An optimal multiplicity estimate for interpolation determinants in three logarithms

David Niedbala Giraudin
ORCID 0009-0009-1526-1178

hexagon:2610.00704v1

Abstract

In the kit of Mignotte and Voutier for linear forms in three logarithms, the order of vanishing at the origin of the interpolation determinant is bounded below by Waldschmidt's general multiplicity lemma; the authors indicate that this estimate should be improvable. We give a lower bound for this order which is optimal for generic points. The functions involved span a space whose initial forms are described by a uniqueness property for a linear differential equation with constant coefficients. As a consequence, the left-hand side of their criterion (2.8) can be taken equal to $\frac{(2K+1)(L-1)}{3}\log\rho$, with main term $\frac{2KL}{3}\log\rho$ instead of $\frac{KL}{2}\log\rho$. On the two examples of their paper, with their public code modified in one line and the conditions of the zero lemma checked, the bounds given by the criterion go from $17.94\cdot10^6$ to $4.79\cdot10^6$ and from $28.85\cdot10^6$ to $7.00\cdot10^6$. The same estimate is the multiplicity input of our kit for three p-adic logarithms.

1 Result

Let $K, L \geq 1$ be integers, $N = K(K+1)L/2$, $\vartheta \in \mathbb{C}^2 \setminus \{0\}$ and $\lambda_0, \dots, \lambda_{L-1}$ pairwise distinct complex numbers. Put

$$V = \mathrm{Span}\big\{ z_1^k z_2^m \, e^{\lambda_\ell \, \vartheta\cdot z} \ : \ k+m \leq K-1,\ 0 \leq \ell \leq L-1 \big\},$$

a space of entire functions of $z = (z_1, z_2)$, and let D_V be the multiset

$$D_V = \big\{ a + c \ : \ 0 \leq a \leq K-1,\ 0 \leq c \leq (K-a)L - 1 \big\},$$

of cardinality $\sum_a (K-a)L = N$. For $0 \leq I \leq N$, let $\Theta_V(I)$ be the sum of the I smallest elements of D_V, and $\Theta(K_0, I)$ the quantity of [5, (3.1)].

Proposition 1 (multiplicity)**.** *Let $W \subset V$ be a subspace of dimension I, with basis $f_1, \dots, f_I$, and let $\xi_1, \dots, \xi_I \in \mathbb{C}^2$. Then $x \mapsto \det\big(f_n(x\xi_j)\big)_{1\leq n,j\leq I}$ vanishes at $x = 0$ to order at least $\Theta_V(I)$. We have $\Theta_V(I) \geq \Theta(K-1, I)$, and*

$$\Theta_V(N) = \frac{K(K^2-1)L}{6} + \frac{K(K+1)(2K+1)L^2}{12} - \frac{K(K+1)L}{4},$$
$$\Theta_V(N) - \sum_{k+m\leq K-1} L\,(k+m) = \frac{N(2K+1)(L-1)}{6}.$$

For $W = V$ and generic points, the order is exactly $\Theta_V(N)$.

For comparison, $\Theta(K-1, N) \sim N^2/(2K) \sim K^3L^2/8$, whereas $\Theta_V(N) \sim K^3L^2/6$: the gain is a factor $4/3$ on the main term.

Proof. Let $w = \vartheta \cdot z$, and let u be a linear form such that (w, u) are coordinates. The polynomials of degree at most $K-1$ in z are those of degree at most $K-1$ in (w, u), so

$$V = \bigoplus_{a=0}^{K-1} u^a \, W_a, \qquad W_a = \mathrm{Span}\{ w^b e^{\lambda_\ell w} \ : \ b \leq K-1-a,\ \ell < L \}.$$

The space W_a, of functions of one variable w, is contained in the solution space of $\prod_\ell (\frac{d}{dw} - \lambda_\ell)^{K-a} y = 0$, of order $n_a = (K-a)L$. A non-zero solution therefore has order at most $n_a - 1$ at $w = 0$: otherwise its first n_a Taylor coefficients would vanish, and the linear recurrence given by the equation, with leading coefficient 1, would kill all the others. For a non-zero $f = \sum_a u^a f_a(w) \in V$, the initial form (the non-zero homogeneous component of lowest degree in (w,u)) is a combination of monomials $u^a w^c$ with $c = \operatorname{ord}_0 f_a \le n_a - 1$; two distinct indices a give distinct monomials, so there is no cancellation. Thus the space $\operatorname{in}(V)$ of initial forms is contained in $\operatorname{Span}\{u^a w^c : (a,c) \text{ as in } D_V\}$, and for every degree d, $\dim \operatorname{in}(W)_d \le \#\{(a,c) : a + c = d\}$.

Choose a basis $g_1, \dots, g_I$ of W whose initial forms are linearly independent (Gaussian elimination by initial degree); then $\det(f_n(x\xi_j)) = c \det(g_n(x\xi_j))$ with $c \neq 0$, and row n is divisible by $x^{\deg \operatorname{in}(g_n)}$, whatever the points. The order is therefore at least $\sum_n \deg \operatorname{in}(g_n)$. Since the initial forms of the g_n are independent, the multiset of their degrees is a sub-multiset of D_V; their sum is therefore at least that of the I smallest elements of D_V. For $W = V$: $\dim \operatorname{in}(V) = \dim V = N = \#D_V$, so each $\operatorname{in}(V)_d$ is the span of all the monomials $u^a w^c$ allowed in degree d, and the g_n can be chosen with initial forms exactly these N monomials. The coefficient of $x^{\Theta_V(N)}$ is then $\det\big(\operatorname{in}(g_n)(\xi_j)\big)$, a non-zero polynomial in the points (distinct monomials), whence equality for generic points. (Equivalently, D_V is the sequence of degrees of the standard monomials of the ideal $\bigcap_\ell (u, w - \lambda_\ell)^K$, that is, the Hilbert function of L collinear points of multiplicity K, in duality with the "least" space of de Boor and Ron [3].) Finally, the number of elements of D_V of degree d is at most $\min(d, K-1)+1$, which gives $\Theta_V \ge \Theta(K-1, \cdot)$. The closed formulas follow from $\sum_a \sum_{c<(K-a)L} (a+c)$ and from $\sum (k+m) = LK(K+1)(K-1)/3$. □

Lemma 2. *Let $I \subset \{1, \dots, N\}$ and let $\Psi(x)$ be an $N \times N$ determinant whose rows of index $i \in I$ are $\big(\varphi_i(x\xi_j)\big)_j$ with $\varphi_i \in V$, and whose other rows have entries analytic in x. Then* $\operatorname{ord}_0 \Psi \ge \Theta_V(|I|)$.

Proof. Expand Ψ by Laplace along the rows with index in I: each $|I| \times |I|$ minor taken from these rows has order at least $\Theta_V(|I|)$ by Proposition 1 (or vanishes if the φ_i, $i \in I$, are dependent), and each complementary minor is analytic. □

2 Application to the complex kit of Mignotte–Voutier

In [5], for $i \in I$, row i of the determinant Ψ_I consists of the $\varphi_i(x\eta_j, x\zeta_j)$, with

$$\varphi_i(\eta, \zeta) = c_i\, \eta^{k_i} \zeta^{m_i} e^{\lambda_i(\eta \log \alpha_1 + \zeta \log \alpha_2)}, \qquad k_i + m_i \le K - 1, \quad \lambda_i = \ell_i - \tfrac{L-1}{2};$$

this is an element of V with $\vartheta = (\log \alpha_1, \log \alpha_2)$. For $i \notin I$, the entries are multiplied by analytic functions. Lemma 2 therefore gives $J_I \ge \Theta_V(|I|)$, instead of $J_I \ge \Theta(K-1, |I|)$ (Lemma 3.6 of [5]).

Theorem 3. *Theorem 2.1 of [5] remains true when the left-hand side of (2.8), $\big(\frac{KL}{2} + \frac{L}{2} - 0.37K - 2\big) \log \rho$, is replaced by*

$$\frac{(2K+1)(L-1)}{3} \log \rho,$$

or by the smaller quantity $\big(\frac{2KL}{3} + \frac{L}{3} - (0.37 + \frac{1}{3})K - 2\big) \log \rho$.

Proof. In the proof of Proposition 3.7 of [5], the coefficient of $\log \rho$ is $\frac{2N(K-1)}{3} - \min_I \big(KL(N - |I|) + J_I\big)$. With $J_I \ge \Theta_V(|I|)$, and since each element of D_V is at most $KL - 1 < KL$, this minimum is at least $\Theta_V(N)$, whence the coefficient $-\frac{N}{2} \cdot \frac{(2K+1)(L-1)}{3}$; in [5], it is bounded above by $-\frac{N^2}{2K}\big(1 - \frac{2}{3L} - \frac{2}{3KL} - \frac{1}{3L^2} - \frac{16}{3K^2 L}\big)$. In the proof of Proposition 3.10 of [5], after division by $N/2$, this last quantity appears exactly as the coefficient of $\log \rho$ in the intermediate inequality, $\frac{KL}{2} + \frac{L}{2} - (\frac{1}{3} + \frac{1}{6L})K - (\frac{2}{3} + \frac{3}{K} + \frac{1}{6L} + \frac{8}{3K^2})$, which (2.8) then bounds below by $\frac{KL}{2} + \frac{L}{2} - 0.37K - 2$; the other terms ($\log N!$, $N \log 2$, 0.001) do not involve $\log \rho$. We replace it by $\frac{(2K+1)(L-1)}{3}$. The second form comes from $\frac{(2K+1)(L-1)}{3} - \big(\frac{KL}{2} + \frac{L}{2} - 0.37K - 2\big) = \frac{KL - 2K - L}{6} + \frac{11K}{300} + \frac{5}{3} \ge \frac{KL - 2K - L}{6}$. □

For the large values of K and L used in practice, the ratio of the two left-hand sides is about 1.33.

The examples of [5]

The code of [5] (`github.com/PV-314/lfl3-kit`) computes (2.8) in the function `get_eqn42` of the file `utils-step3.gp`. For the computations below, we replaced

```
eqn42LHS=(bigK*bigL/2+bigL/2-0.37*bigK-2)*log(rho);
```
by
```
eqn42LHS=(bigK*bigL*2/3+bigL/3-(0.37+1/3)*bigK-2)*log(rho);
```

that is, the second, weaker form of Theorem 3. Moreover, this code does not check the conditions (2.9)–(2.13) of the zero lemma outside debugging mode; we make this check mandatory (function `check_zero_estimate`, completed by the comparison of condition (2.9)), in both versions. The iterations start, as in [5], from Matveev's bound, with the same search grids for both versions, and are continued until they stabilise. The proofs of [5] assume at the outset $p > 10 \cdot 10^6$ (example 1) and $p > 20 \cdot 10^6$ (example 2); a bound below this threshold therefore gives, with no further work, $p \leq 10 \cdot 10^6$ and $p \leq 20 \cdot 10^6$. Going lower would require redoing step (1) of [5] with a smaller threshold, which we do not do: these examples, already solved elsewhere, serve here as benchmarks, and what matters is the ratio of the bounds (about 3.7 and 4.1).

	stated in [5]	code of [5], (2.9)–(2.13) checked	Theorem 3
Example 1 ($y^p = F_n$, [2])	$p < 17.92 \cdot 10^6$	$17.94 \cdot 10^6$	$4.79 \cdot 10^6$
Example 2 ($x^2 + 7 = y^p$)	$p < 25 \cdot 10^6$	$28.85 \cdot 10^6$	$7.00 \cdot 10^6$

3 Application to the p-adic kit

In our p-adic kit [6], the analytic bound with no loss rests on the same multiplicity lemma, applied to the formal series $G_{I,\mu}$. Lemma 2 applies word for word, and one obtains the following statement, which is Theorem 1 of [6].

Theorem 4. *With the notation of [6], and under the class hypothesis of its Theorem 1,*

$$v_p(\Delta) \;\geq\; \min_{0 \leq I \leq N} \big((N - I)\, v_p(\Lambda) + \Theta_V(I) \big) - \sum_{i=1}^{N} (k_i + m_i),$$

and, if $v_p(\Lambda) \geq KL - 1$, $v_p(\Delta) \geq \frac{N}{2} \cdot \frac{(2K+1)(L-1)}{3}$. Consequently, the criterion of [6] holds with $E(K, L) = \frac{(2K+1)(L-1)}{3}$ and the conclusion $v_p(\Lambda) \leq KL - 2$.

The hypotheses $K \geq 3$, $L \geq 5$ are not used here. The bound of Theorem 4 is often attained: over 150 series of two or three integer determinants computed exactly, at least one determinant of the series attains it in 44 series.

4 Remarks

Remark 5. Mignotte and Voutier write [5, Section 1.5 (2)]: "Calculations suggest that the estimate there should be roughly $\Theta(2K, |I|)$ instead of $\Theta(K, |I|)$. The main term on the left-hand side of (2.8) would then become KL, rather than $KL/2$." Since $\Theta(K_0, I)$ decreases in K_0, we read this sentence as announcing an order of about twice as much; this is an interpretation. Proposition 1 shows that, for generic points, the order has main term $K^3L^2/6$, that is 4/3 of Waldschmidt's bound; for generic points, this determinant therefore cannot give more than the main term $2KL/3$. For the points of the lattice of the kit, Proposition 1 is a lower bound; the verifier finds equality

p	B	$(L,\ K,\ \chi)$	total, Theorem 4	Yu [7, 1]	ratio
5	10^{10}	(133, 114 445, 8)	$1.52 \cdot 10^7$	$3.08 \cdot 10^9$	202
5	10^{30}	(521, 259 645, 12)	$1.47 \cdot 10^8$	$9.24 \cdot 10^9$	63
7	10^{10}	(106, 91 045, 8)	$9.76 \cdot 10^6$	$4.27 \cdot 10^9$	438
7	10^{30}	(415, 196 589, 12)	$8.85 \cdot 10^7$	$1.28 \cdot 10^{10}$	145
11	10^{10}	(133, 102 041, 8)	$1.42 \cdot 10^7$	$4.16 \cdot 10^9$	293
11	10^{30}	(210, 553 429, 20)	$1.19 \cdot 10^8$	$1.25 \cdot 10^{10}$	105
13	10^{10}	(133, 106 032, 8)	$1.52 \cdot 10^7$	$6.37 \cdot 10^8$	42
13	10^{30}	(235, 522 896, 20)	$1.23 \cdot 10^8$	$1.91 \cdot 10^9$	16
101	10^{10}	(149, 3 384 594, 30)	$5.27 \cdot 10^8$	$2.43 \cdot 10^8$	0.46
101	10^{30}	(295, 4 144 076, 30)	$1.25 \cdot 10^9$	$7.29 \cdot 10^8$	0.59

Table 1: Complete upper bounds for $v_p(\Lambda)$ for $\Lambda = \alpha_1^{b_1}\alpha_2^{b_2} - \alpha_3^{b_3}$, $b_i \le B$, $p \nmid b_3$ ($\alpha = (2,3,5)$ if $p = 7$, $(2,3,7)$ otherwise), degenerate cases included, with the multiplicity estimate of Theorem 4 and with the two-logarithm step of the degenerate case (2.15) based on the rearrangement bound alone. The final version of [6] also uses Lemma 10 of Bugeaud–Laurent on translates of sublattices in that step, which divides these totals further by 1.46 to 1.77 for $p \le 13$.

for small values of K and L. The mechanism (uniqueness for differential equations with constant coefficients, Hilbert function of multiple points) is classical; we have not found it applied to the multiplicity lemma of interpolation determinants in three logarithms.

Remark 6. For two logarithms, the argument gives the order $N(N-1)/2$, already used by Laurent and by Laurent–Mignotte–Nesterenko [4]: the exponential structure brings nothing more in that case.

Verification

The ancillary file `VERIF_MULT3.py` (Python and numpy, no argument, about ten seconds) checks:

- the order of the determinants $\det(z^\mu e^{\ell\, x\vartheta\cdot z})$ for $W = V$, computed exactly in $\mathbb{F}_q[[x]]$ (q a 61-bit prime), for six pairs (K, L), at generic points and at points of the lattice of the kit: it equals $\Theta_V(N)$;
- the closed formulas for $1 \le K, L < 40$, and $\Theta_V \ge \Theta(K-1, \cdot)$ at about fifty values of I for each (K, L);
- Theorem 4 on 150 series of exact integer determinants, for $p = 2$, 3, 5, 7, 11 and 13;
- each row of the p-adic table.

The figures for the examples of [5] are obtained with their PARI/GP code, modified as indicated; they are not recomputed by the ancillary file.

Acknowledgements. Technical assistance: Claude (Anthropic).

References

[1] A. Alvarado, A. Koutsianas, B. Malmskog, C. Rasmussen, C. Vincent, M. West, A robust implementation for solving the S-unit equation and several applications, arXiv:1903.00977.

[2] Y. Bugeaud, M. Mignotte, S. Siksek, Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers, *Ann. of Math.* **163** (2006), 969–1018.

[3] C. de Boor, A. Ron, On multivariate polynomial interpolation, *Constr. Approx.* **6** (1990), 287–302.

[4] M. Laurent, M. Mignotte, Y. Nesterenko, Formes linéaires en deux logarithmes et déterminants d'interpolation, *J. Number Theory* **55** (1995), 285–321.

[5] M. Mignotte, P. Voutier, A kit for linear forms in three logarithms, *Math. Comp.* **93** (2024), 1903–1951; arXiv:2205.08899.

[6] D. Niedbala Giraudin, A kit for linear forms in three p-adic logarithms, preprint, 2026.

[7] K. Yu, p-adic logarithmic forms and group varieties III, *Forum Math.* **19** (2007), 187–280.