ON p-ADIC G-FUNCTIONS

YUVAL Z. FLICKER

1. *Introduction*

In his well-known paper of 1929, Siegel **[18]** introduced a class of analytic functions, which he called E-functions, and he proceeded to establish some fundamental theorems about their transcendental properties. The E-functions include, for instance, the exponential function, the Bessel functions and the general hypergeometric series. Siegel's work established the algebraic independence of the values at algebraic points of E-functions satisfying linear differential equations of the second order. In a major development of 1959, Shidlovsky **[16]** succeeded in generalising the method so that it applied to differential equations of arbitrary order. Many valuable results have followed as a consequence of these studies (see for instance Shidlovsky's survey **[17]** and Chapter 11 of Baker's book **[6]**).

Siegel also defined in his original paper another class of functions which he called G-functions, and which include, for example, the logarithm function $\log(1+z)$, the binomial function $(1+z)^a$, where a is a rational number, and sums and integrals of the form

$$\sum_{n=0}^{\infty} z^n/(n+\lambda)^k, \qquad \int_c^z (1+t^k)^a \, dt.$$

In contrast to E-functions, which are global, the G-functions are defined only locally, and, as soon becomes clear, Siegel's techniques cannot be applied to demonstrate the algebraic independence of their values at algebraic points. Nevertheless, as Siegel remarks, his method does in fact suffice to establish that certain numbers of the kind in question cannot satisfy an algebraic equation of low degree. This work was recently followed up by Nurmagomedov **[13, 14]**; he obtained, in particular, precise lower bounds, indeed almost best possible, for polynomials of low degree in G-functions at certain algebraic points near to 1. The work was motivated by papers of Baker **[2, 3, 4, 5]**, and later Feldman **[9]**, in which similar lower bounds had been obtained for linear forms in the values of the binomial and logarithmic functions. More recently, Galochkin **[10]** has improved upon Nurmagomedov's results, dealing now with G-functions defined over an arbitrary number field, rather than the rational or quadratic fields.

Although, in the complex case, E-functions are more amenable to analysis of the above kind than G-functions, the situation is completely reversed in the p-adic domain. Indeed, as yet, no natural p-adic generalisation of the Siegel–Shidlovsky theorems has been established, though we recall that the E-functions can certainly be locally defined in a p-adic sense. In the special case of the p-adic exponential function, Mahler **[12]** was able to prove the transcendence at algebraic points, but the method he used does not seem to generalise in the direction of the Siegel–Shidlovsky theory. The purpose of this note is to show that the techniques

Received 16 November, 1976.

[J. LONDON MATH. SOC. (2), 15 (1977), 395–402]

employed by Siegel and Shidlovsky can, however, be successfully applied to study p-adic G-functions. We shall in fact obtain a p-adic analogue of the main Nurmagomedov–Galochkin theorem.

2. *Definitions and Results*

In what follows, K will denote a fixed algebraic number field, and we shall use $\|a\|$ to denote the size of a, which is the maximum of the absolute values of the conjugates of the element a of K. We shall use p to denote a fixed prime number and we signify by $|\ |_p$ any valuation on K extending the normalised p-adic valuation on the rationals.

A G-function is defined as an analytic function of the form

$$g(z) = \sum_{n=0}^{\infty} a_n z^n,$$

where $a_0, a_1, \ldots$ are elements of K, and there exists $c > 1$ and a sequence $b_0, b_1, \ldots$ of natural numbers such that $b_n a_0, \ldots, b_n a_n$ are all algebraic integers and we have $b_n \leqslant c^n$ and $\|a_n\| \leqslant c^n$. Plainly $g(z)$ converges p-adically in a disc of sufficiently small radius about the origin, for we have $|b_n a_n|_p \leqslant 1$, whence

$$|a_n|_p \leqslant |b_n|_p^{-1} \leqslant b_n \leqslant c^n.$$

We shall consider G-functions satisfying a system of linear differential equations

$$y_i' = f_{i0}(z) + \sum_{j=1}^{m} f_{ij}(z) y_j \qquad (i = 1, \ldots, m) \tag{1}$$

where $f_{ij}(z)$ is a rational function over K. On differentiating (1) we obtain

$$y_i^{(k)} = f_{i0k}(z) + \sum_{j=1}^{m} f_{ijk}(z) y_j \qquad (k = 1, 2, \ldots)$$

where f_{ijk} is a rational function over K, and $y^{(k)}$ denotes the kth derivative of y. (It would be enough if the rational functions were defined over the p-adic completion of the algebraic closure of the rationals: *cf.* Lemma 2 of Shidlovsky **[16]**). We shall assume that there exists a non-zero polynomial $f(z)$ with algebraic integer coefficients in K, and a sequence of natural numbers $d_1, d_2, \ldots$ such that

$$(d_l/k!)(f(z))^k f_{ijk}(z) \qquad (k = 1, \ldots, l)$$

are polynomials with algebraic integer coefficients, and that $d_n \leqslant d^n$ for some $d > 1$.

Now let $g_1(z), \ldots, g_m(z)$ be G-functions satisfying a system of linear differential equations as above, but which do not satisfy any algebraic equation with degree at most r, the coefficients being rational functions over the algebraic numbers. Let $P(x_1, \ldots, x_m)$ be any polynomial with degree $s \leqslant r$, and with integer coefficients in K with sizes not exceeding H. Further let

$$u = \binom{r+m}{m}, \qquad v = \binom{r-s+m}{m}$$

and suppose that $t(1-v/u) < 1$, where t denotes the degree of K over Q. We prove the following

THEOREM. *For any* $\varepsilon > 0$ *there exists* $\delta > 0$ *such that, for any natural numbers* q, q' *with* $q' < q$, $(q, q') = 1$ *and* $|q|_p < \delta q^{-1+\delta}$, *we have*

$$|P(g_1(q/q'), \ldots, g_m(q/q'))|_p \gg H^{-\lambda-\varepsilon}$$

where

$$\lambda = tv/\{1 - t(1 - v/u)\}$$

and the implied constant depends on $g_1, \ldots, g_m, p, q, r, s, t, \varepsilon$, *but not on* H.

In the special case of linear forms with rational coefficients, that is when $r = 1$, $t = 1$, we have $s = 1$, $u = m+1$, $v = 1$ and so $\lambda = m+1$; this is the best possible value for λ (*cf.* **[10]**, where Galochkin obtains the best possible value $\lambda = m$ in the complex case). For large values of r, that is when the G-functions are nearly algebraically independent, the dependence on t here is best possible; but one would expect to be able to replace v by a smaller function of m.

The theorem is applicable, in particular, to the G-functions given by

$$g_i(z) = \log(1 + \alpha_i z) \qquad (i = 1, \ldots, m)$$

defined as power series over the p-adic domain, where $\alpha_1, \ldots, \alpha_m$ are distinct non-zero elements of K, with $q = p^n$, $q' = 1$, where n is a sufficiently large integer. Thus we see, for instance, that the numbers $\log(1 + \alpha_i p^n)$ cannot satisfy any algebraic equation of degree r, provided only that $n > n_0(\alpha_1, \ldots, \alpha_m, r)$; more especially we have

$$\log(1+\alpha)\log(1+\beta) \neq \log(1+\gamma)\log(1+\delta)$$

for all numbers $\alpha, \beta, \gamma, \delta$ of the form $\alpha' p^n$ with α' in K and n sufficiently large. We recall that even in the complex case, the question of establishing the algebraic independence of the logarithms of algebraic numbers remains unsolved (*cf.* the first problem of Schneider **[15**; p. 138], and Chapter 12 of Baker's book **[6]**). Indeed, as is well known, the algebraic independence of the p-adic logarithms would yield at once a confirmation of the well-known conjecture on the non-vanishing of the p-adic regulator of an arbitrary number field: *cf.* Leopoldt **[11]**, Ax **[1]**, Brumer **[7]**.

The theorem also applies to the G-functions

$$g_i(z) = \prod_{j=1}^{J} (1 + a_{ij} z)^{v_{ij}},$$

defined as a power series over the p-adic domain where a_{ij} are non-zero rational integers and v_{ij} are rationals between 0 (inclusive) and 1 (exclusive). The special case, where $J = 1$, $m = 2$, gives essentially a result of Bundschuh **[8]**, generalising p-adically the work of Baker **[2, 3]**; our result now generalises **[5]**. Bundschuh suggests that his work would enable one to treat effectively Diophantine equations of the form

$$a^m x^n - b^m y^n = c p_1^{j_1} \ldots p_k^{j_k},$$

but unfortunately this is not so, since the p-adic condition $|q|_p < q^{-1+\delta}$ occurring in our theorem implies that q/q' is p-adically near to 0, and this is not compatible with the complex condition that requires q/q' to be small in the Archimedean sense. It is well known, however, that Diophantine equations as above can be effectively dealt with by the method of linear forms in logarithms; see **[6]**.

3. *Lemmas*

Consider a set of G-functions $G_1(z), \ldots, G_u(z)$, linearly independent over $K(z)$, with the differential properties as specified in §2, and let c, d be constants as indicated there. Let p be a prime and suppose $\varepsilon' > 0$. By c_1, c_2, ... we shall denote positive numbers which, like the constants implied by $\ll$, will depend only on $G_1, \ldots, G_u$, p and ε'. We shall signify by n a natural number sufficiently large for the validity of the subsequent arguments.

LEMMA 1. *There exist u polynomials*

$$P_i(z) = \sum_{l=0}^{n-1} p_{il} z^l \qquad (1 \leqslant i \leqslant u),$$

not all 0, *with the following properties*:

(i) *The function*

$$R(z) = \sum_{i=1}^{u} P_i(z)\, G_i(z)$$

has a zero of order at least $n' = un - [\varepsilon' n] - 1$ *at* $z = 0$.

(ii) *The* $P_i(z)$ *have algebraic integer coefficients in* K, *and* $\|p_{il}\| \ll c_1{}^n$.

(iii) *For all* z *in* K *with* $|z|_p < 1/c$ *we have* $|R(z)|_p \ll (c\,|z|_p)^{n'}$.

Proof. The polynomials $P_i(z)$ are the same as those defined in Lemma 3 of Nurmagomedov **[13]**; they are constructed by the usual box principle (Siegel's lemma). It is shown in **[13]** that (i) and (ii) hold, and using the fact that the coefficients in the G-functions have p-adic valuations $\ll c^h$, (iii) can easily be verified.

We shall restrict our attention in this section to homogeneous systems of differential equations, that is systems of the form (1) with $f_{i0}(z)$ identically 0. We shall later take $G_1(z) = 1$, which amounts to an equivalent restriction. Let $R(z)$ be defined as in Lemma 1, and put

$$R_{j-1}(z) = (d_j/j!)(f(z))^j R^{(j)}(z) \qquad (j = 1, 2, \ldots)$$

where $R^{(j)}$ denotes the jth derivative of R and d_j is specified as in §2. By the above restriction to homogeneous systems we have

$$R_j(z) = \sum_{i=1}^{u} P_{ij}(z)\, G_i(z)$$

where $P_{ij}(z)$ are polynomials with integer coefficients in K (*cf.* Lemma 2 of **[10]**). It is clear from Lemma 5 of **[10]** that the $P_{ij}(z)$ have degrees at most $n + d'j$ where d' is the maximum of the degrees of f and $f f_{ij}$ (see also Lemma 2 below). Put

$$E(z) = \det\left(P_{ij}(z)\right) \qquad (1 \leqslant i, j \leqslant u).$$

Then (*cf.* the account of Shidlovsky's lemma given in Chapter 11 of Baker's book **[6]**) we have $E(z) = z^{n'} D(z)$, where $D(z)$ is a polynomial with integer coefficients in K, not identically 0, and with degree at most $\varepsilon' n + c_2$. Further, as in **[6]**, we see that for any z in K, with $z f(z) \neq 0$, and $|z|_p < 1/c$, and for any $n \gg 1$, there exist u distinct indices $j_1, \dots j_u$, with $j_1 + \dots + j_u \leqslant \varepsilon' n + c_3$ such that

$$\det\left(P_{i, j_l}(z)\right) \neq 0 \qquad (1 \leqslant i, l \leqslant u).$$

Note that the condition $|z|_p < 1/c$ is required to ensure the convergence of the defining series for $R(z)$.

LEMMA 2. *Let q, q' be positive integers with $q > q'$, $(q, q') = 1$, and $|q|_p < 1/c$. Then for any $n \geqslant 1$, and $j \leqslant \varepsilon' n + c_3$, we have*

$$\| P_{ij}(q/q') \| \leqslant (c_4 q/q')^{d'j+n}.$$

Proof. It is easily verified that $P_{ij}(z)$ is given recursively by

$$(d_j/j!) \sum_{l=0}^{j} \binom{j}{l} P_i^{(j-l)}(z) f(z)^{j-l} \sum_{k=1}^{u} (f(z))^l f_{ikl}(z)$$

and that the sum over k here is bounded above by $(c_5 z)^{d'l} l!$, for any rational $z > 1$. The required result now follows on noting that $d_j \leqslant d^j$, that by Lemma 1

$$\| P_i^{(j-l)}(z) \| \ll (n!/(n-j+l)!)(c_6 z)^n$$

for any rational $z > 1$, and we have the usual estimate $\binom{n}{s} \leqslant 2^n$. The work here differs from **[10]** in that there small rationals z were considered, rather than $z > 1$.

Now define

$$q_{ij} = q'^{n+d'j} P_{ij}(q/q') \qquad (1 \leqslant i, j \leqslant u)$$

and note that by virtue of Lemma 2 these are integers in K with sizes $\leqslant (c_4 q)^{n+d'j}$, if $j \leqslant \varepsilon' n + c_3$.

LEMMA 3. *For any j as in Lemma 2 and q, as there, with $|q|_p < \delta \ll 1$, we have*

$$|R_j(q/q')|_p \leqslant (c_7 |q|_p)^{n' - \varepsilon' n - c_3} \leqslant |q|_p^{un - 3\varepsilon' n}.$$

Proof. Plainly

$$|R_j(z)|_p \leqslant |j!|_p^{-1} |R^{(j)}(z)|_p$$

for any rational z with $|z|_p < 1/c$, and furthermore it is easily checked, as in (iii) of Lemma 1, that

$$|R^{(j)}(z)|_p \ll \max_{h \geqslant n'} c^h |h(h-1) \dots (h-j+1) z^{h-j}|_p.$$

Now since $h(h-1) \dots (h-j+1)/j!$ is an integer, we obtain

$$|R^{(j)}(q/q')|_p \leqslant \max_{h \geqslant n'} (c^h |q|_p^{h-j}) \leqslant (c_7 |q|_p)^{n' - \varepsilon' n - c_3}$$

as required.

4. *Proof of the theorem*

Using the notations of §2, we consider the set of functions

$$g_1^{h_1} \dots g_m^{h_m}, \quad 0 \leqslant h_1 + \dots + h_m \leqslant r,$$

and name them $G_1(z), \ldots, G_u(z)$, with the convention $G_1(z) = 1$. We also consider the functions

$$g_1^{h_1} \ldots g_m^{h_m} P(g_1, \ldots, g_m), \quad 0 \leqslant h_1 + \ldots + h_m \leqslant r - s,$$

and denote them by $\psi_1, \ldots, \psi_v$; so we have

$$\psi_k(z) = \sum_{i=1}^{u} c_{ik} G_i(z) \qquad (1 \leqslant k \leqslant v).$$

Here, c_{ik} are algebraic integers in K with $\|c_{ik}\| \leqslant H$. By Lemma 7 of **[10]**, $G_1(z), \ldots, G_u(z)$ are G-functions with parameters $c^{r'}$, $d^{r'}$ in place of c, d, where $r' = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + 1/r$; without loss of generality we shall omit the exponent r' and refer again only to c, d. We are then in a position to apply Lemmas 1, 2 and 3 to $G_1, \ldots, G_u$, and we adapt here the notation of §3. Define $r_j(q/q')$ by

$$r_j(q/q') = q'^{n+d'j} R_j(q/q') = \sum_{i=1}^{u} q_{ij} G_i(q/q').$$

As remarked in §2, there exist distinct non-negative integers

$$j_1, \ldots, j_u \quad \text{with} \quad \sum_{i=1}^{u} j_i \leqslant \varepsilon' n + c_3$$

such that the linear forms

$$r_{j_1}(q/q'), \ldots, r_{j_m}(q/q')$$

are linearly independent; since

$$\psi_1(q/q'), \ldots, \psi_v(q/q')$$

are also linearly independent, we can select $w = u - v$ linear forms, without loss of generality the first w forms, such that

$$r_{j_1}(q/q'), \ldots, r_{j_w}(q/q'), \psi_1(q/q'), \ldots, \psi_v(q/q')$$

are u linearly independent linear forms. Signify their determinant of coefficients by Δ; clearly $\Delta \neq 0$, and since it is an algebraic integer in K we have $|N\Delta| \geqslant 1$, where N denotes the absolute norm on K. By replacing the first column on the left by the sum of the ith columns multiplied by $G_i(q/q')$, and noting that $G_1(q/q') = 1$, we get

$$\Delta = \begin{vmatrix} q_{1,j_1} & q_{2,j_1} & \cdots & q_{u,j_1} \\ \vdots & & & \\ q_{1,j_w} & q_{2,j_w} & \cdots & q_{u,j_w} \\ c_{1,1} & c_{2,1} & \cdots & c_{u,1} \\ \vdots & & & \\ c_{1,v} & c_{2,v} & \cdots & c_{u,v} \end{vmatrix} = \begin{vmatrix} r_{j_1}(q/q') & q_{2,j_1} & \cdots & q_{u,j_1} \\ \vdots & & & \\ r_{j_w}(q/q') & q_{2,j_w} & \cdots & q_{u,j_w} \\ \psi_1(q/q') & c_{2,1} & \cdots & c_{u,1} \\ \vdots & & & \\ \psi_v(q/q') & c_{2,v} & \cdots & c_{u,v} \end{vmatrix}. \tag{2}$$

We estimate now the size of Δ, using the determinant on the left and Lemma 2; since

$$j_1 + \ldots + j_w \leqslant j_1 + \ldots + j_u \leqslant \varepsilon' n + c_3 \leqslant 2\varepsilon' n$$

for $n \geqslant 1$, we obtain

$$\|\Delta\| \leqslant H^v (c_4 q)^{wn + 2\varepsilon' d' n}.$$

Since K has degree t over Q and $q^{-1} \leqslant |q|_p < \delta$, we find that

$$|\Delta|_p \geqslant |N\Delta|^{-1} \geqslant \|\Delta\|^{-t} \geqslant H^{-tv} q^{-(w + 3\varepsilon' d')tn}. \tag{3}$$

We shall now choose n so that

$$|r_{j_i}(q/q')|_p < |\Delta|_p;$$

by Lemma 3, this is satisfied if

$$H^{tv} < \{|q|_p^{-u+3\varepsilon'} q^{-(w+4\varepsilon'd')t}\}^n.$$

Plainly if $0 < \delta < 1 - wt/u$ and $|q|_p < q^{-1+\delta}$, and ε' is small enough, the number in braces on the right is greater than 1 and so the choice of n is possible; we shall in fact take the minimal value.

Finally we use the determinant on the right of (2); this gives:

$$\Delta = \sum_{i=1}^{w} r_{j_i}(q/q')\,\Delta_{j_i} + \sum_{i=1}^{v} \psi_i(q/q')\,\delta_i,$$

where Δ_{j_i} and δ_i are certain minors. Since

$$|\delta_i|_p \leqslant 1, \ |\Delta_{j_i}|_p \leqslant 1 \quad \text{and} \quad |g_i(q/q')|_p \ll 1,$$

it follows that

$$|\Delta|_p \leqslant \max |\psi_i(q/q')|_p \ll |P(g_1(q/q'), \ldots, g_m(q/q'))|_p. \tag{4}$$

By the choice of n and the supposition $|q|_p < q^{-1+\delta}$ we have

$$q^{(u-tw+\varepsilon'')n} < q^{c_8} H^{tv}$$

for some ε'' which tends to 0 with ε' and δ. Since, by definition,

$$\lambda = tv(1 + tw/(u-tw)),$$

we obtain

$$q^{(w+2\varepsilon'd')tn} \leqslant q^{c_9} H^{\lambda - tv + \varepsilon}$$

provided that ε' and δ are chosen small enough. The latter estimate together with (3) and (4) proves the theorem.

It is a pleasure to thank here Prof. Alan Baker for his kind help in preparing this note, and Trinity College, Cambridge, for their generous financial support.

References

1. J. Ax, " On the units of an algebraic number field ", *Illinois J. Math.*, 9 (1965), 584-89.
2. A. Baker, " Rational approximations to certain algebraic numbers ", *Proc. London Math. Soc.*, 4 (1964), 385-98.
3. A. Baker, " Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers", *Quart. J. Math. Oxford*, 15 (1964), 375–83.
4. A. Baker, " Approximations to the logarithms of certain rational numbers ", *Acta Arith.*, 10 (1964), 315–23.
5. A. Baker, " Simultaneous rational approximations to certain algebraic numbers ", *Proc. Cambridge Philos. Soc.*, 63 (1967), 693–702.
6. A. Baker, *Transcendental Number Theory* (Cambridge University Press, Cambridge, 1975).
7. A. Brumer, " On the units of algebraic number fields ", *Mathematika*, 14 (1967), 121-24.
8. P. Bundschuh, " Zur Approximation gewisser p-adischer algebraischer Zahlen durch rationale Zahlen ", *J. Reine Angew. Math.*, 265 (1974), 154–59.
9. N. I. Feldman, " An estimate of the absolute value of a linear form in the logarithms of certain algebraic numbers ", *Mat. Zametki*, 2 (1967), 245–56.
10. A. I. Galochkin, " Lower bounds of polynomials in the values of a certain class of analytic functions " (Russian), *Mat. Sb.*, 95 (137) (1974), 396–417.

11. H. W. Leopoldt, " Zur Arithmetik in Abelschen Zahlköpern ", *J. Reine Angew. Math.*, 209 (1962), 54–71.

12. K. Mahler, " Ein Beweis der Transzendenz der p-adischen Exponentialfunktion ", *J. Reine Angew. Math.*, 169 (1932), 61–66.

13. M. S. Nurmagomedov, " The arithmetic properties of the values of a certain class of analytic functions ", (Russian) *Mat. Sb.*, 85 (127) (1971), 339-65.

14. M. S. Nurmagomedov, " The arithmetical properties of the values of G-functions ", (Russian. English summary). *Vestnik Moskov Univ. Ser.* I *Mat. Meh.*, 26 (1971), no. 6, 79–86.

15. T. Schneider, *Einführung in die transzendenten Zahlen* (Göttingen, Berlin; Springer–Verlag, Heidelberg, 1957).

16. A. B. Shidlovsky, " On a criterion for algebraic independence of the values of a class of integral functions ", *Izv. Akad. Nauk* SSSR, 23 (1959), 35–66; = *Amer. Math. Soc. Trans.*, 22 (1962), 339–70.

17. A. B. Shidlovsky, " On arithmetic properties of values of analytic functions ", *Proc. Steklov. Inst. Math.*, 132 (1973), 193–223.

18. C. L. Siegel, " Über einige Anwendungen diophantischer Approximationen ", *Abh. Preuss. Akad. Wiss.*, no. 1 (1929).

Department of Pure Mathematics and Mathematical Statistics,
Mill Lane,
Cambridge.