A GENERALIZED TRUNCATED LOGARITHM

MARINA AVITABILE AND SANDRO MATTAREI

Abstract. We introduce a generalization $G^{(\alpha)}(X)$ of the truncated logarithm $\pounds_1(X) = \sum_{k=1}^{p-1} X^k/k$ in prime characteristic p, which depends on a parameter α. The main motivation of this study is $G^{(\alpha)}(X)$ being an inverse, in an appropriate sense, of a parametrized generalization of the truncated exponential given by certain Laguerre polynomials. Such Laguerre polynomials play a role in a *grading switching* technique for non-associative algebras, previously developed by the authors, because they satisfy a weak analogue of the functional equation $\exp(X)\exp(Y) = \exp(X+Y)$ of the exponential series. We also investigate functional equations satisfied by $G^{(\alpha)}(X)$ motivated by known functional equations for $\pounds_1(X) = -G^{(0)}(X)$.

1. Introduction

In this paper we investigate a parametrized analogue of the logarithmic function in prime characteristic. This modified version of the logarithm arises as the inverse (in an appropriate sense) of a parametrized modular analogue of the exponential which was introduced in [AM15b]. To provide motivation to this work we give here only a summary introduction to the latter, referring the interested reader to [AM15b, AM15a] for a detailed description.

The usefulness of the exponential function in various part of mathematics ultimately stems from its property $e^x \cdot e^y = e^{x+y}$, sometimes disguised as its essentially equivalent differential formulation $(d/dx)e^x = e^x$. In particular, as a means of connecting additive and multiplicative structures the exponential has always played a role in Lie theory, for local reconstruction of a Lie group from its Lie algebra. The essence of this application is that, under appropriate conditions, *the exponential of a derivation (of a non-associative algebra) is an automorphism.* The simplest setting to see this mechanism in action is the following: if D is a nilpotent derivation of a non-associative algebra A over a field of characteristic zero, then the finite sum $\exp(D) = \sum_{k=0}^{\infty} D^k/k!$ defines an automorphism of A. This can be viewed as a formal consequence of the functional equation $\exp(X) \cdot \exp(Y) = \exp(X+Y)$ satisfied by the exponential series $\exp(X) = \sum_{k=0}^{\infty} X^k/k!$, in the ring of formal power series $\mathbb{Q}[[X, Y]]$.

1991 *Mathematics Subject Classification.* Primary 33E50; secondary 39B52, 05A10, 33C45.

Key words and phrases. truncated logarithm; polylogarithm; Laguerre polynomial; functional equation; Jacobi polynomial.

Over fields prime characteristic p, the *truncated exponential* $E(X) = \sum_{k=0}^{p-1} X^k/k!$ can be used as a substitute for the exponential series, to some extent. In particular, if p is odd and the derivation D satisfies $D^{(p+1)/2} = 0$, then $E(D)$ is an automorphism, but the weaker condition $D^p = 0$ is insufficient to this goal. This apparent shortcoming of $\exp(D)$ was turned into an advantage in the technique of *toral switching* for modular Lie algebras, originally developed by Winter [Win69] in its most basic form. This fundamental tool in the classification theory of simple modular Lie algebras has later undergone substantial generalizations by Block and Wilson [BW82], until reaching its most complete expression in work of Premet [Pre86]. The gist of the technique is that maps similar to exponentials of derivations (of the form $E(D)$ with D a certain inner derivation, or more general constructions in [Pre86]) are used to produce a new torus from a given torus (with certain properties including having maximal dimension). Because those maps are not automorphims, the new torus may have very different properties from the original torus, and better suited to certain purposes.

Now, any torus of a Lie algebra induces a grading given by the corresponding eigenspace decompositions with respect to the adjoint action (called a *generalized root space decomposition*). Therefore, in very broad terms toral switching may be viewed as a technique to pass from a given grading of a Lie algebra to another one. In such generality one may wonder whether some kind of exponential could be used to pass from a given grading to another one without assuming that either of them is associated to some torus. In this spirit a *grading switching* technique for non-associative algebras was developed in [Mat05] for nilpotent derivations, and then extended in [AM15b] for arbitrary derivations. Despite being motivated and strongly inspired by the toral switching technique, to attain greater generality and allow applications such as those in [Mat05, AM05, AM07, AM15a], those papers focus on the algebraic property which makes some generalized exponential of a derivation map a grading of the algebra to another grading. That crucial property boils down to the generalized exponential employed satisfying an appropriately weakened version of the functional equation $\exp(X) \cdot \exp(Y) = \exp(X + Y)$.

In fact, the generalized exponential employed in [Mat05] was the Artin-Hasse exponential series

$$E_p(X) := \exp\Big(\sum_{i=0}^{\infty} X^{p^i}/p^i\Big) = \prod_{i=0}^{\infty} \exp(X^{p^i}/p^i),$$

whose importance in p-adic analysis and number theory stems from all its coefficients being p-integral. In particular, by viewing its coefficients modulo p one can regard $E_p(X) \in \mathbb{F}_p[[X]]$, where $\mathbb{F}_p$ is the field of p elements. As such, $E_p(X)$ was shown in [Mat05] to have the property that all terms of $E_p(X) \cdot E_p(Y)/E_p(X+Y) \in \mathbb{F}_p[[X, Y]]$ have degree multiples of p. This weak version of the fundamental functional equation for $\exp(X)$ is precisely what make grading switching based on

$E_p(D)$ work, for appropriate gradings and nilpotent derivations D. It was shown in [Mat06] that this weak functional equation actually characterizes $E_p(X)$ in $\mathbb{F}_p[[X]]$ up to certain natural variations.

Nilpotence of the derivation D was required in [Mat05] for $E_p(D)$ to make sense algebraically. However, the resulting grading switching matched only a rather special case of the classical toral switching. This limitation was removed in [AM15b] by introducing certain (generalized) Laguerre polynomials as substitutes for exponentials. We defer discussing the connection with the classical Laguerre polynomials $L_n^{(\alpha)}(X)$ to Subsection 2.1, but those of interest to us, once regarded as polynomials in characteristic p, take the form

$$L_{p-1}^{(\alpha)}(X) = (1-\alpha^{p-1})\sum_{k=0}^{p-1} \frac{X^k}{(1+\alpha)(2+\alpha)\cdots(\alpha+k)}.$$

Here α is a parameter, which in the application to grading switching relates to an eigenvalue of the derivation D in a certain way. In the special case where the derivation D is nilpotent its only eigenvalue is zero, and $L_{p-1}^{(0)}(X)$ equals the truncated exponential $E(X)$. The reader who might be puzzled by how a construction using certain Laguerre *polynomials* can extend an earlier one based on Artin-Hasse *power series* will find an explanation of this connection in [AM15a, Proposition 6].

Again, the crucial property which makes $L_{p-1}^{(\alpha)}(X)$ work as a replacement for an exponential in the grading switching application in [AM15b] is that it satisfies a weak version of the fundamental functional equation for $\exp(X)$, its most important feature being that all terms $L_{p-1}^{(\alpha)}(X)\cdot L_{p-1}^{(\beta)}(Y)/L_{p-1}^{(\alpha+\beta)}(X) \in \mathbb{F}_p(\alpha,\beta)[[X,Y]]$ have degree multiples of p. The more precise version of this property given in Theorem 1 below is actually required, and an even more precise one as in [AM15b, Proposition 2] to attain full generality. We skip those details in this introduction, but only mention that the functional equation in more precise form is actually a congruence involving moduli such as $X^p-(\alpha^p-\alpha)$ and $Y^p-(\beta^p-\beta)$. In fact, in this context $L_{p-1}^{(\alpha)}(X)$ is only of interest when regarded modulo $X^p-(\alpha^p-\alpha)$.

We come now to the goal of this paper, which is investigating an appropriate compositional inverse $G^{(\alpha)}(X)$ for the polynomial $L_{p-1}^{(\alpha)}(X)$. We devote Section 2 to a detailed description of our results, along with the necessary technical preliminaries, hence we limit ourselves to a succinct outline in this Introduction. Guidance from the functional properties of $L_{p-1}^{(\alpha)}(X)$ suggests that the correct interpretation of being a left compositional inverse is being a polynomial of degree less than p in X, and with coefficients depending on the parameter α, satisfying

$$G^{(\alpha)}\big(L_{p-1}^{(\alpha)}(X)\big) \equiv X \pmod{X^p-(\alpha^p-\alpha)}.$$

General reasons imply that there is precisely one polynomial $G^{(\alpha)}(X)$ satisfying these requirements. In Theorem 2 we find an explicit expression for it, but

here we limit ourselves to pointing out that specialized to $\alpha = 0$ it becomes $G^{(0)}(X) = -\sum_{k=1}^{p-1} X^k/k$, which is a truncated version of the series for $\log(1-X)$. In terms of the standard notation $\pounds_d(X) = \sum_{k=1}^{p-1} X^k/k^d$ for the *finite polylogarithms* we then have $G^{(0)}(X) = -\pounds_1(X)$. The above equation relating $L_{p-1}^{(\alpha)}(X)$ and $G^{(\alpha)}(X)$, which reads $-\pounds_1\big(E(X)\big) \equiv X \pmod{X^p}$ when $\alpha = 0$, where $E(X)$ is the truncated exponential, may be viewed as an analogue of $\log\big(\exp(X)\big) = X$. This depends on the fact that the *truncated logarithm* $\pounds_1(X)$ (always viewed in characteristic p here) satisfies $\pounds_1(1-X) = \pounds_1(X)$, a functional equation without analogue in characteristic zero, as we explain in the discussion which follows Theorem 2. The polynomial $G^{(\alpha)}(X)$ is also a right compositional inverse of $L_{p-1}^{(\alpha)}(X)$ in an appropriate sense, made explicit in Corollary 3. The proofs of Theorem 2 and Corollary 3 occupy Section 3.

The coefficients of $G^{(\alpha)}(X)$ as given in Theorem 2 are rational expressions in α with numerators 1. We devote Section 4 to an investigation of their denominators, leading to an explicit description of their factorizations, as polynomials in α. In particular, it will turn out that their roots are nonzero elements of the prime field $\mathbb{F}_p$, as stated in Theorem 5, but Theorem 12 allows explicit calculation of which roots occur and with which multiplicities.

This information will be crucial in the next part of the paper, which studies functional equations for $G^{(\alpha)}(X)$. This investigation is motivated by functional equations for the truncated logarithm $\pounds_1(X) = -G^{(0)}(X)$, which besides the already mentioned $\pounds_1(1-X) = \pounds_1(X)$ satisfies $\pounds_1(X) = -X^p\pounds_1(1/X)$. In Theorem 6 we generalize the latter to an equation for $G^{(\alpha)}(X)$, which involves an evaluation of $G^{(\alpha)}$ on one side and one of $G^{(-\alpha)}$ on the other. It remains unclear whether a similar generalization exists for $\pounds_1(1-X) = \pounds_1(X)$, and even which general form it may take.

More interestingly, the functional equation $\log(xy) = \log(x) + \log(y)$ for the ordinary logarithmic function, which matches the fundamental functional equation for the exponential function, has a well-known analogue for the truncated logarithm $\pounds_1(X)$ in the polynomial ring $\mathbb{F}_p[X,Y]$, except that the latter involves four terms, see Equation (4). We are unfortunately unable to generalize this to a corresponding equation for $G^{(\alpha)}(X)$, but in Theorem 8 we produce a version for $G^{(\alpha)}(X)$ of a consequence of $\log(xy) = \log(x) + \log(y)$, namely $\log(x^h) = h\log(x)$ for integer h. Our equation, which is actually a congruence with respect to an appropriate modulus, involves an evaluation of $G^{(\alpha)}$ on one side and one of $G^{(h\alpha)}$ on the other, for $0 < h < p$. We discuss these functional equations extensively in Subsection 2.4, and prove our results in Section 5.

In the final Section 6 we relate polynomials used to describe the coefficients of $G^{(\alpha)}(X)$ in Theorem 2 to certain Jacobi polynomials, showing how some of the properties of the former could alternately be deduced by appropriate manipulation of known equations for the latter.

2. Motivations and statements of the results

In this section we state our results in more precise form than the rough description given in Section 1. In Subsection 2.1 we recall certain generalized Laguerre polynomials $L_{p-1}^{(\alpha)}(X)$ which play a role in the *grading switching* described in [AM15b] because of their exponential-like property. That crucial property is a functional equation, in the form of a congruence, which we quote from [AM15b] in Theorem 1. In Subsection 2.2 we take this as a motivation to produce a certain compositional inverse $G^{(\alpha)}(X)$ of $L_{p-1}^{(\alpha)}(X)$, in a suitable sense, which we describe in Theorem 2, and should have logarithm-like properties. The short Subsection 2.3 aims at a better understanding of the coefficients of $G^{(\alpha)}(X)$, namely their factorizations as rational functions of α. That detailed information is essential for the results of Subsection 2.4, which discusses functional equations for the truncated logarithm, and extends a couple of them to equations for $G^{(\alpha)}(X)$.

2.1. **Some generalized Laguerre polynomials.** The classical (generalized) Laguerre polynomial of degree $n \geq 0$ is defined as

$$L_n^{(\alpha)}(X) = \sum_{k=0}^{n} \binom{\alpha+n}{n-k} \frac{(-X)^k}{k!},$$

where α is a parameter, usually taken in the complex numbers. However, we may also view $L_n^{(\alpha)}(X)$ as a polynomial with rational coefficients in the two indeterminates α and X, hence in the polynomial ring $\mathbb{Q}[\alpha, X]$.

Now fix a prime p. If $0 \leq n < p$ then all coefficients of $L_n^{(\alpha)}(X)$ are p-integral, and hence can be viewed modulo p. We are essentially only interested in the case $n = p-1$, where $L_{p-1}^{(\alpha)}(X)$ modulo p can be considered as a generalization of the *truncated exponential* $E(X) = \sum_{k=0}^{p-1} X^k/k!$ which we mentioned in the Introduction. In fact, we have $L_{p-1}^{(0)}(X) \equiv E(X) \pmod{p}$ because $\binom{p-1}{k} \equiv \binom{-1}{k} = (-1)^k \pmod{p}$ for $0 \leq k < p$.

It is notationally convenient to work directly in characteristic p, and so we will regard $L_{p-1}^{(\alpha)}(X)$ as having coefficients in the field $\mathbb{F}_p$ of p elements, thus viewing

$$L_{p-1}^{(\alpha)}(X) = \sum_{k=0}^{p-1} \binom{\alpha-1}{p-1-k} \frac{(-X)^k}{k!} \in \mathbb{F}_p[\alpha, X]. \tag{1}$$

Hence $L_{p-1}^{(0)}(X) = E(X)$, if we regard the truncated exponential $E(X)$ as a polynomial in $\mathbb{F}_p[X]$ as well. Taking advantage of working in characteristic p, and in particular of the congruence $k!(p-1-k)! \equiv (-1)^{k-1} \pmod{p}$, we find simpler expressions for $L_{p-1}^{(\alpha)}(X)$ by expressing the binomial coefficients involved in terms of *Pochhammer symbols* $(x)_m := x(x-1)\cdots(x-m+1)$, which are defined for x in any commutative ring and m a nonnegative integer, with the natural convention

$(x)_0 := 1$. Thus, we have

$$L_{p-1}^{(\alpha)}(X) = -\sum_{k=0}^{p-1}(\alpha-1)_{p-1-k}\cdot X^k = (1-\alpha^{p-1})\sum_{k=0}^{p-1}\frac{X^k}{(\alpha+k)_k}.$$

The latter expression, which is obtained using $(\alpha-1)_{p-1} = \alpha^{p-1}-1$ in $\mathbb{F}_p[\alpha]$, emphasizes the role of $L_{p-1}^{(\alpha)}(X)$ as a generalization of the more familiar $E(X)$. In particular, note that as a polynomial in X only, its constant term is $L_{p-1}^{(\alpha)}(0) = 1-\alpha^{p-1}$.

The Laguerre polynomials $L_{p-1}^{(\alpha)}(X)$ satisfy a congruence which bears a strong analogy with the functional equation $\exp(X)\exp(Y) = \exp(X+Y)$ of the classical exponential. More precisely, viewing the functional equation for the exponential as an identity in the ring of power series $\mathbb{Q}[[X,Y]]$, its direct consequence $\exp(X)\exp(Y) \equiv \exp(X+Y) \pmod{(X^p,Y^p)}$ in $\mathbb{Q}[[X,Y]]$ is equivalent to $E(X)E(Y) = E(X+Y) \pmod{(X^p,Y^p)}$ in the polynomial ring $\mathbb{Q}[X,Y]$. Because no denominator in this equation is a multiple of p, the equation can be viewed modulo p, that is, in the polynomial ring $\mathbb{F}_p[X,Y]$. As such, it generalizes as follows for $L_{p-1}^{(\alpha)}(X)$.

Theorem 1 ([AM15b, Proposition 2])**.** *Let α, β, X, Y be indeterminates over $\mathbb{F}_p$. There exist rational expressions $c_i(\alpha,\beta) \in \mathbb{F}_p(\alpha,\beta)$, such that*

$$L_{p-1}^{(\alpha)}(X)\cdot L_{p-1}^{(\beta)}(Y) \equiv L_{p-1}^{(\alpha+\beta)}(X+Y)\cdot\Big(c_0(\alpha,\beta)+\sum_{i=1}^{p-1}c_i(\alpha,\beta)X^iY^{p-i}\Big)$$

in $\mathbb{F}_p(\alpha,\beta)[X,Y]$, modulo the ideal generated by $X^p-(\alpha^p-\alpha)$ and $Y^p-(\beta^p-\beta)$.

To be precise, [AM15b, Proposition 2] is actually stronger than Theorem 1, and its formulation slightly more complicated, as it provides finer control over the rational expressions $c_i(\alpha,\beta)$, which is needed in some applications. We will return to this subtlety in Subsection 2.3.

The crucial property of $L_{p-1}^{(\alpha)}(X)$ which allows it to play a role of an exponential in the grading switching described in [AM15b] is that the factor in parentheses at the right-hand side, as well as the moduli, have only terms of total degree a multiple of p.

2.2. **Inverting $L_{p-1}^{(\alpha)}(X)$.** The main goal of this paper is producing a left compositional inverse, and then a corresponding right inverse, of the polynomial $L_{p-1}^{(\alpha)}(X)$ in an appropriate sense. Because of Theorem 1, in the motivating applications to algebra gradings the Laguerre polynomial $L_{p-1}^{(\alpha)}(X)$ is of interest only regarded modulo $X^p-(\alpha^p-\alpha)$, this dictates the context of the desired inverse.

We quickly dispose of the case of characteristic $p=2$, where $L_1^{(\alpha)}(X) = (1+\alpha)+X$ and hence $L_1^{(\alpha)}\big(L_1^{(\alpha)}(X)\big) = X$ in $\mathbb{F}_2[\alpha,X]$. Hence $L_1^{(\alpha)}(X)$ is its own inverse in

this case, and in a strong sense. For the rest of the paper we make the blanket assumption that p is odd.

To describe the coefficients of the desired inverse of $L_{p-1}^{(\alpha)}(X)$, as a polynomial in X, we introduce a family of polynomials $b_{r,s}(\alpha) \in \mathbb{F}_p[\alpha]$ depending on integers $0 < r, s < p$:

$$b_{r,s}(\alpha) := \sum_{k=0}^{p-1} (-r/s)^k \binom{r\alpha - 1}{p-1-k} \binom{s\alpha - 1}{k}. \tag{2}$$

Because $\binom{-1}{k} = (-1)^k$ for $k \geq 0$, for $r+s \neq p$ the polynomials $b_{r,s}(\alpha)$ have constant term $b_{r,s}(0) = \sum_{k=0}^{p-1}(-1)^k(r/s)^k = 1$ (in $\mathbb{F}_p$). More generally, for any positive integer a the expression $b_{r,s}(a)$ equals the coefficient of X^{p-1} in the polynomial $(1 + X/r)^{ra-1}(1 - X/s)^{sa-1} \in \mathbb{F}_p[X]$, having noted that $r^{p-1} \equiv 1 \pmod{p}$. This fact will be used in the proof of Theorem 12 to prove certain properties of the polynomials $b_{r,s}(\alpha)$. For now it shows that $b_{r,p-r}(\alpha) \in \mathbb{F}_p[\alpha]$ is the zero polynomial, as it has degree at most $p-1$ by definition, but $b_{r,p-r}(a) = 0$ for any positive integer a because $(1 + X/r)^{pa-2} = (1 + X/r)^{p-2} \cdot (1 + X^p/r)^{a-1} \in \mathbb{F}_p[X]$ has no term of degree $p - 1$.

We will conveniently allow ourselves to interpret the integers r and s as elements of $\mathbb{F}_p^*$, and write $b_{r,-r}(\alpha)$ instead of $b_{r,p-r}(\alpha)$, for example. With this convention, for $t \in \mathbb{F}_p^*$ we plainly have $b_{rt,st}(\alpha) = b_{r,s}(t\alpha)$. This allows us to assume $r = 1$ in studying such polynomials and, in fact, only the polynomials $b_{1,s}(\alpha)$ are required in stating the following result.

The following result provides the desired left inverse of $L_{p-1}^{(\alpha)}(X)$.

Theorem 2. *Let $\mathbb{F}_p(\alpha)$ be the field of the rational expressions in the indeterminate α. There is a unique polynomial $G^{(\alpha)}(X)$ of degree less than p in $\mathbb{F}_p(\alpha)[X]$ such that*

$$G^{(\alpha)}\big(L_{p-1}^{(\alpha)}(X)\big) \equiv X \pmod{X^p - (\alpha^p - \alpha)},$$

and is given by

$$G^{(\alpha)}(X) = -\sum_{k=1}^{p-1} \frac{1}{k} \frac{X^k}{\prod_{s=1}^{k-1} b_{1,s}(\alpha)}.$$

The denominator $\prod_{s=1}^{k-1} b_{1,s}(\alpha)$ in the expression for $G^{(\alpha)}(X)$ should be read as 1 when $k = 1$.

We now describe in which sense Theorem 2 generalizes a truncated version modulo X^p of the equation $\log\big(\exp(X)\big) = X$ in $\mathbb{Q}[[X]]$. Setting $\alpha = 0$ we have $L_{p-1}^{(0)}(X) = E(X) = \sum_{k=0}^{p-1} X^k/k!$, the truncated exponential in characteristic p, and $G^{(0)}(X) = -\sum_{k=1}^{p-1} X^k/k = -\mathcal{L}_1(X)$. Here $\mathcal{L}_d(X) = \sum_{k=1}^{p-1} X^k/k^d$ denote the *finite polylogarithms*. They are truncated versions of the power series $\mathrm{Li}_d(X) = \sum_{k=1}^{\infty} X^k/k^d$, which serve to define the ordinary *polylogarithms* over the complex

numbers in a neighbourhood of zero. In particular, $\mathrm{Li}_1(X) = -\log(1-X)$ is closely related to the ordinary logarithmic series.

For composition of formal power series to make sense the absence of a constant term is required, and hence the equation $\log\big(\exp(X)\big) = X$ in $\mathbb{Q}[[X]]$ should really be interpreted as $\log\big(1+(\exp(X)-1)\big) = X$. Adopting polylogarithmic notation this reads $-\mathrm{Li}_1\big(1-\exp(X)\big) = X$. Viewing this equation modulo X^p, and then modulo p, it implies $-\pounds_1\big(1-E(X)\big) \equiv X \pmod{X^p}$ in $\mathbb{F}_p[[X]]$, or actually in the polynomial ring $\mathbb{F}_p[X]$. However, setting $\alpha = 0$ in the congruence of Theorem 2 yields $-\pounds_1\big(E(X)\big) \equiv X \pmod{X^p}$ in $\mathbb{F}_p[X]$. This apparent discrepancy is resolved by the functional equation $\pounds_1(1-X) = \pounds_1(X)$, which the polynomial $\pounds_1(X)$ satisfies (see Subsection 2.4 below for more details). Hence Theorem 2 generalizes a truncated version of the familiar fact that the logarithm is a left inverse of the exponential function, modulo an application of the mentioned functional equation for $\pounds_1(X)$.

The left compositional inverse $G^{(\alpha)}(X)$ for $L_{p-1}^{(\alpha)}(X)$ given in Theorem 2 gives rise to a right inverse as follows.

Corollary 3. *We have*

$$L_{p-1}^{(\alpha)}\big(G^{(\alpha)}(X)\big) \equiv X \pmod{X^p - L_{p-1}^{(\alpha^p)}(\alpha^p - \alpha)}$$

in the polynomial ring $\mathbb{F}_p(\alpha)[X]$.

According to [AM15b, Lemma 1], the expression $L_{p-1}^{(\alpha^p)}(\alpha^p - \alpha)$ which appears in the modulus of the congruence in Corollary 3 can be explicitly factorized as

$$L_{p-1}^{(\alpha^p)}(\alpha^p - \alpha) = \prod_{k=1}^{p-1}(1+\alpha/k)^k. \tag{3}$$

2.3. **Additional information on the coefficients of $G^{(\alpha)}(X)$.** As mentioned earlier, Theorem 1 is a weaker and simplified version of [AM15b, Proposition 2]. This is sufficient for an application to grading switching only under special circumstances. For full generality the applications need the following additional information on the rational functions $c_i(\alpha,\beta)$.

Theorem 4 ([AM15b, Proposition 2])**.** *The rational expressions $c_i(\alpha,\beta)$ of Theorem 1 belong to the subring $\mathbb{F}_p\big[\alpha,\beta,\big((\alpha+\beta)^{p-1}-1\big)^{-1}\big]$ of $\mathbb{F}_p(\alpha,\beta)$.*

The relevance of Theorem 4 in the context of grading switching is to guarantee that $c_i(\alpha,\beta)$ can be evaluated on elements $\tilde\alpha, \tilde\beta$ of some extension of $\mathbb{F}_p$ as long as $\tilde\alpha + \tilde\beta \notin \mathbb{F}_p^*$. For example, when $p = 3$ the rational expressions $c_0(\alpha,\beta)$, $c_1(\alpha,\beta)$, and $c_2(\alpha,\beta)$ equal, respectively,

$$\frac{(1-\alpha^2)(1-\beta^2)}{1-(\alpha+\beta)^2}, \qquad \frac{\alpha-1}{1-(\alpha+\beta)^2}, \qquad \frac{\beta-1}{1-(\alpha+\beta)^2}.$$

We supplement our Theorem 2 with corresponding information on the coefficients of $G^{(\alpha)}(X)$.

Theorem 5. *The coefficients of the polynomial $G^{(\alpha)}(X)$ of Theorem 2 belong to the subring $\mathbb{F}_p[\alpha, (\alpha^{p-1}-1)^{-1}]$ of $\mathbb{F}_p(\alpha)$.*

As an example, when $p = 3$ we have $G^{(\alpha)}(X) = -X - X^2/(\alpha+2)$. Theorem 5 will follow at once from the identity $b_{1,s}(\alpha)b_{1,s}(-\alpha) = 1-\alpha^{p-1}$ for $s = 1, \dots, p-2$, which we will prove in Lemma 11 of Section 4. In particular, this identity shows that $b_{1,s}(\alpha)$ is a polynomial of degree $(p-1)/2$, and its roots are exactly half the elements of $\mathbb{F}_p^*$.

We devote the remainder of Section 4 to finding a simple way to decide exactly which elements of $\mathbb{F}_p^*$ are roots of $b_{1,s}(\alpha)$, in Theorem 12. That result provides a simpler description of the polynomials $b_{1,s}(\alpha)$ and, consequently, of the coefficients of $G^{(\alpha)}(X)$.

2.4. **Functional equations for the polynomials $G^{(\alpha)}(X)$.** The interpretation of the polynomials $G^{(\alpha)}(X)$ as generalized logarithms suggests that they might satisfy some analogue of the functional equation $\log(xy) = \log(x) + \log(y)$. After all, according to Theorem 1 the generalized exponentials $L_{p-1}^{(\alpha)}(X)$, which the $G^{(\alpha)}(X)$ suitably invert, satisfy a weak version of the functional equation $\exp(x)\exp(y) = \exp(x+y)$. Unfortunately, switching from a weak functional equation for a weak exponential to a corresponding functional equation for a weak logarithm does not seem to go through as smoothly as it would for their classical analogues. The picture is enriched, but also made much more complex, by the presence of additional functional equations for the truncated logarithm, which we briefly discuss now.

As we observed after Theorem 2, the polynomials $G^{(\alpha)}(X)$ are a parametrized version of the finite polylogarithm $\pounds_1(X) = \sum_{k=1}^{p-1} X^k/k$, because $G^{(0)}(X) = -\pounds_1(X)$. The polynomial $\pounds_1(X)$ (viewed in characteristic p as we do throughout this paper) satisfies certain functional equations which have no analogues for the classical logarithm which it resembles. One such equation is $\pounds_1(X) = -X^p\pounds_1(1/X)$, which is an immediate consequence of Wilson's theorem, $(p-1)! = -1$ in $\mathbb{F}_p$. This functional equation does extend to the following equation for the polynomials $G^{(\alpha)}(X)$.

Theorem 6. *The polynomials $G^{(\alpha)}(X)$ satisfy*

$$\prod_{k=1}^{p-1}(1+\alpha/k)^k \cdot G^{(\alpha)}(X) = -X^p \cdot G^{(-\alpha)}\left(\frac{1-\alpha^{p-1}}{X}\right)$$

in the polynomial ring $\mathbb{F}_p(\alpha)[X]$.

We will prove Theorem 6 in Section 5, using the explicit characterization and properties of their coefficients $b_{1,s}(\alpha)$ obtained in Section 4.

Another functional equation satisfied by $\mathcal{L}_1(X)$ is $\mathcal{L}_1(1-X) = \mathcal{L}_1(X)$. See [MT13, Equation (13)] or [MT18, Equation (28)] for the easy proof, and [MT13, Lemma 3.2] for a generalization, probably already known to Mirimanoff at the beginning of the twentieth century [Mir05]. We do not know whether this functional equation extends to an equation involving polynomials $G^{(\alpha)}(X)$ (in a sensible way), and we formulate this as a question.

Question 7. Do the polynomials $G^{(\alpha)}(X)$, perhaps collectively, satisfy a generalization of the functional equation $\mathcal{L}_1(1-X) = \mathcal{L}_1(X)$ for $\mathcal{L}_1(X) = -G^{(0)}(X)$?

Alternate application of the functional equations $\mathcal{L}_1(X) = \mathcal{L}_1(1-X)$ and $\mathcal{L}_1(X) = -X^p\mathcal{L}_1(1/X)$ generates six equivalent expressions for $\mathcal{L}_1(X)$ (as a polynomial in $\mathbb{F}_p[X]$), namely,

$$\begin{aligned}\mathcal{L}_1(X) = \mathcal{L}_1(1-X) = (X-1)^p\mathcal{L}_1\left(\frac{1}{1-X}\right) = (X-1)^p\mathcal{L}_1\left(\frac{X}{X-1}\right)\\ = -X^p\mathcal{L}_1\left(\frac{X-1}{X}\right) = -X^p\mathcal{L}_1\left(\frac{1}{X}\right).\end{aligned}$$

This invariance of $\mathcal{L}_1(X)$ under a certain group of *symmetries* of order six accounts for multiple representations of any formula involving $\mathcal{L}_1(X)$. See [MT13] for further discussion and applications of those symmetries. Of course generalizations to $G^{(\alpha)}(X)$ remain inaccessible as long as we miss a generalization of $\mathcal{L}_1(X) = \mathcal{L}_1(1-X)$.

The following result, also proved in Section 5, is an analogue of the equation $\log(x^h) = h\log(x)$.

Theorem 8. *For any integer h with $0 < h < p$ we have*

$$G^{(h\alpha)}\left(\frac{X^h}{\prod_{s=1}^{h-1} b_{1,s}(\alpha)}\right) \equiv hG^{(\alpha)}(X) \pmod{X^p - L_{p-1}^{(\alpha^p)}(\alpha^p - \alpha)}$$

in the polynomial ring $\mathbb{F}_p(\alpha)[X]$.

According to Lemma 10, when $h = p-1$ the equation of Theorem 8 can also be written as

$$G^{(-\alpha)}\left(\frac{X^{p-1}\cdot(1-\alpha^{p-1})}{L_{p-1}^{(\alpha^p)}(\alpha^p-\alpha)}\right) \equiv -G^{(\alpha)}(X) \pmod{X^p - L_{p-1}^{(\alpha^p)}(\alpha^p - \alpha)}.$$

However, this last congruence is also a weak consequence of Theorem 6.

Of course $\log(x^h) = h\log(x)$ for integer h is a consequence of the fundamental functional equation $\log(xy) = \log(x) + \log(y)$. That equation has an analogue for $\mathcal{L}_1(X)$ in the polynomial ring $\mathbb{F}_p[X,Y]$, namely,

$$\mathcal{L}_1(X) - \mathcal{L}_1(Y) + X^p\mathcal{L}_1\left(\frac{Y}{X}\right) + (1-X)^p\mathcal{L}_1\left(\frac{1-Y}{1-X}\right) = 0. \tag{4}$$

This equation seems to have been first noticed (at least in recent times) by Kontsevich [Kon02], in a somehow more rudimentary form, see [MT18, Equation (31)] and the subsequent discussion. It admits several proofs, two of which are given in [MT18]. We sketch a variation of one of those proofs which emphasizes its origin in the fundamental functional equation of the logarithm, in its variant

$$-\log(1-X)+\log(1-Y)-\log\left(\frac{1-Y}{1-X}\right)=0,$$

which takes place in the power series ring $\mathbb{Q}[[X,Y]]$. Viewing modulo the ideal $(X,Y)^p$ and then reducing modulo p one finds

$$\pounds_1(X)-\pounds_1(Y)+\pounds_1\left(1-\frac{1-Y}{1-X}\right)\equiv 0 \pmod{(X,Y)^p}$$

in the power series ring $\mathbb{F}_p[[X,Y]]$. Rewriting the last summand using $\pounds_1(1-Z)=\pounds_1(Z)$ we find that a weak version of Equation (4) holds as a congruence modulo the ideal $(X,Y)^p$ of $\mathbb{F}_p[[X,Y]]$. The symmetries (or functional equations) for $\pounds_1(X)$ described earlier allow one to, both recover the missing term in Equation (4), and prove that it holds in full, first in $\mathbb{F}_p[[X,Y]]$ but then in $\mathbb{F}_p[X,Y]$ where Equation (4) takes place, see [MT18, Equation (31)] for the details. Unfortunately, we are not able to extend these arguments to a generalization for $G^{(\alpha)}(X)$, and so we leave that as our final question.

Question 9. Do the polynomials $G^{(\alpha)}(X)$ satisfy a generalization of Equation (4) for $\pounds_1(X)=-G^{(0)}(X)$?

Such a generalization would have to be a congruence in the guise of the equation in Theorem 1, involving $G^{(\alpha)}(X)$, $G^{(\beta)}(Y)$, and other terms.

3. Proofs of Theorem 2 and Corollary 3

The first step towards computing $G^{(\alpha)}\big(L^{(\alpha)}_{p-1}(X)\big)$ modulo $X^p-(\alpha^p-\alpha)$ as in Theorem 2 is computing the powers of $L^{(\alpha)}_{p-1}(X)$ modulo $X^p-(\alpha^p-\alpha)$. For that we need to consider the products $L^{(r\alpha)}_{p-1}(rX)L^{(s\alpha)}_{p-1}(sX)$, for $0<r,s<p$. Note that under the simultaneous substitutions $X'=rX$ and $\alpha'=r\alpha$, for some $0<r<p$, the modulus $X^p-(\alpha^p-\alpha)$ gets simply multiplied by the nonzero scalar r.

Thus, as a special case of Theorem 1, after replacing X with rX, Y with sX, and similar substitutions for the parameters α and β, we find

$$L^{(r\alpha)}_{p-1}(rX)L^{(s\alpha)}_{p-1}(sX)\equiv b'_{r,s}(\alpha)\cdot L^{((r+s)\alpha)}_{p-1}\big((r+s)X\big) \pmod{X^p-(\alpha^p-\alpha)},$$

where

$$b'_{r,s}(\alpha)=c_0(r\alpha,s\alpha)+(\alpha^p-\alpha)\sum_{i=1}^{p-1}c_i(r\alpha,s\alpha)r^is^{p-i}, \tag{5}$$

and $c_i(r\alpha, s\alpha)$ are certain rational expressions in $\mathbb{F}_p(\alpha)$. We now prove that the rational expressions $b'_{r,s}(\alpha)$ are actually polynomials, and coincide with the polynomials $b_{r,s}(\alpha)$ defined in Equation (2) as long as $r + s \neq p$.

Lemma 10. *For integers $0 < r, s < p$ with $r + s \neq p$ we have*

$$L_{p-1}^{(r\alpha)}(rX) \cdot L_{p-1}^{(s\alpha)}(sX) \equiv b_{r,s}(\alpha) \cdot L_{p-1}^{((r+s)\alpha)}\big((r+s)X\big) \pmod{X^p - (\alpha^p - \alpha)},$$

in $\mathbb{F}_p(\alpha)[X]$, where $b_{r,s}(\alpha) \in \mathbb{F}_p[\alpha]$ are the polynomials defined in Equation (2). Furthermore, in the excluded case where $r + s = p$ we have

$$L_{p-1}^{(r\alpha)}(rX) \cdot L_{p-1}^{(-r\alpha)}(-rX) \equiv 1 - \alpha^{p-1} \pmod{X^p - (\alpha^p - \alpha)}.$$

Proof. Expanding the product $L_{p-1}^{(r\alpha)}(rX) \cdot L_{p-1}^{(s\alpha)}(sX)$ according to Theorem 1 we have

$$L_{p-1}^{(r\alpha)}(rX) \cdot L_{p-1}^{(s\alpha)}(sX) = \sum_{k=0}^{p-1} \sum_{h=0}^{p-1} \binom{r\alpha - 1}{p-1-k} \binom{s\alpha - 1}{p-1-h} \frac{(-r)^k (-s)^h}{k!h!} X^{k+h}$$

Separating the terms in the double sum according to whether the degree $k + h$ is less than p or at least p, the sum of the former terms equals

$$\sum_{t=0}^{p-1} \sum_{k=0}^{t} \binom{r\alpha - 1}{p-1-k} \binom{s\alpha - 1}{p-1-t+k} \frac{(-1)^t r^k s^{t-k}}{k!(t-k)!} X^t,$$

having set $k + h = t$, and the sum of the latter is congruent to

$$-s(\alpha^p - \alpha) \sum_{t=0}^{p-2} \sum_{k=t+1}^{p-1} \binom{r\alpha - 1}{p-1-k} \binom{s\alpha - 1}{k-t-1} \frac{(-1)^t r^k s^{t-k}}{k!(p+t-k)!} X^t$$

modulo $X^p - (\alpha^p - \alpha)$, having set $k + h = p + t$ and taken $s^p \equiv s \pmod{p}$ into account.

Note that both sums are polynomials of degree less than p. Hence the rational expression $b'_{r,s}(\alpha)$ of Equation 5 can now be found by equating the coefficients of any suitable power of X in

$$b'_{r,s}(\alpha) \cdot L_{p-1}^{((r+s)\alpha)}\big((r+s)X\big) = b'_{r,s}(\alpha) \cdot \sum_{k=0}^{p-1} \binom{(r+s)\alpha - 1}{p-1-k} \frac{\big(-(r+s)X\big)^k}{k!},$$

and in the expression for $L_{p-1}^{(r\alpha)}(rX) \cdot L_{p-1}^{(s\alpha)}(sX)$ modulo $X^p - (\alpha^p - \alpha)$ found above.

Assuming $r + s \neq 0$ first, the coefficient of X^{p-1} in the former equals $-b'_{r,s}(\alpha)$, and in the latter it equals

$$\sum_{k=0}^{p-1} \binom{r\alpha - 1}{p-1-k} \binom{s\alpha - 1}{k} \frac{r^k s^{p-1-k}}{k!(p-1-k)!}.$$

Because $s^{p-1} \equiv 1 \pmod p$ and $1/\big(k!(p-1-k)!\big) \equiv -\binom{p-1}{k} \equiv -(-1)^k \pmod p$, we conclude that $b'_{r,s}(\alpha) = b_{r,s}(\alpha)$ in this case.

When $r+s = p$ the argument needs to be modified because $L_{p-1}^{((r+s)\alpha)}\big((r+s)X\big) = L_{p-1}^{(0)}(0) = 1$ has no term of degree $p-1$. Hence we compare constant terms instead, which is a little more complicated. The constant term in the reduced expression for $L_{p-1}^{(r\alpha)}(rX) \cdot L_{p-1}^{(-r\alpha)}(-rX)$ found above equals

$$\binom{r\alpha-1}{p-1}\binom{-r\alpha-1}{p-1} + r(\alpha^p-\alpha)\sum_{k=1}^{p-1}\binom{r\alpha-1}{p-1-k}\binom{-r\alpha-1}{k-1}\frac{(-1)^k}{k!(p-k)!}.$$

To deal with the first isolated summand note that $\binom{-r\alpha-1}{p-1} = 1-\alpha^{p-1}$ in $\mathbb{F}_p[\alpha]$, for example because its roots are $1/r, 2/r, \ldots, (p-1)/r$, hence exactly all nonzero elements of $\mathbb{F}_p$, and its leading term equals $(-r\alpha)^{p-1}/(p-1)! = \alpha^{p-1}$ (recalling that p is odd throughout the paper). The sum over k can be transformed using the congruence $k!(p-k)! \equiv (-1)^k k \pmod p$ for $0 < k < p$, and the standard binomial identity $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$. Altogether, the constant term in the reduced expression for $L_{p-1}^{(r\alpha)}(rX) \cdot L_{p-1}^{(-r\alpha)}(-rX)$ found earlier can be written as

$$(1-\alpha^{p-1})\sum_{k=0}^{p-1}\binom{r\alpha-1}{p-1-k}\binom{-r\alpha}{k} = (1-\alpha^{p-1})\binom{-1}{p-1} = 1-\alpha^{p-1}.$$

Comparing this with $b'_{r,p-r}(\alpha) \cdot L_{p-1}^{(0)}(0) = b'_{r,p-r}(\alpha)$ at the other side, we find $b'_{r,p-r}(\alpha) = 1-\alpha^{p-1}$ as desired. □

An inductive application of Lemma 10 now yields

$$\big(L_{p-1}^{(\alpha)}(X)\big)^j \equiv \Big(\prod_{s=1}^{j-1} b_{1,s}(\alpha)\Big) \cdot L_{p-1}^{(j\alpha)}(jX) \pmod{X^p - (\alpha^p-\alpha)}, \tag{6}$$

for $0 < j < p$, where the product over $s = 1, \ldots, j-1$ is interpreted as 1 when $j = 1$. After these preparations we are ready to prove Theorem 2.

Proof of Theorem 2. Let $G^{(\alpha)}(X)$ be an arbitrary polynomial of degree less than p in $\mathbb{F}_p(\alpha)[X]$ satisfying

$$G^{(\alpha)}\big(L_{p-1}^{(\alpha)}(X)\big) \equiv X \pmod{X^p - (\alpha^p-\alpha)}. \tag{7}$$

From the specialization $\alpha = 0$, where $L_{p-1}^{(0)}(X) = E(X)$ is the truncated exponential and hence $-\mathcal{L}_1\big(L_{p-1}^{(0)}(X)\big) \equiv X \pmod{X^p}$ with $\mathcal{L}_1(X) = \sum_{k=1}^{p-1} X^k/k$, we already know that $G^{(0)}(X) = -\mathcal{L}_1(X)$ (see the discussion after Theorem 2.) From this fact together with Equation (6) we expect a cleaner calculation if we write

$G^{(\alpha)}(X)$ directly in the form

$$G^{(\alpha)}(X) = c_0(\alpha) - \sum_{j=1}^{p-1} \frac{c_j(\alpha)}{j} \frac{X^j}{\prod_{s=1}^{j-1} b_{1,s}(\alpha)},$$

where $c_j(\alpha) \in \mathbb{F}_p(\alpha)$ are rational functions to be determined. According to Equation (6) then Equation (7) is equivalent to

$$c_0(\alpha) - \sum_{j=1}^{p-1} \frac{c_j(\alpha)}{j} L_{p-1}^{(j\alpha)}(jX) \equiv X \pmod{X^p - (\alpha^p - \alpha)}.$$

Because both sides are polynomials of degree less than p, the congruence must be an equality. Equating the coefficients of like powers of X on both sides, and because

$$L_{p-1}^{(j\alpha)}(jX) = -\sum_{k=0}^{p-1} (j\alpha - 1)_{p-1-k} \cdot (jX)^k$$

we find the system of linear equations

$$\sum_{j=1}^{p-1} (j\alpha - 1)_{p-1-k} \cdot j^{k-1} \cdot c_j(\alpha) = \begin{cases} -c_0(\alpha) & \text{if } k = 0 \\ 1 & \text{if } k = 1 \\ 0 & \text{if } 1 < k < p \end{cases} \tag{8}$$

for the expressions $c_j(\alpha)$, over the field $\mathbb{F}_p(\alpha)$.

Because $(j\alpha - 1)_{p-1} = (j\alpha)^{p-1} - 1 = \alpha^{p-1} - 1$, the first equation can be written as $(\alpha^{p-1} - 1) \sum_{j=1}^{p-1} j^{-1} \cdot c_j(\alpha) = -c_0(\alpha)$. As to the remaining equations, by successively adding to each equation a suitable linear combination of the equations which follow it, starting from the end, we show that the system is equivalent to

$$\sum_{j=1}^{p-1} j^{k-1} \cdot c_j(\alpha) = \begin{cases} c_0(\alpha)/(1 - \alpha^{p-1}) & \text{if } k = 0 \\ -1 & \text{if } k = 1 \\ 0 & \text{if } 1 < k < p \end{cases} \tag{9}$$

The last equation in (8), namely for $k = p - 1$, reads indeed $\sum_{j=1}^{p-1} j^{p-2} \cdot c_j(\alpha) = 0$, which is the last equation in (9). Now fix $0 < k < p - 1$, assume we have proved the conclusion for all equations with index higher than k (that is, we have already obtained the last $p - 1 - k$ equations in (9)), and consider the equation with index k in (8). If we expand the expression $(j\alpha - 1)_{p-1-k}$ in its left-hand side as a polynomial in α, each term except for the constant term gives rise to a scalar multiple (with scalar in $\mathbb{F}_p(\alpha)$) of the left-hand side of an equation in (9) with index larger than k. The constant term in $(j\alpha - 1)_{p-1-k}$ gives rise precisely to the left-hand side of the equation with index k in (9), multiplied by $(-1)^k(p - 1 - k)!$.

It is now an easy matter to see that the system (9) has the unique solution $c_0(\alpha) = 0$, and $c_j(\alpha) = 1$ for $0 < j < p$, as desired, using the fact that $\sum_{j=1}^{p-1} j^h$

is congruent to -1 modulo p if $p-1$ divides h, and to 0 otherwise. One may also view j as ranging over the multiplicative group $\mathbb{F}_p^*$, interpret equations (9) as performing a discrete Fourier transform over $\mathbb{F}_p^*$, and appropriately invert it. $\square$

Now we prove that the left inverse $G^{(\alpha)}(X)$ for $L_{p-1}^{(\alpha)}(X)$ is also a right inverse, in the appropriate sense stated in Corollary 3.

Proof of Corollary 3. Some care is needed to transfer the problem to a setting where we can use associativity of composition to pass from a unique left inverse to a right inverse, and a convenient setting is that of a ring of formal power series.

The modulus $X^p - (\alpha^p - \alpha)$ in the congruence of Theorem 2 becomes a pth power once we extend the field of coefficients to $\mathbb{F}_p(\alpha^{1/p})$. Viewing $L_{p-1}^{(\alpha)}(X)$ and $G^{(\alpha)}(X)$ as polynomials in $\mathbb{F}_p(\alpha^{1/p})[X]$, and replacing X with $X + \alpha - \alpha^{1/p}$, the congruence of Theorem 2 is equivalent to

$$G^{(\alpha)}\big(L_{p-1}^{(\alpha)}(X + \alpha - \alpha^{1/p})\big) - (\alpha - \alpha^{1/p}) \equiv X \pmod{X^p}$$

in the polynomial ring $\mathbb{F}_p(\alpha^{1/p})[X]$.

Set $\delta = L_{p-1}^{(\alpha)}(\alpha - \alpha^{1/p}) \in \mathbb{F}_p(\alpha^{1/p})$. The polynomial $L_{p-1}^{(\alpha)}(X + \alpha - \alpha^{1/p}) - \delta$ has no constant term, and nonzero term of degree one. Hence it has a compositional (bilateral) inverse $S(X)$ in the power series ring $\mathbb{F}_p(\alpha^{1/p})[[X]]$, meaning that

$$S\big(L_{p-1}^{(\alpha)}(X + \alpha - \alpha^{1/p}) - \delta\big) = X \tag{10}$$

and

$$L_{p-1}^{(\alpha)}\big(S(X) + \alpha - \alpha^{1/p}\big) - \delta = X \tag{11}$$

in $\mathbb{F}_p(\alpha^{1/p})[[X]]$. In particular, Equation (10) yields

$$S\big(L_{p-1}^{(\alpha)}(X + \alpha - \alpha^{1/p}) - \delta\big) \equiv X \pmod{X^p}$$

in $\mathbb{F}_p(\alpha^{1/p})[[X]]$, and because this congruence alone determines $S(X)$ modulo X^p uniquely, we deduce

$$S(X) \equiv G^{(\alpha)}(X + \delta) - (\alpha - \alpha^{1/p}) \pmod{X^p}. \tag{12}$$

Viewing Equation (11) modulo X^p and then taking Equation (12) into account we find

$$L_{p-1}^{(\alpha)}\big(G^{(\alpha)}(X + \delta)\big) - \delta \equiv X \pmod{X^p},$$

in $\mathbb{F}_p(\alpha^{1/p})[[X]]$, but because this congruence involves only polynomials it already takes place in in $\mathbb{F}_p(\alpha^{1/p})[X]$. Substituting $X - \delta$ for X we find

$$L_{p-1}^{(\alpha)}\big(G^{(\alpha)}(X)\big) \equiv X \pmod{X^p - L_{p-1}^{(\alpha^p)}(\alpha^p - \alpha)},$$

and this takes place and holds in $\mathbb{F}_p(\alpha)[X]$, as desired. $\square$

4. Factorizations of the polynomials $b_{1,s}(\alpha)$

In this section we compute the full factorizations in $\mathbb{F}_p[\alpha]$ of the polynomials $b_{1,s}(\alpha)$, which will give a more explicit description of the generalized truncated logarithm $G^{(\alpha)}(X)$. The first step is establishing that all roots in a splitting field are simple and belong to the prime field $\mathbb{F}_p$. One way to show that is by proving the identity of Lemma 11 below, which we will do by suitable manipulations of products of Laguerre polynomials.

Lemma 11. *The polynomials $b_{1,s}(\alpha)$, for $0 < s < p-1$, satisfy*

$$b_{1,s}(\alpha) \cdot b_{1,s}(-\alpha) = 1 - \alpha^{p-1}.$$

In particular, $b_{1,s}(\alpha)$ has degree $(p-1)/2$, and factorizes into a product of distinct linear factors in $\mathbb{F}_p[\alpha]$.

Proof. We prove the claimed equation by induction on s, using the congruences of Lemma 10 and omitting the modulus $X^p - (\alpha^p - \alpha)$ for conciseness. The case $s = 1$ follows by computing

$$\begin{aligned}(1-\alpha^{p-1})^2 &\equiv \left(L_{p-1}^{(\alpha)}(X) \cdot L_{p-1}^{(-\alpha)}(-X)\right)^2 \\ &= L_{p-1}^{(\alpha)}(X)^2 \cdot L_{p-1}^{(-\alpha)}(-X)^2 \\ &\equiv b_{1,1}(\alpha) \cdot L_{p-1}^{(2\alpha)}(2X) \cdot b_{1,1}(-\alpha) \cdot L_{p-1}^{(-2\alpha)}(-2X) \\ &= b_{1,1}(\alpha) \cdot b_{1,1}(-\alpha) \cdot (1-\alpha^{p-1}).\end{aligned}$$

Now let $1 < s < p-1$ and assume we have proved $b_{1,t}(\alpha) \cdot b_{1,t}(-\alpha) = 1 - \alpha^{p-1}$ for $0 < t < s$. Then the induction step follows by computing

$$\begin{aligned}(1-\alpha^{p-1})^{s+1} &\equiv \left(L_{p-1}^{(\alpha)}(X) \cdot L_{p-1}^{(-\alpha)}(-X)\right)^{s+1} \\ &= L_{p-1}^{(\alpha)}(X)^{s+1} \cdot L_{p-1}^{(-\alpha)}(-X)^{s+1} \\ &\equiv \Big(\prod_{t=1}^{s} b_{1,t}(\alpha)\Big) \cdot L_{p-1}^{((s+1)\alpha)}((s+1)X) \\ &\quad \cdot \Big(\prod_{t=1}^{s} b_{1,t}(-\alpha)\Big) \cdot L_{p-1}^{(-(s+1)\alpha)}(-(s+1)X) \\ &= b_{1,s}(\alpha) \cdot b_{1,s}(-\alpha) \cdot (1-\alpha^{p-1})^s.\end{aligned}$$

The statement on the factorization of $b_{1,s}(\alpha)$ follows at once. □

Theorem 5 follows at once. Lemma 11 also tells us that exactly one of each pair of opposite elements of $\mathbb{F}_p^*$ is a root of a given $b_{1,s}(\alpha)$. The following result determines precisely which of them.

Theorem 12. *Let $0 < s < p-1$, and let $0 < a, a' < p$ be integers such that $a' \equiv sa \pmod{p}$. Then $b_{1,s}(a) = 0$ if and only if $a + a' < p$.*

Note that we cannot have $a+a'=p$ because we have assumed $s \not\equiv -1 \pmod{p}$, and so either $a+a'<p$ or $a+a'>p$.

Proof. Suppose first that $a+a'<p$. We have already mentioned that $b_{1,s}(a)$ equals the coefficient of X^{p-1} in the product $(1+X)^{a-1}(1-X/s)^{sa-1} \in \mathbb{F}_p[X]$. Writing $sa = a' + kp$ for some integer $k \geq 0$ we may write

$$(1+X)^{a-1}(1-X/s)^{sa-1} = (1+X)^{a-1}(1-X/s)^{a'-1}\big(1-(X/s)^p\big)^k$$

in $\mathbb{F}_p[X]$. Hence $b_{1,s}(a)$ equals the coefficient of X^{p-1} in the product $(1+X)^{a-1}(1-X/s)^{a'-1}$, which is zero because this polynomial has degree $a+a'-2<p-2$.

Now suppose that $a+a'>p$. Then $(p-a)+(p-a')<p$, applying the implication already proved to $p-a$ in place of a and $p-a'$ in place of a' shows $b_{1,s}(p-a)=0$, which is the same as $b_{1,s}(-a)=0$. According to Lemma 11 this implies $b_{1,s}(a)\neq 0$, which is the desired conclusion. □

Remark 13. Using Lucas' theorem on binomial coefficients modulo p, Theorem 12 admits the following equivalent formulation, which may in some cases be more convenient to apply. Let $0<s<p-1$ and $0<a<p$. Then $b_{1,s}(a)=0$ if and only if p does not divide the binomial coefficient $\binom{a+sa}{a}$.

Theorem 12 gives an explicit way of writing out the complete factorization of each $b_{1,s}(\alpha)$. For example, when $s=1$ in the notation of Theorem 12 we have $a'=a$, and hence the condition $a+a'<p$ reads $a\leq (p-1)/2$. Knowing that the polynomial has constant term 1 yields $b_{1,1}(\alpha)=\prod_{a=1}^{(p-1)/2}(1-\alpha/a)$. The equivalent expression $b_{1,1}(\alpha)=(-1)^{(p-1)/2}\binom{\alpha-1}{(p-1)/2}$ could also be obtained directly by recognizing an alternating sign Chu-Vandermonde convolution in the defining Equation (2). The latter route is not an option when $s=2$, in which case Theorem 12 easily yields

$$b_{1,2}(\alpha) = \Bigg(\prod_{0<a<p/3}(1-\alpha/a)\Bigg)\cdot\Bigg(\prod_{p/2<a<2p/3}(1-\alpha/a)\Bigg).$$

For a further example consider the case of $s=(p-1)/2$. In the notation of Theorem 12, when a is odd we have $a'=(p-a)/2$, whence $a+a'=(p+a)/2<p$, and when a is even we have $a'=p-a/2$, whence $a+a'=p+a/2>p$. Consequently, the roots of $b_{1,(p-1)/2}(\alpha)$ are $1,3,5,\ldots,p-2$ (viewed as elements of $\mathbb{F}_p$), and hence

$$b_{1,(p-1)/2}(\alpha) = (-1)^{\frac{p+1}{2}}\binom{(\alpha-1)/2}{(p-1)/2}.$$

As a more substantial application of Theorem 12, we next use it to establish a symmetry property of the polynomials $b_{1,s}(\alpha)$.

Corollary 14. *For $0<s<p-1$ we have $b_{1,s}(\alpha)=b_{1,p-1-s}(\alpha)$.*

Proof. Because the two polynomials have the same constant term 1, and each has distinct roots, it is sufficient to show that those roots are the same. Also, by symmetry reasons it is sufficient to show that if $b_{1,s}(a) = 0$ for some $0 < a < p$, then $b_{1,p-1-s}(a) = 0$. In fact, according to Theorem 12 the latter condition holds exactly when $a + a' < p$, where $0 < a' < p$ is uniquely determined by $a' \equiv sa \pmod{p}$. But then $p - a - a' \equiv (p - 1 - s)a \pmod{p}$ and $0 < p - a - a' < p$, and because $0 < a + (p - a - a') = p - a' < p$ another application of Theorem 12 yields $b_{1,p-1-s}(a) = 0$, as desired. □

Remark 15. With the alternate interpretation of Remark 13, one can also prove Corollary 14 by noting that $\binom{a+(p-1-s)a}{a} = \binom{pa-sa}{a} \equiv \binom{-sa}{a} \pmod{p}$, and then $\binom{-sa}{a} = (-1)^a\binom{a+sa-1}{a} = (-1)^a\frac{s}{s+1}\binom{a+sa}{a}$.

We can also use Theorem 12 to compute the coefficient of X^{p-1} in $G^{(\alpha)}(X)$, which equals the reciprocal of the product $\prod_{s=1}^{p-2} b_{1,s}(\alpha)$.

Corollary 16. *We have*

$$\prod_{s=1}^{p-2} b_{1,s}(\alpha) = \prod_{k=2}^{p-1}(1 + \alpha/k)^{k-1} = \frac{L_{p-1}^{(\alpha^p)}(\alpha^p - \alpha)}{1 - \alpha^{p-1}}.$$

Proof. Fix $0 < a < p$. As s ranges over $0 < s < p-1$, the residue class of sa ranges over all residue classes modulo p with the exception of the classes of 0 and of $-a$. Consequently, the conditions $a' \equiv sa \pmod{p}$ and $0 < a' < p - a$ of Theorem 12 will be simultaneously satisfied for exactly $p - a - 1$ values of s. This means that a will be a root, and a single root as we know, of exactly $p - a - 1$ of the factors in the product $\prod_{s=1}^{p-2} b_{1,s}(\alpha)$. This proves the first claimed equality. The second equality follows from Equation (3), which was proved in [AM15b, Lemma 1]. □

In the proof of Theorem 12 we have used the fact that if a is positive integer then $b_{r,s}(a)$ equals the coefficient of X^{p-1} in the polynomial $(1+X/r)^{ra-1}(1-X/s)^{sa-1} \in \mathbb{F}_p[X]$. We conclude this section with noting that a similar fact holds true for $b_{r,s}(\alpha)$ as a polynomial, provided that we make sense of powers with exponents $r\alpha - 1$ and $s\alpha - 1$.

The obstacle here is that $(1+X/r)^{r\alpha-1}$ does not have a meaning over the field $\mathbb{F}_p$ if α is an indeterminate. If C is any commutative ring containing $\mathbb{Q}$ as a subring, then for any $c \in C$ we have a binomial series defined as

$$(1 + X)^c = \sum_{k=0}^{\infty} \binom{c}{k} X^k \in C[[X]].$$

This does not generally make sense in prime characteristic p because the binomial coefficients $\binom{c}{k} = c(c - 1)\cdots(c - k + 1)/k!$ involve division by p when $k \geq p$. One way to find a useable substitute is by truncating the series before its term of

degree p. Limiting ourselves, for simplicity, to coefficients in the field of rational functions $\mathbb{F}_p(\alpha)$, for each $f(\alpha) \in \mathbb{F}_p(\alpha)$ we define a polynomial

$$(1+X)_*^{f(\alpha)} = \sum_{k=0}^{p-1} \binom{f(\alpha)}{k} X^k \in \mathbb{F}_p(\alpha)[X].$$

Then for $f(\alpha), g(\alpha) \in \mathbb{F}_p(\alpha)$ we have

$$(1+X)_*^{f(\alpha)+g(\alpha)} \equiv (1+X)_*^{f(\alpha)}(1+X)_*^{g(\alpha)} \pmod{X^p}$$

in $\mathbb{F}_p(\alpha)[X]$. Also, taking the derivative with respect to X of such a product of truncated binomials, or of variations such as $(1+bX)^{f(\alpha)}$, satisfies Leibniz rule modulo X^p. (In formal algebraic terms this means that the standard derivation d/dX of the polynomial ring $\mathbb{F}_p(\alpha)[X]/(X^p)$ induces a derivation of its quotient ring $\mathbb{F}_p(\alpha)[X]/(X^p)$, because it maps the factored ideal (X^p) into itself.) However, we have

$$\frac{d}{dX}(1+X)_*^{f(\alpha)} = f(\alpha)(1+X)_*^{f(\alpha)-1} + \big(f(\alpha)^p - f(\alpha)\big)X^{p-1}.$$

With this definition, the expression $b_{r,s}(\alpha)$ equals the coefficient of X^{p-1} in the polynomial $(1+X/r)_*^{r\alpha-1}(1-X/s)_*^{s\alpha-1}$. As a simple application, we have

$$b_{r,r}(\alpha) = (-1)^{\frac{p-1}{2}} \binom{r\alpha-1}{\frac{p-1}{2}},$$

because this is the coefficient of X^{p-1} in $(1-X^2/r^2)^{r\alpha-1}$. A less trivial application gives the following alternate expression for the polynomials $b_{r,s}(\alpha)$.

Lemma 17. *If $r+s \neq p$ then*

$$b_{r,s}(\alpha) = \sum_{k=0}^{p-1} (-r/s)^k \binom{r\alpha-1}{p-1-k}\binom{s\alpha}{k}.$$

This expression for $b_{r,s}(\alpha)$ would have naturally come up in the proof of Lemma 10, had we compared the coefficients of X^0 rather than X^{p-1} in the general case $r+s \neq p$ as well.

Proof. The lemma claims that $b_{r,s}(\alpha)$ equals the coefficient of X^{p-1} in the polynomial $(1+X/r)_*^{r\alpha-1}(1-X/s)_*^{s\alpha}$, rather than in the polynomial $(1+X/r)_*^{r\alpha-1}(1-X/s)_*^{s\alpha-1}$ as in the defining Equation (2). Hence it suffices to show that the coefficient of X^{p-1} is the same in those two polynomials.

We start with the polynomial $(1+X/r)_*^{r\alpha}(1-X/s)_*^{s\alpha}$ and note that its derivative (with respect to X) has no term of degree $p-1$ (because the derivative of X^p vanishes). The derivative of this product equals

$$\begin{aligned}&\big(\alpha(1+X/r)_*^{r\alpha-1} + (\alpha^p-\alpha)X^{p-1}\big)\cdot(1-X/s)_*^{s\alpha} \\ &\quad - (1+X/r)_*^{r\alpha}\cdot\big(\alpha(1-X/s)_*^{s\alpha-1} + (\alpha^p-\alpha)X^{p-1}\big).\end{aligned}$$

Consequently, there is no term of degree $p-1$ in

$$\alpha(1+X/r)_*^{r\alpha-1}(1-X/s)_*^{s\alpha} - \alpha(1+X/r)_*^{r\alpha}(1-X/s)_*^{s\alpha-1},$$

which in turn equals

$$\frac{(r+s)\alpha}{r}\cdot(1+X/r)_*^{r\alpha-1}(1-X/s)_*^{s\alpha} - \frac{(r+s)\alpha}{r}\cdot(1+X/r)_*^{r\alpha-1}(1-X/s)_*^{s\alpha-1}.$$

Because $r+s \neq p$ the desired conclusion follows. □

5. Proofs of Theorem 6 and Theorem 8

Exploiting several properties of the polynomials $b_{1,s}(\alpha)$ which we have proved in Section 3 we can finally prove the functional equation for the polynomials $G^{(\alpha)}(X)$ announced in Theorem 6.

Proof of Theorem 6. We have

$$\begin{aligned}
\frac{X^p}{\alpha^{p-1}-1}G^{(-\alpha)}\left(\frac{1-\alpha^{p-1}}{X}\right) &= \sum_{k=1}^{p-1}\frac{X^{p-k}}{k}\frac{(1-\alpha^{p-1})^{k-1}}{\prod_{s=1}^{k-1}b_{1,s}(-\alpha)} \\
&= \sum_{k=1}^{p-1}\left(\prod_{s=1}^{k-1}b_{1,s}(\alpha)\right)\frac{X^{p-k}}{k} && \text{by Lemma 11} \\
&= -\sum_{k=1}^{p-1}\left(\prod_{s=1}^{p-k-1}b_{1,s}(\alpha)\right)\frac{X^{k}}{k} \\
&= -\sum_{k=1}^{p-1}\left(\prod_{s=k}^{p-2}b_{1,s}(\alpha)\right)\frac{X^{k}}{k} && \text{by Corollary 14} \\
&= -\prod_{r=1}^{p-2}b_{1,r}(\alpha)\cdot\sum_{k=1}^{p-1}\frac{1}{k}\frac{X^k}{\prod_{s=1}^{k-1}b_{1,s}(\alpha)} \\
&= \prod_{k=2}^{p-1}(1+\alpha/k)^{k-1}\cdot G^{(\alpha)}(X) && \text{by Corollary 16.}
\end{aligned}$$

The desired equation follows upon multiplication by $1-\alpha^{p-1} = \prod_{k=1}^{p-1}(1+\alpha/k)$. □

We conclude this section with proving Theorem 8.

Proof of Theorem 8. Quoting Equation (6), we have

$$\big(L_{p-1}^{(\alpha)}(X)\big)^h \equiv \left(\prod_{s=1}^{h-1}b_{1,s}(\alpha)\right)\cdot L_{p-1}^{(h\alpha)}\big(hX\big) \pmod{X^p-(\alpha^p-\alpha)},$$

for $0<h<p$. In essence, we now would like to apply $G^{(h\alpha)}$ to both sides after dividing them by $\prod_{s=1}^{h-1}b_{1,s}(\alpha)$, and then regard $L_{p-1}^{(\alpha)}(X)$ as the new variable.

However, some care is required to put the change of variable on a rigorous ground, as we are dealing with congruences.

As in the proof of Corollary 3, we extend the field of coefficients of the polynomial ring to $\mathbb{F}_p(\alpha^{1/p})$, so that the modulus $X^p-(\alpha^p-\alpha)$ becomes a pth power. Rename the indeterminate X to x, view $L_{p-1}^{(\alpha)}(x)$ as a polynomial in $\mathbb{F}_p(\alpha^{1/p})[x]$, replace x with $x+\alpha-\alpha^{1/p}$, and divide both sides by $\prod_{s=1}^{h-1} b_{1,s}(\alpha)$. The above congruence then reads

$$\frac{\big(L_{p-1}^{(\alpha)}(x+\alpha-\alpha^{1/p})\big)^h}{\prod_{s=1}^{h-1} b_{1,s}(\alpha)} \equiv L_{p-1}^{(h\alpha)}\big(h(x+\alpha-\alpha^{1/p})\big) \pmod{x^p}$$

in the polynomial ring $\mathbb{F}_p(\alpha^{1/p})[x]$, but we rather view it in the power series ring $\mathbb{F}_p(\alpha^{1/p})[[x]]$. In this setting we can apply the change of indeterminate (or uniformizing parameter)

$$\delta - X = L_{p-1}^{(\alpha)}(x+\alpha-\alpha^{1/p}),$$

where $\delta = L_{p-1}^{(\alpha)}(\alpha-\alpha^{1/p}) \in \mathbb{F}_p(\alpha^{1/p})$. According to Theorem 2 we then have

$$G^{(\alpha)}(\delta - X) \equiv x+\alpha-\alpha^{1/p} \pmod{X^p}$$

in the power series ring $\mathbb{F}_p(\alpha^{1/p})[[X]] = \mathbb{F}_p(\alpha^{1/p})[[x]]$.

Now we are in a position to apply $G^{(h\alpha)}$ to both sides of our congruence, and taking Theorem 2 into account (with $h\alpha$ in place of α and $h(x+\alpha-\alpha^{1/p})$ in place of X) we get

$$G^{(h\alpha)}\left(\frac{(\delta-X)^h}{\prod_{s=1}^{h-1} b_{1,s}(\alpha)}\right) \equiv hG^{(\alpha)}(\delta-X) \pmod{X^p}$$

in $\mathbb{F}_p(\alpha^{1/p})[[X]]$. However, this congruence actually takes place in the polynomial ring $\mathbb{F}_p(\alpha^{1/p})[X]$, and then replacing X with $\delta - X$ we find

$$G^{(h\alpha)}\left(\frac{X^h}{\prod_{s=1}^{h-1} b_{1,s}(\alpha)}\right) \equiv hG^{(\alpha)}(X) \pmod{X^p-\delta^p},$$

which takes place in $\mathbb{F}_p(\alpha)[X]$ because $\delta^p = L_{p-1}^{(\alpha^p)}(\alpha^p-\alpha)$, and is the desired conclusion. □

6. A connection with Jacobi polynomials

In this section we discuss how our polynomials $b_{r,s}(\alpha)$ of Equation (2) relate to certain Jacobi polynomials viewed modulo p. Standard definitions and properties of Jacobi polynomials can be found in the the classical book by Szegö on orthogonal polynomials [Sze75], but readers should note that purely combinatorial proofs of those properties were presented in [LS85].

The classical n-th Jacobi polynomial $P_n^{(\alpha,\beta)}(x)$, for n a non-negative integer, are given by

$$P_n^{(\alpha,\beta)}(x) = \frac{1}{2^n} \sum_{k=0}^{n} \binom{\alpha+n}{n-k} \binom{\beta+n}{k} (x+1)^{n-k}(x-1)^k.$$

Here α and β are parameters, but because $P_n^{(\alpha,\beta)}(x)$ depends polynomially on them we may also view it as a polynomial in three indeterminates, $P_n^{(\alpha,\beta)}(x) \in \mathbb{Q}[\alpha,\beta,x]$.

For p an odd prime, the coefficients of the polynomials $P_{p-1}^{(\alpha,\beta)}(x)$ are p-integral rational numbers, and hence they may be viewed modulo p. Because $2^{p-1} \equiv 1 \pmod{p}$ we have

$$P_{p-1}^{(\alpha,\beta)}(x) \equiv \sum_{k=0}^{p-1} \binom{\alpha-1}{p-1-k} \binom{\beta-1}{k} (x+1)^{p-1-k}(x-1)^k \pmod{p}.$$

Setting $x = (s-r)/(s+r)$ for $0 < r, s < p$ with $r+s \neq p$ we find

$$b_{r,s}(\alpha) \equiv P_{p-1}^{(r\alpha,s\alpha)}\big((s-r)/(s+r)\big) \pmod{p},$$

where we are slightly abusing notation as the right-hand side is a polynomial with p-integral coefficients while $b_{r,s}(\alpha)$ has coefficients in $\mathbb{F}_p$ by our definition. Keeping the same abuse of notation we will now exploit this connection to recover some of the properties of the polynomials $b_{r,s}(\alpha)$.

Beyond the obvious identity $P_n^{(\alpha,\beta)}(x) = (-1)^n P_n^{(\beta,\alpha)}(-x)$, which yields the equally obvious symmetry $b_{r,s}(\alpha) = b_{s,r}(\alpha)$, Jacobi polynomials satisfy

$$(2p+\alpha+\beta) \cdot \frac{x+1}{2} \cdot P_{p-1}^{(\alpha,\beta+1)}(x) = (p+\beta)P_{p-1}^{(\alpha,\beta)}(x) + pP_p^{(\alpha,\beta)}(x)$$

for all positive integers p. This identity is [Sze75, Equation (4.5.4)], where we have written $p-1$ in place of the customary n. With p an odd prime as in the present context, note that the coefficients of $P_p^{(\alpha,\beta)}(x)$ are not all p-integral, but those of $pP_p^{(\alpha,\beta)}(x)$ are, and in fact

$$\begin{aligned} pP_p^{(\alpha,\beta)}(x) &= \frac{p}{2^p} \sum_{k=0}^{p} \binom{\alpha+p}{p-k} \binom{\beta+p}{k} (x+1)^{p-k}(x-1)^k \\ &\equiv \frac{p}{2}\binom{\alpha+p}{p}(x+1)^p + \frac{p}{2}\binom{\beta+p}{p}(x-1)^p \pmod{p} \\ &\equiv \tfrac{1}{2}(\alpha-\alpha^p)(x+1)^p + \tfrac{1}{2}(\beta-\beta^p)(x-1)^p \pmod{p}. \end{aligned}$$

Setting $x = (s-r)/(s+r)$, and replacing α and β with $r\alpha$ and $s\alpha$, respectively, we find

$$P_{p-1}^{(r\alpha,s\alpha+1)}\left(\frac{s-r}{s+r}\right) \equiv P_{p-1}^{(r\alpha,s\alpha)}\left(\frac{s-r}{s+r}\right) \pmod{p},$$

whose left-hand side corresponds to the alternate expression for $b_{r,s}(\alpha)$ which we found in Lemma 17.

Finally, Jacobi polynomials satisfy

$$P_n^{(\alpha,\beta)}(x) = \left(\frac{x+1}{2}\right)^n P_n^{(\alpha,-2n-\alpha-\beta-1)}\left(\frac{3-x}{x+1}\right),$$

which is [Sze75, Equation (4.22.1)]. With the appropriate specializations as above this yields the first of the following congruences

$$P_{p-1}^{(\alpha,s\alpha)}\left(\frac{s-1}{s+1}\right) \equiv P_{p-1}^{(\alpha,(-s-1)\alpha+1)}\left(\frac{s+2}{s}\right) \equiv P_{p-1}^{(\alpha,(-s-1)\alpha)}\left(\frac{s+2}{s}\right) \pmod{p},$$

and the second one is the one found above corresponding to Lemma 17. Altogether, we have recovered that $b_{1,s}(\alpha) = b_{1,-1-s}(\alpha)$ for $0 < s < p-1$, which is our Corollary 14.

References

[AM05] Marina Avitabile and Sandro Mattarei, *Thin Lie algebras with diamonds of finite and infinite type*, J. Algebra **293** (2005), no. 1, 34–64. MR 2173965 (2006f:17018)

[AM07] ———, *Thin loop algebras of Albert-Zassenhaus algebras*, J. Algebra **315** (2007), no. 2, 824–851. MR 2351896 (2008h:17022)

[AM15a] ———, *Grading switching for modular non-associative algebras*, Lie algebras and related topics, Contemp. Math., vol. 652, Amer. Math. Soc., Providence, RI, 2015, pp. 1–14. MR 3453046

[AM15b] ———, *Laguerre polynomials of derivations*, Israel J. Math. **205** (2015), no. 1, 109–126. MR 3314584

[BW82] R. E. Block and R. L. Wilson, *The simple Lie p-algebras of rank two*, Ann. of Math. (2) **115** (1982), no. 1, 93–168. MR 644017 (83j:17008)

[Kon02] Maxim Kontsevich, *The $1\frac{1}{2}$-logarithm. Appendix to: "On poly(ana)logs. I" [Compositio Math* **130** *(2002), no. 2, 161–210; MR1883818 (2002m:11059)] by P. Elbaz-Vincent and H. Gangl*, Compositio Math. **130** (2002), no. 2, 211–214. MR 1884238 (2002m:11060)

[LS85] Pierre Leroux and Volker Strehl, *Jacobi polynomials: combinatorics of the basic identities*, Discrete Math. **57** (1985), no. 1-2, 167–187. MR 816058

[Mat05] Sandro Mattarei, *Artin-Hasse exponentials of derivations*, J. Algebra **294** (2005), no. 1, 1–18. MR 2171626

[Mat06] ———, *Exponential functions in prime characteristic*, Aequationes Math. **71** (2006), no. 3, 311–317. MR 2236408 (2007b:39056)

[Mir05] Dmitry Mirimanoff, *L'équation indéterminée $x^\ell + y^\ell + z^\ell = 0$ et le critérium de Kummer*, J. Reine Angew. Math. **128** (1905), 45–68. MR 1580644

[MT13] Sandro Mattarei and Roberto Tauraso, *Congruences for central binomial sums and finite polylogarithms*, J. Number Theory **133** (2013), no. 1, 131–157. MR 2981405

[MT18] ———, *From generating series to polynomial congruences*, J. Number Theory **182** (2018), 179–205. MR 3703936

[Pre86] A. A. Premet, *Cartan subalgebras of Lie p-algebras*, Izv. Akad. Nauk SSSR Ser. Mat. **50** (1986), no. 4, 788–800, 878–879. MR 88d:17012

[Sze75] Gábor Szegő, *Orthogonal polynomials*, fourth ed., American Mathematical Society, Providence, R.I., 1975, American Mathematical Society, Colloquium Publications, Vol. XXIII. MR 0372517 (51 #8724)

[Win69] D. J. Winter, *On the toral structure of Lie p-algebras*, Acta Math. **123** (1969), 69–81. MR 0251095 (40 #4326)

E-mail address: marina.avitabile@unimib.it

Dipartimento di Matematica e Applicazioni, Università degli Studi di Milano - Bicocca, via Cozzi 55, I-20125 Milano, Italy

E-mail address: smattarei@lincoln.ac.uk

Charlotte Scott Centre for Algebra, University of Lincoln, Brayford Pool Lincoln, LN6 7TS, United Kingdom