A \xrightarrow{\sim} L\eta_p\Omega_A$ gives a Frobenius semilinear equivalence $\Omega_{A_0/k} \xrightarrow{\sim} \eta_p(\Omega_{A_0})/p$. Comparing the left and right-hand sides of (6) recovers the Cartier isomorphism for A_0.

A similar result was proved in [BS19, Theorem 1.16(4)] for the q-de Rham complex: namely, if A is a smooth $\mathbf{Z}_p[\zeta_p]$-algebra, then there is a Frobenius semilinear equivalence $q\Omega_A \xrightarrow{\sim} L\eta_{[p]_q} q\Omega_A$. As above, using (5) with $f = [p]_q$ recovers the q-analogue of the Cartier isomorphism.

As one might expect, there is a décalage result for the s-de Rham complex, too:

Proposition 4.2.6. *Fix a GNS s over R such that:*

1. *there is a ring endomorphism $\varphi : R \to R$ which sends $s(n) \mapsto \frac{s(np)}{s(p)}$.*
2. *$s(1)$ is a unit in $R/s(p)$, and R is $s(p)$-adically complete.*

Write $\mathbf{A}^{1,(p)} = \operatorname{Spec} R[x^p]$, and define a map $\Phi : s\Omega_{\square,\mathbf{A}^{1,(p)}} \to s\Omega_{\square,\mathbf{A}^1}$ via

$$R[x^p] \xrightarrow{\varphi} R[x], \text{ in degree } 0,$$

$$R[x^p]d(x^p) \xrightarrow{\varphi, d(x^p)\mapsto s(p)x^{p-1}dx} R[x]dx, \text{ in degree } 1.$$

Then Φ factors through a quasi-isomorphism $\varphi^* s\Omega_{\square,\mathbf{A}^{1,(p)}} \xrightarrow{\sim} \eta_{s(p)} s\Omega_{\square,\mathbf{A}^1}$.

Proof. Since $s\Omega_{\square,\mathbf{A}^1}$ is $s(p)$-torsionfree, we can directly compute the complex $\eta_{s(p)} s\Omega_{\square,\mathbf{A}^1}$. If $f(x) = \sum_{n\geq 0} a_n x^n \in R[x]$, then

$$\nabla_s f(x) = \sum_{n\geq 0} a_n s(n) x^{n-1}.$$

[2] The existence of a Frobenius on Ω_A is not obvious, and depends on the existence of crystalline cohomology. However, we will only consider this isomorphism in the case when $A = W(k)[t]$, in which case A admits a Frobenius endomorphism sending $t \mapsto t^p$.

Since $s(p)|s(pj)$ for any $j \geq 0$, we see that $\nabla_s f(x) \in s(p)R[x]$ if and only if $s(p)|a_n$ for $p \nmid n$. Therefore,

$$\eta_{s(p)} s\Omega_{\square,\mathbf{A}^1} = \left(R[x^p] + s(p)R[x] \xrightarrow{\nabla_s} s(p)R[x]dx \right).$$

The map Φ clearly factors through the inclusion $\eta_{s(p)} s\Omega_{\square,\mathbf{A}^1} \subseteq s\Omega_{\square,\mathbf{A}^1}$. It remains to check that the map $\varphi^* s\Omega_{\square,\mathbf{A}^{1,(p)}} \to \eta_{s(p)} s\Omega_{\square,\mathbf{A}^1}$ induces an isomorphism on cohomology. Observe that

$$\begin{aligned} \mathrm{H}^0(s\Omega_{\square,\mathbf{A}^{1,(p)}}) &\cong R, \\ \mathrm{H}^1(s\Omega_{\square,\mathbf{A}^{1,(p)}}) &\cong \bigoplus_{n\geq 1} R/s(n)\{(x^p)^{n-1}d(x^p)\}, \end{aligned}$$

and similarly

$$\begin{aligned} \mathrm{H}^0(\eta_{s(p)} s\Omega_{\square,\mathbf{A}^1}) &\cong R, \\ \mathrm{H}^1(\eta_{s(p)} s\Omega_{\square,\mathbf{A}^1}) &\cong \bigoplus_{n\geq 1} (s(p))/(s(np))\{x^{np-1}dx\} \oplus \bigoplus_{p\nmid m} (s(p))/(s(m)s(p))\{x^{m-1}dx\}. \end{aligned}$$

The ring endomorphism φ of R sends $s(n) \mapsto \frac{s(np)}{s(p)}$, and $s(p)$ is a non-zero-divisor in R, we see that φ descends to an isomorphism

$$\varphi^*(R/s(n)) \xrightarrow{\sim} R/\tfrac{s(np)}{s(p)} \xrightarrow{\sim} (s(p))/(s(np)).$$

If $p \nmid m$, then $s(m)$ is a unit in $R/s(p)$ by Lemma 2.2.5; since R is $s(p)$-adically complete, this implies that $s(m)$ is a unit in R itself. It follows that $0 \cong R/s(m) \xrightarrow{\sim} (s(p))/(s(m)s(p))$. Putting these together, we see that the map $\varphi^* s\Omega_{\square,\mathbf{A}^{1,(p)}} \xrightarrow{\sim} \eta_{s(p)} s\Omega_{\square,\mathbf{A}^1}$ is a quasi-isomorphism. □

In Proposition 4.2.6, the condition that R be $s(p)$-adically complete is rather powerful. For instance, one of the most basic tools in p-adic mathematics is the Legendre formula; this admits an analogue for generalized n-series, too.

Proposition 4.2.7 (s-analogue of Legendre formula)**.** *Let s be a GNS over R satisfying the hypotheses of Proposition 4.2.6. For any $n \geq 0$, we have*

$$n!_s = u \prod_{j\geq 1} \varphi^{j-1}(s(p))^{\lfloor n/p^j \rfloor}$$

for some unit $u \in R^\times$.

Proof. The argument is a straightforward adaptation of [BS19, Lemma 12.6]. Since R is $s(p)$-adically complete, we know that if $p \nmid m$, then $s(m)$ is a unit in R. This implies that

$$\begin{aligned} (np)!_s = u \prod_{i=1}^{n} s(np) &= u \prod_{i=1}^{n} \left(\frac{s(np)}{s(p)} \cdot s(p) \right) \\ &= us(p)^n \prod_{i=1}^{n} \varphi(s(n)) = us(p)^n \varphi(n!_s), \end{aligned}$$

where $u = \prod_{1\leq j\leq np, p\nmid j} s(j)$ is a unit in R. Using the above identity to inductively strip powers of p off of n produces the desired claim. □

This implies the following analogue of [BS19, Lemma 12.5], which gives a criterion for admitting "s-divided powers".

Corollary 4.2.8. *Let s be a GNS over R satisfying the hypotheses of Proposition 4.2.6, and suppose that for any $n \geq 0$, $\varphi(n!_s)$ is a non-zero-divisor in $R/s(p)$. Let A be an $s(p)$-completely flat R-algebra equipped with a R-linear multiplicative map $\phi : \varphi^* A \to A$ and an element $x \in A$ such that $\varphi(x) = x^p$, and $\varphi(x)$ is divisible by $s(p)$. Then $n!_s | x^n$, i.e., $\frac{x^n}{n!_s}$ is well-defined in A.*

Proof. Because $s(j)$ is a unit in R is $p \nmid j$, it suffices to show: for any $n \geq 0$, if $n!_s | x^n$, then $(np)!_s | x^{np}$. By (the proof of) Proposition 4.2.7, it suffices to show that $\varphi(n!_s) s(p)^n | x^{np}$. Because $\varphi(n!_s)$ is a non-zero-divisor in $R/s(p)$ (by assumption), it is also a non-zero-divisor in $A/s(p)$ by flatness of A. It therefore suffices to show that $\varphi(n!_s)$ and $s(p)^n$ each individually divide x^{np}. Since $n!_s | x^n$, it is clear that $\varphi(n!_s) | \phi(x^n) = x^{np}$. Since $s(p) | x^p$ by assumption, we also see that $s(p)^n | x^{np}$, as desired. □

4.3. **Formal group law n-series and the s-derivative.** Some of the most important (and accessible) examples of generalized n-series come from formal group laws. Throughout this section, we will fix a base commutative ring R.

Recollection 4.3.1. A (1-dimensional) *formal group law* over a commutative ring R is a two-variable power series $F(x, y) \in R[\![x, y]\!]$ such that $F(F(x, y), z) = F(x, F(y, z))$ and $F(x, y) \equiv x + y \pmod{(x, y)^2}$. It will sometimes be convenient to denote $F(x, y)$ by $x +_F y$. A morphism $f : F \to G$ of formal group laws is a power series $f(x) \in R[\![x]\!]$ such that $f(F(x, y)) = G(f(x), f(y))$; a morphism is called an isomorphism if it admits a compositional inverse.

If $n \geq 0$ is an integer, the n-series of F is defined via the formula

$$[n]_F(t) = \overbrace{F(t, F(t, F(t, \ldots F(t, t) \ldots)))}^{n} = \overbrace{t +_F t +_F \cdots +_F t}^{n}.$$

This can be extended to all integers $n \in \mathbf{Z}$ by using the existence of inverses for the formal group law. The n-series $[n]_F(t)$ is an element of $R[\![t]\!]$, and it is always divisible by t. We will define $\langle n \rangle_F(t) := [n]_F(t)/t$ (where we agree that $\langle 0 \rangle_F(t) = 0$). Sometimes, it will be notationally convenient to simply write these as $[n]_F$ and $\langle n \rangle_F$ (it being implicit that these are functions of t). If R is an $\mathbf{F}_p$-algebra, then either $[p]_F(t) = 0$ or $[p]_F(t) = \lambda t^{p^h} + O(t^{p^h+1})$ for some $h > 0$. If v_j denotes the coefficient of t^{p^j} in $[p]_F(t)$, then F is said to be of *height* $\geq n$ if $v_j = 0$ for $j < n$; if v_n is a unit, then F is said to be of *height* n.

If $\mathbf{Q} \subseteq R$, then every formal group law $F(x, y)$ is isomorphic to the additive formal group law via the *logarithm*. Let $F_y(x, y) = \partial_y F(x, y)$; then, the logarithm is given by the integral

$$\ell_F(x) := \int_0^x \frac{dt}{F_y(t, 0)}.$$

We will write $\mathcal{E}_F(x)$ to denote its compositional inverse, so that $F(x, y) = \mathcal{E}_F(\ell_F(x) + \ell_F(y))$. Observe that $[n]_F(t) = \mathcal{E}_F(n \ell_F(t))$ for any $n \in \mathbf{Z}$.

Example 4.3.2. Fix a base commutative ring R. The polynomial $F(x, y) = x + y$ is known as the *additive* formal group law, and $\langle n \rangle_F(t) = n$. The polynomial $F(x, y) = x + y + xy$ is known as the *multiplicative* formal group law, and

$$\langle n \rangle_F(t) = \frac{(1 + t)^n - 1}{t} \in R[\![t]\!].$$

Note that $\langle n \rangle_F = [n]_q$, where we set $q = t + 1$. The power series $F(x, y) = \frac{x+y}{1+xy}$ is known as the *hyperbolic* formal group law (since it describes the addition law for $\tanh$), and a simple induction on n shows that

$$\langle n \rangle_F(t) = \frac{1}{t} \frac{(1 + t)^n - (1 - t)^n}{(1 + t)^n + (1 - t)^n} = \frac{1}{q - 1} \frac{q^{2n} - 1}{q^{2n} + 1} \in R[\![q - 1]\!].$$

Remark 4.3.3. Given a formal group law $F(x, y)$ over a (torsionfree, say) commutative ring R, one can define a "rescaled" formal group law $\widetilde{F}(x, y)$ over $R[\![t]\!]$ which is characterized by the following property. Over $(R \otimes \mathbf{Q})[\![t]\!]$, the logarithm $\widetilde{\ell}_F(x)$ is given by $\frac{1}{t} \ell_F(tx)$; note that this power series does not have terms with negative powers of t, since $x \mid \ell_F(x)$ (and hence $tx \mid \ell_F(tx)$).

We begin by showing that the map $n \mapsto [n]_F(t)$ is a GNS over $R[\![t]\!]$, as long as F satisfies a mild condition. The existence of the power series ℓ_F is the main reason that GNS arising via formal group laws are particularly well-behaved.

Proposition 4.3.4. *Let F be a formal group law over a ring R, and suppose that $[n]_F(t) \in R[\![t]\!]$ is not a zero-divisor for any $n > 0$. Define $s : \mathbf{Z}_{\geq 0} \to R[\![t]\!]$ by $s(n) = [n]_F(t)$. Then, s is a GNS over $R[\![t]\!]$. Similarly, the function $s_F : \mathbf{Z}_{\geq 0} \to R[\![t]\!]$ sending $s_F(n) = \langle n \rangle_F(t)$ is a GNS over $R[\![t]\!]$.*

Proof. It is easy to see that if s is a GNS, the same is true of s_F. Let us now show that s is a GNS by checking the conditions of Definition 2.1.4. Condition (1) is clear, since $[0]_F = 0$. Condition (2) is already assumed in the theorem statement.

For condition (3), let $G(x) \in R[\![t]\!][\![x]\!]$ be the power series $F(t, x)$. Then,

$$[n+1]_F - [k+1]_F = G([n]_F) - G([k]_F).$$

Since $x - y$ divides $x^j - y^j$ for each $j \geq 0$, and G is a power series, $x - y$ also divides $G(x) - G(y)$. In particular, $s(n) - s(k) = [n]_F - [k]_F$ divides $G([n]_F) - G([k]_F)$; but $G([n]_F) - G([k]_F) = [n + 1]_F - [k+1]_F$ is precisely $s(n+1) - s(k+1)$, so $s(n) - s(k)$ divides $s(n+1) - s(k+1)$. Inducting, we conclude that $s(n) - s(k)$ divides $s(n+j) - s(k+j)$ for all $n, k, j \in \mathbf{Z}_{\geq 0}$. For $k = 0$, this gives $s(n) \mid s(n+j) - s(j)$ for all $n, j \in \mathbf{Z}_{\geq 0}$. After relabeling the indices, this becomes $s(n-k) \mid s(n) - s(k)$, which proves condition (3). □

Lemma 4.3.5. *Let F be a formal group law over a ring R. If $n \in \mathbf{Z}_{>0}$ is not a zero-divisor in R (e.g., R is torsionfree), then $[n]_F$ and $\langle n \rangle_F$ are not zero-divisors in $R[\![t]\!]$.*

Proof. Suppose for the sake of contradiction that $[n]_F(t)$ is a zero-divisor for some n (the same argument works for $\langle n \rangle_F$). Then there exists a power series $f(t) \in R[\![t]\!]$ such that

$$f(t) \cdot [n]_F(t) = 0.$$

It follows that the product of the coefficients of the lowest-degree terms of $f(t)$ and $[n]_F(t)$ must be 0. Since the lowest-degree term of $[n]_F(t)$ is nt, this implies that n times the lowest-degree coefficient of $f(t)$ is 0. In particular, n is a zero-divisor in R. □

Definition 4.3.6. Let F be a formal group law over R such that $[n]_F(t) \in R[\![t]\!]$ is not a zero-divisor for any $n > 0$.[3] Let $F\Omega_{\square,\mathbf{A}^1}$ denote the differential graded $R[\![t]\!]$-algebra given by the s-de Rham complex associated to the GNS $s : \mathbf{Z}_{\geq 0} \to R$ sending $n \mapsto \langle n \rangle_F$. We will refer to $F\Omega_{\square,\mathbf{A}^1}$ as the *F-de Rham complex* of the affine line $\mathbf{A}^1 = \operatorname{Spec} R[x]$; we will abusively also refer to the differential ∇_F as the *F-derivative*.

Example 4.3.7.

- For the additive formal group law, $\langle n \rangle_F = n$; so the resulting F-de Rham complex is simply the usual de Rham complex.
- For the multiplicative formal group law, $\langle n \rangle_F = [n]_q$; so the resulting F-de Rham complex is simply the q-de Rham complex. Note that the F-derivative can be defined directly on polynomials (instead of only on monomials) via $f(x) \mapsto \frac{f(qx)-f(x)}{(q-1)x}$. This can be seen directly from Proposition 4.3.9: indeed,

$$\mathcal{E}_F(\ell_F(t)z) = \frac{(1+t)^z - 1}{t} = \frac{q^z - 1}{q - 1},$$

and the operator $q^{x\partial_x}$ sends $f(x) \mapsto f(qx)$.

[3] Many of the results below do not rely on this assumption; but we keep it nonetheless, since Proposition 4.3.4 allows to immediately transport many results about generalized n-series obtained above. The interested reader should have no trouble removing this condition as necessary in the results below.

Remark 4.3.8. One can consider a slight variant of the F-de Rham complex, given by the complex

$$C^\bullet := (R[\![t]\!][x] \to R[\![t]\!][x]dx)\,,\ x^n \mapsto [n]_F x^{n-1}dx.$$

This is the s-de Rham complex for the function $s : \mathbf{Z}_{\geq 0} \to R$ sending $n \mapsto [n]_F$. Then, there is a quasi-isomorphism $F\Omega_{\square,\mathbf{A}^1} \simeq \eta_t C^\bullet$.

When $\mathbf{Q} \subseteq R$, there is a general formula for the F-derivative.

Proposition 4.3.9. *Suppose that $\mathbf{Q} \subseteq R$, and let F be a formal group law over R. Then there is an equality of $R[\![t]\!]$-linear operators on $R[\![t]\!][x]$:*

$$\nabla_F = \frac{1}{tx}\mathcal{E}_F(\ell_F(t)x\partial_x).$$

In particular, there is a canonical isomorphism $F\Omega_{\square,\mathbf{A}^1} \cong \Omega_{\mathbf{Q}[x]/\mathbf{Q}} \otimes_{\mathbf{Q}} R[\![t]\!]$.

Proof. Let ∇'_F denote the expression on the right-hand side. By definition of ∇_F, it suffices to check that $\nabla'_F(x^m) = \langle m\rangle x^{m-1}$ for every $m \geq 1$. Write $\mathcal{E}_F(t) = \sum_n a_n t^n$; then

$$\begin{aligned}\nabla'_F(x^m) &= \frac{1}{xt}\sum_n a_n \ell_F(t)^n (x\partial_x)^n(x^m)\\ &= \frac{1}{xt}\sum_n a_n (m\ell_F(t))^n x^m\\ &= \frac{1}{t}\mathcal{E}_F(m\ell_F(t))x^{m-1} = \langle m\rangle x^{m-1},\end{aligned}$$

as desired. □

Remark 4.3.10. Since every formal group law over a $\mathbf{Q}$-algebra is isomorphic to the additive formal group law, the final statement of Proposition 4.3.9 is a special case of the following more general observation: if F_1 and F_2 are isomorphic formal group laws, then the associated de Rham complexes are also isomorphic.

Example 4.3.11. Using Proposition 4.3.9, we can make the F-derivative explicit for the hyperbolic formal group law. In this case, $\mathcal{E}_F(t) = \tanh(t)$, so that $\ell_F(t) = \tanh^{-1}(t)$, and

$$\mathcal{E}_F(\ell_F(t)z) = \tanh(z\tanh^{-1}(t)) = \frac{q^{2z}-1}{q^{2z}+1},$$

where $q - 1 = t$. Since the operator $q^{x\partial_x}$ sends $f(x) \mapsto f(qx)$, the F-derivative can be expressed as

$$\nabla_F : f(x) \mapsto \frac{1}{(q-1)x}\frac{f(q^2x)-f(x)}{f(q^2x)+f(x)}.$$

Example 4.3.12. Let $R_0 = \mathbf{F}_p[v_n]$. Then, there is a unique formal group law (known as the *Honda formal group law*; see [Hon70]) over R_0 which is characterized by the property that its p-series is given by $[p]_F(t) = v_n t^{p^n}$. This implies that up to a unit in $R_0[\![t]\!]$, we have $[m]_F(t) = v_n^{v_p(m)} t^{m^n}$, where $v_p(m)$ denotes the p-adic valuation of m. The formal group law over R_0 lifts to a formal group law over $R = \mathbf{Z}_p[v_n]$ such that over $R \otimes \mathbf{Q} \cong \mathbf{Q}_p[v_n]$, its logarithm is given by

$$\ell_F(x) = \sum_{j\geq 0} v_n^{\frac{p^{jn}-1}{p^n-1}} \frac{x^{p^{jn}}}{p^j}.$$

For example, if $n = 1$ and we adjoin a $(p-1)$st root β of v_1, this is essentially the logarithm of the Artin-Hasse exponential, so that

$$\ell_F(x) = -\frac{1}{\beta}\sum_{p\nmid d}\frac{\mu(d)}{d}\log(1-(\beta x)^d).$$

One can say something similar for general n. Recall that the polylogarithm is defined by $\mathrm{Li}_s(x) = \sum_{j\geq 1} \frac{x^j}{j^s}$, so that $\mathrm{Li}_1(x) = -\log(1-x)$. If β denotes a (p^n-1)st root of v_n, then $\ell_F(x)$ can be understood as a "p^n-typical" version of $\frac{1}{\beta}\mathrm{Li}_{1/n}(\beta x)$.

When $n = 1$, the resulting F-de Rham complex over $\mathbf{F}_p[\![t]\!]$ is closely related to the mod p reduction of the q-de Rham complex: indeed, observe that the p-series of the multiplicative formal group law is congruent to $t^p \pmod p$. The resulting lifted formal group law over $\mathbf{Z}_p[v_1]$ is the p-typification of the multiplicative formal group law (see [Rav86, Appendix 2]). For higher n, the resulting F-de Rham complex behaves qualitatively similar to the case $n = 1$. For instance, we have

$$\mathrm{H}^0(F\Omega_{\square,\mathbf{A}^1}) \cong \mathbf{F}_{p^n}[v_n][\![t]\!],\ \mathrm{H}^1(F\Omega_{\square,\mathbf{A}^1}) \cong \bigoplus_{j\geq 1} \mathbf{F}_{p^n}[v_n, t]/(v_n^{v_p(j)} t^{j^n})\{x^{j-1}dx\}.$$

Example 4.3.13. Let $n \geq 1$, let k be an algebraically closed field of characteristic $p > 0$, and let $R = W(k)[\![u_1, \cdots, u_{n-1}]\!]$ denote the Lubin-Tate ring. Let F denote the formal group law associated to the universal deformation of a chosen formal group law of height n over k. Then, the resulting F-de Rham complex specializes to the q-de Rham complex when $n = 1$. For general n, this F-de Rham complex is closely related to deep phenomena in chromatic homotopy theory (see Remark 4.3.25).

Lemma 4.3.14 (F-Taylor expansion)**.** *Let F be a formal group law over R such that $[n]_F(t) \in R[\![t]\!]$ is not a zero-divisor for any $n > 0$. If $f(x) \in (R\otimes\mathbf{Q})[\![t, x-1]\!]$, there is a Taylor expansion*

$$f(x) = \sum_{n\geq 0} \nabla_F^n(f(x))|_{x=1} \frac{(x-1)_s^n}{n!_F}.$$

Here, $(x-1)_s^n$ denotes the symbol from Definition 2.3.5 with $y = -1$.

Proof. This is the same argument as in [AL20, Proposition 4.4]. First, observe that if $g(x) \in (R\otimes\mathbf{Q})[\![t, x-1]\!]$ is a function such that $\nabla_F^n(g(x))|_{x=1} = 0$ for all $n \geq 0$, then $g = 0$. Indeed, since ∇_F is simply the usual derivative modulo t, we see that $g(x)$ is divisible by t. Write $g(x) = tg_1(x)$; then, $\nabla_F^n(g(x))|_{x=1} = 0$ for all $n \geq 0$, so $t|g_1(x)$. Continuing, we see that $g(x)$ is infinitely t-divisible, and hence vanishes (since t is topologically nilpotent).

We can now apply the above observation to

$$g(x) := f(x) - \sum_{n\geq 0} \nabla_F^n(f(x))|_{x=1} \frac{(x-1)_s^n}{n!_F}.$$

By definition of $(x-1)_s^n$, we know that $\nabla_F(\frac{(x-1)_s^n}{n!_F}) = \frac{(x-1)_s^{n-1}}{(n-1)!_s}$; so $\nabla_F^n(g(x))|_{x=1} = 0$ for all $n \geq 0$, and hence $g = 0$, as desired. □

Corollary 4.3.15 (F-logarithm)**.** *Let F be a formal group law over R such that $[n]_F(t) \in R[\![t]\!]$ is not a zero-divisor for any $n > 0$. Consider the function $F\log(x) \in (R\otimes\mathbf{Q})[\![t, x-1]\!]$ given by $\frac{t}{\ell_F(t)}\log(x)$. Then, we have:*

(1) $\nabla_F(F\log(x)) = \frac{1}{x}$.
(2) $F\log(xy) = F\log(x) + F\log(y)$.
(3) There is a series expansion

$$F\log(x) = \sum_{n\geq 1} \frac{\langle -n+1\rangle_F \cdots \langle -1\rangle_F}{n!_F}(x-1)_s^n.$$

Proof. The first statement follows from Proposition 4.3.9. Indeed, write $\mathcal{E}_F(y) = \sum_{n\geq 1} a_n y^n$; the condition that $F(x,y) \equiv x + y \pmod{(x,y)^2}$ forces $a_1 = 1$. Since

$$(x\partial_x)(F\log(x)) = \frac{t}{\ell_F(t)}(x\partial_x)\log(x) = \frac{t}{\ell_F(t)},$$

we see that

$$\begin{aligned} x\nabla_F(F\log(x)) &= \frac{1}{t}\sum_{n\geq 1} a_n \ell_F(t)^n (x\partial_x)^n(F\log(x)) \\ &= \frac{1}{t}\left(\ell_F(t)\cdot\frac{t}{\ell_F(t)} + \sum_{n\geq 2} a_n\ell_F(t)^n(x\partial_x)^n(F\log(x))\right). \end{aligned}$$

The second sum vanishes, since $(x\partial_x)^n(F\log(x)) = 0$ for $n \geq 2$. The first term cancels out to give $x\nabla_F(F\log(x)) = 1$, as desired.

The second statement is clear. For the third statement, observe that

$$\nabla_F^n(F\log(x)) = \nabla_F^{n-1}(1/x) = \langle -n+1\rangle_F \cdots \langle -1\rangle_F x^{-n}.$$

Evaluating at $x = 1$ and using Lemma 4.3.14 gives the desired claim. □

Warning 4.3.16. The F-logarithm $F\log(x)$ is *not* the same as the logarithm $\ell_F(x)$ associated to the formal group law. This unfortunate terminology stems from attempting to simultaneously emulate the standard terminology "q-logarithm" and the "logarithm of the multiplicative formal group law".

Remark 4.3.17. Corollary 4.3.15 implies that $F\log(x)$ is a well-defined class in the ring $R[\![t]\!]\left[x^{\pm 1}, \frac{(x-1)_s^n}{n!_F}\right]$; this is the ring of functions on an F-analogue of the divided power completion of the identity section of $(\mathbf{G}_m)_{R[\![t]\!]}$.

Remark 4.3.18. The formal series in Corollary 4.3.15(3) can be written for arbitry GNS s; when it exists and converges, its s-derivative will formally be $1/x$. However, we have chosen to state Corollary 4.3.15 only in the case of GNS arising via formal group laws, since it is otherwise difficult to get a computational grip on the resulting formal series.

Example 4.3.19. When F is the multiplicative formal group law over $\mathbf{Z}$, the function $F\log(x)$ can be identified with the q-logarithm

$$\log_q(x) = \sum_{n\geq 1}(-1)^{n+1}q^{-\binom{n}{2}}\frac{(x-1)(x-q)\cdots(x-q^{n-1})}{[n]_q} \in \mathbf{Q}[\![q-1, x-1]\!].$$

Indeed, this follows from the second part of Corollary 4.3.15 and the observation that $\langle -j\rangle_F = [-j]_q = -q^{-j}[j]_q$. See [AL20, Section 4] for more on the q-logarithm.

Example 4.3.20. Let F be the hyperbolic formal group law over $\mathbf{Z}$. Then,

$$\langle -j\rangle_F = \frac{q^{-2j}-1}{q^{-2j}+1} = \frac{1-q^{2j}}{1+q^{2j}} = -\langle j\rangle_F.$$

It follows that

$$F\log(x) = \sum_{n\geq 1}(-1)^{n-1}\frac{q^{2n}+1}{q^{2n}-1}(x-1)_s^n.$$

Let us summarize some of the results from the previous section upon specialization to the F-de Rham complex:

Theorem 4.3.21. *Let R be a commutative ring, and let F be a formal group law over R such that $[n]_F(t) \in R[\![t]\!]$ is not a zero-divisor for any $n > 0$. Let $\hat{\mathbf{G}}$ denote the formal group over R. Then:*

1. *Let $R[\![t]\!]\langle x\rangle_F$ denote the ring $R[\![t]\!][x, \frac{x^n}{[n]_F!}]_{n\geq 0}$. Then the Poincaré lemma holds: the cohomology of the complex $F\Omega_{\square,\mathbf{A}^1} \otimes_{R[\![t]\!][x]} R[\![t]\!]\langle x\rangle_F$ is concentrated in degree zero, where it is isomorphic to $R[\![t]\!]$.*

(2) The Cartier isomorphism holds: there is a canonical isomorphism

$$F\Omega^i_{\square,\mathbf{A}^{1,(p)}} \otimes_{R[\![t]\!]} R[\![t]\!]/\langle p\rangle_F \cong \mathrm{H}^i(F\Omega_{\square,\mathbf{A}^1} \otimes_{R[\![t]\!]} R[\![t]\!]/\langle p\rangle_F)$$

sending $(x^p)^n \mapsto x^{np}$ in degree zero and $(x^p)^n d(x^p) \mapsto [x^{np}x^{p-1}dx]$. Note that $\operatorname{Spf} R[\![t]\!]/[p]_F \cong \hat{\mathbf{G}}[p]$.

(3) The décalage isomorphism holds: replace $R[\![t]\!]$ with its $\langle p\rangle_F$-adic completion. Let $\varphi : R[\![t]\!] \to R[\![t]\!]$ denote the R-algebra map sending $t \mapsto [p]_F(t)$, i.e., the map induced on rings by the multiplication-by-p map $\hat{\mathbf{G}} \to \hat{\mathbf{G}}$. Then, there is a quasi-isomorphism $\varphi^* F\Omega_{\square,\mathbf{A}^{1,(p)}} \xrightarrow{\sim} \eta_{\langle p\rangle_F} F\Omega_{\square,\mathbf{A}^1}$.

(4) The hypotheses of Corollary 4.2.8 are satisfied, so that there is a criterion for admitting "F-divided powers". Namely, replace $R[\![t]\!]$ by its $(p, \langle p\rangle_F)$-adic completion, and suppose that for any $n \geq 0$, $\varphi(n!_F)$ is a non-zero-divisor in $R[\![t]\!]/\langle p\rangle_F$. Let A be a $\langle p\rangle_F$-completely flat $R[\![t]\!]$-algebra equipped with a $R[\![t]\!]$-linear multiplicative map $\phi : \varphi^* A \to A$. If $x \in A$ is an element such that $\varphi(x) = x^p$ and $\langle p\rangle_F \mid \varphi(x)$, then $\frac{x^n}{n!_s} \in A$.

Proof. The first part is Proposition 4.2.1. The second part is Proposition 4.2.4, where the hypothesis in the proposition holds because $\langle 1\rangle_F \equiv 1 \pmod{t}$ is a unit modulo the topologically nilpotent ideal $(t) \subseteq R[\![t]\!]$. The third (and fourth) part is an application of Proposition 4.2.6. Note that the first hypothesis holds by construction of $\varphi : R[\![t]\!] \to R[\![t]\!]$: indeed, φ sends

$$s(n) = \frac{[n]_F(t)}{t} \mapsto \frac{[n]_F([p]_F(t))}{[p]_F(t)} = \frac{[np]_F(t)}{[p]_F(t)} = \frac{s(np)}{s(p)}.$$

The second hypothesis follows from the assumption on $R[\![t]\!]$. □

Remark 4.3.22. Using Remark 4.3.10, one can upgrade Theorem 4.3.21 to the case when R (rather, $\operatorname{Spec} R$) is replaced by the moduli stack of formal groups. However, we will not discuss this further in this article.

Motivated by [Sch17, Conjecture 3.1], we propose the following conjecture (which is likely false as stated). Arpon Raksit has informed the first author that he is currently working on some variant of it.

Conjecture 4.3.23. *Let Poly_R denote the category of polynomial R-algebras and R-algebra maps between them. Let F be a formal group law over R such that $[n]_F(t) \in R[\![t]\!]$ is not a zero-divisor for any $n > 0$. Then, there is a functor $\Gamma_{F\text{-dR}}(-) : \mathrm{Poly}_R \to \mathrm{CAlg}(R[\![t]\!])$ landing in the ∞-category of $\mathbf{E}_\infty$-$R[\![t]\!]$-algebras which sends $R[x_1, \cdots, x_n] \mapsto F\Omega_{\square,\mathbf{A}^n}$.*[4] *Furthermore, each part of Theorem 4.3.21 admits a generalization to $\Gamma_{F\text{-dR}}(-)$.*

Remark 4.3.24. If the preceding conjecture is true, then the construction $F\Omega_{\square,-}$ can be extended to all (animated) R-schemes by left Kan extension:

$$\begin{tikzcd}
\mathrm{Poly}_R^{\mathrm{op}} \arrow[r, "\Gamma_{F\text{-dR}}(-)"] \arrow[d] & \mathrm{CAlg}(R[\![t]\!])^{\mathrm{op}} \\
\mathrm{Sch}_R^{\mathrm{op}} \arrow[ur, dashed, "\Gamma_{F\text{-dR}}(-)"']
\end{tikzcd}$$

We expect that the resulting functor $X \mapsto \Gamma_{F\text{-dR}}(X)$, if it exists, should be rather interesting. When F is the multiplicative formal group law, Conjecture 4.3.23 is true, and the resulting assignment $X \mapsto \Gamma_{F\text{-dR}}(X)$ is the q-de Rham cohomology of [BS19].

Let us end this section by discussing the motivation behind the construction of the F-de Rham complex. We will necessarily be brief, since this is not the main subject of the present article.

[4] In other words, the assignment $R[x_1, \cdots, x_n] \mapsto F\Omega_{\square,\mathbf{A}^n}$ is functorial in R-algebra maps of polynomial R-algebras.

Remark 4.3.25. Let A be an even-periodic $\mathbf{E}_\infty$-ring equipped with a complex orientation. Then, Quillen defined a canonical formal group law $F(x, y)$ over $R := \pi_0(A)$. Let $\tau_{\geq 0}A$ denote the connective cover of A, and let $\mathrm{F}^\star_{\mathrm{ev}}\mathrm{HP}(\tau_{\geq 0}A[x]/\tau_{\geq 0}A)$ denote the even filtration on the periodic cyclic homology of $\tau_{\geq 0}A[x]$ (defined in [HRW22]). The assignment $A \mapsto (\tau_{\geq 0}A)^{tS^1}$ is the homotopical analogue of the construction of the "rescaled" formal group law from Remark 4.3.3.

Unpublished work of Arpon Raksit shows that the F-de Rham complex $F\Omega_{\square,\mathbf{A}^1}$ arises as the zeroth associated graded piece $\mathrm{gr}^0_{\mathrm{ev}}\mathrm{HP}(\tau_{\geq 0}A[x]/\tau_{\geq 0}A)$. In particular, in this case, the F-de Rham complex admits the structure of an $\mathbf{E}_\infty$-$R[\![t]\!]$-algebra. There are homotopical analogues of each part of Theorem 4.3.21: for example, the décalage isomorphism of Theorem 4.3.21(3) is proved as [Dev23, Proposition 3.5.3].

When $A = \mathrm{KU}$ is periodic complex K-theory (so $\tau_{\geq 0}A = \mathrm{ku}$ is connective complex K-theory), the formal group law over $\pi_0(A)$ is precisely the multiplicative one; so the q-de Rham complex arises as $\mathrm{gr}^0_{\mathrm{ev}}\mathrm{HP}(\mathrm{ku}[x]/\mathrm{ku})$. As explained in [DR23], the p-completion of $\mathrm{HP}(\mathrm{ku}[x]/\mathrm{ku})$ can be understood via the topological negative cyclic homology of $\mathbf{Z}_p[\zeta_p][x]$; this is a homotopical analogue of the Bhatt-Scholze construction [BS19] of q-de Rham cohomology via prismatic cohomology.

When $A = E_n$ is the Morava E-theory associated to the Lubin-Tate formal group (see Example 4.3.13) and $\tau_{\geq 0}A = e_n$ is its connective cover, the F-de Rham complex of Example 4.3.13 arises as $\mathrm{gr}^0_{\mathrm{ev}}\mathrm{HP}(e_n[x]/e_n)$. The periodic cyclic homology $\mathrm{HP}(e_n[x]/e_n)$ plays an important role in higher chromatic analogues of the work of Bhatt-Morrow-Scholze [BMS19], and will be explored in future work.

Although this does not quite fall into the above framework, the first author hopes to show in future work that when $A = L^s(\mathbf{Z})$ is the symmetric L-theory of the integers (see [HLN21]), the F-de Rham complex associated to the hyperbolic formal group law is closely related to $\mathrm{gr}^0_{\mathrm{ev}}\mathrm{HP}(L^s(\mathbf{Z})[x]/L^s(\mathbf{Z}))$. This is a manifestation of the observation (going back to the Hirzebruch signature theorem) that the logarithm of the formal group law associated to the complex orientation on $L^s(\mathbf{Z})$ is given by the hyperbolic tangent function $\tanh(x)$.

4.4. **An analogue of the Bhatt-Lurie Cartesian square.** Throughout this section, we will fix a p-completely flat $\mathbf{Z}_p$-algebra R and a formal group law $F(x, y)$ over R. The symbol $R[\![t]\!]$ will always denote the *p-adic completion* of the formal power series ring, and all constructions will be done internal to the category of (p, t)-adically $R[\![t]\!]$-schemes. (We have omitted the completion from the notation for readability.) Let $\hat{\mathbf{G}}$ denote the associated formal group, so that its underlying formal scheme is $\mathrm{Spf}\, R[\![t]\!]$.

In [BL22, Lemma 3.5.18], Bhatt-Lurie showed that there is a Cartesian square of group schemes over R:

(7)
$$\begin{tikzcd}
\mathbf{G}_m^\sharp \arrow[r, "\log"] \arrow[d] & \mathbf{G}_a^\sharp \arrow[d, "x\mapsto\exp(px)"] \\
\mathbf{G}_m \arrow[r, "x\mapsto x^p"'] & \mathbf{G}_m^{(1)}.
\end{tikzcd}$$

The proof in *loc. cit.* used the relationship between these group schemes and the ring scheme of Witt vectors. In this section, we prove an F-analogue of this result (see Theorem 4.4.10); in the case of the additive formal group law, this reproves (7). Let us state at the outset that in the case when F is the multiplicative formal group law, this result was obtained in a discussion between the first author and Michael Kural. Moreover, the argument in this section rests crucially on (12), the q-analogue of which (Example 4.4.8) was proved by Michael Kural. Any errors below are solely the fault of the first author!

Definition 4.4.1. Remark 4.3.3 gives a formal group $\hat{\mathbf{G}}_t$ over $\mathrm{Spf}\, R[\![t]\!]$ whose logarithm is $\widetilde{\ell}_F(x) = \frac{1}{t}\ell_F(tx)$. Let x denote the coordinate on $\hat{\mathbf{G}}_t$, so that its underlying formal scheme is $\mathrm{Spf}\, R[\![t, x]\!]$. Let

$\hat{\mathbf{G}}_t^\vee$ denote the Cartier dual $\mathrm{Hom}(\hat{\mathbf{G}}_t, (\mathbf{G}_m)_{R[\![t]\!]})$ of $\hat{\mathbf{G}}_t$; see [Dri21, Section 3] for some generalities on Cartier duals of formal groups. The element $x \in \mathcal{O}_{\hat{\mathbf{G}}_t}$ defines a homomorphism $\tau : \hat{\mathbf{G}}_t^\vee \to (\mathbf{G}_a)_{R[\![t]\!]}$.

Observation 4.4.2. Over $(R \otimes \mathbf{Q})[\![t]\!]$, the rescaled logarithm $\widetilde{\ell}_F$ of Remark 4.3.3 defines an isomorphism $\widetilde{\ell}_F : \hat{\mathbf{G}}_t \xrightarrow{\sim} (\hat{\mathbf{G}}_a)_{(R\otimes\mathbf{Q})[\![t]\!]}$ of formal groups. Therefore, the canonical pairing $\hat{\mathbf{G}}_t \times_{R[\![t]\!]} \hat{\mathbf{G}}_t^\vee \to (\mathbf{G}_m)_{R[\![t]\!]}$ fits into a diagram

$$\begin{tikzcd}
\hat{\mathbf{G}}_t \times_{R[\![t]\!]} \hat{\mathbf{G}}_t^\vee \arrow[d, "\widetilde{\ell}_F \times \mathrm{id}"', "\sim"] \arrow[dr, "\mu"] & \\
(\hat{\mathbf{G}}_a)_{(R\otimes\mathbf{Q})[\![t]\!]} \times_{R[\![t]\!]} \hat{\mathbf{G}}_t^\vee \arrow[r, "\nu"'] & (\mathbf{G}_m)_{(R\otimes\mathbf{Q})[\![t]\!]}.
\end{tikzcd}$$

Since $R[\![t]\!]$ is (p, t)-adically complete, the Cartier dual of $(\hat{\mathbf{G}}_a)_{R[\![t]\!]}$ can be identified with the divided power completion $(\mathbf{G}_a^\sharp)_{R[\![t]\!]}$. The pairing ν is base-changed from $R[\![t]\!]$ itself, where it is given by the formula

$$\nu : (x, y) \mapsto \exp(xy).$$

It follows that the pairing μ is given by

$$\mu(x, y) = \exp(\widetilde{\ell}_F(x)y).$$

This can be expanded as a power series in x:

$$\mu(x, y) = \sum_{n\geq 0} \beta_n(y)x^n.$$

Unwinding the definition of the Cartier dual, and using that $R[\![t]\!]$ is p-torsionfree (using our assumption that R is a p-completely flat $\mathbf{Z}_p$-algebra), we see that the ring of functions on $\hat{\mathbf{G}}_t^\vee$ has underlying $R[\![t]\!]$-module given by (the (p, t)-adic completion of)

$$\mathcal{O}_{\hat{\mathbf{G}}_t^\vee} = R[\![t]\!]\{\beta_n(y)\}_{n\geq 0}.$$

Example 4.4.3. When F is the multiplicative formal group law, the function μ is simply

$$\mu(x, y) = \exp\left(\frac{y}{q-1}\log(1 + (q-1)x)\right) = (1 + (q-1)x)^{y/(q-1)};$$

its power series expansion is given by

$$\mu(x, y) = \sum_{n\geq 0} \frac{\prod_{j=0}^{n-1}(y - j(q-1))}{n!}x^n.$$

This expression plays an important role in [Dri21].

Example 4.4.4. When F is the hyperbolic formal group law (so that $\ell_F(x) = \tanh^{-1}(x) = \frac{1}{2}\log\left(\frac{1+x}{1-x}\right)$), the function μ is

$$\mu(x, y) = \exp\left(\frac{y}{2(q-1)}\log\left(\frac{1 + (q-1)x}{1 - (q-1)x}\right)\right) = \left(\frac{1 + (q-1)x}{1 - (q-1)x}\right)^{y/2(q-1)}.$$

The power series expansion of this function is somewhat complicated: one can show that upon writing $\mu(x, y) = \sum_{n\geq 0} \beta_n(y)x^n$, we have $\beta_0 = 1$, $\beta_1 = y$, and there is a recurrence

$$\beta_{n+2}(y) = \frac{y\beta_{n+1}(y) + n(q-1)^2\beta_n(y)}{n+2}.$$

Using a computer, one can compute that the first few terms of this expansion are

$$\begin{aligned}\mu(x,y) = 1 + yx + \frac{y^2}{2}x^2 + \frac{2(q-1)^2y+y^3}{3!}x^3 + \frac{8(q-1)^2y^2+y^4}{4!}x^4 \\ + \frac{24(q-1)^4y+20(q-1)^2y^3+y^5}{5!}x^5 + \cdots .\end{aligned}$$

Definition 4.4.5. Let $\mathbf{G}_m^{\sharp,F}$ denote the formal scheme over $\operatorname{Spf} R[\![t]\!]$ given by (the (p,t)-adic completion of)

$$\mathbf{G}_m^{\sharp,F} = \operatorname{Spf} R[\![t]\!]\left[y^{\pm 1}, \frac{(y-1)_s^n}{n!_F}\right]_{n\geq 0}.$$

This can be viewed as the "F-divided power hull" of the identity section of $(\mathbf{G}_m)_{R[\![t]\!]}$. Equip $\mathbf{G}_m^{\sharp,F}$ with the structure of a group scheme where the coproduct sends $y \mapsto y \otimes y$. It is not immediate that this is well-defined, but we will prove this below in Corollary 4.4.9. There is a canonical homomorphism $\mathrm{can} : \mathbf{G}_m^{\sharp,F} \to (\mathbf{G}_m)_{R[\![t]\!]}$.

Note that Remark 4.3.17 implies that $F\log(y)$ defines an element of the coordinate ring of $\mathbf{G}_m^{\sharp,F}$, i.e., it defines a map $F\log : \mathbf{G}_m^{\sharp,F} \to (\mathbf{G}_a)_{R[\![t]\!]}$. This is in fact a homomorphism, since $F\log(y_1y_2) = F\log(y_1) + F\log(y_2)$.

Proposition 4.4.6. *Work over the base $(R\otimes\mathbf{Q})[\![t]\!]$. Then, the iterated F-derivative of $\mu(x, F\log(y))$ with respect to the variable y is given by*

$$\nabla_{F,y}^n \mu(x, F\log(y)) = \frac{x(x+\langle -1\rangle_F(t))\cdots(x+\langle -n+1\rangle_F(t))}{y^n}\mu(x, F\log(y)). \tag{8}$$

Proof. Observe that:

$$\begin{aligned}\mu(x, F\log(y)) &= \sum_{n\geq 0}\beta_n(F\log(y))x^n = \exp(F\log(y)\widetilde{\ell}_F(x)) \\ &= \exp\left(\frac{t}{\ell_F(t)}\log(y)\cdot\frac{\ell_F(tx)}{t}\right) = \exp\left(\log(y)\frac{\ell_F(tx)}{\ell_F(t)}\right) = y^{\frac{\ell_F(tx)}{\ell_F(t)}};\end{aligned}$$

the third equality used the definition of $F\log(y)$ via Corollary 4.3.15 and the definition of $\widetilde{\ell}_F(x)$ via Remark 4.3.3. Let us write $a = \frac{\ell_F(tx)}{\ell_F(t)}$ for notational simplicity, so that

$$y^a = \sum_{m\geq 0}\frac{a(a-1)\cdots(a-(m-1))}{m!}(y-1)^m,$$

and $\partial_y y^a = ay^{a-1}$.

We can now inductively compute the iterated F-derivative using Proposition 4.3.9. We begin with the base case $n=1$. Note that $(y\partial_y)y^a = ay^a$, so that

$$(y\partial_y)^m y^a = a^m y^a \tag{9}$$

by an easy induction on m. Write $\mathcal{E}_F(z) = \sum_{m\geq 0} b_m z^m$; then using (9), we have:

$$\begin{aligned}\nabla_{F,y}\mu(x, F\log(y)) &= \frac{1}{yt}\sum_{m\geq 0} b_m\ell_F(t)^m(y\partial_y)^m y^a = \frac{1}{yt}\sum_{m\geq 0} b_m\ell_F(t)^m a^m y^a \\ &= \frac{y^a}{yt}\sum_{m\geq 0} b_m\ell_F(tx)^m = \frac{y^a}{yt}\mathcal{E}_F(\ell_F(tx)) = \frac{tx}{yt}\cdot y^a \\ &= \frac{x}{y}y^a = \frac{x}{y}\mu(x, F\log(y)),\end{aligned}$$

as desired.

The proof of the iterated F-derivative is similar. Indeed, note that (9) implies that for any $j \geq 0$, we have:

$$(y\partial_y)^m \left(\frac{\mu(x, F\log(y))}{y^j} \right) = (y\partial_y)^m y^{a-j} = (a-j)^m y^{a-j} = (a-j)^m \frac{\mu(x, F\log(y))}{y^j}. \tag{10}$$

Assume that (8) holds for n; then:

$$\begin{aligned} \nabla_{F,y}^{n+1} \mu(x, F\log(y)) &= \nabla_{F,y} \nabla_{F,y}^n \mu(x, F\log(y)) \\ &= x(x + \langle -1 \rangle_F(t)) \cdots (x + \langle -n+1 \rangle_F(t)) \nabla_{F,y} \left(\frac{\mu(x, F\log(y))}{y^n} \right). \end{aligned} \tag{11}$$

The derivative on the right-hand side can be calculated as follows:

$$\begin{aligned} \nabla_{F,y} \left(\frac{\mu(x, F\log(y))}{y^j} \right) &= \frac{1}{yt} \sum_{m \geq 0} a_m \ell_F(t)^m (y\partial_y)^m \left(\frac{\mu(x, F\log(y))}{y^j} \right) \\ &= \frac{1}{yt} \sum_{m \geq 0} a_m \ell_F(t)^m \left(\frac{\ell_F(tx)}{\ell_F(t)} - j \right)^m \frac{\mu(x, F\log(y))}{y^j} \\ &= \frac{\mu(x, F\log(y))}{y^j} \frac{1}{yt} \sum_{m \geq 0} a_m (\ell_F(tx) - j\ell_F(t))^m \\ &= \frac{\mu(x, F\log(y))}{y^j} \frac{1}{yt} \mathcal{E}_F(\ell_F(tx) - j\ell_F(t)). \end{aligned}$$

Since

$$\ell_F(tx) - j\ell_F(t) = \ell_F(tx + [-j]_F(t)) = \ell_F(t(x + \langle -j \rangle_F(t))),$$

this becomes

$$\begin{aligned} \nabla_{F,y} \left(\frac{\mu(x, F\log(y))}{y^j} \right) &= \frac{\mu(x, F\log(y))}{y^j} \frac{1}{yt} \mathcal{E}_F(\ell_F(t(x + \langle -j \rangle_F(t)))) \\ &= \frac{\mu(x, F\log(y))}{y^j} \frac{x + \langle -j \rangle_F(t)}{y}. \end{aligned}$$

Plugging this into (11), we get that

$$\nabla_{F,y}^{n+1} \mu(x, F\log(y)) = x(x + \langle -1 \rangle_F(t)) \cdots (x + \langle -n+1 \rangle_F(t))(x + \langle -n \rangle_F(t)) \frac{\mu(x, F\log(y))}{y^{n+1}},$$

as desired. □

Corollary 4.4.7. *There is a dotted map (which is a homomorphism over $R[\![t]\!]$) filling in the following diagram:*

$$\begin{tikzcd} & \hat{\mathbf{G}}_t^\vee \arrow[d, "\tau"] \\ \mathbf{G}_m^{\sharp,F} \arrow[ur, dashed] \arrow[r, "y \mapsto F\log(y)"'] & (\mathbf{G}_a)_{R[\![t]\!]}. \end{tikzcd}$$

Proof. In the notation of Observation 4.4.2, we need to show that $\beta_n(F\log(y)) \in \mathcal{O}_{\mathbf{G}_m^{\sharp,F}}$ for every $n \geq 0$. To prove this, let us work over $(R \otimes \mathbf{Q})[\![t]\!]$, and expand $\mu(x, F\log(y))$ as a power series in $\frac{(y-1)_s^n}{n!_F}$ using Lemma 4.3.14. Evaluating (8) in Proposition 4.4.6 at $y = 1$, we obtain

$$\nabla_{F,y}^n \mu(x, F\log(y))|_{y=1} = x(x + \langle -1 \rangle_F(t)) \cdots (x + \langle -n+1 \rangle_F(t)).$$

It follows from Lemma 4.3.14 that

$$\sum_{n\geq 0} \beta_n(F\log(y))x^n = \mu(x, F\log(y)) = \sum_{n\geq 0} x(x+\langle -1\rangle_F(t))\cdots(x+\langle -n+1\rangle_F(t))\frac{(y-1)_s^n}{n!_F}. \tag{12}$$

Taking the coefficient of x^n on the right-hand side expresses $\beta_n(F\log(y))$ as an $(R\otimes \mathbf{Q})[\![t]\!]$-linear combination of the divided powers $\frac{(y-1)_s^n}{n!_F}$; but since no rational denominators appear, this in fact expresses $\beta_n(F\log(y))$ as an $R[\![t]\!]$-linear combination of the divided powers $\frac{(y-1)_s^n}{n!_F}$, as desired. □

Example 4.4.8. When F is the multiplicative formal group law, (12) reduces to the following identity:

$$\begin{aligned}&\sum_{n\geq 0} \frac{\log_q(y)(\log_q(y)-(q-1))\cdots(\log_q(y)-(n-1)(q-1))}{n!}x^n \\ &= \sum_{n\geq 0} q^{-\binom{j}{2}}x(x-[1]_q)\cdots(x-[n-1]_q)\frac{(y-1)(y-q)\cdots(y-q^{n-1})}{[n]_q!}.\end{aligned}$$

This identity was communicated to the first author by Michael Kural, and was motivation for the more general (12).

Corollary 4.4.9. *The group structure on $\mathbf{G}_m^{\sharp,F}$ is well defined.*

Proof. Suppose that y_1 and y_2 both admit F-divided powers $\frac{(y-1)_s^n}{n!_F}$; we need to show that the same is true of the product y_1y_2. Since $F\log(y_1y_2) = F\log(y_1) + F\log(y_2)$, one can express $\beta_n(F\log(y_1y_2))$ in terms of $\beta_n(F\log(y_1))$ and $\beta_n(F\log(y_2))$. Using the identity (12) in the proof of Corollary 4.4.7 shows that y_1y_2 must also admit F-divided powers, as desired. □

The main result of this section is the following result, which recovers (7) when F is the additive formal group law. Using Remark 4.3.10, one can in fact refine Theorem 4.4.10 to remain true when the base $R[\![t]\!]$ (or rather $\hat{\mathbf{G}} = \operatorname{Spf} R[\![t]\!]$) is replaced by the universal formal group $\hat{\mathbf{G}}^{\mathrm{univ}}$ over the moduli stack of formal groups over p-nilpotent rings.

Theorem 4.4.10. *There is a Cartesian square of group schemes over $R[\![t]\!]$:*

$$\begin{tikzcd} \mathbf{G}_m^{\sharp,F} \arrow[r, "y\mapsto F\log(y)"] \arrow[d, "\mathrm{can}"'] & \hat{\mathbf{G}}_t^\vee \arrow[d, "\langle p\rangle^*"] \\ (\mathbf{G}_m)_{R[\![t]\!]} \arrow[r, "y\mapsto y^p"'] & (\mathbf{G}_m^{(1)})_{R[\![t]\!]}. \end{tikzcd} \tag{13}$$

The right-vertical map is Cartier dual to the homomorphism $p\underline{\mathbf{Z}} \to \hat{\mathbf{G}}_t$ sending $p \mapsto \langle p\rangle_F(t)$. In particular, there is an extension

$$0 \to (\mu_p)_{R[\![t]\!]} \to \mathbf{G}_m^{\sharp,F} \xrightarrow{F\log(y)} \hat{\mathbf{G}}_t^\vee \to 0.$$

Proof. To check that the diagram commutes, we need to check that there is an equality of elements of $\mathcal{O}_{\mathbf{G}_m^{\sharp,F}}$:

$$y^p = \langle p\rangle^*(F\log(y)).$$

Since R is p-completely flat over $\mathbf{Z}_p$, there is an injection $R[\![t]\!] \subseteq (R\otimes\mathbf{Q})[\![t]\!]$; so it suffices to check the desired identity in $(R\otimes\mathbf{Q})[\![t]\!]\{\beta_n(y)\}_{n\geq 0}$. By the discussion in Observation 4.4.2, $\langle p\rangle^*$ can be expressed as

$$\begin{aligned} \langle p\rangle^*(z) &= \exp(z\widetilde{\ell}_F(\langle p\rangle_F(t))) = \exp\left(z\frac{\ell_F(t\langle p\rangle_F(t))}{t}\right) \\ &= \exp\left(z\frac{\ell_F([p]_F(t))}{t}\right) = \exp\left(p\frac{\ell_F(t)}{t}z\right). \end{aligned} \tag{14}$$

Note that this is also $\exp\left(\frac{\ell_F([p]_F(t))}{t}z\right)$. It follows that

$$\langle p\rangle^*(F\log(y)) = \exp\left(p\frac{\ell_F(t)}{t}F\log(y)\right) = \exp\left(p\frac{\ell_F(t)}{t}\frac{t}{\ell_F(t)}\log(y)\right) = \exp(p\log(y)) = y^p,$$

as desired. To check that the square is Cartesian, observe that $F\log(y) = 0$ implies that $\log(y) = 0$, which happens (by the Cartesian square (7)) if and only if $y^p = 1$. Conversely, if $y^p = 1$, then

$$p \cdot F\log(y) = F\log(y^p) = 0,$$

which implies that $F\log(y) = 0$. □

Example 4.4.11. It follows from Theorem 4.4.10 that $\mathbf{G}_m^{\sharp,F}$ is an extension of $\hat{\mathbf{G}}_t^\vee$ by $(\mu_p)_{R[\![t]\!]}$. In the case of the multiplicative formal group law over $R = \mathbf{Z}_p$, this was studied in [Dri21]. Namely, in [Dri21, Section 5.3.1], it is shown that there is an extension $\widetilde{G}_Q$ of $(\hat{\mathbf{G}}_{m,q-1})^\vee$ by $(\mu_p)_{\mathbf{Z}_p[\![q-1]\!]}$, given by the functor

$$\widetilde{G}_Q : R \mapsto \{(q, x, u) \in R^\times \times W(R) \times R^\times | q-1 \text{ is nilpotent}, 1 + \Phi_p([q])x = [u^p]\}.$$

Here, $W(R)$ denotes the ring of p-typical Witt vectors of R. Drinfeld shows that the group scheme $\widetilde{G}_Q$ is isomorphic over $\mathbf{Z}_p[\![q-1]\!]$ to $\mathbf{G}_m^{\sharp,F}$ (as extensions of $(\hat{\mathbf{G}}_{m,q-1})^\vee$ by $(\mu_p)_{\mathbf{Z}_p[\![q-1]\!]}$).

As shown in [Dri21, Appendix D] (see also [Dev23, Remark C.3] and Example 4.4.3), the Cartier dual $(\hat{\mathbf{G}}_{m,q-1})^\vee$ can be identified with

$$(\hat{\mathbf{G}}_{m,q-1})^\vee = \operatorname{Spf} \mathbf{Z}_p[\![q-1]\!]\left[y, \frac{\prod_{j=0}^{n-1}(y - j(q-1))}{n!}\right]_{n\geq 0}.$$

By (14), the homomorphism $\langle p\rangle^*$ corresponds to the invertible element

$$\langle p\rangle^*(z) = \exp\left(p\frac{\log(q)}{q-1}z\right) = q^{pz/(q-1)};$$

this element plays an important role in [Dri21]. Note that this can alternatively be written as

$$\langle p\rangle^*(z) = \sum_{n\geq 0}\frac{\prod_{j=0}^{n-1}(z - j(q-1))}{n!}[p]_q^n = \sum_{n\geq 0}\frac{\prod_{j=0}^{n-1}(pz - j(q-1))}{n!}.$$

In this case, Theorem 4.4.10 therefore specializes to give a Cartesian square over $\mathbf{Z}_p[\![q-1]\!]$:

$$\begin{tikzcd} \mathbf{G}_m^{\sharp,F} \arrow[r, "\sim"] & \widetilde{G}_Q \arrow[r, "y\mapsto\log_q(y)"] \arrow[d, "\mathrm{can}"'] & \hat{\mathbf{G}}_{m,q-1}^\vee \arrow[d, "z\mapsto q^{pz/(q-1)}"] \\ & (\mathbf{G}_m)_{\mathbf{Z}_p[\![q-1]\!]} \arrow[r, "y\mapsto y^p"'] & (\mathbf{G}_m^{(1)})_{\mathbf{Z}_p[\![q-1]\!]}. \end{tikzcd}$$

Remark 4.4.12. In [Dri21, Section 5] (in particular, [Dri21, Remark 5.7.5]), it is shown that $(\hat{\mathbf{G}}_{m,q-1})^\vee$ is isomorphic to the group scheme $W_{\mathbf{Z}_p[\![q-1]\!]}[F - (1 + [q] + \cdots + [q]^{p-1})]$, where $W_{\mathbf{Z}_p[\![q-1]\!]}$ is the Witt scheme over $\mathbf{Z}_p[\![q-1]\!]$ and $[q] \in W(\mathbf{Z}_p[\![q-1]\!])$ is the Teichmüller lift of q. For a more general formal group $\hat{\mathbf{G}}_t$, the methods of this section might give a Witt vector model for the Cartier dual $\hat{\mathbf{G}}_t^\vee$, but we have not explored this direction.

Example 4.4.13. If F is the hyperbolic formal group law, then $\ell_F(t) = \frac{1}{2}\log\left(\frac{t+1}{1-t}\right)$. Setting $t = q-1$, (14) says that

$$\langle p\rangle^*(z) = \exp\left(p\frac{\log(\frac{q}{2-q})}{2(q-1)}z\right) = \left(\frac{q}{2-q}\right)^{pz/2(q-1)}.$$

The denominator of 2 appearing in the exponent implies that the cases $p > 2$ and $p = 2$ behave markedly differently. Since $\frac{q}{2-q} = 1 + (q-1)\cdot\frac{2}{2-q}$, one can alternatively write

$$\langle p\rangle^*(z) = \sum_{n\geq 0}\frac{\prod_{j=0}^{n-1}(pz - 2j(q-1))}{n!}\left(\frac{1}{2-q}\right)^n = \sum_{n\geq 0}\frac{\prod_{j=0}^{n-1}(z-2j(q-1))}{n!2^n}\frac{[p]_q^n}{(2-q)^{pn}}.$$

Write $\hat{\mathbf{G}}_{h,q-1}$ to denote the formal group over $\mathbf{Z}_p\llbracket q-1\rrbracket$ corresponding to the rescaled hyperbolic formal group law. In this case, Theorem 4.4.10 specializes to give a Cartesian square over $\mathbf{Z}_p\llbracket q-1\rrbracket$:

$$\begin{tikzcd}
\mathbf{G}_m^{\sharp,F} \arrow[r, "y\mapsto F\log(y)"] \arrow[d, "\mathrm{can}"'] & \hat{\mathbf{G}}_{h,q-1}^\vee \arrow[d, "z\mapsto\left(\frac{q}{2-q}\right)^{pz/2(q-1)}"] \\
(\mathbf{G}_m)_{\mathbf{Z}_p\llbracket q-1\rrbracket} \arrow[r, "y\mapsto y^p"'] & (\mathbf{G}_m^{(1)})_{\mathbf{Z}_p\llbracket q-1\rrbracket}.
\end{tikzcd}$$

Example 4.4.14. Let F be the formal group law over $\mathbf{Z}_p$ given by specializing the formal group law of Example 4.3.12 to $v_n = 1$. Let $\hat{\mathbf{G}} = \operatorname{Spf}\mathbf{Z}_p\llbracket t\rrbracket$ denote the associated formal group, and let $\hat{\mathbf{G}}_t$ denote the rescaled formal group over $\mathbf{Z}_p\llbracket t\rrbracket$. Then, (14) says that $\langle p\rangle^*(z)$ is a "p^n-typical" version of $\exp\left(p\frac{\mathrm{Li}_{1/n}(t)}{t}z\right)$. If we write $E_p(t)$ to denote the Artin-Hasse exponential, then $\langle p\rangle^*(z)$ can be made explicit when $n = 1$:

$$\langle p\rangle^*(z) = E_p(t)^{pz/t} = \prod_{p\nmid m}(1-t^m)^{-\frac{p\mu(m)z}{tm}}.$$

If we write $t = \widetilde{p}$ (to keep with the notation of [BL22]), then Theorem 4.4.10 in this case specializes to give a Cartesian square over $\mathbf{Z}_p\llbracket\widetilde{p}\rrbracket$:

$$\begin{tikzcd}
\mathbf{G}_m^{\sharp,F} \arrow[r, "y\mapsto F\log(y)"] \arrow[d, "\mathrm{can}"'] & \hat{\mathbf{G}}_{\widetilde{p}}^\vee \arrow[d, "z\mapsto E_p(\widetilde{p})^{pz/\widetilde{p}}"] \\
(\mathbf{G}_m)_{\mathbf{Z}_p\llbracket\widetilde{p}\rrbracket} \arrow[r, "y\mapsto y^p"'] & (\mathbf{G}_m^{(1)})_{\mathbf{Z}_p\llbracket\widetilde{p}\rrbracket}.
\end{tikzcd}$$

This can be viewed as a p-typical version of Example 4.4.11.

Remark 4.4.15. The canonical homomorphism $\mathrm{can}: \mathbf{G}_m^{\sharp,F} \to (\mathbf{G}_m)_{R\llbracket t\rrbracket}$ of group schemes defines a quotient group stack $\mathbf{G}_m^{F\mathrm{dR}} := (\mathbf{G}_m)_{R\llbracket t\rrbracket}/\mathbf{G}_m^{\sharp,F}$ over $R\llbracket t\rrbracket$. One can prove by direct calculation that the derived global sections of the structure sheaf of the stack $\mathbf{G}_m^{F\mathrm{dR}}$ calculates the F-de Rham complex $F\Omega_{\square,\mathbf{G}_m} := F\Omega_{\square,\mathbf{A}^1}\otimes_{R\llbracket t\rrbracket[y]} R\llbracket t\rrbracket[y^{\pm1}]$. The key calculation (which we omit here) is that there is a quasi-isomorphism of $R\llbracket t\rrbracket$-coalgebras

$$R\llbracket t\rrbracket[y^{\pm1}]\otimes_{F\Omega_{\square,\mathbf{G}_m}} R\llbracket t\rrbracket[y^{\pm1}] \simeq R\llbracket t\rrbracket\left[y_1^{\pm1}, y_2^{\pm1}, \frac{(y_1-y_2)_s^n}{n!_F}\right]_{n\geq 0} \simeq \mathcal{O}_{\mathbf{G}_m^{\sharp,F}\times_{\operatorname{Spf} R\llbracket t\rrbracket}\mathbf{G}_m}, \tag{15}$$

where the tensor product on the left-hand side is derived, and both sides are implicitly (p,t)-adically completed. (The final equivalence follows by noting that $(y_1-y_2)_s^n = y_2(y_1y_2^{-1}-1)_s^n$, so adjoining

$\frac{(y_1-y_2)_s^n}{n!_F}$ is equivalent to adjoining the F-divided powers $\frac{(y_1y_2^{-1}-1)_s^n}{n!_F}$.) In the case of the additive formal group law, (15) boils down to the p-complete equivalence

$$\mathbf{Z}_p[y^{\pm 1}] \otimes_{\mathrm{dR}_{\mathbf{Z}_p[y^{\pm 1}]/\mathbf{Z}_p}} \mathbf{Z}_p[y^{\pm 1}] \simeq \mathrm{dR}_{\mathbf{Z}_p[y^{\pm 1}]/\mathbf{Z}_p[y_1^{\pm 1}, y_2^{\pm 1}]} \simeq \mathbf{Z}_p[y_1^{\pm 1}, y_2^{\pm 1}]\langle y_1 - y_2\rangle \cong \mathcal{O}_{\mathbf{G}_m^\sharp \times_{\mathrm{Spf}\,\mathbf{Z}_p} \mathbf{G}_m}$$

which arises via [Bha12, Proposition 8.5]. In the case of the multiplicative formal group law, (15) was shown in [Pri19].

Given this, Theorem 4.4.10 can be rephrased as the following two statements:

(1) The canonical map $(\mathbf{G}_m)_{R[\![t]\!]} \to \mathbf{G}_m^{F\mathrm{dR}}$ factors through the Frobenius $(\mathbf{G}_m)_{R[\![t]\!]} \to (\mathbf{G}_m^{(1)})_{R[\![t]\!]}$.

(2) The map $(\mathbf{G}_m^{(1)})_{R[\![t]\!]} \to \mathbf{G}_m^{F\mathrm{dR}}$ is surjective, and its kernel is isomorphic to the Cartier dual of the rescaled formal group $\hat{\mathbf{G}}_t$. In particular, there is an isomorphism $\mathbf{G}_m^{F\mathrm{dR}} \simeq (\mathbf{G}_m^{(1)})_{R[\![t]\!]}/\hat{\mathbf{G}}_t^\vee$ over $\mathrm{Spf}\, R[\![t]\!]$.

In the case of the multiplicative formal group law, this picture has been discussed in great detail in [Dri21]. As we hope to explain in future work, the above two statements are natural consequences of the homotopy-theoretic perspective on the F-de Rham complex (see Remark 4.3.25). We also hope that Theorem 4.4.10 might be useful in understanding Conjecture 4.3.23, and, in particular, in understanding a "stacky approach" to F-de Rham cohomology (following [BL22, Dri18, Dri22, Bha22]). Indeed, the F-divided power scheme $\mathbf{G}_m^{\sharp,F}$ is *a priori* rather difficult to access algebro-geometrically, but Theorem 4.4.10 says that it can be understood concretely in terms of $(\mathbf{G}_m)_{R[\![t]\!]}$ and the Cartier dual of the rescaled formal group $\hat{\mathbf{G}}_t$.

Let us end by noting that the following is an immediate consequence of Theorem 4.4.10:

Corollary 4.4.16. *Let $(\mathbf{G}_m^{\sharp,F})^\vee$ denote the Cartier dual of $\mathbf{G}_m^{\sharp,F}$. Then, there is a pushout square over $R[\![t]\!]$:*

$$\begin{tikzcd}
\underline{p\mathbf{Z}}_{R[\![t]\!]} \arrow[r, "p \mapsto \langle p \rangle_F(t)"] \arrow[d] & \hat{\mathbf{G}}_t \arrow[d] \\
\underline{\mathbf{Z}}_{R[\![t]\!]} \arrow[r] & (\mathbf{G}_m^{\sharp,F})^\vee.
\end{tikzcd}$$

Example 4.4.17. Let F be the multiplicative formal group law, and (as usual) write $q = t + 1$. Let $\mathbf{G}_{m,q-1} = \mathrm{Spf}\, \mathbf{Z}_p[\![q-1]\!][x, \frac{1}{1+(q-1)x}]$ denote the group scheme where the group structure is given by $(x, y) \mapsto x + y + (q-1)xy$. Since $\hat{\mathbf{G}}_t$ is the rescaled multiplicative formal group, it can be identified with the completion of $\mathbf{G}_{m,q-1}$ at the zero section (cut out by the function x). Corollary 4.4.16 and Example 4.4.11 imply that the Cartier dual of $\widetilde{G}_Q = \mathbf{G}_m^{\sharp,F}$ can be identified with the completion of $\mathbf{G}_{m,q-1}$ at the locus cut out by the polynomial $\prod_{j=0}^{p-1}(x - [j]_q)$.

REFERENCES

[AL20] J. Anschütz and A.-C. Le Bras. The p-completed cyclotomic trace in degree 2. *Ann. K-Theory*, 5(3):539–580, 2020.

[Bha00] M. Bhargava. The factorial function and generalizations. *Amer. Math. Monthly*, 107(9):783–799, 2000.

[Bha12] B. Bhatt. p-adic derived de Rham cohomology. `https://arxiv.org/abs/1204.6560`, 2012.

[Bha22] B. Bhatt. Prismatic F-gauges. Lecture notes available at `https://www.math.ias.edu/~bhatt/teaching/mat549f22/lectures.pdf`, 2022.

[BL22] B. Bhatt and J. Lurie. Absolute prismatic cohomology. `https://arxiv.org/abs/2201.06120`, 2022.

[BMS18] B. Bhatt, M. Morrow, and P. Scholze. Integral p-adic Hodge theory. *Publ. Math. Inst. Hautes Études Sci.*, 128:219–397, 2018.

[BMS19] B. Bhatt, M. Morrow, and P. Scholze. Topological Hochschild homology and integral p-adic Hodge theory. *Publ. Math. Inst. Hautes Études Sci.*, 129:199–310, 2019.

[BO78] P. Berthelot and A. Ogus. *Notes on crystalline cohomology*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1978.

[BS19] B. Bhatt and P. Scholze. Prisms and Prismatic Cohomology. `https://arxiv.org/abs/1905.08229`, 2019.

[Dev23] S. Devalapurkar. Topological Hochschild homology, truncated Brown-Peterson spectra, and a topological Sen operator. Forthcoming, 2023.

[DR23] S. Devalapurkar and A. Raksit. Calculating $\mathrm{THH}(\mathbf{Z}_p)$. Forthcoming, 2023.

[Dri18] V. Drinfeld. A stacky approach to crystals. `https://arxiv.org/abs/1810.11853`, 2018.

[Dri21] V. Drinfeld. A 1-dimensional formal group over the prismatization of Spf $\mathbf{Z}_p$. `http://arxiv.org/abs/2107.11466`, 2021.

[Dri22] V. Drinfeld. Prismatization. `https://arxiv.org/abs/2005.04746`, 2022.

[Haz78] M. Hazewinkel. *Formal groups and applications*, volume 78 of *Pure and Applied Mathematics*. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], New York-London, 1978.

[HLN21] F. Hebestreit, M. Land, and T. Nikolaus. On the homotopy type of L-spectra of the integers. *J. Topol.*, 14(1):183–214, 2021.

[Hon70] T. Honda. On the theory of commutative formal groups. *J. Math. Soc. Japan*, 22:213–246, 1970.

[HRW22] J. Hahn, A. Raksit, and D. Wilson. A motivic filtration on the topological cyclic homology of commutative ring spectra. `https://arxiv.org/abs/2206.11208`, 2022.

[Jac09] F. Jackson. On q-Functions and a certain Difference Operator. *Earth and Environmental Science Transactions of The Royal Society of Edinburgh* , 46(2):253–281, 1909.

[KC02] V. Kac and P. Cheung. *Quantum Calculus*. Universitext. Springer New York, 2002.

[Pri19] J. P. Pridham. On q–de Rham cohomology via Λ-rings. *Math. Ann.*, 375(1-2):425–452, 2019.

[Rav86] D. Ravenel. *Complex cobordism and stable homotopy groups of spheres*. Academic Press, 1986.

[Sas18] Sasha. Is there a lift of the q-Vandermonde identity to some geometric (motivic) identity for Grassmannians over F_q? MathOverflow, 2018. URL:https://mathoverflow.net/q/299582 (version: 2018-05-06).

[Sch17] P. Scholze. Canonical q-deformations in arithmetic geometry. *Ann. Fac. Sci. Toulouse Math. (6)*, 26(5):1163–1192, 2017.