



Finite and p -adic Polylogarithms

AMNON BESSER

Department of Mathematics, Ben-Gurion University of the Negev, PO Box 84105, Beer-Sheva, Israel. e-mail: bessera@math.bgu.ac.il

(Received: 13 July 2000)

Abstract. The finite n th polylogarithm $li_n(z) \in \mathbb{Z}/p[z]$ is defined as $\sum_{k=1}^{p-1} z^k/k^n$. We state and prove the following theorem. Let $Li_k: \mathbb{C}_p \rightarrow \mathbb{C}_p$ be the p -adic polylogarithms defined by Coleman. Then a certain linear combination F_n of products of polylogarithms and logarithms, with coefficients which are independent of p , has the property that $p^{1-n}DF_n(z)$ reduces modulo $p > n + 1$ to $li_{n-1}(\sigma(z))$, where D is the Cathelineau operator $z(1-z)d/dz$ and σ is the inverse of the p -power map. A slightly modified version of this theorem was conjectured by Kontsevich. This theorem is used by Elbaz-Vincent and Gangl to deduce functional equations of finite polylogarithms from those of complex polylogarithms.

Mathematics Subject Classifications (2000). 11G55, 11S80, 11T06.

Key words. Polylogarithms, p -adic integration, Functional equations

1. Introduction

The finite logarithm was introduced by Kontsevich (under the name ‘The $1\frac{1}{2}$ logarithm’) in [5]. The finite logarithm is the case $n = 1$ of the n th polylogarithm $li_n \in \mathbb{Z}/p[z]$ defined by $li_n(z) = \sum_{k=1}^{p-1} z^k/k^n$. Also, Kontsevich proved that the finite logarithm satisfies a 4-term functional equation, known as the fundamental equation of information theory. The same functional equation is satisfied by the so-called infinitesimal dilogarithm $-(x \log |x| + (1-x) \log |1-x|)$. Cathelineau [2] defined general infinitesimal polylogarithms and found that they satisfy interesting functional equations. It was the idea of Elbaz-Vincent and Gangl [4] that these functional equations should be satisfied by finite polylogarithms (The name ‘finite polylogarithm’ is due to them). Inspired by their work, Kontsevich raised the idea that the finite polylogarithm could be a reduction of an infinitesimal version of the p -adic polylogarithm, as defined by Coleman [3]. If such a connection is established, it makes sense to hope that functional equations of the infinitesimal p -adic polylogarithm can be established in a similar way to its complex counterpart and that these then imply by reduction the functional equations of the finite polylogs. A conjectural formula for the precise p -adic polylog whose ‘derivative’, in the sense to be explained below, reduces to the finite polylog was formulated by Kontsevich and proved by him for small n . The purpose of this short note is to prove such a connection between p -adic polylogarithms and finite polylogarithms.

To state the main result we recall that Coleman defined p -adic polylogarithms, $\text{Li}_n: \mathbb{C}_p \rightarrow \mathbb{C}_p$. These functions are locally analytic in the sense that they are given by a convergent power series on each residue disc in \mathbb{C}_p and they satisfy the relations $\text{Li}_0(z) = z/(1 - z)$ and $d\text{Li}_n(z) = \text{Li}_{n-1}(z) dz/z$. We define the differential operator D by $D = z(1 - z)d/dz$. Let $\bar{\mathbb{F}}_p$ be the algebraic closure of the finite field with p elements and let $W = W(\bar{\mathbb{F}}_p)$ be the ring of Witt vectors of $\bar{\mathbb{F}}_p$, so W is the ring of integers of the maximal unramified extension of \mathbb{Q}_p . Let $\sigma: \bar{\mathbb{F}}_p \rightarrow \bar{\mathbb{F}}_p$ be the automorphism which is the inverse of the p -power map. Let $X = \{z \in W: |z| = |z - 1| = 1\}$. Our main result is then:

THEOREM 1.1. *For every $n > 1$ let*

$$F_n(z) = \sum_{k=0}^{n-1} a_k \log^k(z) \text{Li}_{n-k}(z),$$

with $a_0 = -n$ and

$$a_k = \frac{(-1)^k}{(k-1)!} + \frac{(-1)^{k+1}n}{k!},$$

for $k > 0$. Then the following holds for every $p > n + 1$: One has $DF_n(X) \subset p^{n-1}W$ and for every $z \in X$ one has $p^{1-n}DF_n(z) \equiv \text{li}_{n-1}(\sigma(z)) \pmod{p}$. Furthermore, the choice of the coefficients a_k is the unique choice of coefficients in \mathbb{Q} for which the theorem holds for all $p > n + 1$.

We remark that for a given p there will be many other choices of coefficients, for example those which are sufficiently congruent to the a_k .

2. The Proof

The connection between p -adic and finite polylogarithms is made by the following

PROPOSITION 2.1. *Let $\text{Li}_n^{(p)}(z) := \text{Li}_n(z) - \text{Li}_n(z^p)/p^n$. Then $\text{Li}_n^{(p)}(X) \subset W$ and the function $\text{Li}_n^{(p)}$ reduces modulo p to $(1 - z^p)^{-1}\text{li}_n(z)$.*

Proof. According to [3], the function $\text{Li}_n^{(p)}(z)$ can be computed as

$$\text{Li}_n^{(p)}(z) = \int_{\mathbb{Z}_p^\times} x^{-n} d\mu_z(x),$$

where μ_z is the measure on \mathbb{Z}_p defined by

$$\mu_z(a + p^m\mathbb{Z}_p) = \frac{z^a}{1 - z^{p^m}}, \quad a = 0, 1, \dots, p^m - 1.$$

Since for $z \in X$ μ_z takes integral values, this shows the first statement. Reducing modulo p we may replace the function $x \mapsto x^{-k}$ by the function $x \mapsto a^{-k}$ if

$x \equiv a \pmod{p}$, which is congruent to it modulo p on \mathbb{Z}_p^\times . This implies that $\text{Li}_n^{(p)}(z)$ is congruent modulo p to

$$\sum_{a=1}^{p-1} a^{-n} \mu_z(a + p\mathbb{Z}_p) = \sum_{a=1}^{p-1} a^{-n} \frac{z^a}{1 - z^p}.$$

COROLLARY 2.2. *Let $\alpha \in X$ be a root of unity. Then we have $\text{Li}_n(\alpha) \in p^n W$ and $p^{-n} \text{Li}_n(\alpha) \equiv -\text{li}_n(\sigma(\alpha))/(1 - \alpha) \pmod{p}$.*

Proof. Since $\alpha \in X \subset W$ the order of α is prime to p and we have $\alpha^{p^k} = \alpha$ for some k . By using the definition of $\text{Li}_n^{(p)}$ repeatedly we find

$$\begin{aligned} \text{Li}_n(\alpha) &= \text{Li}_n^{(p)}(\alpha) + p^{-n} \text{Li}_n(\alpha^p) \\ &= \text{Li}_n^{(p)}(\alpha) + p^{-n} \text{Li}_n^{(p)}(\alpha^p) + p^{-2n} \text{Li}_n(\alpha^{p^2}) \\ &\dots = \sum_{i=0}^{k-1} p^{-in} \text{Li}_n^{(p)}(\alpha^{p^i}) + p^{-kn} \text{Li}_n(\alpha^{p^k}). \end{aligned}$$

Since $\alpha^{p^k} = \alpha$ we may move the last term to the left-hand side of the equation and obtain

$$\begin{aligned} \text{Li}_n(\alpha) &= \frac{1}{1 - p^{-kn}} \sum_{i=0}^{k-1} p^{-in} \text{Li}_n^{(p)}(\alpha^{p^i}) \\ &= \frac{p^n}{p^{kn} - 1} \sum_{i=0}^{k-1} p^{(k-1-i)n} \text{Li}_n^{(p)}(\alpha^{p^i}) \in p^n W, \end{aligned}$$

and dividing by p^n and reducing modulo p we obtain using the proposition

$$\begin{aligned} -\text{Li}_n^{(p)}(\alpha^{p^{k-1}}) &\equiv (1 - (\alpha^{p^{k-1}})^p)^{-1} \text{li}_n(\alpha^{p^{k-1}}) \\ &\equiv -\text{li}_n(\sigma(\alpha))/(1 - \alpha) \pmod{p}. \end{aligned}$$

PROPOSITION 2.3. *Let α be a root of unity in X . Set $\tilde{\text{Li}}_n(\alpha) = p^{-n} \text{Li}_n(\alpha)$. Then for $w \in W$ we have*

$$p^{-n} \text{Li}_n(\alpha(1 + pw)) \equiv \sum_{k=0}^n \tilde{\text{Li}}_{n-k}(\alpha) \frac{w^k}{k!} \pmod{p}.$$

Proof. Let $g_n(w) = p^{-n} \text{Li}_n(\alpha(1 + pw))$. Then one finds

$$g_0(w) = \frac{\alpha(1 + pw)}{1 - \alpha(1 + pw)} = \frac{\alpha}{1 - \alpha} \frac{1 + pw}{1 - \frac{\alpha}{1 - \alpha} pw} = \tilde{\text{Li}}_0(\alpha) + \sum_{k=1}^{\infty} b_k (pw)^k$$

with $b_n \in W$. Write

$$g_n(w) = \tilde{\text{Li}}_n(\alpha) + \sum_{k=1}^{\infty} d_k^n w^k.$$

It is easy to verify that

$$\frac{d}{dw}g_n(w) = g_{n-1}(w) \frac{1}{1+pw} = g_{n-1}(w) \left(1 + \sum_{k=1}^{\infty} c_k(pw)^k\right),$$

with $c_k \in W$. To find the coefficients d_k^n modulo p for $k < p$ one can simply reduce the above equations modulo p and one easily finds that

$$d_k^n \equiv \begin{cases} \tilde{\text{Li}}_{n-k}(\alpha) & \text{when } k \leq n \\ 0 & \text{when } n < k < p. \end{cases}$$

It thus remains to show that also for $k \geq p$ the coefficient d_k^n is divisible by p . For this it is easier to consider the function $f_n(u) = \text{Li}_n(\alpha + u)$ which satisfies $f_0(u) \in W[[u]]$, $d/du f_{n+1}(u) = g(u)f_n(u)$ with $g(u) \in W[[u]]$ and $f_n(0) \in W$.

LEMMA 2.4. *In the situation above we have $v_p(a_k) \geq -v_p(k!)$, where v_p is the p -adic valuation and a_k is the k th coefficient in the power series expansion with respect to u of any of the functions f_n .*

Proof. Let $a_k(h)$ be the k th coefficient of h for any power series h . We have

$$v_p(a_k(f_n g)) \geq \min_{l < k} [v_p(a_l(f_n))].$$

This implies that

$$v_p(a_k(f_{n+1})) \geq \min_{l < k} [v_p(a_l(f_n))] - v_p(k).$$

The lemma is clearly true for $n = 0$. Suppose it is true for n . Then

$$v_p(a_k(f_{n+1})) \geq \min_{l < k} [-v_p(l!)] - v_p(k) \geq -v_p((k-1)!) - v_p(k) = -v_p(k!).$$

Since $g_n(w) = p^{-n} f_n(\alpha pw)$, to finish the proof we have to check that for every $k \geq p$ we have $k - n - v_p(k!) > 0$. The well known estimate $v_p(k!) \leq k/(p-1)$ and the assumption $n \leq p-2$ imply that it is sufficient to require $k(1 - 1/(p-1)) > p-2$, and this is satisfied for $k \geq p$.

Proof of Theorem 1.1. Using the fact that D is a derivation and that

$$D \log^k(z) = z(1-z) \frac{d}{dz} \log^k(z) = z(1-z) k \log^{k-1}(z) \frac{1}{z} = (1-z) k \log^{k-1}(z)$$

and

$$D \text{Li}_k(z) = z(1-z) \frac{d}{dz} \text{Li}_k(z) = z(1-z) \text{Li}_{k-1}(z) \frac{1}{z} = (1-z) \text{Li}_{k-1}(z)$$

we see that

$$\begin{aligned} DF_n(z) &= D \sum_{k=0}^{n-1} a_k \log^k(z) \text{Li}_{n-k}(z) \\ &= (1-z) \sum_{k=0}^{n-1} a_k (k \log^{k-1}(z) \text{Li}_{n-k}(z) + \log^k(z) \text{Li}_{n-k-1}(z)) \\ &= (1-z) \sum_{k=0}^{n-1} \log^k(z) \text{Li}_{n-k-1}(z) (a_k + (k+1)a_{k+1}). \end{aligned}$$

Here we understand that $a_n = 0$. Every $z \in X$ can be written as $\alpha(1 + pw)$ with α a root of unity in X and $w \in W$. We have

$$p^{-1} \log(\alpha(1 + pw)) = p^{-1} \log(1 + pw) \equiv w \pmod{p}.$$

If we assume that $a_k \in \mathbb{Z}[1/(n+1)!]$ we now find from the last computation and from Proposition 2.3,

$$\begin{aligned} p^{1-n} DF_n(\alpha(1 + pw)) &\equiv (1 - \alpha) \sum_{k=0}^{n-1} w^k (a_k + (k+1)a_{k+1}) \sum_{m=0}^{n-k-1} \frac{1}{m!} \tilde{\text{Li}}_{n-k-1-m}(\alpha) w^m \\ &\equiv (1 - \alpha) \sum_{l=0}^{n-1} w^l \sum_{k=0}^l (a_k + (k+1)a_{k+1}) \frac{1}{(l-k)!} \tilde{\text{Li}}_{n-l-1}(\alpha). \end{aligned}$$

It follows that to make the reduction of $p^{1-n} DF_n$ independent of w for all $p > n + 1$ it is necessary and sufficient that for $l = 1, \dots, n - 1$ we have

$$\sum_{k=0}^l (a_k + (k+1)a_{k+1}) \frac{1}{(l-k)!} = 0. \quad (2.1)$$

If this is satisfied then the reduction of $p^{1-n} DF_n(\alpha(1 + pw))$ is

$$(a_0 + a_1)(1 - \alpha) \tilde{\text{Li}}_{n-1}(\alpha) \equiv -(a_0 + a_1) \text{li}_{n-1}(\sigma(\alpha))$$

so we should also require $a_0 + a_1 = -1$.

Let $A(t) = \sum_{k=0}^{n-1} a_k t^k$. Then the relations (2.1) can be written as

$$e^t(A(t) + dA(t)/dt) \equiv a \pmod{t^n}$$

where a is a constant. This implies that

$$A(t) + dA(t)/dt \equiv ae^{-t} \pmod{t^n}$$

and after solving the resulting differential equation that the $n - 2$ first equations in (2.1) are equivalent to $A(t) \equiv (at + b)e^{-t} \pmod{t^{n-1}}$ for some other constant b . We have

$$-1 = a_0 + a_1 = b + (a - b) = a.$$

Now, in $(b - t)e^{-t}$ the coefficient of t^n is

$$b \frac{(-1)^n}{n!} - \frac{(-1)^{n-1}}{(n-1)!} = \frac{(-1)^{n-1}}{(n-1)!} (1 - b/n).$$

It is easy to see that for Equation (2.1) with $l = n - 1$ to be satisfied, this coefficient must be 0 and hence $b = n$. This gives the choice of the coefficients in the theorem and shows that they are the unique choice in $\mathbb{Z}[1/(n+1)!]$. Now if we have coefficients in \mathbb{Q} satisfying the theorem, then we may clear denominators not dividing $(n+1)!$ and using only independence of w we obtain that these must be a rational multiple of our a_k . But since the reduction of $p^{1-n}DF_n$ is nontrivial the multiplier must be 1.

Remark 2.5. We have the equation

$$F_n(z) = -nL_n(z) - L_{n-1}(z) \log(z),$$

where

$$L_n(z) = \sum_{m=0}^{n-1} \frac{(-1)^m}{m!} \text{Li}_{n-m}(z) \log^m(z)$$

is the function defined in [1]. By loc. cit. the function F_n satisfies $F_n(z) + (-1)^n F_n(1/z) = 0$. Differentiating this relation one gets

$$zDF_n(1/z) + (-1)^n DF_n(z) = 0.$$

Reducing modulo p , we find

$$z\text{li}_{n-1}(1/z) + (-1)^n \text{li}_{n-1}(z) = 0.$$

This relation is easily verified directly.

3. Another Proof of the Main Result

In this section we sketch another proof of the main result. This proof has two interesting features: First of all, it proves directly the formula for F_n in terms of the functions $L_n(z)$ defined at the end of the last section. This formula is of course simpler than the original formula. The other feature is that the key ingredient in the proof is a formula, discovered by Rob de Jeu and the author, which seems to be of some further importance. This formula shows up in the computation of syntomic regulators. These two features suggest that the proof to be described below may in some way be more ‘correct’ than the first one, although it is if anything slightly more complicated.

The formula alluded to above is the content of the following proposition:

PROPOSITION 3.1. *We define a sequence of functions $f_k(z, S)$ inductively as follows:*

$$f_0(z, S) = \frac{S}{1-S}, \quad f_{k+1}(z, S) = \int_z^S f_k(z, t) d \log t.$$

Then, when $z, S \in W$ and $z \equiv S \pmod{p}$ the following formula holds:

$$\sum_{k=0}^n (-1)^k k! \cdot \binom{n}{k} f_{k+1}(z, S) \log^{n-k}(S) = (-1)^n n! (L_{n+1}(S) - L_{n+1}(z)). \quad (3.1)$$

We would like to remark on the potential importance of this formula. The construction of p -adic polylogarithms by Coleman is an inductive procedure. At each step the degree n polylogarithm Li_n is constructed as a locally analytic function satisfying the differential equation $d \text{Li}_n(z) = \text{Li}_{n-1}(z) d \log z$. This determines Li_n up to a locally constant function and a Frobenius condition replaces this by a globally constant function ambiguity. As remarked by Kontsevich the distribution relation removes the ambiguity completely. The formula above allows for a different approach: The functions f_n have no ambiguity in their definitions and are in fact given by converging power series in S and $z - S$. Once the f_n are given, the formula determines L_n up to a locally constant function and the distribution relation determines it completely. The functions Li_n can be determined from the L_n .

For our purposes, the formula is also useful because it allows us to relate the values of L_n at two congruent points.

LEMMA 3.2. *Suppose $z \in X$ and $w \in W$. Then*

$$p^{-n} f_n(z, z(1+pw)) \equiv \frac{z}{1-z} \frac{w^n}{n!} \pmod{p}.$$

The proof is a direct computation similar to the proof of Proposition 2.3. Suppose now that z is a root of unity. Then $\log(z(1+pw)) \equiv pw \pmod{p^2}$. Thus, using (3.1) we immediately obtain

$$p^{-n-1} (-1)^n n! (L_{n+1}(z(1+pw)) - L_{n+1}(z)) \equiv c_{n+1} \frac{z}{1-z} w^{n+1} \pmod{p}$$

with

$$c_{n+1} = \sum_{k=0}^n (-1)^k \frac{k!}{(k+1)!} \binom{n}{k} = \frac{1}{n+1} \sum_{k=0}^n (-1)^k \binom{n+1}{k+1} = \frac{1}{n+1}.$$

so

$$p^{-n} (L_n(z(1+pw)) - L_n(z)) \equiv -(-1)^n \frac{1}{n!} \frac{z}{1-z} w^n \pmod{p}.$$

We can define the derivation D on functions of two variables as

$$D = S(1 - S) \frac{\partial}{\partial S} + z(1 - z) \frac{\partial}{\partial z} .$$

One easily obtains the following

LEMMA 3.3. *If $z, S \in X$ and $z \equiv S \pmod{p}$ then $p^k | Df_k(z, S)$.*

Differentiating the key formula we find, with $S = z(1 + pw)$,

$$\begin{aligned} & p^{-n}(-1)^n n!(DL_{n+1}(S) - DL_{n+1}(z)) \\ &= p^{-n} \sum_{k=0}^n (-1)^k \binom{n}{k} \left[Df_{k+1}(z, S) \log^{n-k}(S) + (n - k)f_{k+1}(z, S) \log^{n-k-1}(S) \right] (1 - S) \\ &\equiv \sum_{k=0}^n (-1)^k \binom{n}{k} (n - k)f_{k+1}(z, S) \log^{n-k-1}(S) (1 - z) \equiv d_{n+1}zw^n \pmod{p}, \end{aligned}$$

where

$$d_{n+1} = \sum_{k=0}^n (-1)^k \frac{k!}{(k + 1)!} \binom{n}{k} (n - k) = - \sum_{l=1}^n (-1)^l \binom{n}{l} = 1 .$$

Let z be a root of unity. Since $\log(z) = 0$ we have

$$\begin{aligned} DL_n(z) &= z(1 - z) \left[\text{Li}_{n-1}(z) \frac{1}{z} + \sum_{m=1}^{n-1} \frac{(-1)^m}{m!} \left(\text{Li}_{n-m-1}(z) \frac{1}{z} \log^m(z) + \right. \right. \\ &\quad \left. \left. + m \text{Li}_{n-m}(z) \log^{m-1}(z) \frac{1}{z} \right) \right] \\ &= (1 - z)(\text{Li}_{n-1}(z) - \text{Li}_{n-1}(z)) = 0. \end{aligned}$$

Thus we find

$$p^{-n} DL_n(S) \equiv -(-1)^n \frac{n}{n!} zw^{n-1} \pmod{p} .$$

Suppose now that we let $F(z) = \sum_{m=1}^n e_m L_m(z) \log^{n-m}(z)$. Substituting first of all a root of unity in X we find $DF(z) = e_{n-1}(1 - z)L_{n-1}(z)$ so we should have

$e_{n-1} = -1$. Then

$$\begin{aligned}
 p^{1-n}DF(S) &= \sum_{m=1}^n e_m \left(DL_m(S) \log^{n-m}(S) + \right. \\
 &\quad \left. + (n-m)L_m(S) \log^{n-m-1}(S)(1-S) \right) p^{1-n} \\
 &\equiv \sum_{m=1}^n e_m \left(-(-1)^m \frac{m}{m!} z w^{m-1} w^{n-m} + \right. \\
 &\quad \left. + (n-m) \left(p^{-m} L_m(z) - (-1)^m \frac{1}{m!} \frac{z}{1-z} w^m \right) w^{n-m-1} (1-z) \right) \\
 &= -z w^{n-1} \sum_{m=1}^n \left((-1)^m e_m \left(\frac{m}{m!} + (n-m) \frac{1}{m!} \right) \right) + \\
 &\quad + \sum_{m=1}^n e_m (n-m) p^{-m} L_m(z) W^{n-m-1} (1-z) \pmod{p}.
 \end{aligned}$$

We wish to choose the coefficients e_m in such a way that this expression is independent of w . Since in the second sum we know by Corollary 2.2 that $p^{-m}L_m(z)$ is not congruent to 0 modulo p (as a function of z) we see that the only nonzero coefficients can be e_n and e_{n-1} . By fixing $e_{n-1} = -1$ we get the equation

$$(-1)^n e_n \frac{n}{n!} + (-1)^n \left(\frac{n-1}{(n-1)!} + \frac{1}{(n-1)!} \right) = 0$$

from which we can recover $e_n = -n$.

Acknowledgements

The author would like to thank M. Kontsevich for explaining the conjecture to him and to H. Gangl for various comments and corrections. He would also like to thank J. Nekovář who first suggested to him the idea of a connection between finite and p -adic polylogarithms.

References

1. Besser, A. and de Jeu, R.: The syntomic regulator for K -theory of fields, Work in progress, 2001.
2. Cathelineau, J.: Remarques sur les différentielles des polylogarithmes uniformes, *Ann. Inst. Fourier (Grenoble)* **46**(5) (1996), 1327–1347.
3. Coleman, R.: Dilogarithms, regulators, and p -adic L -functions, *Invent. Math.* **69** (1982), 171–208.
4. Elbaz-Vincent, P. and Gangl, H.: On poly(ana)logs I, *Compositio Math.* **130** (2001), 161–214 (this issue).
5. Kontsevich, M.: The $1\frac{1}{2}$ -logarithm, Unpublished note, 1995. Reproduced as an appendix to [4] (*Compositio Math.* **130** (2002), 211–214).