ESSENTIAL NUMBER THEORY

2023

vol. 2 no. 1

msp

ESSENTIAL NUMBER THEORY

msp.org/ent

See inside back cover or msp.org/ent for submission instructions.

Essential Number Theory (ISSN 2834-4634 electronic, 2834-4626 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ENT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

https://msp.org/

msp

Essential Number Theory
Vol. 2, No. 1, 2023
https://doi.org/10.2140/ent.2023.2.1

On the Northcott property for infinite extensions

Martin Widmer

We start with a brief survey on the Northcott property for subfields of the algebraic numbers $\overline{\mathbb{Q}}$. Then we introduce a new criterion for its validity (refining the author's previous criterion), addressing a problem of Bombieri. We show that Bombieri and Zannier's theorem, stating that the maximal abelian extension of a number field K contained in $K^{(d)}$ has the Northcott property, follows very easily from this refined criterion. Here $K^{(d)}$ denotes the composite field of all extensions of K of degree at most d.

1. Introduction

Heights are an important tool in Diophantine geometry to study the distribution of algebraic points on algebraic varieties, and in arithmetic dynamics to study preperiodic points under endomorphisms of algebraic varieties. There are various different heights but the most standard one is probably the Weil height on $\mathbb{P}^n$. However, their common fundamental property is that there are only finitely many points of bounded height over a given number field. To which fields of infinite degree does this finiteness property extend? This is the question we are concerned with in this article.

All algebraic field extensions of $\mathbb{Q}$ are considered subfields of some fixed algebraic closure $\overline{\mathbb{Q}}$. Let K be a number field, and for $P = (\alpha_0 : \cdots : \alpha_n) \in \mathbb{P}^n(K)$, with representative $(\alpha_0, \dots, \alpha_n) \in K^{n+1}$, let

$$H(P) = \prod_{v \in M_K} \max\{|\alpha_0|_v, \dots, |\alpha_n|_v\}^{d_v/[K:\mathbb{Q}]}$$

be the absolute multiplicative Weil height of P. Here M_K denotes the set of places of K. For each place v we choose the unique representative $|\cdot|_v$ that either extends the usual Archimedean absolute value on $\mathbb{Q}$ or a usual p-adic absolute value on $\mathbb{Q}$, and $d_v = [K_v : \mathbb{Q}_v]$ denotes the local degree at v. A standard reference for heights is [Bombieri and Gubler 2006]. We use $\mathbb{N} = \{1, 2, 3, \dots\}$ for the set of positive natural numbers.

MSC2020: primary 11G50, 11R04; secondary 11R06, 11R20, 37P30.

Keywords: Weil height, Northcott property, property (N), Northcott's theorem, abelian extensions, Silverman's inequality.

The unique prime factorization of $\mathbb{Z}$ implies that $\prod_{M_\mathbb{Q}} |\alpha|_v^{d_v} = 1$ for every nonzero $\alpha \in \mathbb{Q}$. This identity is known as the product formula and extends to arbitrary number fields K [Bombieri and Gubler 2006, Proposition 1.4.4]. Consequently, the value of the height is independent of the representative $(\alpha_0, \dots, \alpha_n)$ and thus defines a genuine function on $\mathbb{P}^n(K)$. Choosing a representative of P with a coordinate equal to 1 shows that $H(P) \geq 1$. The fundamental identity $\sum_{M_K} d_v = [K : \mathbb{Q}]$, valid for every number field (see [Bombieri and Gubler 2006, Corollary 1.3.2]), shows that the height $H(P)$ is also independent from the number field K containing the coordinates of P. Hence, $H(\cdot)$ is a well-defined function on $\mathbb{P}^n(\overline{\mathbb{Q}})$. D. G. Northcott [1950, Theorem 1] proved the following simple but important result.

Theorem 1 [Northcott 1950]. *Given a number field K, $n \in \mathbb{N}$, and $X \geq 1$, there are only a finite number of points P in $\mathbb{P}^n(K)$ such that $H(P) \leq X$.*

For $P = (1 : \alpha_1 : \cdots : \alpha_n) \in \mathbb{P}^n(\overline{\mathbb{Q}})$ we obviously have $H(P) \geq \max_i H((1 : \alpha_i))$. Consequently, Theorem 1 holds true for a given field $K \subseteq \overline{\mathbb{Q}}$ if and only if it holds for $n = 1$. We define the height $H(\alpha)$ of an algebraic number α to be $H((1 : \alpha))$, and so we are led to the following notion, formally introduced by Bombieri and Zannier [2001].

Definition 2 (Northcott property). A subset S of $\overline{\mathbb{Q}}$ has the *Northcott property* (or shorter, *Property (N)*) if

$$\{\alpha \in S;\, H(\alpha) \leq X\}$$

is finite for every $X \geq 1$.

Theorem 1 was merely an intermediate step in Northcott's seminal work [1950] to show that for any morphism $f : \mathbb{P}^n \to \mathbb{P}^n$ of algebraic degree at least 2 and defined over a number field K there are only finitely many preperiodic points in $\mathbb{P}^n(K)$ under f. His proof also shows that one can replace number field by any field with Property (N).

Another somewhat surprising application of Property (N) builds on work of J. Robinson [1962]. It has been observed by Vidaux and Videla [2016] that the work of Robinson [1962] implies the undecidability of each ring of totally real algebraic integers with Property (N). This connection was further exploited in [Martínez-Ranero et al. 2020] and in [Springer 2020].

These two applications extend interesting properties of number fields to fields with Property (N), suggesting that Property (N) fields behave similarly as number fields. However, this view was shattered by Fehm's discovery [2018, Proposition 1.2] that some fields with Property (N) are pseudoalgebraically closed (PAC).

Next we discuss two arithmetic properties with respect to which *all* fields of infinite degree with Property (N) behave radically different from number fields.

Gaudron and Rémond [2017] introduced the notion of a Siegel field, which is a subfield of $\overline{\mathbb{Q}}$ over which Siegel's lemma holds true; see [Gaudron and Rémond 2017, (∗) on page 189]. It is classical that number fields are Siegel fields, and work of Zhang [1995], and independently of Roy and Thunder [1996], shows that $\overline{\mathbb{Q}}$ is also a Siegel field. A priori it is not easy to find counterexamples but Gaudron and Rémond [2017, Corollaire 1.2] proved that a field of infinite degree with Property (N) cannot be a Siegel field.

A very recent paper of Daans, Kala and Man [Daans et al. 2023] investigates the existence of universal quadratic forms over totally real fields of infinite degree. Whereas it is well-known that for totally real number fields such a form always exists, the existence of a universal quadratic form over a given totally real field of infinite degree is not clear at all. However, they prove [loc. cit., Theorem 1.2] that such a form cannot exist if the field has infinite degree and Property (N).

A point $P = (\alpha_0 : \cdots : \alpha_n) \in \mathbb{P}^n(\overline{\mathbb{Q}})$ defines a number field $\mathbb{Q}(\alpha_i/\alpha_j; \alpha_j \neq 0)$, and the degree of P is the degree of this number field. To prove Theorem 1 Northcott [1950, Lemma 2] proved a stronger result; that for any given $d \in \mathbb{N}$ and $X \geq 1$ there are only finitely many points $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ of degree d and height $H(P)$ at most X. The latter is a direct consequence of what nowadays is usually understood as "Northcott's theorem"; see [Bombieri and Gubler 2006, Theorem 1.6.8].

Theorem 3 (Northcott's theorem). *Let $d \in \mathbb{N}$, then the set $\{\alpha \in \overline{\mathbb{Q}}; [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d\}$ has Property (N).*

Northcott's theorem already implies the existence of fields of infinite degree with Property (N). Indeed, let K be a number field and let $X \geq 1$ be given. Any two distinct quadratic extensions of K only intersect in K, and there are infinitely many such extensions. Hence, there must be one whose elements outside of K all have height bigger than X. Constructing an infinite tower $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots$ where we choose a quadratic extension K_{i+1} of K_i whose elements outside of K_i all have height larger than i say, yields an infinite extension $L = \cup_i K_i$ with Property (N).

Dvornicich and Zannier [2008] observed that Northcott's theorem remains true when replacing the ground field $\mathbb{Q}$ by any field with Northcott property, i.e., if L is a field with Property (N) and $d \in \mathbb{N}$, then the set

$$\{\alpha \in \overline{\mathbb{Q}}; [L(\alpha) : L] \leq d\}$$

also has Property (N). In particular, Property (N) is preserved under finite field extensions. However, it is not always preserved under taking Galois closure over $\mathbb{Q}$, or taking compositum of two fields; see [Widmer 2011, Theorem 5].

Bombieri and Zannier [2001] were the first authors that studied the Northcott property for infinite field extensions of $\mathbb{Q}$.[1] In view of Northcott's theorem it is very appealing to consider the field $\mathbb{Q}^{(d)}$ generated over $\mathbb{Q}$ by all algebraic numbers of degree at most d. Bombieri and Zannier [2001] raised the following question.

Question 4 [Bombieri and Zannier 2001]. Let $d \in \mathbb{N}$. Does $\mathbb{Q}^{(d)}$ have Property (N)?

There is a whole zoo of properties for subfields of $\overline{\mathbb{Q}}$ (including the properties (P), (SP), ($\bar{\text{P}}$), (R), ($\bar{\text{R}}$), (K), see [Narkiewicz 1995; Liardet 1972]; and (SB), (USB), see [Fili and Miner 2015; Pottmeyer 2015]) in arithmetic dynamics, that are all implied by Property (N); see [Checcoli and Widmer 2013; Pottmeyer 2015]. For some of these properties the analogue of Question 4 was posed, explicitly or implicitly.[2] We will not discuss any of these more exotic properties but let us mention that Pottmeyer [2015, Theorem 4.3] showed that $\mathbb{Q}^{(d)}$ has the properties (USB) and (P) (solving a conjecture of Narkiewicz from 1963). However, (USB) and (P) are both strictly weaker than (N), as shown in [Fehm 2018, Proposition 1.3] and in [Dvornicich and Zannier 2008, Theorem 3.3] respectively.

Question 4 is still open but a remarkable step was already made in [Bombieri and Zannier 2001]. For $d \in \mathbb{N}$ and K a number field we write $K^{(d)}$ for the composite field of all extensions of K of degree at most d. Then $K^{(d)}/K$ is a Galois extension, generated over K by all algebraic numbers of relative degree $[K(\alpha) : K]$ at most d. Let $K_{ab}^{(d)}$ be the composite field of all abelian extensions F/K with $F \subset K^{(d)}$. Then $K_{ab}^{(d)}$ is the maximal abelian subextension of $K^{(d)}/K$. If $d \geq 2$ then $\mathbb{Q}(\sqrt{n}; n \in \mathbb{Z}) \subset K_{ab}^{(d)} \subset K^{(d)}$, and so $K_{ab}^{(d)}$ and $K^{(d)}$ both have infinite degree over $\mathbb{Q}$, and thus also over K.

Theorem 5 [Bombieri and Zannier 2001]. *Let K be a number field and let $d \in \mathbb{N}$. The field $K_{ab}^{(d)}$ has the Northcott property. In particular, $K^{(2)}$ has the Northcott property.*

Taking $K = \mathbb{Q}(\zeta_d)$ for a primitive d-the root of unity, and applying Theorem 5 proves that the field

$$\mathbb{Q}(1^{1/d}, 2^{1/d}, 3^{1/d}, 4^{1/d}, \ldots) \tag{1.1}$$

has the Northcott property.

[1] It is worthwhile mentioning that Julia Robinson [1962] proved that the ring of integers of $\mathbb{Q}(\sqrt{n}; n \in \mathbb{N})$ has the "Northcott property" with respect to the house (instead of Weil height), and deduced from this that $\mathbb{N}$ is first order definable in this ring.

[2] Narkiewicz [1971; 1963, Problem 10(i)] conjectured that $K^{(d)}$ has (P) for all d. Further, for various pairs of these properties it was asked whether they are equivalent to each other; see [Narkiewicz 1995; Checcoli and Widmer 2013].

Theorem 5 is a very interesting result for its own sake but it also has interesting applications. Specifically, to list some of the recent applications, Theorem 5 was used:

- In [Vidaux and Videla 2016] to show that the maximal totally real subfield of $K_{ab}^{(d)}$ is undecidable, in [Springer 2020] to show that $\mathbb{Q}_{ab}^{(d)}$ is undecidable, and in [Martínez-Ranero et al. 2020] as one of the ingredients that led the authors to conjecture that $K^{(d)}$ is undecidable (proved for $\mathbb{Q}^{(2)}$ in the same paper).
- In [Daans et al. 2023] to deduce that if L is a totally real subfield of $K_{ab}^{(d)}$ of infinite degree, then no universal quadratic form exists over L. In particular, this holds if $L \subset \mathbb{Q}^{[d]}$ and d is a prime or a prime square, where $\mathbb{Q}^{[d]}$ denotes the compositum of all totally real Galois fields of degree exactly d over $\mathbb{Q}$.
- In [Checcoli and Dill 2023, Corollary 1] to prove that if K is a number field, A is an abelian variety defined over K, and $K(A_{\mathrm{tors}})$ is the minimal field extension of K over which all torsion points of A are defined, then each subfield of $K(A_{\mathrm{tors}})$ which is Galois over K, and whose Galois group has finite exponent, has the Northcott property.

An abelian extension $L/\mathbb{Q}$ lies in $\mathbb{Q}^{(d)}$ for some d if and only if its Galois group has finite exponent; see [Checcoli 2013, Theorem 1]. As pointed out in [Checcoli and Dill 2023, Section 5] this remains true when replacing the ground field $\mathbb{Q}$ with an arbitrary number field K. Therefore Theorem 5 gives a purely Galois theoretic criterion for the Northcott property of a field, i.e., every abelian extension of a number field K with finite exponent has the Northcott property.

However, the restriction to abelian extensions (and finite exponent) in Theorem 5 is very rigid and rules out many interesting examples. In a survey article Bombieri [2009, page 52] states:

> *"It remains an open problem to determine whether the Northcott property holds for $K^{(d)}$ if $d \geq 3$ and, more generally, to determine workable conditions for its validity."*

In this paper we are particularly concerned with the second part of Bombieri's statement.

Problem 6 [Bombieri 2009]. Determine workable conditions for the validity of the Northcott property for subfields of $\overline{\mathbb{Q}}$.

The author [Widmer 2011] gave a criterion which is robust and often easy to apply. For an extension M/K of number fields we write $D_{M/K}$ for the relative discriminant, and we write $N_{K/F}(\,\cdot\,)$ for the norm from K to F. If $F = \mathbb{Q}$ and $\mathfrak{A}$ is a nonzero ideal in the ring of integers $\mathcal{O}_K$ of K then we interpret $N_{K/F}(\mathfrak{A})$ as the unique positive rational integer that generates the principle ideal $N_{K/F}(\mathfrak{A})$.

Theorem 7 [Widmer 2011, Theorem 3]. *Let K be a number field, let $K = K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq \cdots$ be a nested sequence of finite extensions and set $L = \bigcup_i K_i$. Suppose that*

$$\inf_{K_{i-1} \subsetneq M \subset K_i} (N_{K_{i-1}/\mathbb{Q}}(D_{M/K_{i-1}}))^{1/([M:K_0][M:K_{i-1}])} \to \infty \tag{1.2}$$

as i tends to infinity where the infimum is taken over all intermediate fields M strictly larger than K_{i-1}. Then the field L has the Northcott property.

Theorem 7 implies the following refinement of (1.1). Let K be a number field, let $p_1 < p_2 < p_3 < \cdots$ be a sequence of positive primes and let $d_1, d_2, d_3, \ldots$ be a sequence of positive integers. Then the field

$$K(p_1^{1/d_1}, p_2^{1/d_2}, p_3^{1/d_3}, \ldots)$$

has the Northcott property if and only if $\log p_i/d_i \to \infty$ as i tends to infinity. The fact that every direct product of finite solvable groups can be realized over $\mathbb{Q}$ by a Galois extension with Property (N) can also easily be deduced from Theorem 7; see [Checcoli and Widmer 2013, Theorem 4]. Fehm's aforementioned construction of PAC fields with Property (N) also used Theorem 7. And finally, Theorem 7 allows to construct fairly large nonabelian subfields of $\mathbb{Q}^{(d)}$ with Property (N) (see [Widmer 2011, Corollaries 3, 4, and 5]), providing another result on Question 4.

Theorem 7 is based on a fundamental height lower bound of Silverman [1984, Theorem 2]. Here we give only a simplified version sufficient for our purposes. Let $\alpha \in \overline{\mathbb{Q}}$, let F be a number field, let $K = F(\alpha)$, $m = [F : \mathbb{Q}]$, and $d = [K : F]$. Then

$$H(\alpha) \geq \tfrac{1}{2} N_{F/\mathbb{Q}}(D_{K/F})^{1/(2md^2)}. \tag{1.3}$$

Using the optimal choice of F for given α to maximize the right hand-side in (1.3) plays an important role in our results. For the convenience of the reader we will give a proof of inequality (1.3) in Section 2.

Obviously Theorem 7 does not follow from Theorem 5. How does one prove Theorem 7? Let $\alpha \in L$ be of height at most X, and let K_{i_0} be the maximal field not containing α. Applying (1.3) with $F = K_{i_0}$, and using (1.2), shows that i_0 is bounded from above in terms of X and L, and thus, by Northcott's theorem, the field L has the Northcott property.

However, the choice K_{i_0} for the ground field F can be far from optimal, and so we do not use the full force of (1.3). Therefore, Theorem 7 does not seem strong enough to deduce Theorem 5 either.

The aim of this short note is to provide a refined criterion, using the full force of (1.3), that easily implies Theorem 7 and Theorem 5. To this end we introduce the following invariant for an extension of number fields M/K:

$$\gamma(M/K) = \sup_{K \subset F} (N_{F/\mathbb{Q}}(D_{MF/F}))^{1/([MF:\mathbb{Q}][MF:F])}, \tag{1.4}$$

where the supremum runs over all number fields F containing K, and MF denotes the composite field of M and F. We can now state a more powerful version of the criterion given in Theorem 7.

Theorem 8. *Let K be a number field, and let L be an infinite algebraic field extension of K. Suppose that*

$$\liminf_{K\subset M\subset L} \gamma(M/K) = \infty,$$

where M runs over all number fields in L containing K. Then L has the Northcott property.

Proof. Suppose that L does not have the Northcott property. Thus there exists $X \geq 1$ and a sequence $(\alpha_i)_i$ of pairwise distinct elements in L with $H(\alpha_i) \leq X$ for all i. By Northcott's theorem the degrees of $M_i = K(\alpha_i)$ must tend to infinity. After passing to a subsequence we can assume all the M_i are distinct. Note that $M_i F = F(\alpha_i)$ for each F that contains K. We apply inequality (1.3) to get

$$\begin{aligned} 4X^2 &\geq \liminf_i (2H(\alpha_i))^2 \\ &\geq \liminf_i \Big(\sup_{K\subset F} N_{F/\mathbb{Q}}(D_{M_iF/F})^{1/([M_iF:\mathbb{Q}][M_iF:F])} \Big) \\ &\geq \liminf_{K\subset M\subset L} \Big(\sup_{K\subset F} N_{F/\mathbb{Q}}(D_{MF/F})^{1/([MF:\mathbb{Q}][MF:F])} \Big) \\ &= \liminf_{K\subset M\subset L} \gamma(M/K). \end{aligned}$$

□

Theorem 8 implies Theorem 7,[3] but why does it also imply Theorem 5, and how does this proof differ from the original one in [Bombieri and Zannier 2001]? We will discuss these questions in detail in Section 3.

Are there any known criteria for Property (N) for field extensions of infinite degree that we have not mentioned so far? The author is only aware of one such criterion. Let $L/\mathbb{Q}$ be a Galois extension and let $S(L)$ be the set of rational primes for which L can be embedded in a finite extension of $\mathbb{Q}_p$. For $p \in S(L)$ let e_p and f_p be the ramification index and the inertia degree above p. Bombieri and Zannier [2001, Theorem 2] proved that

$$\liminf_{\alpha\in L} H(\alpha) \geq \exp\left(\tfrac{1}{2} \sum_{p\in S(L)} \frac{\log p}{e_p(p^{f_p}+1)} \right). \tag{1.5}$$

In particular, L has the Northcott property whenever the sum on the right hand-side of (1.5) diverges. The above criterion does not seem very workable. Bombieri and

[3] Let (M_j) be a sequence of distinct fields with $K \subset M_j \subset L$ and $\gamma(M_j/K) < X$, and let $i = i(j)$ be minimal with $M_j \subset K_i$. Set $M_j' = K_{i-1}M_j$ so that $K_{i-1} \subsetneq M_j' \subset K_i$. The choice $F = K_{i-1}$ on the right-hand side of (1.4) shows that (1.2) has a bounded subsequence.

Zannier asked whether this sum can diverge for infinite extensions but considered this unlikely. However, it was shown by Checcoli and Fehm [2021] that there are Galois extensions $L/\mathbb{Q}$ of infinite degree for which the above sum diverges, and even such extensions for which neither Theorem 5 nor 7 applies, so it constitutes an independent criterion for the Northcott property, albeit one for which natural examples still need to be found.

2. Silverman's inequality

In this section we give a proof of Silverman's inequality (1.3). For the special case $F = \mathbb{Q}$ a very simple proof was given by Roy and Thunder [1995, Lemmas 1 and 2]. We extend the argument in [loc. cit.] to arbitrary ground fields F, providing a slightly different proof from Silverman's original one [Silverman 1984]. Yet another proof of Silverman's inequality was given by Ellenberg and Venkatesh [2007, Lemma 2.2].

We first fix the notation and recall some basic facts. Let F be a number field of degree m, let K/F be a field extension of degree d, and let $\sigma_1, \dots, \sigma_d : K \to K^{(G)}$ be the d distinct field homomorphisms of K to the Galois closure $K^{(G)}$ of K/F, fixing F. Let $(z_1, \dots, z_d)$ be a d-tuple of elements in K. Then $D_{K/F}(z_1, \dots, z_d) = \det[\sigma_i(z_j)]^2$, and for a nonzero ideal $\mathfrak{A}$ in $\mathcal{O}_K$ the discriminant $D_{K/F}(\mathfrak{A})$ is the ideal in $\mathcal{O}_F$ generated by the numbers $D_{K/F}(z_1, \dots, z_d)$ as the tuples $(z_1, \dots, z_d)$ run over all F-bases of K and each basis element is contained in $\mathfrak{A}$. In particular, $D_{K/F}(\mathfrak{A})$ divides the principle ideal in $\mathcal{O}_F$ generated by $D_{K/F}(z_1, \dots, z_d)$ for each such tuple $(z_1, \dots, z_d)$; see [Lang 1994, III, Section 3]. Recall that we write $D_{K/F}$ for $D_{K/F}(\mathcal{O}_K)$. We will use the basic identity (see [Lang 1994, III, Section 3, Proposition 13])

$$D_{K/F}(\mathfrak{A}) = D_{K/F} N_{K/F}(\mathfrak{A})^2. \tag{2.1}$$

Lemma 9 [Silverman 1984]. *Let F be a number field of degree m. Let $\alpha \in \overline{\mathbb{Q}} \backslash F$, set $K = F(\alpha)$, and $d = [K : F]$. Then*

$$H(\alpha) \geq d^{-1/(2(d-1))} N_{F/\mathbb{Q}}(D_{K/F})^{1/(2md(d-1))}.$$

Proof. Choose $\omega_0, \omega_1 \in \mathcal{O}_K$ such that $\omega_0 \neq 0$ and $\alpha = \omega_1/\omega_0$. For $1 \leq j \leq d$ let $z_j = \omega_0^{d-j}\omega_1^{j-1}$, so that $P = (1 : \alpha : \cdots : \alpha^{d-1}) = (z_1 : \cdots : z_d) \in \mathbb{P}^{d-1}(K)$ and $H(\alpha)^{d-1} = H(P)$. We will bound

$$H(P)^{2md} = \prod_{v \nmid \infty} \max_j \{|z_j|_v\}^{2d_v} \prod_{v \mid \infty} \max_j \{|z_j|_v\}^{2d_v}$$

from below. Note that $z_1, \dots, z_d$ is an integral F-basis of K. Let $\mathfrak{A} = \sum_j z_j \mathcal{O}_K$ be the ideal in $\mathcal{O}_K$ generated by the z_j. For the non-Archimedean places of K we

have

$$\prod_{v\nmid\infty} \max_j\{|z_j|_v\}^{2d_v} = N_{K/\mathbb{Q}}(\mathfrak{A})^{-2}.$$

For each embedding $\tau : F \to \mathbb{C}$ we choose an extension $\tilde{\tau} : K^{(G)} \to \mathbb{C}$ of τ to $K^{(G)}$. Then the d distinct maps $\tilde{\tau} \circ \sigma_i : K \to \mathbb{C}$ are precisely the d embeddings of K that extend τ. Ranging over all embeddings τ of F gives the full set of embeddings of K. Hence, for the Archimedean places of K we get

$$\prod_{v\mid\infty} \max_j\{|z_j|_v\}^{2d_v} = \prod_{\tau} \prod_{i=1}^{d} \max\{|\tilde{\tau} \circ \sigma_i(z_1)|, \ldots, |\tilde{\tau} \circ \sigma_i(z_d)|\}^2.$$

Writing $\boldsymbol{z}_{\tau,i}$ for the complex row vector $(\tilde{\tau} \circ \sigma_i(z_1), \ldots, \tilde{\tau} \circ \sigma_i(z_d))$, and applying Hadamard's inequality yields

$$\begin{aligned}\prod_{i=1}^{d} \max\{|\tilde{\tau} \circ \sigma_i(z_1)|, \ldots, |\tilde{\tau} \circ \sigma_i(z_d)|\}^2 &\geq d^{-d} \prod_{i=1}^{d} |\boldsymbol{z}_{\tau,i}|^2 \\ &\geq d^{-d} |\det[\tilde{\tau} \circ \sigma_i(z_j)]^2| \\ &= d^{-d} |\tilde{\tau}(\det[\sigma_i(z_j)]^2)| \\ &= d^{-d} |\tau(\det[\sigma_i(z_j)]^2)|,\end{aligned}$$

where in the last step we used that $\det[\sigma_i(z_j)]^2 = D_{K/F}(z_1, \ldots, z_d)$ lies in F. Taking the product over all τ, and using that $D_{K/F}(\mathfrak{A})$ divides the ideal generated by $\det[\sigma_i(z_j)]^2$ in $\mathcal{O}_F$, yields

$$\prod_{v\mid\infty} \max_j\{|z_j|_v\}^{2d_v} \geq d^{-md} N_{F/\mathbb{Q}}(D_{K/F}(\mathfrak{A})).$$

Now we use (2.1), and that $N_{F/\mathbb{Q}}(D_{K/F} N_{K/F}(\mathfrak{A}))^2) = N_{F/\mathbb{Q}}(D_{K/F}) N_{K/\mathbb{Q}}(\mathfrak{A})^2$ to get

$$H(\alpha)^{2md(d-1)} = H(P)^{2md} \geq d^{-md} N_{F/\mathbb{Q}}(D_{K/F}),$$

which proves the claim. □

3. Theorem 8 implies Bombieri and Zannier's Theorem 5

In this section we show that Theorem 8 gives a short and straightforward proof of Theorem 5. We also compare this new proof with the original one from [Bombieri and Zannier 2001]. Both proofs have a common part which we extract and formulate below as a separate lemma.

Lemma 10 [Bombieri and Zannier 2001]. *Let $d \in \mathbb{N}$, let K be a number field, and let M be a number field with $K \subset M \subset K_{ab}^{(d)}$. Then p_M, the largest prime that ramifies in M, tends to infinity as M runs over all such intermediate fields M. Further, if $p > d$ is prime and $\mathfrak{B}$ is a prime ideal in $\mathcal{O}_M$ above p and $\mathfrak{p} = \mathfrak{B} \cap K$, then the ramification index $e(\mathfrak{B}/\mathfrak{p})$ divides $d!$.*

Proof. We follow Bombieri and Zannier's argument [2001]. Let M be a number field with $K \subset M \subset K_{ab}^{(d)}$. Then M/K is an abelian extension of exponent dividing $d!$,[4] and thus $\mathrm{Gal}(M/K)$ is isomorphic to a direct product $A_1 \times \cdots \times A_r$ of cyclic groups of order dividing $d!$. Therefore M can be written as composite field of extensions E of K of degree at most $d!$. Indeed, let $\varphi : A_1 \times \cdots \times A_r \to \mathrm{Gal}(M/K)$ be an isomorphism and let $E_i = \mathrm{Fix}(\varphi(H_i))$ where H_i is the subgroup that picks the trivial group in the i-th component and the full A_j in all other components. By the Galois-correspondence we have $\mathrm{Gal}(M/E_1 \cdots E_r) = \cap_i \varphi(H_i) = \varphi(\cap_i H_i) = \{id\}$. Hence, $M = E_1 \cdots E_r$. Now the largest power of a prime dividing the discriminant of E can be bounded solely in terms of K and d; see [Bombieri and Gubler 2006, Theorem B.2.12]. Thus, by Hermite's theorem, p_M, the largest prime that ramifies in M, tends to infinity as M runs over all such intermediate fields M.

For the second claim note that the inertia group $I(\mathfrak{B}/\mathfrak{p})$ is a subgroup of $\mathrm{Gal}(M/K)$, and so its order is not divisible by p, whenever $p > d$ is prime. Since the ramification index $e(\mathfrak{B}/\mathfrak{p})$ is equal to the order of $I(\mathfrak{B}/\mathfrak{p})$ it follows that $\mathfrak{p}$ is tamely ramified in M. Hence (see [Bombieri and Gubler 2006, B.2.18(e)]), $I(\mathfrak{B}/\mathfrak{p})$ is cyclic, and thus $e(\mathfrak{B}/\mathfrak{p})$ divides $d!$. □

Now let us show that Theorem 8 together with Lemma 10 implies Theorem 5.

Proof of Theorem 5. Let M be a number field with $K \subset M \subset K_{ab}^{(d)}$. Then M is abelian over K. By Lemma 10 $p_M > |D_{K/\mathbb{Q}}| + d$ for all but finitely many M, and thus we can assume p_M is unramified in K and $p_M > d$. Therefore, one of the prime ideal divisors of $p_M \mathcal{O}_K$, say $\mathfrak{p}$, must ramify in M. Let $\mathfrak{p}\mathcal{O}_M = (\mathfrak{B}_1 \cdots \mathfrak{B}_g)^e$ be the decomposition in $\mathcal{O}_M$ with $\mathfrak{B}_1, \ldots, \mathfrak{B}_g$ distinct prime ideals. Let T_i be the fixed field for the inertia group $I(\mathfrak{B}_i/\mathfrak{p})$, and let $\mathfrak{p}_i = \mathfrak{B}_i \cap T_i$. Then $e(\mathfrak{p}_i/\mathfrak{p}) = 1$, and $e = e(\mathfrak{B}_i/\mathfrak{p}_i) = [M : T_i]$. It follows that $\mathfrak{p}_i^{e-1} \mid D_{M/T_i}$, and that $f(\mathfrak{B}_i/\mathfrak{p}) = f(\mathfrak{p}_i/\mathfrak{p})$ for the residue degree. Now the $I(\mathfrak{B}_i/\mathfrak{p})$ are conjugated to each other and since M/K is abelian they are all equal, and thus all the fixed fields T_i are equal to T, say. Therefore $(\mathfrak{p}_1 \cdots \mathfrak{p}_g)^{e-1} \mid D_{M/T}$, which implies $p_M^{[M:K]/2} \le N_{T/\mathbb{Q}}(D_{M/T})$. Choosing $F = T$ in (1.4) shows that $\gamma(M/K) \ge p_M^{1/(2e[K:\mathbb{Q}])}$ which, by Lemma 10,

[4] If K_1, K_2 are two finite Galois extensions of K then $\sigma \to (\sigma_{|K_1}, \sigma_{|K_2})$ induces an injective group homomorphism from $\mathrm{Gal}(K_1K_2/K)$ to $\mathrm{Gal}(K_1/K) \times \mathrm{Gal}(K_2/K)$. This implies that for each Galois extension M/K with $M \subset K^{(d)}$ the Galois group $\mathrm{Gal}(M/K)$ has exponent dividing $d!$, and no prime $p > d$ divides the order of $\mathrm{Gal}(M/K)$.

tends to infinity as M runs over all number fields with $K \subset M \subset K_{ab}^{(d)}$. Applying Theorem 8 completes the proof. □

Remark 11. Alternatively, one can use the decomposition of M as compositum of extensions E of K of degree at most $d!$ as in the proof of Lemma 10. Hence, $\mathfrak{p}$ ramifies in at least one of the fields E, and thus $\mathfrak{p} \mid D_{E/K}$. Since $D_{M/K} = D_{E/K}^{[M:E]} N_{E/K}(D_{M/E})$ we conclude $\mathfrak{p}^{[M:E]} \mid D_{M/K}$. Since $\mathfrak{p}$ is unramified in T, and $D_{M/K} = D_{T/K}^{[M:T]} N_{T/K}(D_{M/T})$ we get $\mathfrak{p}^{[M:E]} \mid N_{T/K}(D_{M/T})$. Taking norms and using $[M:T] = e$ gives $\gamma(M/K) \geq p^{1/([K:\mathbb{Q}]d!e)}$.

To compare we now discuss Bombieri and Zannier's original proof of Theorem 5. We leave out some of the more technical details but the basic argument is as follows. We mostly use the notation of [Bombieri and Zannier 2001]; see also [Bombieri and Gubler 2006, Theorem 4.5.4] for a slightly more detailed approach.

Proof of Theorem 5 (after Bombieri and Zannier). By enlarging K we can assume K contains a primitive $d!$-th root of unity. Let $\alpha \in K_{ab}^{(d)}$ be of height at most X, and set $L = K(\alpha)$. Then L is abelian over K. Let $p > d$ be a prime unramified in K, let v be a place in K above p, and write e for the ramification index of v in L. Then e divides $d!$ by Lemma 10.

Now set $\theta = p^{1/e}$. Then $L(\theta)$ is again an abelian extension of K. Since $x^e - p \in K[x]$ is a v-Eisenstein polynomial it follows that $[K(\theta) : K] = e$ and v is totally ramified in $K(\theta)$. By Abhyankar's Lemma the ramification indices of the places in $L(\theta)$ above v are again e. As $\mathrm{Gal}(L(\theta)/K)$ is abelian the inertia groups of each place in $L(\theta)$ above v are equal, and of size e. Let U be their common fixed field, so that $[L(\theta) : U] = e$. Now v is unramified in U and totally ramified in $K(\theta)$ and thus $[U(\theta) : U] = e$. Hence, $L(\theta) = U(\theta)$, and thus

$$\alpha = \beta_0 + \beta_1\theta + \cdots + \beta_{e-1}\theta^{e-1}$$

for certain coefficients $\beta_i \in U$. Now the trace from $U(\theta)$ to U of $\alpha\theta^{-j}$ is the sum of the conjugates of $\alpha\theta^{-j}$ over U. It is not hard to see that this trace is also just $e\beta_j$. Combining both, and using standard height inequalities, gives an upper bound for the height of $\gamma_j := \beta_j p^{j/e}$ in terms of d and X.

Let us now assume that $1 \leq j \leq e-1$ and $b_j \neq 0$. Let u be a place in $U(\theta)$ above v, and let $\mathfrak{q} = \mathfrak{q}_u$ be the corresponding prime ideal in the ring of integers of $U(\theta)$. Then the exact order to which $\mathfrak{q}$ divides b_j is a (possibly negative) multiple of e, whereas the exact order to which it divides $p^{j/e}$ is j. This implies that the exact order to which $\mathfrak{q}$ divides γ_j is nonzero. Using this fact for all places in $U(\theta)$ above v yields a lower bound for the height of γ_j of the form $H(\gamma_j) \geq p^{1/(2e[K:\mathbb{Q}])}$, provided $1 \leq j \leq e-1$ and $b_j \neq 0$.

Combining the upper and lower bounds for the height of γ_j, and using that e is bounded in terms of d, gives an upper bound $B(K, d, X)$ for p in terms of d, $[K : \mathbb{Q}]$, and X, whenever one among $b_1, \dots, b_{e-1}$ is nonzero.

This means that for each place v of K lying above a prime $p > B(K, d, X)$ we have $\alpha \in U$, and v is unramified in U. Therefore, $K(\alpha)$ is unramified at each prime p whenever $p > B(K, d, X)$ (assuming, as we can, $B(K, d, X) > |D_{K/\mathbb{Q}}|$). But, by Lemma 10, the largest prime p ramifying in $K(\alpha)$ tends to infinity when $K(\alpha)$ runs over an infinite set of subfields of $K_{ab}^{(d)}$. Hence, we conclude that α lies in a number field, depending only on K, d and X, and thus, by Northcott's theorem, there are only finitely many possibilities for α. This completes the proof. □

The first proof of Theorem 5 (using Theorem 8) only requires e to be bounded in terms of d, whereas the second proof above requires the ramification index e to divide $d!$ to conclude that $L(\theta)/K$ is Galois (and abelian).

The fact that $K_{ab}^{(d)}/K$ is abelian is used in both proofs in three different ways, namely to ensure that:

(i) p_M in Lemma 10 tends to infinity.

(ii) M/K is Galois for every number field $K \subset M \subset K_{ab}^{(d)}$.

(iii) The inertia groups $I(\mathfrak{B}/\mathfrak{p})$ for the different prime ideals $\mathfrak{B} \subset \mathcal{O}_M$ above $\mathfrak{p} \subset \mathcal{O}_K$ are all equal.

The second claim of Lemma 10 remains true for $K^{(d)}/K$ (replace M by its Galois closure over K in the proof) but the proof of the first claim falls apart for $K^{(d)}$ when $d \geq 3$. This is because not all finite extensions of K in $K^{(d)}$ can be written as compositum of number fields of uniformly bounded degree over K as was shown by Checcoli [2013, Theorem 1], at least if $d \geq 27$. Gal and Grizzard [2014, Corollary 1.2] showed that $d \geq 3$ suffices.

However, Gal and Grizzard also showed [2014, Theorem 1.3] that every number field in $K^{(3)}$ that is Galois over K can be written as a compositum of extensions of K of degree at most 3. This means that if we only consider α in the set $K_G^{(3)} = \{\alpha \in K^{(3)}; K(\alpha)/K \text{ is Galois}\}$ then (i) and (ii) are automatically satisfied for each $M = K(\alpha)$. This raises the question whether $K_G^{(3)}$ has the Northcott property. An affirmative answer would be a significant extension of the case $d = 3$ in Theorem 5.

Acknowledgements

It is my pleasure to thank the anonymous referees for their numerous and valuable comments, they have substantially improved this article.

References

[Bombieri 2009] E. Bombieri, "Problems and results on the distribution of algebraic points on algebraic varieties", *J. Théor. Nombres Bordeaux* **21**:1 (2009), 41–57. MR Zbl

[Bombieri and Gubler 2006] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs **4**, Cambridge University Press, 2006. MR Zbl

[Bombieri and Zannier 2001] E. Bombieri and U. Zannier, "A note on heights in certain infinite extensions of $\mathbb{Q}$", *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei* (9) *Mat. Appl.* **12** (2001), 5–14. MR Zbl

[Checcoli 2013] S. Checcoli, "Fields of algebraic numbers with bounded local degrees and their properties", *Trans. Amer. Math. Soc.* **365**:4 (2013), 2223–2240. MR Zbl

[Checcoli and Dill 2023] S. Checcoli and G. A. Dill, "On a Galois property of fields generated by the torsion of an abelian variety", preprint, 2023. arXiv 2306.12138v2

[Checcoli and Fehm 2021] S. Checcoli and A. Fehm, "On the Northcott property and local degrees", *Proc. Amer. Math. Soc.* **149**:6 (2021), 2403–2414. MR Zbl

[Checcoli and Widmer 2013] S. Checcoli and M. Widmer, "On the Northcott property and other properties related to polynomial mappings", *Math. Proc. Cambridge Philos. Soc.* **155**:1 (2013), 1–12. MR Zbl

[Daans et al. 2023] N. Daans, V. Kala, and S. H. Man, "Universal quadratic forms and Northcott property of infinite number fields", preprint, 2023. arXiv 2308.16721v1

[Dvornicich and Zannier 2008] R. Dvornicich and U. Zannier, "On the properties of Northcott and of Narkiewicz for fields of algebraic numbers", *Funct. Approx. Comment. Math.* **39** (2008), 163–173. MR Zbl

[Ellenberg and Venkatesh 2007] J. S. Ellenberg and A. Venkatesh, "Reflection principles and bounds for class group torsion", *Int. Math. Res. Not.* **2007**:1 (2007), art. id. rnm002. MR Zbl

[Fehm 2018] A. Fehm, "Three counterexamples concerning the Northcott property of fields", *Atti Accad. Naz. Lincei Rend. Lincei Mat. Appl.* **29**:2 (2018), 309–314. MR Zbl

[Fili and Miner 2015] P. Fili and Z. Miner, "Equidistribution and the heights of totally real and totally p-adic numbers", *Acta Arith.* **170**:1 (2015), 15–25. MR Zbl

[Gal and Grizzard 2014] I. Gal and R. Grizzard, "On the compositum of all degree d extensions of a number field", *J. Théor. Nombres Bordeaux* **26**:3 (2014), 655–673. MR Zbl

[Gaudron and Rémond 2017] E. Gaudron and G. Rémond, "Corps de Siegel", *J. Reine Angew. Math.* **726** (2017), 187–247. MR Zbl

[Lang 1994] S. Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics **110**, Springer, 1994. MR Zbl

[Liardet 1972] P. Liardet, "Sur les transformations polynomiales et rationnelles", (1972), art. id. 29. MR Zbl

[Martínez-Ranero et al. 2020] C. Martínez-Ranero, J. Utreras, and C. R. Videla, "Undecidability of $\mathbb{Q}^{(2)}$", *Proc. Amer. Math. Soc.* **148**:3 (2020), 961–964. MR Zbl

[Narkiewicz 1963] W. Narkiewicz, "Problèmes", *Colloq. Math.* **10**:1 (1963), 183–187. Problème 414.

[Narkiewicz 1971] W. Narkiewicz, "Some unsolved problems", pp. 159–164 in *Colloque de Théorie des Nombres*, *Univ. Bordeaux* (Bordeaux, 1969), Supplément au Bull. Soc. Math. France **Tome 99**, Soc. Math. France, Paris, 1971. MR Zbl

[Narkiewicz 1995] W. a. a. Narkiewicz, *Polynomial mappings*, Lecture Notes in Mathematics **1600**, Springer, 1995. MR Zbl

[Northcott 1950] D. G. Northcott, "Periodic points on an algebraic variety", *Ann. of Math.* (2) **51** (1950), 167–177. MR Zbl

[Pottmeyer 2015] L. Pottmeyer, "Heights and totally p-adic numbers", *Acta Arith.* **171**:3 (2015), 277–291. MR Zbl

[Robinson 1962] J. Robinson, "On the decision problem for algebraic rings", pp. 297–304 in *Studies in mathematical analysis and related topics*, Stanford Studies in Mathematics and Statistics **IV**, Stanford Univ. Press, 1962. MR Zbl

[Roy and Thunder 1995] D. Roy and J. L. Thunder, "A note on Siegel's lemma over number fields", *Monatsh. Math.* **120**:3-4 (1995), 307–318. MR Zbl

[Roy and Thunder 1996] D. Roy and J. L. Thunder, "An absolute Siegel's lemma", *J. Reine Angew. Math.* **476** (1996), 1–26. MR Zbl

[Silverman 1984] J. H. Silverman, "Lower bounds for height functions", *Duke Math. J.* **51**:2 (1984), 395–403. MR Zbl

[Springer 2020] C. Springer, "Undecidability, unit groups, and some totally imaginary infinite extensions of $\mathbb{Q}$", *Proc. Amer. Math. Soc.* **148**:11 (2020), 4705–4715. MR Zbl

[Vidaux and Videla 2016] X. Vidaux and C. R. Videla, "A note on the Northcott property and undecidability", *Bull. Lond. Math. Soc.* **48**:1 (2016), 58–62. MR Zbl

[Widmer 2011] M. Widmer, "On certain infinite extensions of the rationals with Northcott property", *Monatsh. Math.* **162**:3 (2011), 341–353. MR Zbl

[Zhang 1995] S. Zhang, "Positive line bundles on arithmetic varieties", *J. Amer. Math. Soc.* **8**:1 (1995), 187–221. MR Zbl

Received 31 May 2022. Revised 27 Sep 2023.

MARTIN WIDMER:

martin.widmer@rhul.ac.uk

Department of Mathematics, Royal Holloway, University of London, Egham, United Kingdom

msp

Essential Number Theory
Vol. 2, No. 1, 2023
https://doi.org/10.2140/ent.2023.2.15

The Kelley–Meka bounds for sets free of three-term arithmetic progressions

Thomas F. Bloom and Olof Sisask

We give a self-contained exposition of the recent remarkable result of Kelley and Meka: if $A \subseteq \{1, \dots, N\}$ has no nontrivial three-term arithmetic progressions then $|A| \leq \exp(-c(\log N)^{1/12})N$, where $c > 0$ is a constant.

Although our proof is identical to that of Kelley and Meka in all of the main ideas, we also incorporate some minor simplifications relating to Bohr sets. This eases some of the technical difficulties tackled by Kelley and Meka and widens the scope of their method. As a consequence, we improve the lower bounds for the problem of finding long arithmetic progressions in $A + A + A$, where $A \subseteq \{1, \dots, N\}$.

How large can a subset of $\{1, \dots, N\}$ be without containing a nontrivial three-term arithmetic progression $\{a, a+d, a+2d\}$? (Nontrivial here means that $d \neq 0$.) This seemingly innocuous question, asked by Erdős and Turán [1936], has led to a wealth of interesting mathematics, and has become one of the central questions in additive combinatorics. A large part of the reason for this is that the tools and techniques that have been developed to tackle it, starting with the argument of Roth [1953], have turned out to be very influential, not only in dealing with other problems in additive number theory, but also in motivating the development of tools in other areas of mathematics — particularly in harmonic analysis.

This note gives an exposition of a recent remarkable breakthrough result of Kelley and Meka [2023] concerning this question: they prove a very strong upper bound for the maximal size of sets free of three-term progressions, far smaller than any previously available.

Let $A \subseteq \{1, \dots, N\}$ be a set which does not contain any (nontrivial) three-term arithmetic progressions. Even establishing that $|A| = o(N)$ is a difficult problem, this being Roth's landmark result [1953]. Since Roth's work there has been a sequence of quantitative improvements to the upper bound, all of the form $|A| \leq N/(\log N)^C$ for some constant $C > 0$, culminating in recent work of the authors [Bloom and Sisask 2020], who showed that $C = 1 + c$ is permissible, where $c > 0$ is some tiny constant (we refer to the introduction of [loc. cit.] for further history).

MSC2020: 11B25, 11B30.
Keywords: additive combinatorics, arithmetic progressions.

Kelley and Meka's new upper bound is of a whole new order of magnitude.

Theorem 1 (Kelley–Meka). *If $A \subseteq \{1, \dots, N\}$ contains no nontrivial three-term arithmetic progressions, then*

$$|A| \leq \frac{N}{\exp(c(\log N)^{1/12})}$$

for some absolute constant $c > 0$.

The Kelley–Meka bound is a huge leap forward, and tantalisingly close to the best possible such bound. Indeed, we know that there are subsets of $\{1, \dots, N\}$ of size at least $\exp(-c(\log N)^{1/2})N$, where $c > 0$ is some universal constant, that contain no nontrivial three-term progressions. This was first proved by Behrend [1946] using a beautiful construction that uses lattice points on high-dimensional spheres; small improvements have also been established by Elkin [2011] and Green and Wolf [2010]. Getting anywhere near Behrend-style bounds for this problem has been a long-standing goal in the area, and the argument of Kelley and Meka achieves this in a beautiful and elegant way.

Our reasons for writing this note are:

(1) To explain the Kelley–Meka approach using terminology and a perspective perhaps more familiar to researchers in additive combinatorics.

(2) To provide some minor technical refinements which allow for a proof of the full Theorem 1 which involves only "classical" Bohr set techniques, rather than the ad hoc method employed in [Kelley and Meka 2023] (in particular we answer [loc. cit., Question 6.2] of whether such an approach is possible in the affirmative). This widens the scope of potential applications over the integers, and allows for integer analogues of the other main results in [loc. cit.].

It must be made clear, however, that our sole contribution is at the technical level, allowing the Bohr set machinery to run a little more smoothly; all of the main ideas are the same as in [loc. cit.].

The finite field case. As usual in this area, a simpler model case is provided by replacing $\{1, \dots, N\}$ with the vector space $\mathbb{F}_q^n$. We will present Kelley and Meka's ideas in this model setting before the general case, since the former is technically much simpler, while still containing all of the important new ideas. Kelley and Meka's argument in $\mathbb{F}_q^n$ establishes the following.

Theorem 2 (Kelley–Meka). *If q is an odd prime and $A \subseteq \mathbb{F}_q^n$ has no nontrivial three-term progressions, then $|A| \leq q^{n-cn^{1/9}}$ for some constant $c > 0$.*

The utility of Theorem 2 is as a demonstration of the proof techniques, since for the result itself a stronger bound of $|A| \leq q^{n-cn}$ is available via the polynomial

method, as shown by Ellenberg and Gijswijt [2017]. Unfortunately, however, there is no known analogue of the polynomial method for the integer problem, so achieving strong bounds for the integer problem via this method is out of reach. Kelley and Meka's proof of Theorem 2 uses no polynomial methods, and instead uses techniques from probability and Fourier analysis, which can be generalised (using classical Bohr set machinery) to the integer setting.

After presenting the Kelley–Meka argument for $\mathbb{F}_q^n$ we will generalise this, using the language of Bohr sets, to prove Theorem 1. Kelley and Meka take a different, more ad hoc route, iterating over high-dimensional progressions. This is an ingenious alternative, that may itself have further applications, but our aim here is to show that more classical existing techniques also suffice. As a consequence, we can also establish the following integer analogue of [Kelley and Meka 2023, Corollary 1.12], which finds large subspaces in $A+A+A$ for $A \subseteq \mathbb{F}_q^n$.

Theorem 3. *If $A \subseteq \{1, \dots, N\}$ has size αN, then $A+A+A$ contains an arithmetic progression of length*

$$\geq \exp(-C \log(2/\alpha)^3) N^{c/\log(2/\alpha)^9},$$

where $C, c > 0$ are constants.

For comparison, the previously best bound known was $N^{\alpha^{1+o(1)}}$, originally due to Sanders [2008]. A construction due to Freiman, Halberstam, and Ruzsa [Freiman et al. 1992] shows that no exponent better than $c/\log(2/\alpha)$ is possible.

Kelley and Meka deduce the above bounds for sets without three-term arithmetic progressions, and more besides, from a more general type of structure result. This says, roughly speaking, that for any reasonably large set A inside a finite abelian group there exists some structured set V (e.g., an affine subspace in the $\mathbb{F}_q^n$ case) such that A restricted to V is very "regular" in its additive behaviour — that is, for "most" x the number of solutions to $x = a + b$ with $a, b \in A \cap V$ is very close to the average number of solutions.

We will first state a precise version of this structural result for $\mathbb{F}_q^n$. It is convenient to introduce the notion of a normalised indicator function: if $A \subseteq G$ is nonempty with size $|A| = \alpha |G|$ then we write $\mu_A = \alpha^{-1} 1_A$. (For a set A, we write 1_A for the indicator function of A, taking the value 1 on A and 0 elsewhere.) If $V \subseteq G$ and $1 \leq p < \infty$, then we denote the $L^p(V)$ norm of $f : G \to \mathbb{C}$ by

$$\|f\|_{p(\mu_V)} = \left(\frac{1}{|V|} \sum_{x \in V} |f(x)|^p \right)^{1/p}.$$

Note, for example, that our choice of normalisation is chosen to ensure $\|\mu_A\|_{1(\mu_G)} = 1$. We will measure the aforementioned regularity of $A \subseteq V$ by bounding the $L^p(V)$

norm of the difference between the convolution

$$\mu_A * \mu_A(x) = \frac{1}{|G|} \sum_{a,b \in G} 1_{a+b=x} \mu_A(a)\mu_A(b) = \frac{|G|}{|A|^2} \sum_{a,b \in A} 1_{a+b=x}$$

and its expected value. An elementary calculation shows that, when $V \leq G$ is a subgroup and $A \subseteq V$,

$$\|\mu_A * \mu_A\|_{1(\mu_V)} = \frac{|G|}{|V|} = \|\mu_V\|_{1(\mu_V)}.$$

That is, the average of $\mu_A * \mu_A$ over V agrees with the average of μ_V itself.

Note carefully that, even though we are taking a *local* L^p norm restricted to V we are keeping μ_A and $*$ normalised relative to the *global* group G. This is a little confusing at first, but when we move from $\mathbb{F}_q^n$ to general groups it is much more convenient to keep as many definitions as possible global, rather than relativising to the local V, since in general (e.g., when we move from $\mathbb{F}_q^n$ to $\mathbb{Z}/N\mathbb{Z}$) the subgroup V will be replaced with a set that is only approximately structured.

Theorem 4 (Kelley–Meka). *Let $\epsilon > 0$. There is a constant $C = C(\epsilon) > 0$ such that the following holds. Let $G = \mathbb{F}_q^n$ for some prime q and $n \geq 1$. Let $p \geq 1$. For any nonempty $A \subseteq G$ with $|A| = \alpha|G|$ there exists a subspace $V \leq G$ with*

$$\operatorname{codim}(V) \leq Cp^4 \log(2/\alpha)^5$$

and $x \in G$ such that, if $A' = (A - x) \cap V$, then

(1) $|A'| \geq (1 - \epsilon)\alpha|V|$ *and*

(2) $\|\mu_{A'} * \mu_{A'} - \mu_V\|_{p(\mu_V)} \leq \epsilon \frac{|G|}{|V|}$.

The factor $\frac{|G|}{|V|}$ here can be thought of as a normalising/scaling factor, corresponding to the fact that the convolution is defined over G rather than over V.

Intuitively, the second item of the conclusion says, as $p \to \infty$, that $\mu_{A'} * \mu_{A'} = (1 + O(\epsilon))\mu_V$ with high probability, as x ranges uniformly over V. Therefore, when studying many problems involving the additive behaviour of A', one can replace A' with a random subset of V of the same density. This is, of course, a very powerful tool. The cost is that we have had to restrict our original set A to an affine subspace $x + V$ to find this regularity, and so having the codimension of V be as small as possible is important for quantitative applications. For example, in the deduction of Theorem 2 from this one may take p to be around $\log(2/\alpha)$ and ϵ a constant. The resulting codimension bound of $C \log(2/\alpha)^9$ then corresponds to the exponent $\frac{1}{9}$ in Theorem 2.

The general group case: Bohr sets. To prove Theorems 1 and 3 we shall use a more general version of Theorem 4, applicable to any finite abelian group (which in applications will be $\mathbb{Z}/N\mathbb{Z}$). One difficulty in even writing down the appropriate statement is working out what should play the role of subspaces for general abelian groups. This is not obvious; fortunately for us, however, this was already done by Bourgain [1999], who showed that a suitable generalisation of a subspace, for these purposes, is a *Bohr set*. A Bohr set is an approximate level set of some characters, or more precisely, a set of the shape

$$B = \mathrm{Bohr}_\nu(\Gamma) = \{x \in G : |1 - \gamma(x)| \leq \nu \text{ for all } \gamma \in \Gamma\}$$

for some $\nu \geq 0$ (known as the width) and some $\Gamma \subseteq \widehat{G}$ (known as the frequency set). Often the most important thing about the frequency set is its size $d = |\Gamma|$, which is called the rank of the Bohr set.

Background material on Bohr sets can be found in the Appendix, but the unfamiliar reader can for now think of the above Bohr set B of rank $d = |\Gamma|$ as roughly like the embedding in G of the lattice points in a d-dimensional box in $\mathbb{R}^d$ of side-length proportional to ν. Writing B_ρ for the same Bohr set but with the "width" ν replaced by $\rho \cdot \nu$, one then has the approximate closure property that $B + B_\rho \approx B$ provided ρ is small — in particular, $B + B_\rho$ is not much larger than B provided ρ is small compared to $1/d$. It turns out that this approximate additive closure property of Bohr sets of rank d can, for the purposes of this paper, be used in place of the exact rigid structure provided by subspaces of codimension d in $\mathbb{F}_q^n$ (which are indeed Bohr sets themselves, of rank d and width $\nu = 0$).

Since Bohr sets only enjoy an approximate closure property, statements involving them necessarily require more technical conditions and quantitative overhead. This is why the use of the finite field model of $\mathbb{F}_q^n$ is invaluable in this area: an idea can be tested with subspaces in a relatively clean way, and only once the idea has been proven to have real quantitative strength does the work of translating the argument to work over general Bohr sets need to begin.

The following is the generalisation of Theorem 4 required for our applications. Kelley and Meka did not prove such a statement, but speculated that this should be possible in [Kelley and Meka 2023, Footnote 9].

The reader should compare the statement to Theorem 4, and at first reading may wish to pretend that $B = B' = B_\rho$ is the same subspace $V \leq \mathbb{F}_q^n$. For comparison to the conclusion of Theorem 4 it may help to note that, when B is a subspace and $A' \subseteq B$, then

$$\mu_B * \mu_B = \mu_B = \mu_{A'} * \mu_B,$$

and so

$$(\mu_{A'} - \mu_B) * (\mu_{A'} - \mu_B) = \mu_{A'} * \mu_{A'} - \mu_B.$$

Theorem 5. *There is a constant $c > 0$ such that the following holds. Let $\delta, \epsilon \in (0, 1)$, let $p \geq 1$ and let k be a positive integer such that $(k, |G|) = 1$. There is a constant $C = C(\epsilon, \delta, k) > 0$ such that the following holds.*

For any finite abelian group G and any subset $A \subseteq G$ with $|A| = \alpha|G|$ there exists a regular Bohr set B with

$$\mathrm{rk}(B) \leq Cp^4 \log(2/\alpha)^5$$

and

$$|B| \geq \exp(-Cp^5 \log(2p/\alpha) \log(2/\alpha)^6)|G|$$

and $A' \subseteq (A - x) \cap B$ for some $x \in G$ such that

(1) $|A'| \geq (1 - \epsilon)\alpha|B|$,

(2) $|A' \cap B'| \geq (1 - \epsilon)\alpha|B'|$, *where $B' = B_\rho$ is a regular Bohr set with $\rho \in \left(\frac{1}{2}, 1\right) \cdot c\delta\alpha/dk$, and*

$$\|(\mu_{A'} - \mu_B) * (\mu_{A'} - \mu_B)\|_{p(\mu_{k\cdot B'})} \leq \epsilon \frac{|G|}{|B|}. \tag{3}$$

In other words, for any dense set A, we can find a low-rank Bohr set B such that the restriction of (a translate of) A to B has almost the same relative density and has its convolution extremely balanced: it is close to its average, as measured in an L^p-sense over another large Bohr set. This roughly means that, when studying additive problems involving this restriction, we can replace A by a random set of the same density. Part (2) of the conclusion is there for somewhat technical reasons: since we need to work with both the Bohr set B and a narrowed copy B_ρ, as described above, we want to know that A' has large density on B_ρ as well as on B.

To give an idea of the parameters: to deduce Theorem 1, we shall take ϵ and δ some small constants, $k = 2$, and $p \asymp \log(2/\alpha)$. (The dependence on ϵ, δ, k is not hard to track explicitly, but is a distraction for the present applications.) An identical proof gives a statement with the measure $\mu_{k\cdot B'}$ in part (3) replaced by $\mu_{k\cdot B'+t}$ for any $t \in B$, or indeed μ_B or $\mu_B * \mu_B$, the latter two of which may appear more natural. These are, however, slightly weaker, and certainly for the application to three-term arithmetic progressions it is important that the measure over which the L^p norm is taken is supported on some suitably narrowed copy of B.

In Section 1 we provide an informal overview of the main steps of the argument. In Section 2 we prove what are, in our opinion, the most important steps of the argument in sufficient generality for the results over both $\mathbb{F}_q^n$ and $\{1, \dots, N\}$. In Section 3 we make the overview more precise and provide full proofs for the $\mathbb{F}_q^n$ case. Finally, in Sections 4 and 5 we show how this argument can be directly adapted for the integers using Bohr sets. We will proceed by proving Theorem 5 first and then deducing Theorems 1 and 3.

Improvements. Although Kelley and Meka's breakthrough is close to the best possible bound, there is still a gap between the exponent $\frac{1}{12}$ of Theorem 1 and the exponent $\frac{1}{2}$ in the Behrend example, and it is natural to ask whether further progress is possible. Indeed, a small modification of the method as presented in this paper allows for a slight improvement: the $\frac{1}{12}$ of Theorem 1 can be replaced by $\frac{1}{9}$ with a relatively clean argument (the only modification required is to the almost-periodicity part). A further tedious lengthy technical optimisation allows for an exponent of $\frac{5}{41}$. Since the focus of this paper is an exposition of the method and results of Kelley and Meka, we will detail these improvements in a separate forthcoming note. The same modification leads to an improvement of the exponent in Theorem 2 from $\frac{1}{9}$ to $\frac{1}{7}$, and an improvement of the exponent in Theorem 3 from 9 to 7.

We believe that an exponent of $\frac{1}{7}$ (in the statement of Theorem 1) is the natural limit of these methods, in that achieving anything better will require significant new ideas. Of course, the Behrend exponent of $\frac{1}{2}$ would be the final target, but this seems quite far out of reach still; indeed, an exponent of $\frac{1}{3}$ (or perhaps even $\frac{1}{4}$) seems to be the limit of any argument that uses any sort of "density increment" argument with Bohr sets (whether using Kelley–Meka ideas or a more traditional Fourier analytic approach).

Notational conventions. Logarithmic factors will appear often, and so in this paper we use the convenient abbreviation $\mathcal{L}(\alpha)$ to denote $\log(2/\alpha)$. (The 2 here is just a convenient device to make sure that $\mathcal{L}(\alpha) \geq \frac{1}{2}$, say, whenever $\alpha \in (0, 1]$.)

In statements which refer to G, this can be taken to be any finite abelian group (although for the applications this will always be either $\mathbb{F}_q^n$ or $\mathbb{Z}/N\mathbb{Z}$). We use the normalised counting measure on G, so that

$$\langle f, g\rangle = \mathop{\mathbb{E}}_{x\in G} f(x)\overline{g(x)} \quad \text{and} \quad \|f\|_p = \left(\mathop{\mathbb{E}}_{x\in G} |f(x)|^p\right)^{1/p} \text{ for } 1 \leq p < \infty,$$

where $\mathbb{E}_{x\in G} = \frac{1}{|G|}\sum_{x\in G}$. For any $f, g : G \to \mathbb{C}$ we define the convolution and the difference convolution[1] as

$$f * g(x) = \mathop{\mathbb{E}}_{y} f(y)g(x-y) \quad \text{and} \quad f \circ g(x) = \mathop{\mathbb{E}}_{y} f(x+y)\overline{g(y)}.$$

Note the useful adjoint property

$$\langle f, g * h\rangle = \langle f \circ h, g\rangle.$$

We furthermore write $f^{(p)}$ for the p-fold convolution $f^{(p)} = f * f * \cdots * f$, where there are p copies of f.

[1]We caution that, while convolution is commutative and associative, difference convolution is in general neither.

For some purposes it is conceptually cleaner to work relative to other nonnegative functions on G, so that if $\mu : G \to \mathbb{R}_{\geq 0}$ has $\|\mu\|_1 = 1$ we write

$$\langle f, g\rangle_\mu = \mathop{\mathbb{E}}_{x\in G} \mu(x) f(x)\overline{g(x)} \quad \text{and} \quad \|f\|_{p(\mu)} = \left(\mathop{\mathbb{E}}_{x\in G} \mu(x)|f(x)|^p\right)^{1/p}$$

for $1 \leq p < \infty$. (The special case above is the case when $\mu \equiv 1$.)

We use the slight abuse of notation that if $\mu : G \to \mathbb{R}_{\geq 0}$ with $\|\mu\|_1 = 1$, then $\mu(A) = \|1_A\|_{1(\mu)}$ is the density of A relative to μ. Unless specified otherwise, μ is the uniform measure on G. (So that, for example, $\mu(A) = \alpha = |A|/|G|$ is the density of A within G.) We write $\mu_A = \alpha^{-1}1_A$ for the normalised indicator function of A (so that $\|\mu_A\|_1 = 1$). We will sometimes speak of $A \subseteq B$ with relative density $\alpha = |A|/|B|$.

The Fourier transform of $f : G \to \mathbb{R}$ is $\hat{f} : \widehat{G} \to \mathbb{C}$ defined for $\gamma \in \widehat{G}$ as

$$\hat{f}(\gamma) = \mathop{\mathbb{E}}_{x\in G} f(x)\overline{\gamma(x)},$$

where $\widehat{G} = \{\gamma : G \to \mathbb{C}^\times : \gamma \text{ a homomorphism}\}$ is the dual group of G. We will also use convolution of functions $f, g : \widehat{G} \to \mathbb{C}$, defined as $f * g(\gamma) = \sum_{\chi\in\widehat{G}} f(\chi)g(\gamma - \chi)$, and denote k-fold convolution again by $f^{(k)}$ for such functions.[2] We note the following elementary facts:

- $\widehat{f * g} = \hat{f} \cdot \widehat{g}$ and $\widehat{f \circ f} = |\hat{f}|^2$ (so in particular the Fourier transform of $f \circ f$ is a nonnegative function on $\widehat{G}$).
- $\mathbb{E}_x f(x)^k = \hat{f} * \cdots * \hat{f}(0_{\widehat{G}})$, where the convolution is k-fold.
- If $\mu : G \to \mathbb{R}_{\geq 0}$ has $\|\mu\|_1 = 1$, then the Fourier transform of $\mu - 1$ is $\widehat{\mu}1_{\neq 0_{\widehat{G}}}$.

Note that these three facts immediately imply that the Fourier transform of $\mu_A \circ \mu_A - 1$ is nonnegative, that $\mathbb{E}(\mu_A \circ \mu_A - 1)^k \geq 0$ for any integer k, and (coupled with the triangle inequality) that $\|\mu_A * \mu_A - 1\|_p \leq \|\mu_A \circ \mu_A - 1\|_p$ when p is an even integer. Although easily seen via the Fourier transform, the latter two facts also have purely "physical" proofs, as we will see later.

Finally, we use the Vinogradov notation $X \ll Y$ to mean $X = O(Y)$, that is, there exists some constant $C > 0$ such that $|X| \leq CY$. We write $X \asymp Y$ to mean $X \ll Y$ and $Y \ll X$, and $X = \Omega(Y)$ to mean $Y = O(X)$. An expression like $1 + \Omega(1)$ thus means a quantity bounded below by an absolute constant strictly bigger than 1. The appearance of parameters as subscripts indicates that the implied constant may depend on these parameters (in some unspecified fashion).

[2]Note that we are using additive notation for the group operation on $\widehat{G}$.

1. Sketch of the argument

In this section we provide a sketch of the Kelley–Meka proof of the finite field model case, Theorem 2, along with some personal commentary and context. Kelley and Meka also include some fascinating comparisons of this approach with earlier work and speculations about it and alternative approaches, and we encourage the reader to study Appendices A and B of [Kelley and Meka 2023] and consider the interesting questions therein (although note that we answer their Question A.4 in the affirmative below).

Let $A \subseteq \mathbb{F}_q^n$ be a set of density α and $C \subseteq \mathbb{F}_q^n$ a set of density γ. (Note that a three-term arithmetic progression is a solution to $x + y = 2z$, and thus for their study we will choose

$$C = 2 \cdot A = \{2a : a \in A\},$$

in which case $\gamma = \alpha$.) How many solutions to $a_1 + a_2 = c$ with $a_1, a_2 \in A$ and $c \in C$ do we expect? If A, C are random sets, then we expect $\approx \alpha^2 \gamma q^{2n}$ many such solutions, which is to say

$$\langle \mu_A * \mu_A, \mu_C \rangle \approx 1.$$

The Kelley–Meka approach begins with some constant discrepancy from this expected count, say $\langle \mu_A * \mu_A, \mu_C \rangle \leq \frac{1}{2}$, and shows that this leads to a large density increment of A on some subspace $V \leq \mathbb{F}_q^n$ with codimension $O(\mathcal{L}(\alpha)^{O(1)})$ (that is, shows that there is such a subspace V and a translate A' of A such that $\mu_V(A') \geq (1 + \Omega(1))\alpha$, meaning that A' has significantly larger density in V than A has in $\mathbb{F}_q^n$). This is done using mostly physical-based methods, rather than the Fourier-based methods that have dominated the study of three-term progressions thus far.

Our presentation of the Kelley–Meka strategy breaks it down into five key steps.

Step 1 (Hölder lifting). If $\langle \mu_A * \mu_A, \mu_C \rangle \leq \frac{1}{2}$, then $\|\mu_A \circ \mu_A - 1\|_p \geq \frac{1}{4}$ for some $p \ll \mathcal{L}(\gamma)$.

This is essentially a one-line application of Hölder's inequality:

$$\tfrac{1}{2} \leq |\langle \mu_A * \mu_A - 1, \mu_C \rangle| \leq \|\mu_A * \mu_A - 1\|_p \|\mu_C\|_{p/(p-1)} \leq 2\|\mu_A * \mu_A - 1\|_p$$

for sufficiently large p, since $\|\mu_C\|_{p/(p-1)} = \gamma^{-1/p}$, and noting that $\|\mu_A * \mu_A - 1\|_p \leq \|\mu_A \circ \mu_A - 1\|_p$ when p is an even integer. Although trivial, the passage from few three-term arithmetic progressions to large L^p norm of $\mu_A \circ \mu_A - 1$ was rarely used in previous work, most of which begins with the Fourier deduction that $\sum_{\gamma \neq 0} |\widehat{\mu_A}(\gamma)|^2 |\widehat{\mu_C}(\gamma)| \gg 1$.

This physical Hölder step was used (along with almost-periodicity) in [Bloom and Sisask 2019] to achieve density bounds of $\alpha \leq (\log N)^{-1+o(1)}$. Indeed, in a sense the approach of [loc. cit.] corresponds to carrying out Steps 1, 4, and 5 of the

present sketch. The advancement of [Bloom and Sisask 2020] past the logarithmic density barrier couples this with delicate structural information on the Fourier side (following seminal ideas of Bateman and Katz [2012]).

It is incredible that the following two steps, which are simple enough to prove in only a couple of pages, perform far better quantitatively than this elaborate Fourier-side approach.

Step 2 (unbalancing). For any $f : G \to \mathbb{R}$ such that $\hat{f} \geq 0$, if $\|f\|_p \geq \frac{1}{4}$, then $\|f+1\|_{p'} \geq 1+\frac{1}{8}$ for some $p' \ll p$. In particular, if $\|\mu_A \circ \mu_A - 1\|_p \geq \frac{1}{4}$, then $\|\mu_A \circ \mu_A\|_{p'} \geq 1+\frac{1}{8}$.

This step is essential to the success of the Kelley–Meka argument, and rests on the fact that the Fourier transform of f is nonnegative. (Note that it is not true for an arbitrary function.) While the spectral nonnegativity of $\mu_A \circ \mu_A - 1$ has played a role in some arguments before (e.g., in the spectral boosting aspect of [Bloom and Sisask 2020]), to our knowledge it has not before been so cleanly expressed, and its potential had not been fully appreciated within additive combinatorics.

We remark that, as pointed out to the authors by Shkredov, an entirely physical proof of this step is possible, with no mention of the Fourier transform at all, if we replace the assumption $\hat{f} \geq 0$ with $f = g \circ g$ for some function $g : \mathbb{R} \to \mathbb{C}$ (note that this is indeed satisfied in our application since $\mu_A \circ \mu_A - 1 = (\mu_A - 1) \circ (\mu_A - 1)$). We refer to the proof of Lemma 7 for details.

At this point we digress to note that, instead of following Steps 1 and 2 as Kelley and Meka do, one could obtain the conclusion $\|\mu_A \circ \mu_A\|_p \geq 1 + \Omega(1)$ for some $p \ll \mathcal{L}(\gamma)$ from the assumption that $\langle \mu_A * \mu_A, \mu_C \rangle \leq \frac{1}{2}$ using more classical Fourier-based methods. (In particular this observation answers [Kelley and Meka 2023, Question A.4] in the affirmative.) By converting the inner product to Fourier space and applying the triangle inequality we observe that

$$\tfrac{1}{2} \leq \sum_{\lambda \neq 0} |\widehat{\mu_A}(\lambda)|^2 |\widehat{\mu_C}(\lambda)|.$$

It follows that, for some choice of signs $c_\lambda \in \mathbb{C}$, we have

$$1 + \tfrac{1}{2} \leq \sum_{\lambda} |\widehat{\mu_A}(\lambda)|^2 |\widehat{\mu_C}(\lambda)| = \mathop{\mathbb{E}}_{x \in C} \sum_{\lambda} c_\lambda |\widehat{\mu_A}(\lambda)|^2 \lambda(-x).$$

Applying Hölder's inequality to the left-hand side and using orthogonality of characters yields, for any even integer p,

$$1 + \tfrac{1}{2} \leq \gamma^{-1/p} \Bigg(\sum_{\lambda_1, \dots, \lambda_p} c_{\lambda_1} \cdots \overline{c_{\lambda_p}} |\widehat{\mu_A}(\lambda_1)|^2 \cdots |\widehat{\mu_A}(\lambda_p)|^2 1_{\lambda_1 + \cdots - \lambda_p = 0} \Bigg)^{1/p}.$$

We can discard the signs c_λ by the triangle inequality, and then by orthogonality the sum here is in fact equal to $\|\mu_A \circ \mu_A\|_p$, and we are done choosing p suitably large. This sort of step has already played a major role in previous Fourier-based approaches to Roth's theorem, although generally with the $\widehat{\mu_A}$ restricted to some "large spectrum", where it then yields information about the additive relations within this large spectrum. A striking feature of the work of Kelley and Meka is that this information is far more useful on the physical side.

We end our digression here and return to the sketch.

Step 3 (dependent random choice). If $\|\mu_A \circ \mu_A\|_p \geq 1 + \frac{1}{8}$, then there are $A_1, A_2 \subseteq A$ of density at least $\alpha^{O(p)}$ such that

$$\langle \mu_{A_1} \circ \mu_{A_2}, 1_S \rangle \geq 1 - \tfrac{1}{32}$$

where $S = \{x : \mu_A \circ \mu_A(x) > 1 + \frac{1}{16}\}$.

This is, in our opinion, the most important step (although of course every step is necessary, and in particular the previous unbalancing step is crucial to obtaining the information required for this step). In combination with the previous two steps, we have now converted the original three variable deficiency information of $\langle \mu_A * \mu_A, \mu_C \rangle \leq \frac{1}{2}$ into four variable abundancy information $\langle \mu_{A_1} \circ \mu_{A_2}, \mu_A \circ \mu_A \rangle \geq 1 + \Omega(1)$. This is very promising, since Schoen and the second author [Schoen and Sisask 2016] have already shown that almost-periodicity can prove quasipolynomial bounds (that is, of the same shape as the Kelley–Meka bound) for 4 variable equations. Another indication of the strength of the conclusion obtained in Step 3 is that Sanders [2012b] has shown (also using almost-periodicity) that S contains a large proportion of a large subspace with codimension $O(\mathcal{L}(\alpha)^{O(1)})$.

The proof of this step, called sifting in [Kelley and Meka 2023], is completely elementary, and uses dependent random choice — one takes A_i to be the intersection of p randomly chosen translates of A. A simple expectation calculation combined with the L^p information then verifies that there must exist some choice of translates which satisfy both the density conditions and the inner product condition.

Arguments of this kind have appeared before in additive combinatorics, dating back in some form to Gowers' proof [1998] of Szemerédi's theorem. For example, when $p = 2$ this method was used by Schoen [2015] to prove strong bounds for the Balog–Szemerédi–Gowers theorem, and similar manipulations for larger p have played an extensive role in work of Schoen and Shkredov; see for example [Schoen and Shkredov 2013; Shkredov 2013]. A very similar statement also appears in work of Sanders [2010, Lemma 1.9], itself a generalisation of an argument of Gowers [1998, Lemma 11].

Despite this previous work, the true potential of this method (when coupled with the powerful technique of almost-periodicity) in applications to the study

of three-term progressions and related problems had been overlooked before the breakthrough of Kelley and Meka.

Step 4 (almost periodicity). For any sets $A_1, A_2, S \subseteq \mathbb{F}_q^n$, if A_1, A_2 have density at least α, then there is a subspace V with codimension $O(\mathcal{L}(\alpha)^4)$ such that

$$|\langle \mu_V * \mu_{A_1} \circ \mu_{A_2}, 1_S\rangle - \langle \mu_{A_1} \circ \mu_{A_2}, 1_S\rangle| \leq \tfrac{1}{100}.$$

Almost-periodicity statements of this type have played an important role in additive combinatorics since their introduction by Croot and the second author [Croot and Sisask 2010], most notably in the work of Sanders achieving quasipolynomial bounds for inverse sumset theorems [Sanders 2012b; 2013]. The conventional wisdom was that, despite their success in inverse sumset problems and for translation invariant equations in four or more variables (see [Schoen and Sisask 2016] and the earlier [Schoen and Shkredov 2014] for six or more variables), they were not able to achieve significant results for three-term arithmetic progressions. (Although the argument of [Bloom and Sisask 2020] did make fundamental use of almost-periodicity, most of the work in that paper was Fourier-analytic.) Kelley and Meka have dispelled this illusion completely.

It should be noted, however, that there is no novelty in the actual form of almost-periodicity used by Kelley and Meka — the new strength is a result of the context in which they use it.

Step 5 (density increment). If $\langle \mu_A * \mu_A, \mu_C\rangle \leq \frac{1}{2}$, then there is an affine subspace V of codimension $O(\mathcal{L}(\alpha)^4\mathcal{L}(\gamma)^4)$ on which A has density at least $\big(1 + \frac{1}{100}\big)\alpha$.

This is just a trivial combination of the previous 4 steps (noting that the density increment condition can also be phrased as $\|\mu_A * \mu_V\|_\infty \geq 1 + \frac{1}{100}$). This density increment condition can now be iteratively applied to eventually obtain a lower bound for $\langle \mu_{A'} * \mu_{A'}, \mu_C\rangle$ (with A' now perhaps some subset of a translate of A).

For example, the deduction of Theorem 2 is routine with $C = 2 \cdot A$. Indeed, a density increment such as $\alpha \mapsto (1 + \Omega(1))\alpha$ can occur at most $O(\mathcal{L}(\alpha))$ many times, after which we must halt with many three-term arithmetic progressions found in the intersection of A with some affine subspace, the codimension of which is bounded above by $O(\mathcal{L}(\alpha)^9)$.

Alternatively, carrying through these steps with C being the complement of $A + A$ leads to the following.

Theorem 6 (Kelley–Meka). *If $A \subseteq \mathbb{F}_q^n$ has density α and $\gamma \in (0, 1]$, then there is some affine subspace $V \leq \mathbb{F}_q^n$ of codimension $O(\mathcal{L}(\alpha)^5\mathcal{L}(\gamma)^4)$ such that*

$$|(A + A) \cap V| \geq (1 - \gamma)|V|.$$

For comparison, the best bound previously available, due to Sanders [2012b], had codimension $O(\mathcal{L}(\alpha)^4\gamma^{-2})$. The latter is slightly better when γ is constant (as

was the case of interest in [loc. cit.]) but much weaker when $\gamma \approx \alpha$, which is the regime of interest for three-term arithmetic progressions.

2. The key new lemmas

In this section we prove general forms of Steps 2 and 3 that will be used for both the $\mathbb{F}_q^n$ and integer case.

2.1. ***Unbalancing of spectrally nonnegative functions.*** The following precise form of Step 2 will suffice for all our applications.

Lemma 7. *Let $\epsilon \in (0,1)$ and $\nu : G \to \mathbb{R}_{\geq 0}$ satisfy $\|\nu\|_1 = 1$ and $\widehat{\nu} \geq 0$. Let $f : G \to \mathbb{R}$ be such that $\hat{f} \geq 0$. (Or, alternatively, assume that $f = g \circ g$ and $\nu = h \circ h$ for some $g, h : G \to \mathbb{C}$.)*

If $\|f\|_{p(\nu)} \geq \epsilon$ for some $p \geq 1$, then

$$\|f + 1\|_{p'(\nu)} \geq 1 + \tfrac{1}{2}\epsilon$$

for some $p' \ll_\epsilon p$.

We have left the dependence on ϵ unspecified since our applications only use $\epsilon \gg 1$. The proof below delivers $p' \ll \epsilon^{-1}\log(\epsilon^{-1})p$. Kelley and Meka use a different method (see [Kelley and Meka 2023, Appendix D]) which is more efficient, giving $p' \ll \epsilon^{-1}p$, but requires use of an external (though simple) fact about the binomial distribution.

Proof. We first establish the important fact that, for any integer $k \geq 1$,

$$\langle \nu, f^k \rangle \geq 0. \tag{1}$$

We will give two proofs of (1), depending on whether the Fourier assumption $\hat{f}, \widehat{\nu} \geq 0$ or the physical assumption $f = g \circ g$ and $\nu = h \circ h$ is used. Given (1) no further use of the Fourier transform is required, and the proofs converge.

The Fourier proof of (1), which is used by Kelley and Meka, is immediate from Parseval's identity:

$$\langle \nu, f^k \rangle = \langle \widehat{\nu}, \hat{f}^{(k)} \rangle,$$

where we recall that $f^{(k)} = f * f * \cdots * f$ denotes the k-fold convolution, and the right-hand side is nonnegative since $\hat{f}, \widehat{\nu} \geq 0$.

We now present the alternative physical proof of (1), assuming $f = g \circ g$ and $\nu = h \circ h$. This argument was pointed out to the authors by Shkredov, who has made extensive use of the following kind of manipulations; for example in [Shkredov

2013]. We observe that

$$\begin{aligned}\langle \nu, f^k\rangle &= \mathop{\mathbb{E}}_x h\circ h(x) g\circ g(x)^k\\ &= \mathop{\mathbb{E}}_{y_1,y_2} h(y_1)\overline{h(y_2)}\Big(\mathop{\mathbb{E}}_z g(y_1+z)\overline{g(y_2+z)}\Big)^k\\ &= \mathop{\mathbb{E}}_{z_1,\dots,z_k}\mathop{\mathbb{E}}_{y_1,y_2} h(y_1)\overline{h(y_2)}g(y_1+z_1)\cdots\overline{g(y_2+z_k)}\\ &= \mathop{\mathbb{E}}_{z_1,\dots,z_k}\Big|\mathop{\mathbb{E}}_y h(y)g(y+z_1)\cdots g(y+z_k)\Big|^2,\end{aligned}$$

which is clearly nonnegative as each summand is.

We now show how (1) implies the conclusion. Without loss of generality we can assume that $p\geq 5$ is an odd integer. Using (1), since $2\max(x,0)=x+|x|$ for $x\in\mathbb{R}$ and $f^{p-1}=|f|^{p-1}$, we have

$$2\langle \max(f,0), f^{p-1}\rangle_\nu = \langle \nu, f^p\rangle + \langle |f|, f^{p-1}\rangle_\nu \geq \|f\|_{p(\nu)}^p \geq \epsilon^p.$$

Therefore, if $P=\{x : f(x)\geq 0\}$, then $\langle 1_P, f^p\rangle_\nu \geq \frac{1}{2}\epsilon^p$. Furthermore, if $T=\big\{x\in P : f(x)\geq \frac{3}{4}\epsilon\big\}$, then $\langle 1_{P\setminus T}, f^p\rangle_\nu < \big(\frac{3}{4}\epsilon\big)^p \leq \frac{1}{4}\epsilon^p$, and hence by the Cauchy–Schwarz inequality

$$\nu(T)^{1/2}\|f\|_{2p(\nu)}^p \geq \langle 1_T, f^p\rangle_\nu \geq \tfrac{1}{4}\epsilon^p.$$

On the other hand, by the triangle inequality

$$\|f\|_{2p(\nu)} \leq 1+\|f+1\|_{2p(\nu)} \leq 3,$$

or else we are done, with $p'=2p$. Hence $\nu(T)\geq(\epsilon/10)^{2p}$. It follows that, for any $p'\geq 1$,

$$\|f+1\|_{p'(\nu)} \geq \langle 1_T, |f+1|^{p'}\rangle_\nu^{1/p'} \geq \big(1+\tfrac{3}{4}\epsilon\big)(\epsilon/10)^{2p/p'}.$$

The desired bound now follows if we choose p' a sufficiently large multiple (depending on ϵ) of p. □

2.2. ***An application of dependent random choice.*** We now use dependent random choice (or what Kelley and Meka call "sifting") to prove a general form of Step 3. This makes use of (a generalisation of) the fact that

$$\|1_A\circ 1_A\|_p^p = \mathop{\mathbb{E}}_{s_1,\dots,s_p\in G}\mu((A+s_1)\cap\cdots\cap(A+s_p))^2$$

to convert L^p-information about a convolution to information about the nested intersections appearing in the right-hand side. This identity features extensively in some works of Shkredov (see [Shkredov 2013] for example) and Schoen and Shkredov [2014], and is already implicitly used in work of Sanders [2010, Lemma 1.9], but its

strength and utility in the current context was far from apparent before the work of Kelley and Meka. At a first reading of the following result the reader may wish to take $B_1 = B_2 = G$, in which case $\mu = \mu_{B_1} \circ \mu_{B_2}$ is just the usual uniform measure on G.

Lemma 8. *Let $p \geq 1$ be an integer and $\epsilon, \delta > 0$. Let $B_1, B_2 \subseteq G$, and let $\mu = \mu_{B_1} \circ \mu_{B_2}$. For any finite set $A \subseteq G$ with density α, if*

$$S = \{x \in G : \mu_A \circ \mu_A(x) > (1-\epsilon)\|\mu_A \circ \mu_A\|_{p(\mu)}\},$$

then there are $A_1 \subseteq B_1$ and $A_2 \subseteq B_2$ such that

$$\langle \mu_{A_1} \circ \mu_{A_2}, 1_S \rangle \geq 1 - \delta$$

and

$$\min\left(\frac{|A_1|}{|B_1|}, \frac{|A_2|}{|B_2|}\right) \gg (\alpha\|\mu_A \circ \mu_A\|_{p(\mu)})^{2p+O_{\epsilon,\delta}(1)}.$$

Again, since we will apply this only in the case $\epsilon, \delta \gg 1$, we are not concerned with the behaviour of the $O_{\epsilon,\delta}(1)$ term, although we record here that the proof (which is identical to that in [Kelley and Meka 2023]) in fact allows for $O(\epsilon^{-1}\log(\delta^{-1}))$. We furthermore note that A_i will take the form $B_i \cap (A + s_1) \cap \cdots \cap (A + s_p)$ for some randomly chosen shifts $s_j \in G$.

We shall prove Lemma 8 after Lemma 10 below, but first we note the following immediate special case, which is all we use when studying $\mathbb{F}_q^n$.

Corollary 9. *Let $p \geq 1$ be an integer and $\epsilon > 0$. If $A \subseteq G$ is such that $\|\mu_A \circ \mu_A\|_p \geq 1 + \epsilon$ and $S = \{x : \mu_A \circ \mu_A(x) > 1 + \epsilon/2\}$, then there are $A_1, A_2 \subseteq G$, both of density*

$$\gg \alpha^{2p+O_\epsilon(1)},$$

such that

$$\langle \mu_{A_1} \circ \mu_{A_2}, 1_S \rangle \geq 1 - \epsilon/8.$$

We encode the dependent random choice argument underpinning Lemma 8 as the following general lemma.

Lemma 10. *Let $p \geq 2$ be an even integer. Let $B_1, B_2 \subseteq G$ and $\mu = \mu_{B_1} \circ \mu_{B_2}$. For any finite set $A \subseteq G$ with density α and function $f : G \to \mathbb{R}_{\geq 0}$ there exist $A_1 \subseteq B_1$ and $A_2 \subseteq B_2$ such that*

$$\langle \mu_{A_1} \circ \mu_{A_2}, f \rangle \leq 2\frac{\langle (\mu_A \circ \mu_A)^p, f \rangle_\mu}{\|\mu_A \circ \mu_A\|_{p(\mu)}^p}$$

and

$$\min\left(\frac{|A_1|}{|B_1|}, \frac{|A_2|}{|B_2|}\right) \geq \tfrac{1}{4}\alpha^{2p}\|\mu_A \circ \mu_A\|_{p(\mu)}^{2p}.$$

Proof. For $s \in G^p$ let $A_1(s) = B_1 \cap (A+s_1) \cap \cdots \cap (A+s_p)$, and similarly for $A_2(s)$. Note that

$$\begin{aligned}\langle (\mu_A \circ \mu_A)^p, f\rangle_\mu &= \mathop{\mathbb{E}}_{\substack{b_1\in B_1\\ b_2\in B_2}} \mu_A\circ\mu_A(b_1-b_2)^p f(b_1-b_2)\\ &= \mathop{\mathbb{E}}_{\substack{b_1\in B_1\\ b_2\in B_2}} \left(\alpha^{-2}\mathop{\mathbb{E}}_{t\in G} 1_{A+t}(b_1)1_{A+t}(b_2)\right)^p f(b_1-b_2)\\ &= \alpha^{-2p}\mathop{\mathbb{E}}_{\substack{b_1\in B_1\\ b_2\in B_2}}\mathop{\mathbb{E}}_{s\in G^p} 1_{A_1(s)}(b_1)1_{A_2(s)}(b_2) f(b_1-b_2)\\ &= \tfrac{\alpha^{-2p}|G|^2}{|B_1||B_2|}\mathop{\mathbb{E}}_{s\in G^p}\langle 1_{A_1(s)}\circ 1_{A_2(s)}, f\rangle.\end{aligned}$$

In particular, applying this with $f\equiv 1$ we see that, if $\alpha_i(s) = |A_i(s)|/|G|$, then

$$\|\mu_A\circ\mu_A\|_{p(\mu)}^p = \tfrac{\alpha^{-2p}|G|^2}{|B_1||B_2|}\mathop{\mathbb{E}}_s \alpha_1(s)\alpha_2(s)$$

and

$$\frac{\langle (\mu_A\circ\mu_A)^p, f\rangle_\mu}{\|\mu_A\circ\mu_A\|_{p(\mu)}^p} = \frac{\mathbb{E}_s\langle 1_{A_1(s)}\circ 1_{A_2(s)}, f\rangle}{\mathbb{E}_s\,\alpha_1(s)\alpha_2(s)} = \eta,$$

say. Note that, if

$$M = \tfrac{1}{2}\alpha^p(|B_1||B_2|/|G|^2)^{1/2}\|\mu_A\circ\mu_A\|_{p(\mu)}^p,$$

then

$$\begin{aligned}\mathop{\mathbb{E}}_s 1_{\alpha_1(s)\alpha_2(s)<M^2}\alpha_1(s)\alpha_2(s) &< M\left(\mathop{\mathbb{E}}_s\mathop{\mathbb{E}}_{x\in G} 1_{A_1(s)}(x)\right)^{1/2}\left(\mathop{\mathbb{E}}_s\mathop{\mathbb{E}}_{x\in G} 1_{A_2(s)}(x)\right)^{1/2}\\ &= M\alpha^p(|B_1||B_2|/|G|^2)^{1/2}\\ &= \tfrac{1}{2}\mathop{\mathbb{E}}_s\alpha_1(s)\alpha_2(s)\end{aligned}$$

and so

$$\mathop{\mathbb{E}}_s\langle 1_{A_1(s)}\circ 1_{A_2(s)}, f\rangle = \eta\mathop{\mathbb{E}}_s\alpha_1(s)\alpha_2(s) < 2\eta\mathop{\mathbb{E}}_s\alpha_1(s)\alpha_2(s)1_{\alpha_1(s)\alpha_2(s)\geq M^2}.$$

In particular there must exist some s such that

$$\langle 1_{A_1(s)}\circ 1_{A_2(s)}, f\rangle < 2\eta\alpha_1(s)\alpha_2(s)1_{\alpha_1(s)\alpha_2(s)\geq M^2},$$

and the claim follows (note that the left-hand side is trivially ≥ 0 and hence such an s must satisfy $\alpha_1(s)\alpha_2(s)\geq M^2$). □

The deduction of Lemma 8 is immediate from Lemma 10 with $f = 1_{G\setminus S}$. Indeed, by nesting of L^p norms we can assume that p is sufficiently large in terms of ϵ and δ (this is where the $O_{\epsilon,\delta}(1)$ term arises in the exponent), and that p is an even integer. It then suffices to note that

$$\langle \mu_{A_1} \circ \mu_{A_2}, 1_S \rangle = 1 - \langle \mu_{A_1} \circ \mu_{A_2}, 1_{G\setminus S} \rangle$$

and by definition of S we have

$$\frac{\langle (\mu_A \circ \mu_A)^p, 1_{G\setminus S} \rangle}{\|\mu_A \circ \mu_A\|_p^p} \leq (1-\epsilon)^p$$

which is $\leq \delta/2$ if p is large enough.

3. The finite field case

In this section we prove Theorem 2, following the sketch of Section 1. Theorem 4 can proved in a very similar way. The following straightforward lemma is a form of Step 1.

Lemma 11. *Let $\epsilon > 0$. If $A, C \subseteq G$, where C has density at least γ, then either*

(1) $|\langle \mu_A * \mu_A, \mu_C \rangle - 1| \leq \epsilon$ *or*

(2) $\|\mu_A \circ \mu_A - 1\|_p \geq \epsilon/2$ *for some* $p \ll \mathcal{L}(\gamma)$.

Proof. If the first alternative fails, then by Hölder's inequality, for any $p \geq 1$

$$\epsilon < |\langle \mu_A * \mu_A - 1, \mu_C \rangle| \leq \|\mu_A * \mu_A - 1\|_p \gamma^{-1/p}.$$

In particular, if we choose $p = 2\lceil K\mathcal{L}(\gamma)\rceil$ for some large constant K, then we deduce that

$$\|\mu_A * \mu_A - 1\|_p \geq \tfrac{1}{2}\epsilon.$$

It remains to note that, assuming without loss of generality that p is an even integer,

$$\|\mu_A * \mu_A - 1\|_p^p = (\widehat{\mu_A}^2 1_{\neq 0_{\widehat{G}}})^{(p)}(0_{\widehat{G}}) \leq (|\widehat{\mu_A}|^2 1_{\neq 0_{\widehat{G}}})^{(p)}(0_{\widehat{G}}) = \|\mu_A \circ \mu_A - 1\|_p^p.$$

Again, although we have used a one-line Fourier proof here, this can also be seen using an entirely physical argument, which we sketch here. Note that $\mu_A * \mu_A - 1 = (\mu_A - 1) * (\mu_A - 1)$ and similarly for $\mu_A \circ \mu_A - 1$. It suffices therefore to show that, for any function $f : G \to \mathbb{C}$, we have

$$\|f * f\|_p^p \leq \|f \circ f\|_p^p.$$

We can write the left-hand side as

$$\|f*f\|_p^p = \mathop{\mathbb{E}}_{x,y}\Big(\mathop{\mathbb{E}}_{u} f(x+u)f(y-u)\Big)^p$$
$$= \mathop{\mathbb{E}}_{u_1,\dots,u_p}\Big(\mathop{\mathbb{E}}_{x} f(x+u_1)\cdots f(x+u_p)\Big)\Big(\mathop{\mathbb{E}}_{y} f(y-u_1)\cdots f(y-u_p)\Big)$$

and the right-hand side as

$$\|f\circ f\|_p^p = \mathop{\mathbb{E}}_{x,y}\Big(\mathop{\mathbb{E}}_{u} f(x+u)\overline{f(y+u)}\Big)^p = \mathop{\mathbb{E}}_{u_1,\dots,u_p}\Big|\mathop{\mathbb{E}}_{x} f(x+u_1)\cdots f(x+u_p)\Big|^2,$$

and the desired inequality now follows from the Cauchy–Schwarz inequality. □

Steps 2 and 3 have already been proved as Lemma 7 and Corollary 9. For Step 4 we can use the following almost-periodicity result, which is [Schoen and Sisask 2016, Theorem 3.2], as a black box.

Theorem 12 (almost-periodicity). *If $A_1, A_2, S \subseteq \mathbb{F}_q^n$ are such that A_1 and A_2 both have density at least α, then there is a subspace V of codimension*

$$\operatorname{codim}(V) \ll_\epsilon \mathcal{L}(\alpha)^4$$

such that

$$|\langle \mu_V * \mu_{A_1} * \mu_{A_2}, 1_S\rangle - \langle \mu_{A_1} * \mu_{A_2}, 1_S\rangle| \le \epsilon.$$

Importantly, note that no assumption is made on S, and there is no dependency on the density of S. We now complete the final step by combining everything thus far into a single density increment statement, which suffices for Theorem 2 as discussed in Section 1.

Proposition 13. *Let $\epsilon \in (0,1)$. If $A, C \subseteq \mathbb{F}_q^n$, where C has density at least γ, then either*

(1) $|\langle \mu_A * \mu_A, \mu_C\rangle - 1| \le \epsilon$ *or*

(2) *there is a subspace V of codimension*

$$\ll_\epsilon \mathcal{L}(\gamma)^4\mathcal{L}(\alpha)^4$$

such that $\|1_A * \mu_V\|_\infty \ge (1+\Omega(\epsilon))\alpha$.

Proof. By Lemma 11, if the first alternative fails, then $\|\mu_A \circ \mu_A - 1\|_p \ge \epsilon/2$ for some $p \ll \mathcal{L}(\gamma)$. By Lemma 7 (applied to $f = \mu_A \circ \mu_A - 1$) we deduce that $\|\mu_A \circ \mu_A\|_p \ge 1 + \epsilon/4$ for some $p \ll_\epsilon \mathcal{L}(\gamma)$. Hence, by Corollary 9, there are A_1, A_2, both of density

$$\ge \alpha^{O_\epsilon(\mathcal{L}(\gamma))},$$

such that

$$\langle \mu_{A_1} \circ \mu_{A_2}, 1_S \rangle \geq 1 - \epsilon/32,$$

where $S = \{x : \mu_A \circ \mu_A(x) \geq 1 + \epsilon/8\}$. By Theorem 12 there is a subspace V of the required codimension such that

$$\langle \mu_V * \mu_{A_1} \circ \mu_{A_2}, 1_S \rangle \geq 1 - \tfrac{1}{16}\epsilon.$$

By definition of S, it follows that

$$\begin{aligned} 1 + \Omega(\epsilon) &\leq (1 + \epsilon/8)(1 - \epsilon/16) \\ &\leq \langle \mu_V * \mu_{A_1} \circ \mu_{A_2}, \mu_A \circ \mu_A \rangle \\ &\leq \|\mu_V * \mu_A\|_\infty \|\mu_A * \mu_{A_2} \circ \mu_{A_1}\|_1 \\ &= \|\mu_V * 1_A\|_\infty \alpha^{-1}, \end{aligned}$$

and the proof is complete. □

4. The integer case

A useful strategy in additive combinatorics is to first prove a result of interest over $\mathbb{F}_q^n$, making use of the abundancy of subspaces, and then translate this to a result over the integers, replacing various equalities with approximate equalities and subspaces with Bohr sets.

Bohr sets of low rank are analogues of subspaces of low codimension, and have played a central role in additive combinatorics since the work of Bourgain [1999], with much of the theory further developed by Sanders [2011; 2012a]. We have recalled the relevant definitions and properties in the Appendix.

In this section we will employ Steps 3, 4, and 5 of the Kelley–Meka approach, performed relative to Bohr sets, to prove the following technical statement, whose statement is convenient for the iterative proof. In the following section we will show how it, together with unbalancing and the regularity of Bohr sets, implies Theorem 5, and thence Theorems 1 and 3.

We apologise for the daunting appearance and technicality of the statements in this and the next section; a certain overhead of notation and caveats is a sad fact of life when working with Bohr sets. The reader should be reassured, however, that all the essential ideas are as in the $\mathbb{F}_q^n$ case.

The approach taken here should be compared with that in [Kelley and Meka 2023, Section 8] — there Kelley and Meka also follow the $\mathbb{F}_q^n$ model, but instead use mixed analogues over multidimensional progressions and Bohr sets, instead of just Bohr sets as we do here. The two objects are, in a heuristic sense, identical, but the need to pass between them adds some complexity to the argument of Kelley and Meka.

Theorem 14. *There is a constant $c > 0$ such that the following holds. Let $\epsilon, \delta \in (0,1)$ and $p, k \geq 1$ be integers such that $(k, |G|) = 1$. For any $A \subseteq G$ with density α there is a regular Bohr set B with*

$$d = \mathrm{rk}(B) = O_\epsilon(\mathcal{L}(\alpha)^5 p^4) \quad \text{and} \quad |B| \geq \exp(-O_{\epsilon,\delta}(\mathcal{L}(\alpha)^6 p^5 \mathcal{L}(\alpha/p)))|G|$$

and some $A' \subseteq (A-x) \cap B$ for some $x \in G$ such that

(1) $|A'| \geq (1-\epsilon)\alpha|B|$,

(2) $|A' \cap B'| \geq (1-\epsilon)\alpha|B'|$, *where $B' = B_\rho$ is a regular Bohr set with $\rho \in \left(\frac{1}{2}, 1\right) \cdot c\delta\alpha/d$, and*

(3) $\|\mu_{A'} \circ \mu_{A'}\|_{p(\mu_{k\cdot B''} \circ \mu_{k\cdot B''} * \mu_{k\cdot B'''} \circ \mu_{k\cdot B'''})} < (1+\epsilon)\mu(B)^{-1}$, *for any regular Bohr sets $B'' = B'_{\rho'}$ and $B''' = B''_{\rho''}$ satisfying $\rho', \rho'' \in \left(\frac{1}{2}, 1\right) \cdot c\delta\alpha/d$.*

The proof of Theorem 14 proceeds by repeated application of the following statement, which is suitable for iteration.

Proposition 15. *There is a constant $c > 0$ such that the following holds. Let $\epsilon > 0$ and $p, k \geq 1$ be integers such that $(k, |G|) = 1$. Let $B, B', B'' \subseteq G$ be regular Bohr sets of rank d such that $B'' \subseteq B'_{c/d}$ and $A \subseteq B$ with relative density α. If*

$$\|\mu_A \circ \mu_A\|_{p(\mu_{k\cdot B'} \circ \mu_{k\cdot B'} * \mu_{k\cdot B''} \circ \mu_{k\cdot B''})} \geq (1+\epsilon)\mu(B)^{-1},$$

then there is a regular Bohr set $B''' \subseteq B''$ of rank at most

$$\mathrm{rk}(B''') \leq d + O_\epsilon(\mathcal{L}(\alpha)^4 p^4)$$

and size

$$|B'''| \geq \exp(-O_\epsilon(dp\mathcal{L}(\alpha/d) + \mathcal{L}(\alpha)^5 p^5))|B''|$$

such that

$$\|\mu_{B'''} * \mu_A\|_\infty \geq (1+c\epsilon)\mu(B)^{-1}.$$

We first explain how Theorem 14 follows by iteration. In doing so we shall require a regularity "narrowing" trick originally due to Bourgain. The following form is [Bloom and Sisask 2020, Lemma 12.1].

Lemma 16. *There is a constant $c > 0$ such that the following holds. Let B be a regular Bohr set of rank d, suppose $A \subseteq B$ has density α, let $\epsilon > 0$, and suppose $B', B'' \subseteq B_\rho$ where $\rho \leq c\alpha\epsilon/d$. Then either*

(1) *there is some translate A' of A such that $|A' \cap B'| \geq (1-\epsilon)\alpha|B'|$ and $|A' \cap B''| \geq (1-\epsilon)\alpha|B''|$, or*

(2) $\|1_A * \mu_{B'}\|_\infty \geq (1+\epsilon/2)\alpha$, *or*

(3) $\|1_A * \mu_{B''}\|_\infty \geq (1+\epsilon/2)\alpha$.

Proof of Theorem 14 assuming Proposition 15. Let C_ϵ, $D_{\epsilon,\delta} \geq 1$ be parameters to be specified later, and let c be the smaller of $\frac{1}{2}$ and the constant c in Proposition 15. Let $t \geq 0$ be maximal such that there is a sequence of regular Bohr sets, say $B^{(0)}, \dots, B^{(t)}$, and subsets of translates of A, say $A_0, \dots, A_t$, such that the following holds:

(1) $B^{(0)} = G$ and $A_0 = A$.

(2) Each $B^{(i)}$ is a regular Bohr set of rank d_i and

$$d_{i+1} \leq d_i + C_\epsilon \mathcal{L}(\alpha)^4 p^4$$

and

$$|B^{(i+1)}| \geq \exp(-D_{\epsilon,\delta}(dp\mathcal{L}(\alpha/d) + \mathcal{L}(\alpha)^5 p^5))|B^{(i)}|.$$

(3) Each A_i is a subset of $B^{(i)}$ with density α_i such that $\alpha_{i+1} \geq (1 + c\epsilon/4)\alpha_i$ for $0 \leq i < t$.

Observe from point (3), and the trivial fact that $\alpha_i \leq 1$, that $t \ll_\epsilon \mathcal{L}(\alpha)$. Note that this implies $d_t \ll_\epsilon \mathcal{L}(\alpha)^5 p^4$.

We apply Lemma 16 with $c\epsilon/2$ in place of ϵ, and $B = B^{(t)}$, $B' = B_{c'\alpha\epsilon/d_t}$ and $B'' = B'_{c''\delta\alpha/d_t}$, where the constants are in particular chosen to ensure that B', B'' are both regular. Provided we pick $D_{\epsilon,\delta}$ large enough in terms of C_ϵ, ϵ, and δ, Lemma A.4 and the maximality of t ensure that we must be in the first alternative of Lemma 16's conclusion: there exists a translate $A_t - x$ such that $|(A_t - x) \cap B'| \geq (1 - c\epsilon/2)\alpha|B'|$ and $|(A_t - x) \cap B''| \geq (1 - c\epsilon/2)\alpha|B''|$.

We claim that $A' = (A_t - x) \cap B'$, with the B' and B'' above playing the role of B and B' respectively, satisfies the conclusions of Theorem 14. Indeed, the bounds on the rank and size of B', and the density conditions on A', are clearly satisfied.

Suppose for a contradiction that

$$\|\mu_{A'} \circ \mu_{A'}\|_{p(\mu_{k\cdot B'''} \circ \mu_{k\cdot B'''} * \mu_{k\cdot B''''} \circ \mu_{k\cdot B''''})} \geq (1+\epsilon)\mu(B')^{-1},$$

for some regular Bohr sets $B''' = B''_\rho$ and $B'''' = B'''_{\rho'}$ satisfying $\rho, \rho' \in \left(\frac{1}{2}, 1\right) \cdot c\delta\alpha/d_t$.

The conditions of Proposition 15 are met, and hence we deduce there is some $\tilde{B} \subseteq B''''$ of rank

$$\mathrm{rk}(\tilde{B}) \leq \mathrm{rk}(B) + O_\epsilon(\mathcal{L}(\alpha)^4 p^4)$$

and

$$|\tilde{B}| \geq \exp(-O_\epsilon(d_t p\mathcal{L}(\alpha/d_t) + \mathcal{L}(\alpha)^5 p^5))|B''|$$

and there is a translate of A_t, say $A_t - y$, such that

$$\mu_{\tilde{B}}(A_t - y) \geq (1 + c\epsilon)(1 - c\epsilon/2)\alpha \geq (1 + c\epsilon/4)\alpha,$$

say. This a contradiction to the maximality of t, provided C_ϵ matches the implicit constant in the first O_ϵ-term, since we can take $B^{(t+1)} = \tilde{B}$ and $A_{t+1} = (A_t - y) \cap \tilde{B}$,

noting that by Lemma A.4

$$|B''''| \geq \exp(-O_{\epsilon,\delta}(d\mathcal{L}(\alpha/d_t)))|B^{(t)}|. \qquad \square$$

Proposition 15 is a consequence of Steps 3 and 4 (dependent random choice and almost-periodicity) of the Kelley–Meka approach. We will use the following version of almost-periodicity, which is essentially [Schoen and Sisask 2016, Theorem 5.4].

Theorem 17 (almost-periodicity). *There is a constant $c > 0$ such that the following holds. Let $\epsilon > 0$ and $B, B' \subseteq G$ be regular Bohr sets of rank d. Suppose that $A_1 \subseteq B$ with density α_1 and A_2 is such that there exists x with $A_2 \subseteq B' - x$ with density α_2. Let S be any set with $|S| \leq 2|B|$. There is a regular Bohr set $B'' \subseteq B'$ of rank at most*

$$d + O_\epsilon(\mathcal{L}(\alpha_1)^3\mathcal{L}(\alpha_2))$$

and size

$$|B''| \geq \exp(-O_\epsilon(d\mathcal{L}(\alpha_1\alpha_2/d) + \mathcal{L}(\alpha_1)^3\mathcal{L}(\alpha_2)\mathcal{L}(\alpha_1\alpha_2/d)))|B'|$$

such that

$$|\langle \mu_{B'} * \mu_{A_1} \circ \mu_{A_2}, 1_S\rangle - \langle \mu_{A_1} \circ \mu_{A_2}, 1_S\rangle| \leq \epsilon.$$

Proof. We apply [Schoen and Sisask 2016, Theorem 5.4] with the choices (with apologies for the unfortunate clash in variable naming between papers)

$$A \to -A_2, \quad M \to A_1, \quad L \to -S, \quad S \to B'_{c/d}, \quad B \to B'_{c/d}$$

and note that

$$|-A_2 + B'_{c/d}| \leq |B' + B'_{c/d}| \leq 2|B'| \leq 2\alpha_2^{-1}|A_2|$$

by regularity of B'. The statement now almost follows from [loc. cit., Theorem 5.4] after observing that (in that theorem's language) we have $K \leq 2\alpha_2^{-1}$, $\sigma = 1$, and $\eta \geq \alpha_1/2$, except that there the statement has a constraint on the rank and the width of B'', rather than the rank and the size. Nonetheless the width condition can be immediately converted into a lower bound for the size of B'' with Lemma A.4. $\square$

We will now use this almost-periodicity together with Lemma 8 to deduce the iterative step.

Proof of Proposition 15. By averaging there exists some $x \in k \cdot B' + k \cdot B''$ such that

$$\|\mu_A \circ \mu_A\|_{p(\mu_{k\cdot B'} * \mu_{k\cdot B''-x})} \geq (1+\epsilon)\mu(B)^{-1}.$$

We now apply Lemma 8 with $B_1 = k \cdot B'$ and $B_2 = k \cdot B'' + x$. This produces some $A_1 \subseteq k\cdot B'$ and $A_2 \subseteq k\cdot B'' - x$ such that, with $S = \{x : \mu_A \circ \mu_A(x) \geq (1+\epsilon/2)\mu(B)^{-1}\}$,

$$\langle \mu_{A_1} \circ \mu_{A_2}, 1_S\rangle \geq 1 - \epsilon/4$$

and

$$\min\left(\frac{|A_1|}{|B'|}, \frac{|A_2|}{|B''|}\right) \gg \alpha^{2p+O_\epsilon(1)}.$$

We now apply Theorem 17 (with $k \cdot B'$ and $k \cdot B''$ playing the roles of B and B' respectively), noting that we can, without loss of generality, take S to be supported in $A_1 - A_2 \subseteq k \cdot B' + k \cdot B'' - x$ and so by regularity of B'

$$|S| \leq |B' + B''| \leq 2|B'|.$$

This produces some $B''' \subseteq k \cdot B''$ of the required rank and size such that

$$\langle \mu_{B'''} * \mu_{A_1} \circ \mu_{A_2}, \mu_A \circ \mu_A \rangle \geq (1+\epsilon/2)(1-\epsilon/4)(1-\epsilon/8)\mu(B)^{-1} \geq (1+c\epsilon)\mu(B)^{-1}$$

for some absolute constant $c > 0$. The result now follows from averaging, since

$$\begin{aligned}\langle \mu_{B'''} * \mu_{A_1} \circ \mu_{A_2}, \mu_A \circ \mu_A \rangle &\leq \|\mu_{B'''} * \mu_A\|_\infty \|\mu_{A_2} \circ \mu_{A_1} * \mu_A\|_1 \\ &= \|\mu_{B'''} * \mu_A\|_\infty. \qquad \square\end{aligned}$$

5. Deduction of Theorems 5, 1 and 3

Finally, in this section we deduce Theorem 5 from Theorem 14 (using Step 2) and show (using Step 1) how it implies Theorems 1 and 3. The following form of unbalancing relative to Bohr sets is sufficient.

Proposition 18. *There is a constant $c > 0$ such that the following holds. Let $\epsilon > 0$ and $p \geq 2$ be an integer. Let $B \subseteq G$ be a regular Bohr set and $A \subseteq B$ with relative density α. Let $\nu : G \to \mathbb{R}_{\geq 0}$ be supported on B_ρ, where $\rho \leq c\epsilon\alpha/\operatorname{rk}(B)$, such that $\|\nu\|_1 = 1$ and $\widehat{\nu} \geq 0$. If*

$$\|(\mu_A - \mu_B) \circ (\mu_A - \mu_B)\|_{p(\nu)} \geq \epsilon\mu(B)^{-1},$$

then there exists $p' \ll_\epsilon p$ such that

$$\|\mu_A \circ \mu_A\|_{p'(\nu)} \geq \left(1 + \tfrac{1}{4}\epsilon\right)\mu(B)^{-1}.$$

Proof. Let us write

$$g = \mu_A \circ \mu_B + \mu_B \circ \mu_A - \mu_B \circ \mu_B$$

and note that for any $p' \geq 1$

$$\begin{aligned}\|\mu_A \circ \mu_A\|_{p'(\nu)} &= \|(\mu_A - \mu_B) \circ (\mu_A - \mu_B) + \mu(B)^{-1} + g - \mu(B)^{-1}\|_{p'(\nu)} \\ &\geq \|(\mu_A - \mu_B) \circ (\mu_A - \mu_B) + \mu(B)^{-1}\|_{p'(\nu)} - \|g - \mu(B)^{-1}\|_{p'(\nu)}.\end{aligned}$$

To bound the error term, note that $\mu_A \circ \mu_B(0) = \mu(B)^{-1}$ and that by regularity (for example with Lemma A.5), for $x \in \mathrm{supp}(\nu)$,

$$\begin{aligned}|\mu_A \circ \mu_B(x) - \mu_A \circ \mu_B(0)| &\leq \alpha^{-1}\mu(B)^{-1}\|\mu_B(\cdot + x) - \mu_B\|_1 \\ &\ll \rho \,\mathrm{rk}(B)\alpha^{-1}\mu(B)^{-1} \\ &\leq \tfrac{1}{12}\epsilon\mu(B)^{-1},\end{aligned}$$

say, assuming ρ is sufficiently small, and similarly for the other terms constituting g. Hence

$$\|g - \mu(B)^{-1}\|_{p'(\nu)} \leq \|g - \mu(B)^{-1}\|_{L^\infty(\mathrm{supp}(\nu))} \leq \tfrac{1}{4}\epsilon\mu(B)^{-1}.$$

It therefore suffices to find some $p' \ll_\epsilon p$ such that

$$\|(\mu_A - \mu_B) \circ (\mu_A - \mu_B) + \mu(B)^{-1}\|_{p'(\nu)} \geq (1 + \tfrac{1}{2}\epsilon)\mu(B)^{-1}.$$

This is immediate from Lemma 7 applied to $f = \mu(B)(\mu_A - \mu_B) \circ (\mu_A - \mu_B)$. □

To deduce Theorem 5 from Theorem 14 we will need to pass from the measure μ_B to $\mu_{B'} \circ \mu_{B'} * \mu_{B''} \circ \mu_{B''}$. This is a technical issue with Bohr sets that does not arise in the $\mathbb{F}_q^n$ model case (note that these measures are identical when $B = B' = B'' = G$).

Proposition 19. *There is a constant $c > 0$ such that the following holds. Let $p \geq 2$ be an even integer. Let $f : G \to \mathbb{R}$, let $B \subseteq G$ and $B', B'' \subseteq B_{c/\mathrm{rk}(B)}$ all be regular Bohr sets. Then*

$$\|f \circ f\|_{p(\mu_{B'} \circ \mu_{B'} * \mu_{B''} \circ \mu_{B''})} \geq \tfrac{1}{2}\|f * f\|_{p(\mu_B)}.$$

Proof. By an application of Lemma A.6 with $L = 4$, $\rho = c/4\,\mathrm{rk}(B)$ and $\nu = \mu_{B'} * \mu_{B'} * \mu_{B''} * \mu_{B''}$, we have

$$\mu_B \leq 2\mu_{B_{1+4\rho}} * \nu.$$

Hence

$$\begin{aligned}\|f * f\|_{p(\mu_B)}^p &= \mathbb{E}_{x \in G}\mu_B(x) f * f(x)^p \\ &\leq 2\mathbb{E}_{x \in G}(\mu_{B_{1+4\rho}} * \nu)(x) f * f(x)^p \\ &= 2\mathbb{E}_{t \in B_{1+4\rho}}\mathbb{E}_{x \in G}\nu(x - t) f * f(x)^p.\end{aligned}$$

By averaging there exists some t such that

$$\begin{aligned}\|f * f\|_{p(\mu_B)}^p &\leq 2\mathbb{E}_{x \in G}\nu(x - t) f * f(x)^p \\ &= 2\sum_{\gamma \in \widehat{G}} \widehat{\nu}(\gamma)\gamma(-t)(\hat{f}^2)^{(p)}(\gamma) \\ &\leq 2\sum_{\gamma \in \widehat{G}} \widehat{\nu}(\gamma)(|\hat{f}|^2)^{(p)}(\gamma) \\ &= 2\|f \circ f\|_{p(\nu)}^p,\end{aligned}$$

where we have used the fact that $\widehat{\nu} \geq 0$. □

Proof of Theorem 5. We may, without loss of generality, assume that δ is sufficiently small in terms of ϵ and k. Let $p' \ll_\epsilon p$ satisfy the condition in Proposition 18. Let A' and B be the regular Bohr sets provided by Theorem 14 applied with p replaced by p' and ϵ replaced by $\epsilon/8$. We claim that this choice satisfies the conclusion of Theorem 5. It suffices to prove

$$\|(\mu_{A'} - \mu_B) * (\mu_{A'} - \mu_B)\|_{p(\mu_{k\cdot B'})} \le \epsilon \mu(B)^{-1}.$$

Suppose not. Let $B'' = B'_\rho$ and $B''' = B''_{\rho'}$ be regular Bohr sets with $\rho = c_1/d$ and $\rho' = c_2/d$ for some sufficiently small constants $c_1, c_2 > 0$. By Proposition 19 we have, if we let $f = \mu_{A'} - \mu_B$ for brevity,

$$\|f * f\|_{p(\mu_{k\cdot B'})} \le 2\|f \circ f\|_{p(\nu)}$$

where $\nu = \mu_{k\cdot B''} \circ \mu_{k\cdot B''} * \mu_{k\cdot B'''} \circ \mu_{k\cdot B'''}$. In particular, $\|f \circ f\|_{p(\nu)} > \frac{1}{2}\epsilon\mu(B)^{-1}$, and so by Proposition 18 (noting that ν is supported on $k(B'' + B'' + B''' + B''') \subseteq B'_{4k\rho} \subseteq B_{c/d}$) we deduce that

$$\|\mu_{A'} \circ \mu_{A'}\|_{p'(\nu)} \ge (1 + \epsilon/8)\mu(B)^{-1},$$

which contradicts the conclusion of Theorem 14, and we are done. □

Finally, to apply Theorem 5 to three-term progressions and finding long arithmetic progressions in $A + A + A$, we record the following version of the Hölder lifting Step 1.

Proposition 20. *There is a constant $c > 0$ such that the following holds. Let $\epsilon > 0$. Let $B \subseteq G$ be a regular Bohr set and $A \subseteq B$ with relative density α, and let $B' \subseteq B_{c\epsilon\alpha/\operatorname{rk}(B)}$ be a regular Bohr set and $C \subseteq B'$ with relative density γ. Either*

(1) $|\langle \mu_A * \mu_A, \mu_C\rangle - \mu(B)^{-1}| \le \epsilon\mu(B)^{-1}$ *or*

(2) *there is some $p \ll \mathcal{L}(\gamma)$ such that $\|(\mu_A - \mu_B) * (\mu_A - \mu_B)\|_{p(\mu_{B'})} \ge \frac{1}{2}\epsilon\mu(B)^{-1}$.*

Proof. We first note that

$$\langle \mu_A * \mu_A, \mu_C\rangle = \langle (\mu_A - \mu_B) * (\mu_A - \mu_B), \mu_C\rangle + 2\langle \mu_A * \mu_B, \mu_C\rangle - \langle \mu_B * \mu_B, \mu_C\rangle.$$

By the regularity of B (more specifically Lemma A.5) and the fact that $C \subseteq B_{c\epsilon/\operatorname{rk}(B)}$, we have

$$|\langle \mu_B * \mu_B, \mu_C\rangle - \mu(B)^{-1}| \le \|\mu_B\|_\infty \|\mu_B * \mu_C - \mu_B\|_1 \le \tfrac{1}{8}\epsilon\mu(B)^{-1}.$$

Similarly, the fact that $C \subseteq B_{c\epsilon\alpha/\operatorname{rk}(B)}$ implies that

$$|\langle \mu_A * \mu_B, \mu_C\rangle - \mu(B)^{-1}| \le \|\mu_A\|_\infty \|\mu_B * \mu_C - \mu_B\|_1 \le \tfrac{1}{16}\epsilon\mu(B)^{-1}.$$

It follows that, with $f = (\mu_A - \mu_B) * (\mu_A - \mu_B)$, we have

$$|\langle \mu_A * \mu_A, \mu_C\rangle - \mu(B)^{-1} - \langle f, \mu_C\rangle| \le \tfrac{1}{4}\epsilon\mu(B)^{-1}.$$

Therefore, if the first possibility fails, then

$$\gamma^{-1}|\langle f, 1_C\rangle_{\mu_{B'}}| = |\langle f, \mu_C\rangle| \geq \tfrac{3}{4}\epsilon\mu(B)^{-1}.$$

By Hölder's inequality, for any $p \geq 1$,

$$\|f\|_{p(\mu_{B'})}\gamma^{1-1/p} \geq |\langle f, 1_C\rangle_{\mu_{B'}}|.$$

We can choose some $p \ll \mathcal{L}(\gamma)$ such that $\gamma^{-1/p} \leq \frac{3}{2}$, and the proof is complete. □

5.1. ***Three-term arithmetic progressions.*** Theorem 1 is an immediate consequence of the following result that gives a lower bound for the number of three-term arithmetic progressions in an arbitrary set, coupled with the observation that if A contains only trivial three-term arithmetic progressions then this count is at most N.

Theorem 21 (Kelley–Meka). *If $A \subseteq \{1, \dots, N\}$ has size $|A| = \alpha N$, then A contains at least*

$$\exp(-O(\mathcal{L}(\alpha)^{12}))N^2$$

many three-term arithmetic progressions.

Proof. As usual, we begin by considering $A \subseteq \{1, \dots, N\}$ as a subset of $G = \mathbb{Z}/(2N+1)\mathbb{Z}$ — the density of this set within G is still $\asymp \alpha$, and any three-term arithmetic progression in $A \subseteq G$ yields one in $A \subseteq \{1, \dots, N\}$.

We apply Theorem 5 with $\epsilon = \frac{1}{4}$, $k = 2$, and $p = \lceil K\mathcal{L}(\alpha)\rceil$ for some large constant K. Let $A'' = A' \cap B'$. If

$$\langle \mu_{A'} * \mu_{A'}, \mu_{2\cdot A''}\rangle \geq \tfrac{1}{2}\mu(B)^{-1}$$

we are done, since the left-hand side is at most $\ll \alpha^{-3}\mu(B)^{-2}\mu(B')^{-1}$ times the number of three-term arithmetic progressions in A, and by Lemma A.4 we have

$$\mu(B)\mu(B') \geq \exp(-O_\epsilon(\mathcal{L}(\alpha)^{12})).$$

Otherwise, we are in the second case of Proposition 20, which contradicts the conclusion of Theorem 5, and we are done. □

5.2. ***Arithmetic progressions in $A+A+A$.*** As in the previous section, Theorem 3 follows immediately from the following statement for general groups, by embedding $\{1, \dots, N\}$ in a cyclic group $\mathbb{Z}/M\mathbb{Z}$ for a prime M between $2N$ and $4N$.

Theorem 22. *If $A \subseteq G$ has size αN, then $A + A + A$ contains a translate of a Bohr set B with*

$$\mathrm{rk}(B) \ll \mathcal{L}(\alpha)^9 \quad \textit{and} \quad \mu(B) \geq \exp(-O(\mathcal{L}(\alpha)^{12}).$$

In particular, if $G = \mathbb{Z}/N\mathbb{Z}$ for a prime N, then $A + A + A$ contains an arithmetic progression of length

$$\geq \exp(-O(\mathcal{L}(\alpha)^3))N^{\Omega(1/\mathcal{L}(\alpha)^9)}.$$

Proof. We apply Theorem 5 with $\epsilon = \frac{1}{4}$, $k = 1$, and $p = \lceil K\mathcal{L}(\alpha)\rceil$ for some large constant K. Let B, B' be the Bohr sets produced by that conclusion, and $A' = (A - x) \cap B$ the corresponding restricted translate of A.

We first argue that $|(A' + A') \cap B'| \geq (1 - \alpha/4)|B'|$. Indeed, otherwise if we let $C = B'\backslash(A' + A')$, then the first case of Proposition 20 is violated and the conclusion of Theorem 5 means the second also cannot hold.

Let $B'' = B'_{c\alpha/d}$, where $c > 0$ is some small constant. We argue that $B'' \subseteq A' + A' + A'$. If not, there is some $x \in B''$ such that $(A' + A') \cap (x - A') = \varnothing$, and so

$$|A' \cap (B' - x)| = |(x - A') \cap B'| \leq |B'\backslash(A' + A')| \leq \tfrac{\alpha}{4}|B'|.$$

By regularity, however, the left-hand side is at least

$$|A' \cap B'| - |B\backslash(B' - x)| \geq |A' \cap B'| - \tfrac{1}{4}\alpha|B'| \geq \tfrac{\alpha}{2}|B'|,$$

which is a contradiction.

We have found some Bohr set B'' of rank $O(\mathcal{L}(\alpha)^9)$ and density

$$\mu(B'') \geq \exp(-O(\mathcal{L}(\alpha)^{12}))$$

such that $B'' \subseteq A' + A' + A'$. It remains to note that $A' + A' + A'$ is contained in a translate of $A + A + A$ and to appeal to Lemma A.7 to find an arithmetic progression in B'' of length

$$\geq \exp(-O(\mathcal{L}(\alpha)^3))N^{\Omega(1/\mathcal{L}(\alpha)^9)}. \qquad \square$$

Appendix: Bohr sets

In abelian groups more general than $\mathbb{F}_q^n$, a useful substitute for genuine subgroups is the class of Bohr sets, introduced to additive combinatorics by Bourgain [1999]. Below we collect some standard facts about Bohr sets.

Definition A.1 (Bohr sets). For a nonempty $\Gamma \subseteq \widehat{G}$ and $\nu \in [0, 2]$ we define the Bohr set $B = \mathrm{Bohr}_\nu(\Gamma)$ as

$$\mathrm{Bohr}_\nu(\Gamma) = \{x \in G : |1 - \gamma(x)| \leq \nu \text{ for all } \gamma \in \Gamma\}.$$

We call Γ the *frequency set* of B and ν the *width*, and define the *rank* of B to be the size of Γ, denoted by $\mathrm{rk}(B)$. We note here that all Bohr sets are symmetric and contain 0.

In fact, when we speak of a Bohr set we implicitly refer to the triple

$$(\Gamma, \nu, \mathrm{Bohr}_\nu(\Gamma)),$$

since the set $\mathrm{Bohr}_\nu(\Gamma)$ alone does not uniquely determine the frequency set nor the width. When we use subset notation, such as $B' \subseteq B$, this refers only to the

set inclusion (and does not, in particular, imply any particular relation between the associated frequency sets or width functions). Furthermore, if $B = \mathrm{Bohr}_\nu(\Gamma)$ and $\rho \in (0, 1]$, then we write B_ρ for the same Bohr set with the width dilated by ρ, i.e., $\mathrm{Bohr}_{\rho\nu}(\Gamma)$, which is known as a *dilate* of B.

Bohr sets are, in general, not even approximately group-like, and may grow exponentially under addition. Bourgain [1999] observed that certain Bohr sets are approximately closed under addition in a weak sense which is suitable for our applications.

Definition A.2 (regularity[3]). A Bohr set B of rank d is regular if for all $|\kappa| \leq \frac{1}{100d}$ we have

$$(1 - 100d|\kappa|)|B| \leq |B_{1+\kappa}| \leq (1 + 100d|\kappa|)|B|.$$

We record here the useful observation, frequently used in this paper, that if $(k, |G|) = 1$ and B is a regular Bohr set of rank d then $k \cdot B$ is also a regular Bohr set of rank d (and of course the same density), simply by replacing each character in the frequency set by an appropriate dilate.

For further introductory discussion of Bohr sets see, for example, [Tao and Vu 2006, Chapter 4], in which the following basic lemmas are established.

Lemma A.3. *For any Bohr set B there exists $\rho \in \left[\frac{1}{2}, 1\right]$ such that B_ρ is regular.*

Lemma A.4. *If $\rho \in (0, 1)$ and B is a Bohr set of rank d, then $|B_\rho| \geq (\rho/4)^d |B|$.*

The following standard lemmas indicate how regularity of Bohr sets will be exploited. The following is proved as, for example, [Bloom and Sisask 2020, Lemma 4.5].

Lemma A.5. *If B is a regular Bohr set of rank d and $\mu : G \to \mathbb{R}_{\geq 0}$ is supported on B_ρ, with $\rho \in (0, 1)$, then*

$$\|\mu_B * \mu - \mu_B\|_1 \ll \rho d \|\mu\|_1.$$

The following is a minor generalisation of, for example, [Bloom and Sisask 2020, Lemma 4.7], which is stated with $\nu = \mu_{B'}^{(L)}$ for a subset $B' \subseteq B_\rho$; the proof is identical.

Lemma A.6. *There is a constant $c > 0$ such that the following holds. Let B be a regular Bohr set of rank d and $L \geq 1$ be any integer. If $\nu : G \to \mathbb{R}_{\geq 0}$ is supported on LB_ρ, where $\rho \leq c/Ld$, and $\|\nu\|_1 = 1$, then*

$$\mu_B \leq 2\mu_{B_{1+L\rho}} * \nu.$$

Finally, we note the following simple lemma, which is useful for finding arithmetic progressions.

[3]The constant 100 here is fairly arbitrary. Smaller constants are permissible.

Lemma A.7. *If N is a prime and $B \subseteq \mathbb{Z}/N\mathbb{Z}$ is a Bohr set of rank d, then B contains an arithmetic progression of length*

$$\gg |B|^{1/d}.$$

Proof. Let $\rho = 4(2/|B|)^{1/d}$, and note that by Lemma A.4 we have

$$|B_\rho| \geq (\rho/4)^d |B| = 2.$$

In particular there exists some $x \in B_\rho \backslash \{0\}$. By the triangle inequality it is clear that $\{x, \dots, \lfloor \rho^{-1} \rfloor x\} \subseteq B$, whence B contains an arithmetic progression of length $\gg \rho^{-1}$. □

Acknowledgements

Bloom is supported by a Royal Society University Research Fellowship. We would like to thank Zander Kelley and Raghu Meka for generously sharing a copy of their preprint with us, and their encouragement in writing this exposition. We would also like to thank Ben Green for helpful conversations, Ilya Shkredov for showing us an alternative argument for the proof of Lemma 7, and an anonymous referee for useful suggestions.

References

[Bateman and Katz 2012] M. Bateman and N. H. Katz, "New bounds on cap sets", *J. Amer. Math. Soc.* **25**:2 (2012), 585–613. MR Zbl

[Behrend 1946] F. A. Behrend, "On sets of integers which contain no three terms in arithmetical progression", *Proc. Nat. Acad. Sci. U.S.A.* **32** (1946), 331–332. MR Zbl

[Bloom and Sisask 2019] T. F. Bloom and O. Sisask, "Logarithmic bounds for Roth's theorem via almost-periodicity", *Discrete Anal.* (2019), art. id. 4. MR Zbl

[Bloom and Sisask 2020] T. F. Bloom and O. Sisask, "Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions", preprint, 2020. arXiv 2007.03528

[Bourgain 1999] J. Bourgain, "On triples in arithmetic progression", *Geom. Funct. Anal.* **9**:5 (1999), 968–984. MR Zbl

[Croot and Sisask 2010] E. Croot and O. Sisask, "A probabilistic technique for finding almost-periods of convolutions", *Geom. Funct. Anal.* **20**:6 (2010), 1367–1396. MR Zbl

[Elkin 2011] M. Elkin, "An improved construction of progression-free sets", *Israel J. Math.* **184** (2011), 93–128. MR Zbl

[Ellenberg and Gijswijt 2017] J. S. Ellenberg and D. Gijswijt, "On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression", *Ann. of Math.* (2) **185**:1 (2017), 339–343. MR Zbl

[Erdös and Turán 1936] P. Erdös and P. Turán, "On Some Sequences of Integers", *J. London Math. Soc.* **11**:4 (1936), 261–264. MR Zbl

[Freiman et al. 1992] G. A. Freiman, H. Halberstam, and I. Z. Ruzsa, "Integer sum sets containing long arithmetic progressions", *J. London Math. Soc.* (2) **46**:2 (1992), 193–201. MR Zbl

[Gowers 1998] W. T. Gowers, "A new proof of Szemerédi's theorem for arithmetic progressions of length four", *Geom. Funct. Anal.* **8**:3 (1998), 529–551. MR Zbl

[Green and Wolf 2010] B. Green and J. Wolf, "A note on Elkin's improvement of Behrend's construction", pp. 141–144 in *Additive number theory*, edited by D. Chudnovsky and G. Chudnovsky, Springer, 2010. MR Zbl

[Kelley and Meka 2023] Z. Kelley and R. Meka, "Strong Bounds for 3-Progressions", preprint, 2023. arXiv 2302.05537

[Roth 1953] K. F. Roth, "On certain sets of integers", *J. London Math. Soc.* **28** (1953), 104–109. MR Zbl

[Sanders 2008] T. Sanders, "Additive structures in sumsets", *Math. Proc. Cambridge Philos. Soc.* **144**:2 (2008), 289–316. MR

[Sanders 2010] T. Sanders, "Popular difference sets", *Online J. Anal. Comb.* 5 (2010), 4. MR

[Sanders 2011] T. Sanders, "On Roth's theorem on progressions", *Ann. of Math.* (2) **174**:1 (2011), 619–636. MR

[Sanders 2012a] T. Sanders, "On certain other sets of integers", *J. Anal. Math.* **116** (2012), 53–82. MR

[Sanders 2012b] T. Sanders, "On the Bogolyubov–Ruzsa lemma", *Anal. PDE* **5**:3 (2012), 627–655. MR

[Sanders 2013] T. Sanders, "The structure theory of set addition revisited", *Bull. Amer. Math. Soc.* (*N.S.*) **50**:1 (2013), 93–127. MR

[Schoen 2015] T. Schoen, "New bounds in Balog–Szemerédi–Gowers theorem", *Combinatorica* **35**:6 (2015), 695–701. MR Zbl

[Schoen and Shkredov 2013] T. Schoen and I. D. Shkredov, "Higher moments of convolutions", *J. Number Theory* **133**:5 (2013), 1693–1737. MR Zbl

[Schoen and Shkredov 2014] T. Schoen and I. D. Shkredov, "Roth's theorem in many variables", *Israel J. Math.* **199**:1 (2014), 287–308. MR Zbl

[Schoen and Sisask 2016] T. Schoen and O. Sisask, "Roth's theorem for four variables and additive structures in sums of sparse sets", *Forum Math. Sigma* **4** (2016), art. id. e5. MR Zbl

[Shkredov 2013] I. D. Shkredov, "Some new results on higher energies", *Trans. Moscow Math. Soc.* (2013), 31–63. MR Zbl

[Tao and Vu 2006] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics **105**, Cambridge University Press, 2006. MR Zbl

Received 20 Feb 2023. Revised 21 Nov 2023.

THOMAS F. BLOOM:

bloom@maths.ox.ac.uk
Mathematical Institute, University of Oxford, Oxford, United Kingdom

OLOF SISASK:

olof.sisask@math.su.se
Department of Mathematics, Stockholm University, Stockholm, Sweden

msp

Essential Number Theory
Vol. 2, No. 1, 2023
https://doi.org/10.2140/ent.2023.2.45

On gamma factors for representations of finite general linear groups

David Soudry and Elad Zelingher

We use the Langlands–Shahidi method in order to define the Shahidi gamma factor for a pair of irreducible generic representations of $\mathrm{GL}_n(\mathbb{F}_q)$ and $\mathrm{GL}_m(\mathbb{F}_q)$. We prove that the Shahidi gamma factor is multiplicative and show that it is related to the Jacquet–Piatetski-Shapiro–Shalika gamma factor. As an application, we prove a converse theorem based on the absolute value of the Shahidi gamma factor, and improve the converse theorem of Nien. As another application, we give explicit formulas for special values of the Bessel function of an irreducible generic representation of $\mathrm{GL}_n(\mathbb{F}_q)$.

1. Introduction

In the representation theory of p-adic groups, one method of studying irreducible representations is by attaching local factors to the representations. These local factors are complex valued functions of a complex variable. They encode various properties of the representations in question. These local factors usually arise from global integrals representing L-functions attached to automorphic representations. Studying these local factors is crucial for understanding the global situation. This has been done successfully in many cases, including the pioneering works of Jacquet, Piatetski-Shapiro and Shalika [Jacquet et al. 1983] and Shahidi [1984; 1990].

Let $\mathbb{F}$ be a finite field with cardinality q. A local theory of local factors often has a finite field analog. It allows one to attach "local constants" to irreducible representations of the $\mathbb{F}$-points version of the group in consideration. One famous example is the book by Piatetski-Shapiro [1983], in which he developed the theory of gamma factors for the tensor product representation of $\mathrm{GL}_2 \times \mathrm{GL}_1$ over finite fields. We also mention the works [Roditty-Gershon 2010; Nien 2014; Ye and Zelingher 2020; Liu and Zhang 2022a; 2022b] as examples. These local constants usually encode properties analogous to their local factors counterparts. Moreover, these local constant theories often allow one to consider "toy models" for analogous local problems. For instance, shortly after Nien's proof [2014] of the analog of

MSC2020: 11F66, 11T24, 20C33.

Keywords: Langlands–Shahidi method, Jacquet–Piatetski-Shapiro–Shalika, Rankin–Selberg, Gamma factors, Bessel function, Kloosterman sums, Representations of GLn(Fq).

Jacquet's conjecture for finite fields, Chai [2019] proved the conjecture for the p-adic group case where in his proof he used tools analogous to the ones used by Nien.

In her master's thesis Roditty-Gershon [2010] defined a finite field analog of the gamma factor of Jacquet, Piatetski-Shapiro and Shalika [1983]. This gamma factor represents the tensor product representation, attached to two irreducible generic representations π and σ of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}_m(\mathbb{F})$, respectively, and is denoted $\gamma(\pi \times \sigma, \psi)$. Later, Rongqing Ye [2019] showed that $\gamma(\pi \times \sigma, \psi)$ is related to its local field counterpart through level zero supercuspidal representations. Using this relation and the local Langlands correspondence, Rongqing Ye and the second author were able to express $\gamma(\pi \times \sigma, \psi)$ as a product of Gauss sums [Ye and Zelingher 2021].

The theory of the finite field version of the gamma factor associated to the tensor product, as it currently appears in the literature, is in some sense not complete. The first problem is that the gamma factor $\gamma(\pi \times \sigma, \psi)$ is currently not defined for all irreducible generic representations π and σ. It is only defined when $n \geq m$, and under the assumption that π is cuspidal (and if $n = m$, σ is also required to be cuspidal). One can tweak the proofs so they will work for all irreducible generic representations π and σ, such that π and $\sigma^\vee$ have disjoint cuspidal support, but that is not enough in order to define $\gamma(\pi \times \sigma, \psi)$ for all pairs π and σ. One can try to define $\gamma(\pi \times \sigma, \psi)$ naively using the expression involving the Bessel functions of π and σ (see Section 2B1 for the definition of the Bessel function), but this leads to the second problem. The second problem is that the current theory lacks the multiplicativity property of the gamma factor. If one naively extends the definition $\gamma(\pi \times \sigma, \psi)$ using the approach suggested above, it is not clear that the gamma factor would be multiplicative. Both of these difficulties need to be resolved for applications as in [Zelingher 2023].

The Langlands–Shahidi method provides an alternative approach that solves both of these problems. In this paper, we use this method to define a finite field version of the Shahidi gamma factor. We briefly describe the construction now. Let π and σ be representations of Whittaker type of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}_m(\mathbb{F})$, respectively. In Section 3A, we consider an intertwining operator $U_{\sigma,\pi} : \sigma \circ \pi \to \pi \circ \sigma$, where $\circ$ denotes parabolic induction. In Section 3B, given Whittaker vectors $v_{\pi,\psi} \in \pi$ and $v_{\sigma,\psi} \in \sigma$, we define Whittaker vectors $v_{\pi,\sigma,\psi} \in \pi \circ \sigma$ and $v_{\sigma,\pi,\psi} \in \sigma \circ \pi$. By uniqueness of the Whittaker vectors, we have that there exists a constant $\Gamma(\pi \times \sigma, \psi) \in \mathbb{C}$, such that

$$U_{\sigma,\pi} v_{\sigma,\pi,\psi} = \Gamma(\pi \times \sigma, \psi) \cdot v_{\pi,\sigma,\psi}.$$

We call $\Gamma(\pi \times \sigma, \psi)$ the *Shahidi gamma factor associated to π and σ*. This is a finite analog of Shahidi's local coefficient [1984].

We prove properties of $\Gamma(\pi \times \sigma, \psi)$, the most important one is that it is multiplicative (Theorem 3.9).

Theorem 1.1. *Let π, σ_1 and σ_2 be representations of Whittaker type of $\mathrm{GL}_n(\mathbb{F})$, $\mathrm{GL}_{m_1}(\mathbb{F})$ and $\mathrm{GL}_{m_2}(\mathbb{F})$, respectively. Then*

$$\Gamma(\pi \times (\sigma_1 \circ \sigma_2), \psi) = \Gamma(\pi \times \sigma_1, \psi) \cdot \Gamma(\pi \times \sigma_2, \psi).$$

We also express $\Gamma(\pi \times \sigma, \psi)$ in terms of the Bessel functions associated with π and σ when both representations are irreducible. We show that if $n \geq m$, then up to some simple factors, $\Gamma(\pi \times \sigma, \psi)$ is given by the naive extension of $\gamma(\pi \times \sigma^\vee, \psi)$ discussed above (Theorem 3.14). We deduce a relation between the Shahidi gamma factor and the Jacquet–Piatetski-Shapiro–Shalika gamma factor (Corollary 3.15).

Theorem 1.2. *Let π and σ be irreducible generic representations of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}_m(\mathbb{F})$, respectively. Suppose that π is cuspidal and $n \geq m$. If $n = m$, suppose that σ is also cuspidal. Then*

$$\Gamma(\pi \times \sigma, \psi) = q^{m(2n-m-1)/2} \omega_\sigma(-1) \gamma(\pi \times \sigma^\vee, \psi).$$

The relation between both gamma factors allows us to give a representation theoretic interpretation for the absolute value of the Shahidi gamma factor. We show that, in some sense, the absolute value of the Shahidi gamma factor serves as a good substitute for the order of the pole of the local L-factor associated with the tensor product representation. Let us stress that the relation to the Jacquet–Piatetski-Shapiro–Shalika gamma factor is crucial for these results. The following theorem can be seen as an analog of [Jacquet et al. 1983, Section 8.1].

Theorem 1.3. *Let π be an irreducible generic representation of $\mathrm{GL}_n(\mathbb{F})$ and let σ be an irreducible cuspidal representation of $\mathrm{GL}_m(\mathbb{F})$. Then*

$$|q^{-nm/2} \cdot \Gamma(\pi \times \sigma, \psi)| = q^{-d_\pi(\sigma)m/2},$$

where $d_\pi(\sigma)$ is the number of times σ appears in the cuspidal support of π.

This allows us to deduce a converse theorem based on the absolute value of the normalized Shahidi gamma factor. Similar theorems in the local setting were given by Gan and his collaborators in many works (see [Gan and Savin 2012, Lemma 12.3], [Gan and Ichino 2016, Lemma A.6] and [Atobe and Gan 2017, Lemma A.6]), but our proof is done on the "group side" rather than on the "Galois side".

Theorem 1.4. *Let π_1 and π_2 be two irreducible generic representations of $\mathrm{GL}_{n_1}(\mathbb{F})$ and $\mathrm{GL}_{n_2}(\mathbb{F})$, respectively. Assume that for every m and every irreducible cuspidal representation σ of $\mathrm{GL}_m(\mathbb{F})$ we have*

$$|q^{-n_1 m/2} \cdot \Gamma(\pi_1 \times \sigma, \psi)| = |q^{-n_2 m/2} \cdot \Gamma(\pi_2 \times \sigma, \psi)|.$$

Then $n_1 = n_2$ and $\pi_1 \cong \pi_2$.

Our results combined with Nien's converse theorem [2014] allow us to deduce a converse theorem that holds under weaker assumptions. This is similar to [Jiang et al. 2015, Section 2.4].

Theorem 1.5. *Let π_1 and π_2 be irreducible generic representations of $\mathrm{GL}_n(\mathbb{F})$ with the same central character. Suppose that for any $1 \leq m \leq \frac{n}{2}$ and any irreducible cuspidal representation σ of $\mathrm{GL}_m(\mathbb{F})$ we have*

$$\Gamma(\pi_1 \times \sigma, \psi) = \Gamma(\pi_2 \times \sigma, \psi).$$

Then $\pi_1 \cong \pi_2$.

As another application of our results, we find explicit formulas for special values of the Bessel function of an irreducible generic representation π. The first formula (Theorem 4.10) expresses $\mathcal{J}_{\pi,\psi}\left(\begin{smallmatrix} & I_{n-1} \\ c & \end{smallmatrix}\right)$ as an exotic Kloosterman sum [Katz 1993, Page 152]. This formula is already known in the literature by the work of Curtis and Shinoda [2004], but our proof is based on multiplicativity of the Shahidi gamma factor, rather than on Deligne–Lusztig theory. The second formula we find (Theorem 4.14) expresses

$$\mathcal{J}_{\pi,\psi}\begin{pmatrix} & & -c' \\ & I_{n-2} & \\ c & & \end{pmatrix}$$

as a twisted convolution of values of the form $\mathcal{J}_{\pi,\psi}\left(\begin{smallmatrix} & I_{n-1} \\ c & \end{smallmatrix}\right)$ and $\mathcal{J}_{\pi,\psi}\left(\begin{smallmatrix} & c' \\ I_{n-1} & \end{smallmatrix}\right)$. Such a formula was given by Chang [1976] for $n = 3$ and then generalized by Shinoda and Tulunay [2005] for $n = 4$. Chang's method is based on the Gelfand–Graev algebra, while our method is based on formulas we found for the Shahidi gamma factor.

This paper is based on a unpublished note by the first author [Soudry 1979].

2. Preliminaries

2A. ***Parabolic induction.*** Given a sequence of positive integers $n_1, \ldots, n_r$, we denote by $P_{n_1,\ldots,n_r}$ the parabolic subgroup of $\mathrm{GL}_{n_1+\cdots+n_r}(\mathbb{F})$ corresponding to the composition $(n_1, \ldots, n_r)$. That is,

$$P_{n_1,\ldots,n_r} = D_{n_1,\ldots,n_r} \ltimes N_{n_1,\ldots,n_r},$$

where

$$D_{n_1,\ldots,n_r} = \{\mathrm{diag}(g_1, \ldots, g_r) \mid \forall 1 \leq j \leq r,\, g_j \in \mathrm{GL}_{n_j}(\mathbb{F})\},$$

$$N_{n_1,\ldots,n_r} = \left\{ \begin{pmatrix} I_{n_1} & * & * & * \\ & I_{n_2} & * & * \\ & & \ddots & * \\ & & & I_{n_r} \end{pmatrix} \right\}.$$

Given representations $\pi_1, \dots, \pi_r$ of $\mathrm{GL}_{n_1}(\mathbb{F}), \dots, \mathrm{GL}_{n_r}(\mathbb{F})$, respectively, we denote by $\pi_1 \overline{\otimes} \dots \overline{\otimes} \pi_r$ the inflation of $\pi_1 \otimes \cdots \otimes \pi_r$ to $P_{n_1,\dots,n_r}$. That is, $\pi_1 \overline{\otimes} \dots \overline{\otimes} \pi_r$ is a representation of $P_{n_1,\dots,n_r}$, acting on the space of $\pi_1 \otimes \cdots \otimes \pi_r$, and its action on pure tensors is given by

$$(\pi_1 \overline{\otimes} \dots \overline{\otimes} \pi_r)(du) v_1 \otimes \cdots \otimes v_r = \pi_1(g_1) v_1 \otimes \cdots \otimes \pi_r(g_r) v_r,$$

where $d = \mathrm{diag}(g_1, \dots, g_r) \in D_{n_1,\dots,n_r}$ and $u \in N_{n_1,\dots,n_r}$, and for every $1 \le j \le r$, $v_j \in \pi_j$.

The parabolic induction $\pi_1 \circ \dots \circ \pi_r$ is defined as the following representation of $\mathrm{GL}_{n_1+\cdots+n_r}(\mathbb{F})$:

$$\pi_1 \circ \dots \circ \pi_r = \mathrm{Ind}_{P_{n_1,\dots,n_r}}^{\mathrm{GL}_{n_1+\cdots+n_r}(\mathbb{F})} \pi_1 \overline{\otimes} \dots \overline{\otimes} \pi_r.$$

A representation π of $\mathrm{GL}_n(\mathbb{F})$ is called *cuspidal* if for every composition $(n_1, \dots, n_r) \ne (n)$ of n, there does not exist $0 \ne v \in \pi$ such that v is invariant under $N_{n_1,\dots,n_r}$, i.e., if $v \in \pi$ is such that $\pi(u)v = v$ for every $u \in N_{n_1,\dots,n_r}$ then $v = 0$. If π is irreducible, π is cuspidal if and only if it is not a subrepresentation of $\pi_1 \circ \dots \circ \pi_r$ for some $\pi_1, \dots, \pi_r$ as above, where $r > 1$.

By [Gel'fand 1970, Theorem 2.4], if π is an irreducible representation of $\mathrm{GL}_n(\mathbb{F})$, then there exist $n_1, \dots, n_r > 0$ with $n_1 + \cdots + n_r = n$ and irreducible cuspidal representations $\pi_1, \dots, \pi_r$, of $\mathrm{GL}_{n_1}(\mathbb{F}), \dots, \mathrm{GL}_{n_r}(\mathbb{F})$, such that π is isomorphic to a subrepresentation of the parabolic induction $\pi_1 \circ \dots \circ \pi_r$. Such $\pi_1, \dots, \pi_r$ are unique up to ordering. We define the *cuspidal support of* π to be the multiset $\{\pi_1, \dots, \pi_r\}$.

2B. ***Generic representations.*** Let $\psi : \mathbb{F} \to \mathbb{C}^*$ be a nontrivial additive character. Let $Z_n \le \mathrm{GL}_n(\mathbb{F})$ be the upper triangular unipotent subgroup. We define a character $\psi : Z_n \to \mathbb{C}^*$ by the formula

$$\psi \begin{pmatrix} 1 & a_1 & * & \dots & * \\ & 1 & a_2 & \dots & * \\ & & \ddots & \ddots & \vdots \\ & & & 1 & a_{n-1} \\ & & & & 1 \end{pmatrix} = \psi\left(\sum_{k=1}^{n-1} a_k\right).$$

Let π be a finite dimensional representation of $\mathrm{GL}_n(\mathbb{F})$. π is said to be *generic* if

$$\mathrm{Hom}_{Z_n}(\mathrm{Res}_{Z_n} \pi, \psi) \ne 0.$$

This condition does not depend on the choice of ψ. See Section 3B1. We call a nonzero element in $\mathrm{Hom}_{Z_n}(\mathrm{Res}_{Z_n} \pi, \psi)$ a *ψ-Whittaker functional*. The representation π is generic if and only if there exists $0 \ne v \in \pi$, such that $\pi(u)v = \psi(u)v$ for every $u \in Z_n$. We call such vector a *Whittaker vector with respect to ψ*, or a *ψ-Whittaker vector*. The dimension of the subspace spanned by the ψ-Whittaker vectors of π is $\dim \mathrm{Hom}_{Z_n}(\mathrm{Res}_{Z_n} \pi, \psi)$.

Definition 2.1. We say that π *is of Whittaker type* if π is generic and the subspace spanned by its ψ-Whittaker vectors is one-dimensional.

By a well known result of Gelfand and Graev, we have that if π is generic and irreducible, then it is of Whittaker type [Gel'fand 1970, Theorem 0.5; Silberger and Zink 2000, Corollary 5.6]. It is well known that irreducible cuspidal representations of $\mathrm{GL}_n(\mathbb{F})$ are generic [Silberger and Zink 2000, Lemma 5.2]. The following result is also well known [loc. cit., Theorem 5.5].

Theorem 2.2. *Let $\pi_1, \ldots, \pi_r$ be representations of Whittaker type of $\mathrm{GL}_{n_1}(\mathbb{F}), \ldots, \mathrm{GL}_{n_r}(\mathbb{F})$, respectively. Then the parabolic induction $\pi_1 \circ \ldots \circ \pi_r$ is a representation of Whittaker type.*

2B1. *Whittaker models and Bessel functions.* Let π be an irreducible generic representation of $\mathrm{GL}_n(\mathbb{F})$. Since π is of Whittaker type, Frobenius reciprocity implies that

$$\dim \mathrm{Hom}_{\mathrm{GL}_n(\mathbb{F})}(\pi, \mathrm{Ind}_{Z_n}^{\mathrm{GL}_n(\mathbb{F})} \psi) = 1.$$

We denote by $\mathcal{W}(\pi, \psi)$ the unique subspace of $\mathrm{Ind}_{Z_n}^{\mathrm{GL}_n(\mathbb{F})} \psi$ that is isomorphic to π. This is *the Whittaker model of π with respect to ψ*.

Recall that for an irreducible representation π of $\mathrm{GL}_n(\mathbb{F})$, we have that its contragredient $\pi^\vee$ is isomorphic to π^ι, where π^ι is the representation acting on the space of π by $\pi^\iota(g) = \pi(g^\iota)$, where for $g \in \mathrm{GL}_n(\mathbb{F})$,

$$g^\iota = {}^t(g^{-1}).$$

(This follows from the fact that for $g \in \mathrm{GL}_n(\mathbb{F})$, the trace characters of π and $\pi^\vee$ are related by $\mathrm{tr}\, \pi^\vee(g) = \mathrm{tr}\, \pi(g^{-1})$, and from the fact that g^{-1} and ${}^t(g^{-1})$ are conjugate.)

Using the isomorphism $\pi^\vee \cong \pi^\iota$, we get an isomorphism of vector spaces $\mathcal{W}(\pi, \psi) \to \mathcal{W}(\pi^\vee, \psi^{-1})$, given by $W \mapsto \tilde{W}$, where

$$\tilde{W}(g) = W(w_n g^\iota),$$

and where $w_n \in \mathrm{GL}_n(\mathbb{F})$ is the long Weyl element

$$w_n = \begin{pmatrix} & & & 1 \\ & & 1 & \\ & \iddots & & \\ 1 & & & \end{pmatrix}.$$

Under the realization of π by its Whittaker model $\mathcal{W}(\pi, \psi)$, the one-dimensional subspace spanned by the ψ-Whittaker vectors of π is realized as the one-dimensional subspace of $\mathcal{W}(\pi, \psi)$ consisting of functions $W \in \mathcal{W}(\pi, \psi)$, such that $W(gu) = \psi(u)W(g)$, for every $u \in Z_n$ and every $g \in \mathrm{GL}_n(\mathbb{F})$. By [Gel'fand 1970, Proposition 4.5], there exists a (unique) element W in this one-dimensional subspace such that $W(I_n) = 1$. We call this W the *normalized Bessel function of π with respect*

to ψ, and denote it by $\mathcal{J}_{\pi,\psi}$. To summarize, the Bessel function $\mathcal{J}_{\pi,\psi}$ is the unique element in $\mathcal{W}(\pi, \psi)$, such that:

(1) $\mathcal{J}_{\pi,\psi}(I_n) = 1$.

(2) $\mathcal{J}_{\pi,\psi}(gu) = \psi(u)\mathcal{J}_{\pi,\psi}(g)$, for every $g \in \mathrm{GL}_n(\mathbb{F})$ and $u \in Z_n$.

The Bessel function enjoys the following identities that relate it to its complex conjugate and to its contragredient [Nien 2014, Propositions 2.15 and 3.5].

Proposition 2.3. *For any irreducible generic representation* π *of* $\mathrm{GL}_n(\mathbb{F})$ *and any* $g \in \mathrm{GL}_n(\mathbb{F})$, *we have the following identities*:

(1) $\mathcal{J}_{\pi,\psi}(g^{-1}) = \overline{\mathcal{J}_{\pi,\psi}(g)}$.

(2) $\mathcal{J}_{\pi,\psi}(g^{-1}) = \mathcal{J}_{\pi^\vee,\psi^{-1}}(g)$.

Remark 2.4. Let $v_{\pi,\psi}$ be a nonzero ψ-Whittaker vector. If we choose an inner product $(\cdot,\cdot)_\pi$ on π which is invariant under the $\mathrm{GL}_n(\mathbb{F})$-action, we have that the assignment $\ell_{\pi,\psi}\colon \pi \to \mathbb{C}$ given by $v_\pi \mapsto (v_\pi, v_{\pi,\psi})_\pi$ defines a Whittaker functional. The Whittaker model of π can be described using Frobenius reciprocity as $\mathcal{W}(\pi, \psi) = \{W_{v_\pi} \mid v_\pi \in \pi\}$, where for $g \in \mathrm{GL}_n(\mathbb{F})$ and $v_\pi \in \pi$, we define $W_{v_\pi}(g) = (\pi(g)v_\pi, v_{\pi,\psi})_\pi$. The Bessel function is given by

$$\mathcal{J}_{\pi,\psi}(g) = \frac{(\pi(g)v_{\pi,\psi}, v_{\pi,\psi})_\pi}{(v_{\pi,\psi}, v_{\pi,\psi})_\pi}.$$

All of the properties of the Bessel function listed above now follow immediately from the fact that $(\cdot,\cdot)_\pi$ is an inner product, and that $v_{\pi,\psi}$ is a ψ-Whittaker vector. Moreover, the projection operator to the one-dimensional subspace spanned by the ψ-Whittaker vectors $\mathrm{pr}_{\mathbb{C}v_{\pi,\psi}}$ can be described in two ways. The first way is by using the inner product, in which case for $v_\pi \in \pi$,

$$\mathrm{pr}_{\mathbb{C}v_{\pi,\psi}}(v_\pi) = \frac{(v_\pi, v_{\pi,\psi})_\pi}{(v_{\pi,\psi}, v_{\pi,\psi})_\pi} v_{\pi,\psi}.$$

The second way is by averaging, in which case

$$\mathrm{pr}_{\mathbb{C}v_{\pi,\psi}}(v_\pi) = \frac{1}{|Z_n|} \sum_{u \in Z_n} \psi^{-1}(u)\pi(u)v_\pi.$$

By completing $v_{\pi,\psi}$ to an orthogonal basis of π and using the fact that the subspace spanned by the ψ-Whittaker vectors is one dimensional, we see that

$$\mathrm{tr}(\mathrm{pr}_{\mathbb{C}v_{\pi,\psi}} \circ \pi(g)) = \mathcal{J}_{\pi,\psi}(g).$$

This is [Gel'fand 1970, Proposition 4.5].

2C. ***Jacquet–Piatetski-Shapiro–Shalika gamma factors.*** Let π and σ be irreducible generic representations of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}_m(\mathbb{F})$, respectively. For most π and σ, one can define a constant attached to π and σ called the *Jacquet–Piatetski-Shapiro–Shalika gamma factor of π and σ*. It is also known as the *Rankin–Selberg gamma factor of π and σ*. This is a finite field analog of the definition given by Jacquet, Piatetski-Shapiro and Shalika [1983] for p-adic groups. These were explained in Piatetski-Shapiro's lectures in 1976 and studied in an unpublished note from 1979 by the first author [Soudry 1979]. The case $n > m$ was also studied in Roddity-Gershon's master's thesis under the supervision of the first author.

2C1. *The case $n > m$.* In her master's thesis Edva Roditty-Gershon [2010] defined the Jacquet–Piatetski-Shapiro–Shalika gamma factor $\gamma(\pi \times \sigma, \psi)$, under the assumption that π is cuspidal and that $n > m$. Roddity-Gershon's thesis is unpublished, but her main results are presented by Nien [2014]. We briefly review these results now.

The first result is a functional equation that defines the Jacquet–Piatetski-Shapiro–Shalika gamma factor. Suppose that $n > m$ and that π is cuspidal. For any $W \in \mathcal{W}(\pi, \psi)$ and $W' \in \mathcal{W}(\sigma, \psi^{-1})$, and any $0 \le j \le n-m-1$, we define

$$Z_j(W, W'; \psi) = \sum_{h \in Z_m \backslash \mathrm{GL}_m(\mathbb{F})} \sum_{x \in M_{(n-m-j-1)\times m}(\mathbb{F})} W \begin{pmatrix} h & & \\ x & I_{n-m-j-1} & \\ & & I_{j+1} \end{pmatrix} W'(h).$$

We are now ready to state the functional equation.

Theorem 2.5 [Nien 2014, Theorem 2.10]. *There exists a nonzero constant $\gamma(\pi \times \sigma, \psi) \in \mathbb{C}$, such that for every $0 \le j \le n-m-1$, every $W \in \mathcal{W}(\pi, \psi)$ and every $W' \in \mathcal{W}(\sigma, \psi^{-1})$, we have*

$$q^{mj}\gamma(\pi \times \sigma, \psi) Z_j(W, W'; \psi) = Z_{n-m-j-1}\left(\pi^\vee \begin{pmatrix} I_m & \\ & w_{n-m} \end{pmatrix} \tilde{W}, \tilde{W}'; \psi^{-1}\right),$$

where $w_{n-m} \in \mathrm{GL}_{n-m}(\mathbb{F})$ is the long Weyl element.

The second result expresses the gamma factor $\gamma(\pi \times \sigma, \psi)$ in terms of the Bessel functions of π and σ.

Proposition 2.6 [Nien 2014, Proposition 2.16]. *Under the assumptions above, we have*

$$\gamma(\pi \times \sigma, \psi) = \sum_{h \in Z_m \backslash \mathrm{GL}_m(\mathbb{F})} \mathcal{J}_{\pi,\psi} \begin{pmatrix} & I_{n-m} \\ h & \end{pmatrix} \mathcal{J}_{\sigma,\psi^{-1}}(h).$$

It follows from Propositions 2.6 and 2.3 that

$$\overline{\gamma(\pi \times \sigma, \psi)} = \gamma(\pi^\vee \times \sigma^\vee, \psi^{-1}).$$

Moreover, applying Theorem 2.5 twice, we get the following corollary regarding the absolute value of $\gamma(\pi \times \sigma, \psi)$.

Corollary 2.7. *We have that*

$$\gamma(\pi \times \sigma, \psi)\gamma(\pi^\vee \times \sigma^\vee, \psi^{-1}) = q^{-m(n-m-1)},$$

and therefore

$$|\gamma(\pi \times \sigma, \psi)| = q^{-m(n-m-1)/2}.$$

2C2. *The case $n = m$.* The case $n = m$ was discussed in Piatetski-Shapiro's lecture and is explained briefly in Rongqing Ye's work [2019].

Let $\mathcal{S}(\mathbb{F}^n)$ be the space of functions $\phi\colon \mathbb{F}^n \to \mathbb{C}$. For a function $\phi \in \mathcal{S}(\mathbb{F}^n)$, we define its Fourier transform $\mathcal{F}_\psi\phi\colon \mathbb{F}^n \to \mathbb{C}$ by the formula

$$\mathcal{F}_\psi\phi(y) = \sum_{x \in \mathbb{F}^n} \phi(x)\psi(\langle x, y\rangle),$$

where if $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$ and $y = (y_1, \ldots, y_n) \in \mathbb{F}^n$, then $\langle x, y\rangle$ is the standard pairing

$$\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i.$$

Let π and σ be irreducible cuspidal representations of $\mathrm{GL}_n(\mathbb{F})$. We define for any $W \in \mathcal{W}(\pi, \psi)$, $W' \in \mathcal{W}(\sigma, \psi^{-1})$ and any $\phi \in \mathcal{S}(\mathbb{F}^n)$

$$Z(W, W', \phi; \psi) = \sum_{g \in Z_n \backslash \mathrm{GL}_n(\mathbb{F})} W(g)W'(g)\phi(e_n g),$$

where $e_n = (0, \ldots, 0, 1) \in \mathbb{F}^n$. We are now ready to introduce the functional equation that defines $\gamma(\pi \times \sigma, \psi)$.

Theorem 2.8 [Ye 2019, Theorem 2.3]. *There exists a nonzero constant $\gamma(\pi \times \sigma, \psi)$, such that for any $W \in \mathcal{W}(\pi, \psi)$, $W' \in \mathcal{W}(\sigma, \psi^{-1})$, and any $\phi \in \mathcal{S}(\mathbb{F}^n)$ with $\phi(0) = 0$, we have*

$$Z(\tilde{W}, \tilde{W}', \mathcal{F}_\psi\phi; \psi^{-1}) = \gamma(\pi \times \sigma, \psi)Z(W, W', \phi; \psi).$$

Similarly to the case $n > m$, we have an expression of $\gamma(\pi \times \sigma, \psi)$ in terms of the Bessel functions of π and σ.

Proposition 2.9 [Ye 2019, Equation (4.4)]. *Let π and σ be irreducible cuspidal representations of* $\mathrm{GL}_n(\mathbb{F})$. *Then*

$$\gamma(\pi \times \sigma, \psi) = \sum_{g \in Z_n \backslash \mathrm{GL}_n(\mathbb{F})} \mathcal{J}_{\pi,\psi}(g)\mathcal{J}_{\sigma,\psi^{-1}}(g)\psi(\langle e_n g^{-1}, e_1\rangle),$$

where $e_1 = (1, 0, \ldots, 0) \in \mathbb{F}^n$.

It follows from Propositions 2.9 and 2.3 that

$$\gamma(\pi^\vee \times \sigma^\vee, \psi^{-1}) = \overline{\gamma(\pi \times \sigma, \psi)}.$$

We now move to discuss the absolute value of $\gamma(\pi \times \sigma, \psi)$. In order to do that, we first explain how to extend the functional equation in Theorem 2.8 to all functions in $\mathcal{S}(\mathbb{F}^n)$ for most cases. To begin, we notice that for the indicator function of $0 \in \mathbb{F}^n$, which we denote δ_0, we have that $Z(W, W', \delta_0; \psi) = 0$. We also notice that if π is not isomorphic to $\sigma^\vee$, then $Z(W, W', 1; \psi) = 0$, where 1 represents the constant function. This is because

$$Z(W, W', 1; \psi) = \sum_{g \in Z_n \backslash \mathrm{GL}_n(\mathbb{F})} W(g) W'(g)$$

defines a $\mathrm{GL}_n(\mathbb{F})$-invariant pairing $\mathcal{W}(\pi, \psi) \otimes \mathcal{W}(\sigma, \psi^{-1}) \to \mathbb{C}$, but such nontrivial pairing exists only when π is isomorphic to $\sigma^\vee$. These two observations imply the following extension of the functional equation, in the special case where π is not isomorphic to $\sigma^\vee$.

Proposition 2.10. *Suppose that $\pi \ncong \sigma^\vee$. Then for any $\phi \in \mathcal{S}(\mathbb{F}^n)$ we have*

$$Z(\tilde{W}, \tilde{W}', \mathcal{F}_\psi \phi; \psi^{-1}) = \gamma(\pi \times \sigma, \psi) Z(W, W', \phi; \psi).$$

Proof. Write $\phi = \phi_0 + \phi_1$, where $\phi_0 = \phi - \phi(0)$ and $\phi_1 = \phi(0)$. Then $\phi_0(0) = 0$ and $\mathcal{F}_\psi \phi_1 = q^n \phi(0) \delta_0$. Since Z is linear in ϕ, we have from the discussion above that

$$Z(W, W', \phi; \psi) = Z(W, W', \phi_0; \psi)$$

and that

$$Z(\tilde{W}, \tilde{W}', \mathcal{F}_\psi \phi; \psi^{-1}) = Z(\tilde{W}, \tilde{W}', \mathcal{F}_\psi \phi_0; \psi^{-1}).$$

The statement now follows from Theorem 2.8. □

As a result, we get the following corollary regarding the absolute value of $\gamma(\pi \times \sigma, \psi)$.

Corollary 2.11. *Let π and σ be irreducible cuspidal representations of $\mathrm{GL}_n(\mathbb{F})$ such that $\pi \ncong \sigma^\vee$. Then*

$$\gamma(\pi \times \sigma, \psi) \gamma(\pi^\vee \times \sigma^\vee, \psi^{-1}) = q^n,$$

and therefore

$$|\gamma(\pi \times \sigma, \psi)| = q^{n/2}.$$

Proof. This follows by applying Proposition 2.10 twice, and from the fact that the Fourier transform satisfies

$$\mathcal{F}_{\psi^{-1}} \mathcal{F}_\psi \phi = q^n \phi,$$

for any $\phi \in \mathcal{S}(\mathbb{F}^n)$. □

We are left to deal with the case $\pi \cong \sigma^\vee$. In this case, the gamma factor $\gamma(\pi \times \pi^\vee, \psi)$ can be computed explicitly and it equals -1; see the Appendix.

We summarize all cases in the following proposition.

Proposition 2.12. *Let π and σ be irreducible cuspidal representations of* $\mathrm{GL}_n(\mathbb{F})$:

- *If $\pi \ncong \sigma^\vee$ then $|\gamma(\pi \times \sigma, \psi)| = q^{n/2}$.*
- *If $\pi \cong \sigma^\vee$ then $|\gamma(\pi \times \sigma, \psi)| = 1$.*

3. Shahidi gamma factors (local coefficients)

In this section, we use the Langlands–Shahidi method in order to define a gamma factor for two representations of Whittaker type of finite general linear groups. This is the finite field analog of Shahidi's local coefficient, which uses an intertwining operator. The treatment in Sections 3A–3C is a finite field analog of Shahidi's work on local coefficients over local fields [Shahidi 1984]. Unlike the Jacquet–Piatetski-Shapiro–Shalika gamma factors discussed in Section 2C, the Shahidi gamma factor can be defined uniformly for all irreducible generic representations of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}_m(\mathbb{F})$, regardless of $n > m$ or whether the representations are cuspidal. We prove properties of the Shahidi gamma factor, where the most important one is the multiplicativity property, which explains how this gamma factor behaves under parabolic induction. We end this section by expressing the Shahidi gamma factor in terms of the Bessel functions associated with the representations, and showing its relation to the Jacquet–Piatetski-Shapiro–Shalika gamma factor.

3A. ***The intertwining operator.*** Let n and m be positive integers and let π and σ be representations of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}_m(\mathbb{F})$, respectively. We define a linear map $\sigma \otimes \pi \to \pi \otimes \sigma$ acting on pure tensors by component swap:

$$\mathrm{sw}_{\sigma,\pi}(v_\sigma \otimes v_\pi) = v_\pi \otimes v_\sigma .$$

For a function $f\colon \mathrm{GL}_{n+m}(\mathbb{F}) \to \sigma \otimes \pi$, we denote by $\tilde{f}\colon \mathrm{GL}_{n+m}(\mathbb{F}) \to \pi \otimes \sigma$ the function $\tilde{f}(g) = \mathrm{sw}_{\sigma,\pi}(f(g))$.

We consider the following intertwining operator $T_{\sigma,\pi}\colon \sigma \circ \pi \to \pi \circ \sigma$, defined for $f \in \sigma \circ \pi$ and $g \in \mathrm{GL}_{n+m}(\mathbb{F})$ by the formula

$$T_{\sigma,\pi} f(g) = \sum_{p \in P_{n,m}} (\pi \overline{\otimes} \sigma)(p^{-1}) \tilde{f}(\hat{w}_{n,m} p g),$$

where $\hat{w}_{n,m}$ is the following Weyl element

$$\hat{w}_{n,m} = \begin{pmatrix} & I_m \\ I_n & \end{pmatrix}.$$

Using the decomposition $P_{n,m} = D_{n,m} \ltimes N_{n,m}$, we may write every $p \in P_{n,m}$ in a unique way $p = du$, where $u \in N_{n,m}$ and $d = \mathrm{diag}(g_1, g_2) \in D_{n,m}$, with $g_1 \in \mathrm{GL}_n(\mathbb{F})$ and $g_2 \in \mathrm{GL}_m(\mathbb{F})$. It follows from the identity

$$\mathrm{diag}(g_2, g_1)\hat{w}_{n,m} = \hat{w}_{n,m}\,\mathrm{diag}(g_1, g_2),$$

and from the left $D_{m,n}$-equivariance property of f that

$$T_{\sigma,\pi} f(g) = |D_{n,m}| \cdot U_{\sigma,\pi} f(g),$$

where

$$U_{\sigma,\pi} f(g) = \sum_{u \in N_{n,m}} \tilde{f}(\hat{w}_{n,m} u g).$$

By construction, we have that $T_{\sigma,\pi}$ and $U_{\sigma,\pi}$ are nonzero elements of the space

$$\mathrm{Hom}_{\mathrm{GL}_{n+m}(\mathbb{F})}(\sigma \circ \pi, \pi \circ \sigma).$$

3B. ***The Shahidi gamma factor.*** Suppose now that π and σ are representations of Whittaker type of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}_m(\mathbb{F})$, respectively. By Theorem 2.2 we have that the parabolically induced representations $\sigma \circ \pi$ and $\pi \circ \sigma$ are also of Whittaker type. Let $v_{\sigma,\psi} \in \sigma$ and $v_{\pi,\psi} \in \pi$ be nonzero ψ-Whittaker vectors for σ and π, respectively. We may define a nonzero ψ-Whittaker vector $f_{v_{\sigma,\psi}, v_{\pi,\psi}}$ for $\sigma \circ \pi$ by the formula

$$f_{v_{\sigma,\psi}, v_{\pi,\psi}}(g) = \begin{cases} \psi(u)(\sigma \overline{\otimes} \pi)(p) v_{\sigma,\psi} \otimes v_{\pi,\psi} & g = p\hat{w}_{n,m}u,\ p \in P_{m,n},\ u \in Z_{n+m}, \\ 0 & \text{otherwise.} \end{cases}$$

Similarly, we may define $f_{v_{\pi,\psi}, v_{\sigma,\psi}} \in \pi \circ \sigma$.

Since $U_{\sigma,\pi}$ is an intertwining operator, we have that $U_{\sigma,\pi} f_{v_{\sigma,\psi}, v_{\pi,\psi}}$ is a ψ-Whittaker vector of $\pi \circ \sigma$. Since $f_{v_{\pi,\psi}, v_{\sigma,\psi}}$ is the unique nonzero ψ-Whittaker vector of $\pi \circ \sigma$ up to scalar, we must have that

$$U_{\sigma,\pi} f_{v_{\sigma,\psi}, v_{\pi,\psi}} = \gamma \cdot f_{v_{\pi,\psi}, v_{\sigma,\psi}},$$

where $\gamma \in \mathbb{C}$. It is easy to check that this number γ does not depend on the choice of ψ-Whittaker vectors $v_{\sigma,\psi}$ and $v_{\pi,\psi}$.

In order to ease the notation, we denote $v_{\sigma,\pi,\psi} = f_{v_{\sigma,\psi}, v_{\pi,\psi}}$, where we suppress $v_{\sigma,\psi}$ and $v_{\pi,\psi}$ from the notation. Similarly, we denote $v_{\pi,\sigma,\psi} = f_{v_{\pi,\psi}, v_{\sigma,\psi}}$.

Definition 3.1. The Shahidi gamma factor of π and σ with respect to ψ is the unique number $\Gamma(\pi \times \sigma, \psi) \in \mathbb{C}$, such that

$$U_{\sigma,\pi} v_{\sigma,\pi,\psi} = \Gamma(\pi \times \sigma, \psi) \cdot v_{\pi,\sigma,\psi}.$$

Remark 3.2. If $\pi \circ \sigma$ is irreducible, then so is $\sigma \circ \pi$, and since $U_{\sigma,\pi}$ is a nonzero intertwining operator, it is an isomorphism and $\Gamma(\pi \times \sigma, \psi)$ must be nonzero.

However, in the general case it is not obvious at this point that $\Gamma(\pi \times \sigma, \psi)$ is nonzero. We will show this later.

Remark 3.3. As in Remark 2.4, we may choose invariant inner products $(\cdot\,,\cdot)_\pi$ and $(\cdot\,,\cdot)_\sigma$ on π and σ, respectively. We then have a natural inner product $(\cdot\,,\cdot)_{\sigma\otimes\pi}$ on $\sigma \otimes \pi$, which defines an inner product on $\sigma \circ \pi$ by the formula

$$(f_1, f_2)_{\sigma\circ\pi} = \sum_{g \in P_{m,n}\backslash \mathrm{GL}_{n+m}(\mathbb{F})} (f_1(g), f_2(g))_{\sigma\otimes\pi}.$$

Using this inner product, the Whittaker functional $\ell_{\sigma\circ\pi,\psi}(f) = (f, v_{\sigma,\pi,\psi})_{\sigma\circ\pi}$ is related to the Whittaker functionals $\ell_{\sigma,\psi}(v_\sigma) = (v_\sigma, v_{\sigma,\psi})_\sigma$ and $\ell_{\pi,\psi}(v_\pi) = (v_\pi, v_{\pi,\psi})_\pi$ by the formula

$$\ell_{\sigma\circ\pi,\psi}(f) = \sum_{u \in N_{n,m}} \ell_{\sigma,\psi} \otimes \ell_{\pi,\psi}(f(\hat{w}_{n,m}u))\psi^{-1}(u).$$

Similarly, by exchanging the roles of π and σ, we have that Whittaker functional $\ell_{\pi\circ\sigma,\psi}$ is given by a similar formula. Using the definitions of the inner products, and the fact that elements in $\pi \circ \sigma$ are left invariant under $N_{n,m}$, we see that $U_{\pi,\sigma}$ is the adjoint of $U_{\sigma,\pi}$, with respect to our choice of inner products. Using the relation between $v_{\sigma,\pi,\psi}$ and $v_{\pi,\sigma,\psi}$, we obtain the following relation

$$\ell_{\sigma\circ\pi,\psi} \circ U_{\pi,\sigma} = \Gamma(\pi \times \sigma, \psi) \cdot \ell_{\pi\circ\sigma,\psi}.$$

This is how the Shahidi gamma factor is usually defined in the literature.

3B1. *Dependence on ψ.* For any $a \in \mathbb{F}^*$, let $\psi_a : \mathbb{F} \to \mathbb{C}^*$ be the additive character

$$\psi_a(x) = \psi(ax).$$

It is well known that all nontrivial additive characters of $\mathbb{F}$ are of the form ψ_a for some $a \in \mathbb{F}^*$. In this section, we give a relation between $\Gamma(\pi \times \sigma, \psi)$ and $\Gamma(\pi \times \sigma, \psi_a)$.

Let $a \in \mathbb{F}^*$. Suppose that τ is a generic representation of $\mathrm{GL}_k(\mathbb{F})$ with a nonzero ψ-Whittaker vector $v_{\tau,\psi}$. Let

$$d_k = \mathrm{diag}(1, a, a^2, \ldots, a^{k-1}).$$

Then we have that $\tau(d_k)v_{\tau,\psi}$ is a nonzero ψ_a-Whittaker vector of τ. The map $v \mapsto \tau(d_k)v$ is a linear isomorphism from the subspace spanned by the ψ-Whittaker vectors of τ to the subspace spanned by the ψ_a-Whittaker vectors of τ. In particular, if $v_{\tau,\psi}$ is the unique (up to scalar multiplication) ψ-Whittaker vector of τ, then $\tau(d_k)v_{\tau,\psi}$ is the unique (up to scalar multiplication) ψ_a-Whittaker vector of τ.

Let π and σ be representations of Whittaker type of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}_m(\mathbb{F})$, respectively. Let $v_{\pi,\psi} \in \pi$ and $v_{\sigma,\psi} \in \sigma$ be nonzero ψ-Whittaker vectors. Assume

that π and σ have central characters, and denote them by ω_π and ω_σ, respectively. Let

$$v_{\sigma,\pi,\psi_a} = f_{\sigma(d_m)v_{\sigma,\psi},\pi(d_n)v_{\pi,\psi}}.$$

Similarly, we define v_{π,σ,ψ_a}.

We first express v_{σ,π,ψ_a} in terms of $v_{\sigma,\pi,\psi}$. We will use this relation later to show a relation between the gamma factors $\Gamma(\pi \times \sigma, \psi_a)$ and $\Gamma(\pi \times \sigma, \psi)$.

Proposition 3.4. *We have*

$$v_{\sigma,\pi,\psi_a} = \omega_\sigma(a)^{-n}\rho(d_{n+m})v_{\sigma,\pi,\psi},$$

where $\rho(d_{n+m})$ denotes right translation by d_{n+m}.

Proof. Let $f = \omega_\sigma(a)^{-n}\rho(d_{n+m})v_{\sigma,\pi,\psi} \in \sigma \circ \pi$. By the discussion above, f is a ψ_a-Whittaker vector of $\sigma \circ \pi$.

We have that

$$f(\hat{w}_{n,m}) = \omega_\sigma(a)^{-n}v_{\sigma,\pi,\psi}(\hat{w}_{n,m}d_{n+m}).$$

Writing $d_{n+m} = \mathrm{diag}(d_n, a^n d_m)$, we have $\hat{w}_{n,m}d_{n+m} = \mathrm{diag}(a^n d_m, d_n)\hat{w}_{n,m}$, and hence

$$f(\hat{w}_{n,m}) = (\sigma(d_m) \otimes \pi(d_n))v_{\sigma,\pi,\psi}(\hat{w}_{n,m}) = \sigma(d_m)v_{\sigma,\psi} \otimes \pi(d_n)v_{\pi,\psi}.$$

This shows that $f = v_{\sigma,\pi,\psi_a}$, as both are ψ_a-Whittaker vectors in $\sigma \circ \pi$, and both agree at the point $\hat{w}_{n,m}$. □

Theorem 3.5. *We have*

$$\Gamma(\pi \times \sigma, \psi_a) = \omega_\pi(a)^m \cdot \omega_\sigma(a)^{-n} \cdot \Gamma(\pi \times \sigma, \psi).$$

Proof. By definition, we have that

$$\Gamma(\pi \times \sigma, \psi_a)v_{\pi,\sigma,\psi_a} = U_{\sigma,\pi}v_{\sigma,\pi,\psi_a}.$$

By Proposition 3.4,

$$\Gamma(\pi \times \sigma, \psi_a)\omega_\pi(a)^{-m}\rho(d_{n+m})v_{\pi,\sigma,\psi} = \omega_\sigma(a)^{-n}U_{\sigma,\pi}\rho(d_{n+m})v_{\sigma,\pi,\psi}.$$

Therefore, we get that

$$\Gamma(\pi \times \sigma, \psi_a)\omega_\sigma(a)^n\omega_\pi(a)^{-m}v_{\pi,\sigma,\psi} = U_{\sigma,\pi}v_{\sigma,\pi,\psi},$$

which implies that

$$\Gamma(\pi \times \sigma, \psi_a)\omega_\sigma(a)^n\omega_\pi(a)^{-m} = \Gamma(\pi \times \sigma, \psi),$$

as required. □

3B2. *Relation between* $\Gamma(\pi \times \sigma, \psi)$ *and* $\Gamma(\sigma^\vee \times \pi^\vee, \psi^{-1})$. In this section, we analyze the relation between $\Gamma(\pi \times \sigma, \psi)$ and $\Gamma(\sigma^\vee \times \pi^\vee, \psi)$.

Recall that for a finite dimensional representation τ of $\mathrm{GL}_k(\mathbb{F})$, we have that $\tau^\vee \cong \tau^\iota$. See Section 2B1. If $v_{\tau,\psi}$ is a nonzero ψ-Whittaker vector for τ, then $\tau(w_k)v_{\tau,\psi}$ is a nonzero ψ^{-1}-Whittaker vector for τ^ι.

We have that

$$\pi^\iota \circ \sigma^\iota \cong (\sigma \circ \pi)^\iota$$

by the isomorphism $S_{\sigma,\pi}\colon (\sigma \circ \pi)^\iota \cong \pi^\iota \circ \sigma^\iota$ that sends $f \in (\sigma \circ \pi)^\iota$ to the function

$$(S_{\sigma,\pi} f)(g) = \tilde{f}(\hat{w}_{n,m} g^\iota).$$

Let

$$v_{\pi^\iota,\sigma^\iota,\psi^{-1}} = f_{\pi(w_n)v_{\pi,\psi},\sigma(w_m)v_{\sigma,\psi}} \in \pi^\iota \circ \sigma^\iota.$$

Then $v_{\pi^\iota,\sigma^\iota,\psi^{-1}}$ is a nonzero ψ^{-1}-Whittaker vector of $\pi^\iota \circ \sigma^\iota$. On the other hand, by the discussion above, a nonzero ψ^{-1}-Whittaker vector of $(\sigma \circ \pi)^\iota$ is given by $\rho(w_{m+n})v_{\sigma,\pi,\psi}$, where $\rho(w_{m+n})$ represents right translation by w_{m+n}. Therefore $S_{\sigma,\pi}\rho(w_{m+n})v_{\sigma,\pi,\psi}$ is another nonzero ψ^{-1}-Whittaker vector of $\pi^\iota \circ \sigma^\iota$.

Proposition 3.6. *We have*

$$v_{\pi^\iota,\sigma^\iota,\psi^{-1}} = S_{\sigma,\pi}\rho(w_{m+n})v_{\sigma,\pi,\psi}. \tag{3-1}$$

Proof. We have that

$$S_{\sigma,\pi}\rho(w_{m+n})v_{\sigma,\pi,\psi}(\hat{w}_{m,n}) = \mathrm{sw}_{\sigma,\pi}\, v_{\sigma,\pi,\psi}(w_{m+n}) = \pi(w_n)v_{\pi,\psi} \otimes \sigma(w_m)v_{\sigma,\psi},$$

where in the last step we used the fact that $\mathrm{diag}(w_m, w_n)\hat{w}_{n,m} = w_{n+m}$.

Since $S_{\sigma,\pi}\rho(w_{m+n})v_{\sigma,\pi,\psi}$ and $v_{\pi^\iota,\sigma^\iota,\psi^{-1}}$ are both ψ^{-1}-Whittaker vectors for the representation of Whittaker type $\pi^\iota \circ \sigma^\iota$, and they both agree at the point $\hat{w}_{m,n}$, they are equal. □

Similarly, let

$$v_{\sigma^\iota,\pi^\iota,\psi^{-1}} = f_{\sigma(w_m)v_{\sigma,\psi},\pi(w_n)v_{\pi,\psi}} \in \sigma^\iota \circ \pi^\iota.$$

Using Proposition 3.6 with roles of the representations π and σ exchanged, we have

$$v_{\sigma^\iota,\pi^\iota,\psi^{-1}} = S_{\pi,\sigma}\rho(w_{m+n})v_{\pi,\sigma,\psi}. \tag{3-2}$$

Theorem 3.7. *Let* π *and* σ *be representations of Whittaker type of* $\mathrm{GL}_n(\mathbb{F})$ *and* $\mathrm{GL}_m(\mathbb{F})$, *respectively. Then*

$$\Gamma(\pi \times \sigma, \psi) = \Gamma(\sigma^\vee \times \pi^\vee, \psi^{-1}).$$

Proof. By definition,

$$U_{\pi^\iota,\sigma^\iota} v_{\pi^\iota,\sigma^\iota,\psi^{-1}} = \Gamma(\sigma^\iota \times \pi^\iota, \psi^{-1}) \cdot v_{\sigma^\iota,\pi^\iota,\psi^{-1}}. \tag{3-3}$$

Substituting (3-1) and (3-2) in (3-3), we get

$$U_{\pi^\iota,\sigma^\iota} S_{\sigma,\pi} \rho(w_{m+n}) v_{\sigma,\pi,\psi} = \Gamma(\sigma^\iota \times \pi^\iota, \psi^{-1}) \cdot S_{\pi,\sigma} \rho(w_{m+n}) v_{\pi,\sigma,\psi}.$$

A simple computation shows that

$$U_{\pi^\iota,\sigma^\iota} \circ S_{\sigma,\pi} = S_{\pi,\sigma} \circ U_{\sigma,\pi}.$$

Hence, we get that

$$S_{\pi,\sigma} \rho(w_{m+n}) U_{\sigma,\pi} v_{\sigma,\pi,\psi} = \Gamma(\sigma^\iota \times \pi^\iota, \psi^{-1}) \cdot S_{\pi,\sigma} \rho(w_{m+n}) v_{\pi,\sigma,\psi},$$

which implies that

$$U_{\sigma,\pi} v_{\sigma,\pi,\psi} = \Gamma(\sigma^\iota \times \pi^\iota, \psi^{-1}) \cdot v_{\pi,\sigma,\psi}.$$

Therefore, we must have

$$\Gamma(\sigma^\iota \times \pi^\iota, \psi^{-1}) = \Gamma(\pi \times \sigma, \psi),$$

and the statement in the theorem follows, since $\sigma^\iota \cong \sigma^\vee$ and $\pi^\iota \cong \pi^\vee$. □

Combining Theorem 3.7 with Theorem 3.5, we get the following corollary.

Corollary 3.8. *Let π and σ be representations of Whittaker type of* $\mathrm{GL}_n(\mathbb{F})$ *and* $\mathrm{GL}_m(\mathbb{F})$, *respectively. Assume that both π and σ have central characters, and denote them by ω_π and ω_σ, respectively. Then*

$$\Gamma(\pi \times \sigma, \psi) = \Gamma(\sigma^\vee \times \pi^\vee, \psi) \cdot \omega_\pi(-1)^m \omega_\sigma(-1)^n.$$

3C. ***Multiplicativity of Gamma factors.*** In this section, we show that $\Gamma(\pi \times \sigma, \psi)$ is multiplicative.

Let π be a representation of Whittaker type of $\mathrm{GL}_n(\mathbb{F})$. Let $m = m_1 + m_2$, and let σ_1 and σ_2 be representations of Whittaker type of $\mathrm{GL}_{m_1}(\mathbb{F})$ and $\mathrm{GL}_{m_2}(\mathbb{F})$, respectively. By Theorem 2.2, the parabolic induction $\sigma_1 \circ \sigma_2$ is also a representation of Whittaker type. Hence, the gamma factor $\Gamma(\pi \times (\sigma_1 \circ \sigma_2), \psi)$ is well defined. We will show the following theorem.

Theorem 3.9. $\Gamma(\pi \times (\sigma_1 \circ \sigma_2), \psi) = \Gamma(\pi_1 \times \sigma_1, \psi) \cdot \Gamma(\pi_2 \times \sigma_2, \psi).$

The proof of this theorem will occupy the remaining subsections of this section.

Remark 3.10. Let $\sigma \subset \sigma_1 \circ \sigma_2$ be the unique irreducible generic subrepresentation of $\sigma_1 \circ \sigma_2$. We have that ψ-Whittaker vectors of σ are the same as ψ-Whittaker vectors of $\sigma_1 \circ \sigma_2$. Hence, Theorem 3.9 implies that

$$\Gamma(\pi \times \sigma, \psi) = \Gamma(\pi \times \sigma_1, \psi) \cdot \Gamma(\pi \times \sigma_2, \psi).$$

Before proving the theorem, we mention two other multiplicative properties that follow immediately from the theorem.

The first property is that the gamma factor is also multiplicative in the first variable. This follows from Theorem 3.9 combined with Theorem 3.7.

Corollary 3.11. *Let π_1 and π_2 be representations of Whittaker type of $\mathrm{GL}_{n_1}(\mathbb{F})$ and $\mathrm{GL}_{n_2}(\mathbb{F})$, respectively, and let σ be a representation of Whittaker type of $\mathrm{GL}_m(\mathbb{F})$. Then*

$$\Gamma((\pi_1 \circ \pi_2) \times \sigma, \psi) = \Gamma(\pi_1 \times \sigma, \psi) \cdot \Gamma(\pi_2 \times \sigma, \psi).$$

The second corollary allows us to express the gamma factor of two parabolically induced representations as the product of the gamma factors of the components of the parabolic induction. It follows by repeatedly using multiplicativity in both variables.

Corollary 3.12. *Let $\pi_1, \ldots, \pi_r$ and $\sigma_1, \ldots, \sigma_t$ be irreducible generic representations of $\mathrm{GL}_{n_1}(\mathbb{F}), \ldots, \mathrm{GL}_{n_r}(\mathbb{F})$ and $\mathrm{GL}_{m_1}(\mathbb{F}), \ldots, \mathrm{GL}_{m_t}(\mathbb{F})$, respectively. Then*:

(1) *We have*

$$\Gamma((\pi_1 \circ \ldots \circ \pi_r) \times (\sigma_1 \circ \ldots \circ \sigma_t), \psi) = \prod_{i=1}^{r} \prod_{j=1}^{t} \Gamma(\pi_i \times \sigma_j, \psi).$$

(2) *If π is the unique irreducible generic subrepresentation of $\pi_1 \circ \ldots \circ \pi_r$ and σ is the unique irreducible generic subrepresentation of $\sigma_1 \circ \ldots \circ \sigma_t$, then*

$$\Gamma(\pi \times \sigma, \psi) = \prod_{i=1}^{r} \prod_{j=1}^{t} \Gamma(\pi_i \times \sigma_j, \psi).$$

In the next subsections we make preparations for the proof of Theorem 3.9.

3C1. *Transitivity of parabolic induction.* Let τ_1, τ_2 and τ_3 be finite dimensional representations of $\mathrm{GL}_{n_1}(\mathbb{F})$, $\mathrm{GL}_{n_2}(\mathbb{F})$ and $\mathrm{GL}_{n_3}(\mathbb{F})$, respectively.

We realize elements in $(\tau_1 \circ \tau_2) \otimes \tau_3$ as functions $\mathrm{GL}_{n_1+n_2}(\mathbb{F}) \to \tau_1 \otimes \tau_2 \otimes \tau_3$ in the obvious way. Similarly, we realize elements in $\tau_1 \otimes (\tau_2 \circ \tau_3)$ as functions $\mathrm{GL}_{n_2+n_3} \to \tau_1 \otimes \tau_2 \otimes \tau_3$ in the obvious way.

Consider the space $(\tau_1 \circ \tau_2) \circ \tau_3$. We will regard elements of this space as functions

$$f\colon\ \mathrm{GL}_{n_1+n_2+n_3}(\mathbb{F}) \times \mathrm{GL}_{n_1+n_2}(\mathbb{F}) \to \tau_1 \otimes \tau_2 \otimes \tau_3,$$

where $f(g; h)$ means evaluating f at $g \in \mathrm{GL}_{n_1+n_2+n_3}(\mathbb{F})$ and then evaluating the resulting function at $h \in \mathrm{GL}_{n_1+n_2}(\mathbb{F})$. We will similarly regard elements of $\tau_1 \circ (\tau_2 \circ \tau_3)$ as functions

$$f\colon\ \mathrm{GL}_{n_1+n_2+n_3}(\mathbb{F}) \times \mathrm{GL}_{n_2+n_3}(\mathbb{F}) \to \tau_1 \otimes \tau_2 \otimes \tau_3.$$

We have an isomorphism of representations

$$L_{\tau_1,\tau_2;\tau_3}\colon (\tau_1 \circ \tau_2) \circ \tau_3 \to \tau_1 \circ \tau_2 \circ \tau_3,$$

given by mapping a function $f \in (\tau_1 \circ \tau_2) \circ \tau_3$ to

$$L_{\tau_1,\tau_2;\tau_3} f(g) = f(g; I_{n_1+n_2}),$$

where $g \in \mathrm{GL}_{n_1+n_2+n_3}(\mathbb{F})$.

Similarly, we have an isomorphism of representations

$$L_{\tau_1;\tau_2,\tau_3}\colon \tau_1 \circ (\tau_2 \circ \tau_3) \to \tau_1 \circ \tau_2 \circ \tau_3,$$

given by mapping a function $f \in \tau_1 \circ (\tau_2 \circ \tau_3)$ to

$$L_{\tau_1;\tau_2,\tau_3} f(g) = f(g; I_{n_2+n_3}),$$

where again $g \in \mathrm{GL}_{n_1+n_2+n_3}(\mathbb{F})$.

Assume now that τ_1, τ_2 and τ_3 have nonzero ψ-Whittaker vectors, $v_{\tau_1,\psi}$, $v_{\tau_2,\psi}$ and $v_{\tau_3,\psi}$, respectively, and assume that up to scalar multiplication, these Whittaker vectors are unique. We denote, as before, the following nonzero ψ-Whittaker vectors $v_{\tau_1,\tau_2,\psi} = f_{v_{\tau_1,\psi},v_{\tau_2,\psi}} \in \tau_1 \circ \tau_2$ and $v_{\tau_2,\tau_3,\psi} = f_{v_{\tau_2,\psi},v_{\tau_3,\psi}} \in \tau_2 \circ \tau_3$. We also define the following nonzero ψ-Whittaker vectors $v_{\tau_1,\tau_2\circ\tau_3,\psi} = f_{v_{\tau_1,\psi},v_{\tau_2,\tau_3,\psi}} \in \tau_1 \circ (\tau_2 \circ \tau_3)$ and $v_{\tau_1\circ\tau_2,\tau_3,\psi} = f_{v_{\tau_1,\tau_2,\psi},v_{\tau_3,\psi}} \in (\tau_1 \circ \tau_2) \circ \tau_3$. Finally, we define

$$v_{\tau_1,\tau_2,\tau_3,\psi} = L_{\tau_1;\tau_2,\tau_3} v_{\tau_1,\tau_2\circ\tau_3,\psi} = L_{\tau_1,\tau_2;\tau_3} v_{\tau_1\circ\tau_2,\tau_3,\psi} \in \tau_1 \circ \tau_2 \circ \tau_3.$$

Then $v_{\tau_1,\tau_2,\tau_3,\psi}$ is the ψ-Whittaker vector in $\tau_1 \circ \tau_2 \circ \tau_3$ supported on the double coset $P_{n_1,n_2,n_3}\hat{w}_{n_3,n_2,n_1}Z_{n_1+n_2+n_3}$, with $v_{\tau_1,\tau_2,\tau_3,\psi}(\hat{w}_{n_3,n_2,n_1}) = v_{\tau_1,\psi} \otimes v_{\tau_2,\psi} \otimes v_{\tau_3,\psi}$, where

$$\hat{w}_{n_3,n_2,n_1} = \begin{pmatrix} & & I_{n_1} \\ & I_{n_2} & \\ I_{n_3} & & \end{pmatrix}.$$

3C2. *Intertwining operators.* We return to the notations of the beginning of this section. Let π be a representation of Whittaker type of $\mathrm{GL}_n(\mathbb{F})$. Let $m = m_1 + m_2$, and let σ_1 and σ_2 be representations of Whittaker type of $\mathrm{GL}_{m_1}(\mathbb{F})$ and $\mathrm{GL}_{m_2}(\mathbb{F})$, respectively.

Using the isomorphisms from the previous section, we obtain maps such that the following diagrams are commutative:

$$\begin{array}{ccc} \sigma_1 \circ (\sigma_2 \circ \pi) & \xrightarrow{\mathrm{id}_{\sigma_1} \otimes U_{\sigma_2,\pi}} & \sigma_1 \circ (\pi \circ \sigma_2) \\ \downarrow{\scriptstyle L_{\sigma_1;\sigma_2,\pi}} & & \downarrow{\scriptstyle L_{\sigma_1;\pi,\sigma_2}} \\ \sigma_1 \circ \sigma_2 \circ \pi & \xrightarrow{\tilde{U}_{\sigma_2,\pi}} & \sigma_1 \circ \pi \circ \sigma_2 \end{array} \tag{3-4}$$

$$\begin{array}{ccc} (\sigma_1 \circ \pi) \circ \sigma_2 & \xrightarrow{U_{\sigma_1,\pi} \otimes \mathrm{id}_{\sigma_2}} & (\pi \circ \sigma_1) \circ \sigma_2 \\ \downarrow{\scriptstyle L_{\sigma_1,\pi;\sigma_2}} & & \downarrow{\scriptstyle L_{\pi,\sigma_1;\sigma_2}} \\ \sigma_1 \circ \pi \circ \sigma_2 & \xrightarrow{\tilde{U}_{\sigma_1,\pi}} & \pi \circ \sigma_1 \circ \sigma_2 \end{array} \tag{3-5}$$

$$\begin{array}{ccc} (\sigma_1 \circ \sigma_2) \circ \pi & \xrightarrow{U_{\sigma_1 \circ \sigma_2,\pi}} & \pi \circ (\sigma_1 \circ \sigma_2) \\ \downarrow{\scriptstyle L_{\sigma_1,\sigma_2;\pi}} & & \downarrow{\scriptstyle L_{\pi;\sigma_1,\sigma_2}} \\ \sigma_1 \circ \sigma_2 \circ \pi & \xrightarrow{\tilde{U}_{\sigma_1 \circ \sigma_2,\pi}} & \pi \circ \sigma_1 \circ \sigma_2 \end{array} \tag{3-6}$$

Let us explain these diagrams. We begin with explaining (3-4). The map $\mathrm{id}_{\sigma_1} \otimes U_{\sigma_2,\pi} : \sigma_1 \otimes (\sigma_2 \circ \pi) \to \sigma_1 \otimes (\pi \circ \sigma_2)$ is a homomorphism of representations. It defines a homomorphism $\sigma_1 \circ (\sigma_2 \circ \pi) \to \sigma_1 \circ (\pi \circ \sigma_2)$, which we keep denoting by $\mathrm{id}_{\sigma_1} \otimes U_{\sigma_2,\pi}$. By unwrapping the definitions, we see that the map $\tilde{U}_{\sigma_2,\pi} : \sigma_1 \circ \sigma_2 \circ \pi \to \sigma_1 \circ \pi \circ \sigma_2$ is given by the formula

$$\tilde{U}_{\sigma_2,\pi}(f)(g) = \sum_{u_{n,m_2} \in N_{n,m_2}} \mathrm{sw}_{\sigma_2,\pi}\, f\left(\begin{pmatrix} I_{m_1} & & \\ & & I_{m_2} \\ & I_n & \end{pmatrix} \begin{pmatrix} I_{m_1} & & \\ & u_{n,m_2} & \end{pmatrix} g \right). \tag{3-7}$$

The commutative diagram (3-5) is similar. We get by unwrapping the definitions that the map $\tilde{U}_{\sigma_1,\pi} : \sigma_1 \circ \pi \circ \sigma_2 \to \pi \circ \sigma_1 \circ \sigma_2$ is given by

$$\tilde{U}_{\sigma_1,\pi}(f)(g) = \sum_{u_{n,m_1} \in N_{n,m_1}} \mathrm{sw}_{\sigma_1,\pi}\, f\left(\begin{pmatrix} & I_{m_1} & \\ I_n & & \\ & & I_{m_2} \end{pmatrix} \begin{pmatrix} u_{n,m_1} & & \\ & & I_{m_2} \end{pmatrix} g \right). \tag{3-8}$$

Finally, in the diagram (3-6), we have that $\tilde{U}_{\sigma_1 \circ \sigma_2,\pi} : \sigma_1 \circ \sigma_2 \circ \pi \to \pi \circ \sigma_1 \circ \sigma_2$ is given by

$$\tilde{U}_{\sigma_1 \circ \sigma_2,\pi}(f)(g) = \sum_{u_{n,m} \in N_{n,m}} \tilde{f}\left(\begin{pmatrix} & I_{m_1} & \\ & & I_{m_2} \\ I_n & & \end{pmatrix} u_{n,m} g \right), \tag{3-9}$$

where for $g \in \mathrm{GL}_{n+m}(\mathbb{F})$, we mean $\tilde{f}(g) = \mathrm{sw}_{\sigma_1,\pi}\, \mathrm{sw}_{\sigma_2,\pi}\, f(g)$.

Proposition 3.13. *We have*

$$\tilde{U}_{\sigma_1\circ\sigma_2,\pi} = \tilde{U}_{\sigma_1,\pi} \circ \tilde{U}_{\sigma_2,\pi}.$$

Proof. Let $f \in \sigma_1 \circ \sigma_2 \circ \pi$ and $g \in \mathrm{GL}_{n+m}(\mathbb{F})$. Then by (3-7) and (3-8),

$$(\tilde{U}_{\sigma_1,\pi}\circ\tilde{U}_{\sigma_2,\pi} f)(g) = \sum_{X\in M_{n\times m_1}(\mathbb{F})} \sum_{Y\in M_{n\times m_2}(\mathbb{F})} \tilde{f}\left(\begin{pmatrix} I_{m_1} & & \\ & & I_{m_2} \\ & I_n & \end{pmatrix}\begin{pmatrix} I_{m_1} & & \\ & I_n & Y \\ & & I_{m_2}\end{pmatrix} \times \begin{pmatrix} & I_{m_1} & \\ I_n & & \\ & & I_{m_2}\end{pmatrix}\begin{pmatrix} I_n & X & \\ & I_{m_1} & \\ & & I_{m_2}\end{pmatrix} g\right).$$

A simple computation shows that

$$\begin{pmatrix} I_{m_1} & & \\ & & I_{m_2} \\ & I_n & \end{pmatrix}\begin{pmatrix} I_{m_1} & & \\ & I_n & Y \\ & & I_{m_2}\end{pmatrix}\begin{pmatrix} & I_{m_1} & \\ I_n & & \\ & & I_{m_2}\end{pmatrix}\begin{pmatrix} I_n & X & \\ & I_{m_1} & \\ & & I_{m_2}\end{pmatrix} = \begin{pmatrix} & I_{m_1} & \\ & & I_{m_2} \\ I_n & & \end{pmatrix}\begin{pmatrix} I_n & X & Y \\ & I_{m_1} & \\ & & I_{m_2}\end{pmatrix}.$$

Hence, we get

$$(\tilde{U}_{\sigma_1,\pi}\circ\tilde{U}_{\sigma_2,\pi} f)(g) = \sum_{X\in M_{n\times m_1}(\mathbb{F})} \sum_{Y\in M_{n\times m_2}(\mathbb{F})} \tilde{f}\left(\begin{pmatrix} & I_{m_1} & \\ & & I_{m_2} \\ I_n & & \end{pmatrix}\begin{pmatrix} I_n & X & Y \\ & I_{m_1} & \\ & & I_{m_2}\end{pmatrix} g\right),$$

and the last sum is $\tilde{U}_{\sigma_1\circ\sigma_2,\pi}(f)(g)$ by (3-9). □

3C3. *Proof of Theorem 3.9.* Let $v_{\pi,\psi}$, $v_{\sigma_1,\psi}$ and $v_{\sigma_2,\psi}$ be nonzero ψ-Whittaker vectors of π, σ_1 and σ_2, respectively. We keep the notations from the previous section. We are now ready to prove Theorem 3.9.

Proof. By definition, we have

$$(\mathrm{id}_{\sigma_1} \otimes U_{\sigma_2,\pi})(v_{\sigma_1,\sigma_2\circ\pi,\psi}) = \Gamma(\pi\times\sigma_2,\psi) v_{\sigma_1,\pi\circ\sigma_2,\psi}.$$

Since $L_{\sigma_1;\sigma_2,\pi} v_{\sigma_1,\sigma_2\circ\pi,\psi} = v_{\sigma_1,\sigma_2,\pi,\psi}$ and $L_{\sigma_1;\pi,\sigma_2} v_{\sigma_1,\pi\circ\sigma_2,\psi} = v_{\sigma_1,\pi,\sigma_2,\psi}$, we get from the commutative diagram (3-4) that

$$\tilde{U}_{\sigma_2,\pi} v_{\sigma_1,\sigma_2,\pi,\psi} = \Gamma(\pi\times\sigma_2,\psi) v_{\sigma_1,\pi,\sigma_2,\psi}.$$

Similarly, we have that

$$(U_{\sigma_1,\pi} \otimes \mathrm{id}_{\sigma_2})(v_{\sigma_1\circ\pi,\sigma_2,\psi}) = \Gamma(\pi\times\sigma_1,\psi) v_{\pi\circ\sigma_1,\sigma_2,\psi},$$

and we get from the commutative diagram (3-5) that

$$\tilde{U}_{\sigma_1,\pi} v_{\sigma_1,\pi,\sigma_2,\psi} = \Gamma(\pi \times \sigma_1, \psi) v_{\pi,\sigma_1,\sigma_2,\psi}.$$

Finally, we have

$$U_{\sigma_1\circ\sigma_2,\pi} v_{\sigma_1\circ\sigma_2,\pi,\psi} = \Gamma(\pi \times (\sigma_1 \circ \sigma_2), \psi) v_{\pi,\sigma_1\circ\sigma_2,\psi}.$$

Since $L_{\sigma_1,\sigma_2;\pi} v_{\sigma_1\circ\sigma_2,\pi,\psi} = v_{\sigma_1,\sigma_2,\pi,\psi}$ and $L_{\pi;\sigma_1,\sigma_2} v_{\pi,\sigma_1\circ\sigma_2,\psi} = v_{\pi,\sigma_1,\sigma_2,\psi}$, we get from the commutative diagram (3-6)

$$\tilde{U}_{\sigma_1\circ\sigma_2,\pi} v_{\sigma_1,\sigma_2,\pi,\psi} = \Gamma(\pi \times (\sigma_1 \circ \sigma_2), \psi) v_{\pi,\sigma_1,\sigma_2,\psi}.$$

Since $\tilde{U}_{\sigma_1\circ\sigma_2,\pi} = \tilde{U}_{\sigma_1,\pi} \circ \tilde{U}_{\sigma_2,\pi}$, we get that

$$\Gamma(\pi \times (\sigma_1 \circ \sigma_2), \psi) v_{\pi,\sigma_1,\sigma_2,\psi} = \Gamma(\pi \times \sigma_1, \psi)\Gamma(\pi \times \sigma_2, \psi) v_{\pi,\sigma_1,\sigma_2,\psi},$$

and the theorem follows. □

3D. ***Expression in terms of Bessel functions.*** In this section, we express the Shahidi gamma factor of two irreducible generic representations in terms of their Bessel functions.

Let π and σ be irreducible generic representations of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}_m(\mathbb{F})$, respectively. We assume that π and σ are realized by their Whittaker models $\mathcal{W}(\pi, \psi)$ and $\mathcal{W}(\sigma, \psi)$, respectively. We choose the Whittaker vectors of π and σ to be their corresponding Bessel functions, i.e., we choose $v_{\pi,\psi} = \mathcal{J}_{\pi,\psi}$ and $v_{\sigma,\psi} = \mathcal{J}_{\sigma,\psi}$. We denote $\mathcal{J}_{\sigma,\pi,\psi} = v_{\sigma,\pi,\psi} = f_{\mathcal{J}_{\sigma,\psi},\mathcal{J}_{\pi,\psi}}$ and similarly $\mathcal{J}_{\pi,\sigma,\psi} = v_{\pi,\sigma,\psi} = f_{\mathcal{J}_{\pi,\psi},\mathcal{J}_{\sigma,\psi}}$.

Assume that $n \geq m$. By definition, we have that for any $g \in \mathrm{GL}_{n+m}(\mathbb{F})$,

$$(U_{\sigma,\pi}\mathcal{J}_{\sigma,\pi,\psi})(g) = \Gamma(\pi \times \sigma, \psi)\mathcal{J}_{\pi,\sigma,\psi}(g).$$

Substituting $g = \hat{w}_{m,n}$, we get

$$\Gamma(\pi \times \sigma, \psi)\mathcal{J}_{\pi,\sigma,\psi}(\hat{w}_{m,n}) = \sum_{u \in N_{n,m}} \mathrm{sw}_{\sigma,\pi}\, \mathcal{J}_{\sigma,\pi,\psi}(\hat{w}_{n,m} u \hat{w}_{m,n}),$$

and therefore

$$\Gamma(\pi \times \sigma, \psi)\mathcal{J}_{\pi,\psi} \otimes \mathcal{J}_{\sigma,\psi} = \sum_{A \in M_{n\times m}(\mathbb{F})} \mathrm{sw}_{\sigma,\pi}\, \mathcal{J}_{\sigma,\pi,\psi} \begin{pmatrix} I_m & \\ A & I_n \end{pmatrix}. \tag{3-10}$$

In order for $\mathcal{J}_{\sigma,\pi,\psi}\left(\begin{smallmatrix} I_m & \\ A & I_n \end{smallmatrix}\right)$ not to vanish, we must have $\left(\begin{smallmatrix} I_m & \\ A & I_n \end{smallmatrix}\right) \in P_{m,n}\hat{w}_{n,m}Z_{n+m}$, so there must exist $\left(\begin{smallmatrix} p_1 & x \\ & p_2 \end{smallmatrix}\right) \in P_{m,n}$ and $\left(\begin{smallmatrix} u_1 & y \\ & u_2 \end{smallmatrix}\right) \in Z_{n+m}$, where $u_1 \in Z_n$ and $u_2 \in Z_m$, such that

$$\begin{pmatrix} p_1 & x \\ & p_2 \end{pmatrix} \begin{pmatrix} I_m & \\ A & I_n \end{pmatrix} = \begin{pmatrix} & I_m \\ I_n & \end{pmatrix} \begin{pmatrix} u_1 & y \\ & u_2 \end{pmatrix},$$

i.e.,

$$\begin{pmatrix} p_1 + xA & x \\ p_2 A & p_2 \end{pmatrix} = \begin{pmatrix} & u_2 \\ u_1 & y \end{pmatrix}.$$

Therefore, we have $p_1 + xA = 0$ and $x = (0_{m\times(n-m)}, u_2)$.

In order to proceed, we will separate two cases, the case where $n > m$ and the case where $n = m$.

3D1. *The case $n > m$.* In this case, we write $A = \binom{A_1}{A_2}$, where $A_1 \in M_{(n-m)\times m}(\mathbb{F})$ and $A_2 \in M_{m\times m}(\mathbb{F})$ and $x = (0_{m\times(n-m)}, u_2)$. Then $p_1 + xA = 0$ implies $p_1 + u_2 A_2 = 0$, and therefore A_2 is invertible.

Write

$$\begin{aligned} \begin{pmatrix} I_n & \\ A & I_m \end{pmatrix} &= \begin{pmatrix} I_m & & \\ A_1 & I_{n-m} & \\ A_2 & & I_m \end{pmatrix} \\ &= \begin{pmatrix} I_m & & -A_2^{-1} \\ A_1 & I_{n-m} & \\ A_2 & & \end{pmatrix} \begin{pmatrix} I_m & & A_2^{-1} \\ & I_{n-m} & -A_1 A_2^{-1} \\ & & I_m \end{pmatrix} \\ &= \begin{pmatrix} -A_2^{-1} & I_m & \\ & A_1 & I_{n-m} \\ & A_2 & \end{pmatrix} \hat{w}_{n,m} \begin{pmatrix} I_m & & A_2^{-1} \\ & I_{n-m} & -A_1 A_2^{-1} \\ & & I_m \end{pmatrix}. \end{aligned}$$

Therefore, we have

$$\begin{aligned} &\mathcal{J}_{\sigma,\pi,\psi} \begin{pmatrix} I_m & \\ A & I_n \end{pmatrix} \\ &\qquad = \psi \begin{pmatrix} I_{n-m} & -A_1 A_2^{-1} \\ & I_m \end{pmatrix} \sigma(-A_2^{-1}) \otimes \pi \begin{pmatrix} A_1 & I_{n-m} \\ A_2 & \end{pmatrix} \mathcal{J}_{\sigma,\psi} \otimes \mathcal{J}_{\pi,\psi}. \end{aligned} \tag{3-11}$$

Substituting (3-11) back in (3-10), we get

$$\begin{aligned} &\Gamma(\pi \times \sigma, \psi) \mathcal{J}_{\pi,\psi} \otimes \mathcal{J}_{\sigma,\psi} \\ &= \sum_{\substack{A_1 \in M_{(n-m)\times m}(\mathbb{F}) \\ A_2 \in \mathrm{GL}_m(\mathbb{F})}} \psi \begin{pmatrix} I_{n-m} & -A_1 A_2^{-1} \\ & I_m \end{pmatrix} \pi \begin{pmatrix} A_1 & I_{n-m} \\ A_2 & \end{pmatrix} \otimes \sigma(-A_2^{-1}) \mathcal{J}_{\pi,\psi} \otimes \mathcal{J}_{\sigma,\psi}. \end{aligned} \tag{3-12}$$

We evaluate both sides of (3-12) at (I_n, I_m) to get

$$\Gamma(\pi \times \sigma, \psi) = \sum_{\substack{A_1 \in M_{(n-m)\times m}(\mathbb{F}) \\ A_2 \in \mathrm{GL}_m(\mathbb{F})}} \psi \begin{pmatrix} I_{n-m} & -A_1 A_2^{-1} \\ & I_m \end{pmatrix} \mathcal{J}_{\pi,\psi} \begin{pmatrix} A_1 & I_{n-m} \\ A_2 & \end{pmatrix} \mathcal{J}_{\sigma,\psi}(-A_2^{-1}).$$

Writing

$$\begin{pmatrix} A_1 & I_{n-m} \\ A_2 & \end{pmatrix} = \begin{pmatrix} I_{n-m} & A_1 A_2^{-1} \\ & I_m \end{pmatrix} \begin{pmatrix} & I_{n-m} \\ A_2 & \end{pmatrix},$$

we get

$$\mathcal{J}_{\pi,\psi} \begin{pmatrix} A_1 & I_{n-m} \\ A_2 & \end{pmatrix} = \psi \begin{pmatrix} I_{n-m} & A_1 A_2^{-1} \\ & I_m \end{pmatrix} \mathcal{J}_{\pi,\psi} \begin{pmatrix} & I_{n-m} \\ A_2 & \end{pmatrix},$$

and therefore

$$\Gamma(\pi \times \sigma, \psi) = \sum_{\substack{A_1 \in M_{(n-m)\times m}(\mathbb{F}) \\ A_2 \in \mathrm{GL}_m(\mathbb{F})}} \mathcal{J}_{\pi,\psi} \begin{pmatrix} & I_{n-m} \\ A_2 & \end{pmatrix} \mathcal{J}_{\sigma,\psi}(-A_2^{-1}).$$

The summand is independent of A_1. Using the equivariance properties of the Bessel function, we get that the summand is invariant under Z_m left translations of A_2. Finally, using the properties of the Bessel function discussed in Section 2B1, we get

$$\Gamma(\pi \times \sigma, \psi) = q^{m(2n-m-1)/2} \omega_\sigma(-1) \sum_{x \in Z_m \backslash \mathrm{GL}_m(\mathbb{F})} \mathcal{J}_{\pi,\psi} \begin{pmatrix} & I_{n-m} \\ x & \end{pmatrix} \mathcal{J}_{\sigma^\vee,\psi^{-1}}(x),$$

where $q^{m(2n-m-1)/2} = |M_{(n-m)\times m}(\mathbb{F})| \cdot |Z_m|$.

3D2. *The case $n = m$.* In this case, we have $-p_1 = xA$, and therefore A is invertible. We write

$$\begin{pmatrix} I_n & \\ A & I_n \end{pmatrix} = \begin{pmatrix} I_n & -A^{-1} \\ A & \end{pmatrix} \begin{pmatrix} I_n & A^{-1} \\ & I_n \end{pmatrix} = \begin{pmatrix} -A^{-1} & I_n \\ & A \end{pmatrix} \hat{w}_{n,n} \begin{pmatrix} I_n & A^{-1} \\ & I_n \end{pmatrix}.$$

Therefore, we have

$$\mathcal{J}_{\sigma,\pi,\psi} \begin{pmatrix} I_m & \\ A & I_n \end{pmatrix} = \psi \begin{pmatrix} I_n & A^{-1} \\ & I_n \end{pmatrix} \sigma(-A^{-1}) \otimes \pi(A) \mathcal{J}_{\sigma,\psi} \otimes \mathcal{J}_{\pi,\psi}. \tag{3-13}$$

Substituting (3-13) in (3-10), we get

$$\Gamma(\pi \times \sigma, \psi) \mathcal{J}_{\pi,\psi} \otimes \mathcal{J}_{\sigma,\psi} = \sum_{A \in \mathrm{GL}_n(\mathbb{F})} \psi \begin{pmatrix} I_n & A^{-1} \\ & I_n \end{pmatrix} \pi(A) \otimes \sigma(-A^{-1}) \mathcal{J}_{\pi,\psi} \otimes \mathcal{J}_{\sigma,\psi}. \tag{3-14}$$

Evaluating both sides of (3-14) at (I_n, I_n), we get

$$\Gamma(\pi \times \sigma, \psi) = \sum_{A \in \mathrm{GL}_n(\mathbb{F})} \psi \begin{pmatrix} I_n & A^{-1} \\ & I_n \end{pmatrix} \mathcal{J}_{\pi,\psi}(A) \mathcal{J}_{\sigma,\psi}(-A^{-1}).$$

The summand is invariant under Z_n left translations. Using the properties of the Bessel function discussed in Section 2B1, we get

$$\Gamma(\pi \times \sigma, \psi) = q^{n(n-1)/2}\omega_\sigma(-1) \sum_{x \in Z_n \backslash \mathrm{GL}_n(\mathbb{F})} \psi \begin{pmatrix} I_n & x^{-1} \\ & I_n \end{pmatrix} \mathcal{J}_{\pi,\psi}(x)\mathcal{J}_{\sigma^\vee,\psi^{-1}}(x).$$

3D3. *Summary of cases.* We conclude this section by writing down formulas for the Shahidi gamma factor for a pair of irreducible generic representations, in terms of their Bessel functions for all cases. In order to do that, we use Theorem 3.7 and the formulas from Sections 3D1 and 3D2.

Theorem 3.14. *Let π and σ be irreducible generic representations of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}_m(\mathbb{F})$, respectively*:

(1) *If $n > m$, then*

$$\Gamma(\pi \times \sigma, \psi) = q^{m(2n-m-1)/2}\omega_\sigma(-1) \sum_{x \in Z_m \backslash \mathrm{GL}_m(\mathbb{F})} \mathcal{J}_{\pi,\psi} \begin{pmatrix} & I_{n-m} \\ x & \end{pmatrix} \mathcal{J}_{\sigma^\vee,\psi^{-1}}(x).$$

(2) *If $n = m$, then*

$$\Gamma(\pi \times \sigma, \psi) = q^{n(n-1)/2}\omega_\sigma(-1) \sum_{x \in Z_n \backslash \mathrm{GL}_n(\mathbb{F})} \psi \begin{pmatrix} I_n & x^{-1} \\ & I_n \end{pmatrix} \mathcal{J}_{\pi,\psi}(x)\mathcal{J}_{\sigma^\vee,\psi^{-1}}(x).$$

(3) *If $n < m$, then*

$$\Gamma(\pi \times \sigma, \psi) = q^{n(2m-n-1)/2}\omega_\pi(-1) \sum_{x \in Z_n \backslash \mathrm{GL}_n(\mathbb{F})} \mathcal{J}_{\pi,\psi}(x)\mathcal{J}_{\sigma^\vee,\psi^{-1}} \begin{pmatrix} & I_{m-n} \\ x & \end{pmatrix}.$$

Theorem 3.14 allows us to give a relation between the Jacquet–Piatetski-Shapiro–Shalika gamma factors defined in Section 2C and the Shahidi gamma factor. By Propositions 2.6 and 2.9, we get the following corollary.

Corollary 3.15. *Let π be an irreducible cuspidal representation of $\mathrm{GL}_n(\mathbb{F})$ and let σ be an irreducible generic representation of $\mathrm{GL}_m(\mathbb{F})$. Then we have the equality*

$$\Gamma(\pi \times \sigma, \psi) = q^{m(2n-m-1)/2}\omega_\sigma(-1)\gamma(\pi \times \sigma^\vee, \psi)$$

in either of the following cases:

(1) $n > m$.

(2) $n = m$ *and* σ *is cuspidal.*

4. Applications

4A. ***Quantitative interpretation of gamma factors.*** In this section, we give a representation theoretic interpretation of the absolute value of the Shahidi gamma factor. Our results relate the absolute value of a normalized version of the Shahidi gamma factor with the cuspidal support of the representations.

For irreducible generic representations π and σ of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}_m(\mathbb{F})$, respectively, we define the normalized Shahidi gamma factor by

$$\Gamma^*(\pi \times \sigma, \psi) = q^{-nm/2}\Gamma(\pi \times \sigma, \psi).$$

It follows from Corollary 3.12 that under this normalization, the gamma factor is still multiplicative, i.e., the following proposition holds.

Proposition 4.1. *Let $\pi_1, \ldots, \pi_r$ and $\sigma_1, \ldots, \sigma_t$ be irreducible generic representations of $\mathrm{GL}_{n_1}(\mathbb{F}), \ldots, \mathrm{GL}_{n_r}(\mathbb{F})$ and $\mathrm{GL}_{m_1}(\mathbb{F}), \ldots, \mathrm{GL}_{m_t}(\mathbb{F})$. Suppose that π is the unique irreducible generic subrepresentation of $\pi_1 \circ \ldots \circ \pi_r$ and that σ is the unique irreducible generic subrepresentation of $\sigma_1 \circ \ldots \circ \sigma_t$. Then*

$$\Gamma^*(\pi \times \sigma, \psi) = \prod_{i=1}^{r}\prod_{j=1}^{t} \Gamma^*(\pi_i \times \sigma_j, \psi).$$

By Corollaries 3.15 and 2.7 and Proposition 2.12, we have the following proposition, which allows us to express the size of the absolute value of $\Gamma(\pi \times \sigma, \psi)$ where π and σ are cuspidal.

Proposition 4.2. *Let π and σ be irreducible cuspidal representations of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}_m(\mathbb{F})$, respectively. Then*

$$|\Gamma^*(\pi \times \sigma, \psi)| = \begin{cases} q^{-n/2} & n = m \text{ and } \pi \cong \sigma, \\ 1 & \text{otherwise.} \end{cases}$$

Proposition 4.2 tells us that the size of the normalized Shahidi gamma factor serves as a "Kronecker delta function" for cuspidal representations. It could be thought of an analog of [Jacquet et al. 1983, Section 8.1]. Combining this with the multiplicativity property, we get the following theorem, that allows us to recover the cuspidal support of an irreducible generic representation π by computing $|\Gamma^*(\pi \times \sigma, \psi)|$ for any irreducible cuspidal σ.

Theorem 4.3. *Let π be an irreducible generic representation of $\mathrm{GL}_n(\mathbb{F})$ and let σ be an irreducible cuspidal representation of $\mathrm{GL}_m(\mathbb{F})$. Then*

$$|\Gamma^*(\pi \times \sigma, \psi)| = q^{-d_\pi(\sigma)m/2},$$

where $d_\pi(\sigma)$ is the number of times that σ appears in the cuspidal support of π.

Proof. Suppose that the cuspidal support of π is $\{\pi_1, \ldots, \pi_r\}$. Then π is the unique irreducible generic subrepresentation of $\pi_1 \circ \ldots \circ \pi_r$. The result now follows immediately from Propositions 4.1 and 4.2. □

As a corollary, we get the following converse theorem, which allows us to determine whether generic representations of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}_m(\mathbb{F})$ are isomorphic based on the absolute value of their normalized gamma factors. It is an analog of [Atobe and Gan 2017, Lemma A.6], but our proof is on the "group side" rather than on the "Galois side".

Theorem 4.4. *Let π_1 and π_2 be irreducible generic representations of $\mathrm{GL}_{n_1}(\mathbb{F})$ and $\mathrm{GL}_{n_2}(\mathbb{F})$, respectively. Suppose that for every $m > 0$ and every irreducible cuspidal representation σ of $\mathrm{GL}_m(\mathbb{F})$ we have*

$$|\Gamma^*(\pi_1 \times \sigma, \psi)| = |\Gamma^*(\pi_2 \times \sigma, \psi)|.$$

Then $n_1 = n_2$ and $\pi_1 \cong \pi_2$.

Proof. By Theorem 4.3, π_1 and π_2 have the same cuspidal support. By Theorem 2.2, there exists a unique irreducible generic representation with a given cuspidal support. □

As another corollary, we explain that the functional equations in Theorem 2.5 and Proposition 2.10 fail for π and σ, whenever the cuspidal support of π has a nonempty intersection with the cuspidal support of $\sigma^\vee$.

Corollary 4.5. *Suppose that π and σ are irreducible generic representations of $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{GL}_m(\mathbb{F})$, respectively, and that $n > m$ (respectively, $n = m$). Suppose that the cuspidal support of π has a nonempty intersection with the cuspidal support of $\sigma^\vee$. Then the functional equation in Theorem 2.5 (respectively, Theorem 2.8) does not hold for π and σ.*

Proof. If the functional equation holds for π and σ, then it also holds for $\pi^\vee$ and $\sigma^\vee$. This can be seen by applying complex conjugation to the functional equation, which sends the ψ-Whittaker functions to ψ^{-1}-Whittaker functions of the contragredient. As in Corollary 2.7 (respectively, Corollary 2.11), we get that $|\gamma(\pi \times \sigma, \psi)| = q^{-m(n-m-1)/2}$. Whenever $\gamma(\pi \times \sigma, \psi)$ is defined, it is given by the formula in Proposition 2.6 (respectively, Proposition 2.9), and therefore the formula in Corollary 3.15 holds. This implies that $|\Gamma^*(\pi \times \sigma^\vee, \psi)| = 1$.

On the other hand, because π and $\sigma^\vee$ have common elements in their cuspidal support, we have that $|\Gamma^*(\pi \times \sigma^\vee, \psi)| < 1$. □

Remark 4.6. In his unpublished manuscript [Soudry 1979], the first author showed that whenever the cuspidal support of π does not intersect the cuspidal support of $\sigma^\vee$, the relevant functional equation holds. Due to length considerations, we do not include the proofs here.

4B. ***Consequences for the converse theorem.*** Our results from Section 4A allow us to improve Nien's results regarding the converse theorem for irreducible generic representations of finite general linear groups.

Nien [2014] showed the following theorem.

Theorem 4.7. *Let π_1 and π_2 be two irreducible cuspidal representations of $\mathrm{GL}_n(\mathbb{F})$ with the same central character. Suppose that for every $1 \leq m \leq \frac{n}{2}$, and every irreducible generic representation σ of $\mathrm{GL}_m(\mathbb{F})$ we have*

$$\gamma(\pi_1 \times \sigma, \psi) = \gamma(\pi_2 \times \sigma, \psi). \tag{4-1}$$

Then $\pi_1 \cong \pi_2$.

Using our results and Theorem 4.7, we are able to deduce the following converse theorem, where π_1 and π_2 can be arbitrary generic representations (rather than just cuspidal representations), and (4-1) needs to be verified only for cuspidal representations σ (rather than for all generic representations). This is similar to [Jiang et al. 2015, Section 2.4].

Theorem 4.8. *Let π_1 and π_2 be two irreducible generic representations of $\mathrm{GL}_n(\mathbb{F})$ with the same central character. Suppose that for every $1 \leq m \leq \frac{n}{2}$, and every irreducible cuspidal representation σ of $\mathrm{GL}_m(\mathbb{F})$ we have*

$$\Gamma^*(\pi_1 \times \sigma, \psi) = \Gamma^*(\pi_2 \times \sigma, \psi). \tag{4-2}$$

Then $\pi_1 \cong \pi_2$.

Proof. Our proof is by induction on the cardinality of the cuspidal support of π_1.

We first notice that by Proposition 4.1, we have that for any $1 \leq m \leq \frac{n}{2}$ and any irreducible generic representation σ of $\mathrm{GL}_m(\mathbb{F})$,

$$\Gamma^*(\pi_1 \times \sigma, \psi) = \Gamma^*(\pi_2 \times \sigma, \psi).$$

Suppose that π_1 is cuspidal, then its cuspidal support is of cardinality 1. If π_2 is not cuspidal, then its cuspidal support contains an irreducible cuspidal representation τ of $\mathrm{GL}_k(\mathbb{F})$, where $k \leq \frac{n}{2}$. Since $k < n$, we have by Theorem 4.3 that $|\Gamma^*(\pi_1 \times \sigma, \psi)| = 1$. We also have by Theorem 4.3 that $|\Gamma^*(\pi_2 \times \sigma, \psi)| < 1$, which is a contraction. Therefore, π_2 is also cuspidal, and by Corollary 3.15 and Theorem 4.7, we have that π_1 and π_2 are isomorphic.

Suppose now that π_1 is not cuspidal. Let $\{\tau_1, \ldots, \tau_r\}$ the cuspidal support of π_1 and let $\{\tau_1', \ldots, \tau_{r'}'\}$ be the cuspidal support of π_2. Without loss of generality, we have that τ_1 is an irreducible cuspidal representation of $\mathrm{GL}_{n_1}(\mathbb{F})$, where $n_1 \leq \frac{n}{2}$. Then by Theorem 4.3 we have that $|\Gamma^*(\pi_1 \times \tau_1, \psi)| < 1$. Since $n_1 \leq \frac{n}{2}$, we have that $\Gamma^*(\pi_1 \times \tau_1, \psi) = \Gamma^*(\pi_2 \times \tau_1, \psi)$, and therefore $|\Gamma^*(\pi_2 \times \tau_1, \psi)| < 1$. By Theorem 4.3, this implies that τ_1 is in the cuspidal support of π_2. Without loss of

generality, we may assume that $\tau_1' = \tau_1$. By Proposition 4.1, we deduce that for any irreducible generic representation σ of $\mathrm{GL}_m(\mathbb{F})$ where $m \leq \frac{n}{2}$,

$$\prod_{j=2}^{r} \Gamma^*(\tau_j \times \sigma, \psi) = \prod_{j=2}^{r'} \Gamma^*(\tau_j' \times \sigma, \psi). \tag{4-3}$$

Let π_1' be the unique irreducible generic representation of $\mathrm{GL}_{n-n_1}(\mathbb{F})$ with cuspidal support $\{\tau_2, \dots, \tau_r\}$, and let π_2' be the unique irreducible generic representation of $\mathrm{GL}_{n-n_1}(\mathbb{F})$ with cuspidal support $\{\tau_2', \dots, \tau_{r'}'\}$. For $i = 1, 2$, the central characters of π_i and π_i' are related by $\omega_{\pi_i} = \omega_{\pi_i'} \cdot \omega_{\tau_1}$. Therefore, we have that π_1' and π_2' also have the same central character. By Proposition 4.1, we have that (4-3) implies that for every $m \leq \frac{n}{2}$ and every irreducible generic representation σ of $\mathrm{GL}_m(\mathbb{F})$,

$$\Gamma^*(\pi_1' \times \sigma, \psi) = \Gamma^*(\pi_2' \times \sigma, \psi).$$

By induction $\pi_1' \cong \pi_2'$, and therefore $\{\tau_2, \dots, \tau_r\} = \{\tau_2', \dots, \tau_{r'}'\}$. Hence, $\pi_1 \cong \pi_2$, as required. □

4C. ***Special values of the Bessel function.*** In this section, we use our results regarding multiplicativity of the Shahidi gamma factor, and its relation to the Jacquet–Piatetski-Shapiro–Shalika gamma factor in order to find an explicit formula for special values of the Bessel function of irreducible generic representations of $\mathrm{GL}_n(\mathbb{F})$. For two blocks, such a formula was given by Curtis and Shinoda [2004, Lemma 3.5]. However, their proof uses Deligne–Lusztig theory, while our proof only uses Green's character values for irreducible cuspidal representation of $\mathrm{GL}_n(\mathbb{F})$; see [Gel'fand 1970, Section 6] and [Nien 2017, Section 3.1]. We also provide a formula for a simple value consisting of three blocks. This generalizes a formula of Chang [1976] for irreducible generic representations of $\mathrm{GL}_3(\mathbb{F})$.

4C1. *Special value formula for two blocks.* Fix an algebraic closure $\bar{\mathbb{F}}$ of $\mathbb{F}$. For every positive integer n, let $\mathbb{F}_n$ be the unique extension of degree n in $\bar{\mathbb{F}}$. Let $\mathrm{N}_{\mathbb{F}_n/\mathbb{F}} : \mathbb{F}_n^* \to \mathbb{F}^*$ and $\mathrm{Tr}_{\mathbb{F}_n/\mathbb{F}} : \mathbb{F}_n \to \mathbb{F}$ be the norm and the trace maps, respectively. Let $\widehat{\mathbb{F}_n^*}$ be the character group consisting of all multiplicative characters $\alpha : \mathbb{F}_n^* \to \mathbb{C}^*$.

It is known that irreducible cuspidal representations of $\mathrm{GL}_n(\mathbb{F})$ are in a bijection with Frobenius orbits of size n of $\widehat{\mathbb{F}_n^*}$, that is, every irreducible cuspidal representation π of $\mathrm{GL}_n(\mathbb{F})$ corresponds to a set of size n of the form $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$, where $\alpha \in \widehat{\mathbb{F}_n^*}$.

We first recall Nien's result regarding the computation of the Jacquet–Piatetski-Shapiro–Shalika gamma factor $\gamma(\pi \times \chi, \psi)$ where π is an irreducible cuspidal representation of $\mathrm{GL}_n(\mathbb{F})$ and χ is a representation of $\mathrm{GL}_1(\mathbb{F})$, that is, $\chi : \mathbb{F}^* \to \mathbb{C}^*$ is a multiplicative character. Nien's result expresses $\gamma(\pi \times \chi, \psi)$ as a Gauss sum.

Proposition 4.9 [Nien 2014, Theorem 1.1]. *Let π be an irreducible cuspidal representation of $\mathrm{GL}_n(\mathbb{F})$ associated with the Frobenius orbit $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$, where $\alpha \in \widehat{\mathbb{F}^*_n}$. Let $\chi : \mathbb{F}^* \to \mathbb{C}^*$ be a multiplicative character. Then*

$$\gamma(\pi \times \chi, \psi) = (-1)^{n+1}\chi(-1)^{n+1}q^{-n+1}\sum_{\xi\in\mathbb{F}^*_n}\alpha^{-1}(\xi)\chi^{-1}(\mathrm{N}_{\mathbb{F}_n/\mathbb{F}}(\xi))\psi(\mathrm{Tr}_{\mathbb{F}_n/\mathbb{F}}(\xi)).$$

Nien's proof only uses Green's character formula for irreducible cuspidal representations, and does not use Deligne–Lusztig theory.

We are ready to state our result regarding special two blocks values of the Bessel function.

Theorem 4.10. *Let $n > 1$, and let π be an irreducible generic representation of $\mathrm{GL}_n(\mathbb{F})$ with cuspidal support $\{\pi_1, \dots, \pi_r\}$, where for every $1 \le j \le r$, π_j is an irreducible cuspidal representation of $\mathrm{GL}_{n_j}(\mathbb{F})$ corresponding to the Frobenius orbit $\{\alpha_j, \alpha_j^q, \dots, \alpha_j^{q^{n_j-1}}\}$, where $\alpha_j \in \widehat{\mathbb{F}^*_{n_j}}$ is a multiplicative character. Then for any $c \in \mathbb{F}^*$,*

$$\mathcal{J}_{\pi,\psi}\begin{pmatrix} & I_{n-1}\\ c & \end{pmatrix} = (-1)^{n+r}q^{-n+1}\sum_{\substack{\xi_1\in\mathbb{F}^*_{n_1},\dots,\xi_r\in\mathbb{F}^*_{n_r}\\ \prod_{j=1}^r \mathrm{N}_{\mathbb{F}_{n_j}/\mathbb{F}}(\xi_j)=(-1)^{n-1}c^{-1}}}\prod_{j=1}^{r}\big(\alpha_j^{-1}(\xi_j)\psi(\mathrm{Tr}_{\mathbb{F}_{n_j}/\mathbb{F}}(\xi_j))\big).$$

Proof. By Theorem 3.14, we have that

$$\Gamma(\pi \times \chi, \psi) = q^{n-1}\sum_{x\in\mathbb{F}^*}\mathcal{J}_{\pi,\psi}\begin{pmatrix} & I_{n-1}\\ x & \end{pmatrix}\chi^{-1}(-x).$$

Multiplying by $\chi(-c)$ and averaging over all $\chi \in \widehat{\mathbb{F}^*}$, and using the fact that a sum of a nontrivial character on a group is zero, we get

$$\frac{1}{|\mathbb{F}^*|}\sum_{\chi\in\widehat{\mathbb{F}^*}}\Gamma(\pi \times \chi, \psi)\chi(-c) = q^{n-1}\mathcal{J}_{\pi,\psi}\begin{pmatrix} & I_{n-1}\\ c & \end{pmatrix}. \tag{4-4}$$

By Corollary 3.12, we have that

$$\Gamma(\pi \times \chi, \psi) = \prod_{j=1}^{r}\Gamma(\pi_j \times \chi, \psi).$$

By Corollary 3.15 and Proposition 4.9, we have that

$$\Gamma(\pi_j \times \chi, \psi) = (-1)^{n_j+1}\chi(-1)^{n_j}\sum_{\xi\in\mathbb{F}^*_{n_j}}\alpha_j^{-1}(\xi)\chi(\mathrm{N}_{\mathbb{F}_{n_j}/\mathbb{F}}(\xi))\psi(\mathrm{Tr}_{\mathbb{F}_{n_j}/\mathbb{F}}(\xi)).$$

Therefore, we get that $\Gamma(\pi\times\chi,\psi)$ is given by

$$(-1)^{n+r}\sum_{\xi_1\in\mathbb{F}_{n_1}^*,\dots,\xi_r\in\mathbb{F}_{n_r}^*}\left(\prod_{j=1}^{r}\alpha_j^{-1}(\xi_j)\psi(\mathrm{Tr}_{\mathbb{F}_{n_j}/\mathbb{F}}(\xi_j))\right)\chi\left((-1)^n\prod_{j=1}^{r}\mathrm{N}_{\mathbb{F}_{n_j}/\mathbb{F}}(\xi_j)\right). \tag{4-5}$$

Substituting the expression (4-5) for $\Gamma(\pi\times\chi,\psi)$ in (4-4), and using the fact that a sum of a nontrivial of character over a group is zero, we get the desired result. □

Remark 4.11. The expression for $\Gamma(\pi\times\chi,\psi)$ in (4-5) is originally due to Kondo [1963]. He computed it for the Godement–Jacquet gamma factor. One can show directly that the Godement–Jacquet gamma factor coincides with the Shahidi gamma factor for representations for which both factors are defined. Our proof, which is based on Nien's result and on multiplicativity of gamma factors, is different than the one given by Kondo. See also another proof in [Macdonald 1998, Chapter IV, Section 6, Example 4].

Remark 4.12. In [Zelingher 2023], a vast generalization of the method in the proof of Theorem 4.10 is used in order to find formulas for

$$\mathcal{J}_{\pi,\psi}\begin{pmatrix} & I_{n-m}\\ cI_m & \end{pmatrix}.$$

However, [Zelingher 2023] relies on the results of [Ye and Zelingher 2021], which in turn rely on the local Langlands correspondence. The proof given here does not rely on such results.

4C2. *Special value formula for three blocks.* In this subsection, we use our results to prove a formula for special values of the Bessel function, for a simple value consisting of three blocks. This generalizes a formula given by Chang [1976] for $\mathrm{GL}_3(\mathbb{F})$, generalized later by Shinoda and Tulunay [2005] to $\mathrm{GL}_4(\mathbb{F})$. Our proof is different from Chang's proof, which is based on the Gelfand–Graev algebra.

We start with the following proposition.

Proposition 4.13. *Let π be an irreducible generic representation of $\mathrm{GL}_n(\mathbb{F})$. Then for any $c\in\mathbb{F}^*$, and any $g\in\mathrm{GL}_n(\mathbb{F})$, we have*

$$\mathcal{J}_{\pi,\psi}(g)\mathcal{J}_{\pi,\psi}\begin{pmatrix} & I_{n-1}\\ c & \end{pmatrix}$$
$$=q^{-(n-1)}\sum_{{}^tx=(x_1,\dots,x_{n-1})\in\mathbb{F}^{n-1}}\psi(-x_{n-1})\mathcal{J}_{\pi,\psi}\left(g\begin{pmatrix} I_{n-1} & x\\ & 1\end{pmatrix}\begin{pmatrix} & I_{n-1}\\ c & \end{pmatrix}\right).$$

Proof. Let $m = 1$ and let $\sigma = \chi : \mathbb{F}^* \to \mathbb{C}^*$ be a multiplicative character. By (3-12), we have

$$\Gamma(\pi \times \chi, \psi)\mathcal{J}_{\pi,\psi} = \sum_{\substack{{}^t x \in \mathbb{F}^{n-1} \\ a \in \mathbb{F}^*}} \chi(-a^{-1})\psi\begin{pmatrix} I_{n-1} & -a^{-1}x \\ & 1 \end{pmatrix} \pi \begin{pmatrix} x & I_{n-1} \\ a & \end{pmatrix} \mathcal{J}_{\pi,\psi}.$$

We multiply by $\chi(-c)$ and average over $\chi \in \widehat{\mathbb{F}^*}$. Using the fact that a sum of a nontrivial character over a group is zero, and using (4-4), we get

$$q^{n-1}\mathcal{J}_{\pi,\psi}\begin{pmatrix} & I_{n-1} \\ c & \end{pmatrix}\mathcal{J}_{\pi,\psi} = \sum_{{}^t x = (x_1,\dots,x_{n-1}) \in \mathbb{F}^{n-1}} \psi(-c^{-1}x_{n-1})\pi\begin{pmatrix} x & I_{n-1} \\ c & \end{pmatrix}\mathcal{J}_{\pi,\psi}.$$

Using the decomposition

$$\begin{pmatrix} x & I_{n-1} \\ c & \end{pmatrix} = \begin{pmatrix} I_{n-1} & c^{-1}x \\ & 1 \end{pmatrix}\begin{pmatrix} & I_{n-1} \\ c & \end{pmatrix},$$

and changing the summation variable x to $c \cdot x$, we get the desired result. □

Theorem 4.14. *Suppose $n \geq 3$. Then for any irreducible generic representation π of $\mathrm{GL}_n(\mathbb{F})$ and any $c, c' \in \mathbb{F}^*$, we have*

$$\mathcal{J}_{\pi,\psi}\begin{pmatrix} & & -c' \\ & I_{n-2} & \\ c & & \end{pmatrix} = \sum_{s \in \mathbb{F}^*} \mathcal{J}_{\pi,\psi}\begin{pmatrix} & I_{n-1} \\ s^{-1}c & \end{pmatrix}\mathcal{J}_{\pi,\psi}\begin{pmatrix} & sc' \\ I_{n-1} & \end{pmatrix}(\psi(s) - 1) + \frac{\delta_{cc',1}}{q^{n-2}},$$

where

$$\delta_{cc',1} = \begin{cases} 1 & cc' = 1, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. We substitute $g = \left(\begin{smallmatrix} & c' \\ I_{n-1} & \end{smallmatrix}\right)$ in Proposition 4.13 to get

$$\mathcal{J}_{\pi,\psi}\begin{pmatrix} & I_{n-1} \\ c & \end{pmatrix}\mathcal{J}_{\pi,\psi}\begin{pmatrix} & c' \\ I_{n-1} & \end{pmatrix} = q^{-(n-1)} \sum_{{}^t x = (x_1,\dots,x_{n-1}) \in \mathbb{F}^{n-1}} \psi(-x_{n-1})\mathcal{J}_{\pi,\psi}\begin{pmatrix} cc' & \\ cx & I_{n-1} \end{pmatrix}.$$

If $x_{n-1} = 0$, then $\left(\begin{smallmatrix} cc' & \\ cx & I_{n-1} \end{smallmatrix}\right)$ lies in the mirabolic subgroup. By [Nien 2014, Lemma 2.14], we have that the Bessel function is zero for elements in the mirabolic subgroup that do not lie in the upper unipotent subgroup Z_n. Therefore, we get that

if $x_{n-1}=0$, then $x=0$ and

$$\psi(x_{n-1})\mathcal{J}_{\pi,\psi}\begin{pmatrix} cc' & \\ cx & I_{n-1}\end{pmatrix}=\delta_{cc',1}.$$

Suppose now that $x_{n-1}=t\neq 0$. Denote

$${}^t x'=(x_1,\ldots,x_{n-2})\in\mathbb{F}^{n-2}.$$

Then we have

$$\begin{pmatrix} cc' & \\ cx & I_{n-1}\end{pmatrix}=\begin{pmatrix} 1 & 0 & t^{-1}c' \\ & I_{n-2} & t^{-1}x' \\ & & 1\end{pmatrix}\begin{pmatrix} & & -t^{-1}c' \\ & I_{n-2} & \\ tc & & \end{pmatrix}\begin{pmatrix} 1 & 0 & (tc)^{-1} \\ & I_{n-2} & -t^{-1}x' \\ & & 1\end{pmatrix}.$$

Since we have q^{n-2} elements in $\mathbb{F}^{n-1}$ with $x_{n-1}=t$, we get that

$$\mathcal{J}_{\pi,\psi}\begin{pmatrix} & I_{n-1} \\ c & \end{pmatrix}\mathcal{J}_{\pi,\psi}\begin{pmatrix} & c' \\ I_{n-1} & \end{pmatrix}=\frac{\delta_{cc',1}}{q^{n-1}}+q^{-1}\sum_{t\in\mathbb{F}^*}\psi(-t)\mathcal{J}_{\pi,\psi}\begin{pmatrix} & & -t^{-1}c' \\ & I_{n-2} & \\ tc & & \end{pmatrix}.$$

We proceed as in [Chang 1976, Page 379; Shinoda and Tulunay 2005, Lemma 4.2]. We replace c with $s^{-1}c$ and c' with sc', where $s\in\mathbb{F}^*$, to get

$$\begin{aligned}\mathcal{J}_{\pi,\psi}\begin{pmatrix} & I_{n-1} \\ s^{-1}c & \end{pmatrix}\mathcal{J}_{\pi,\psi}\begin{pmatrix} & sc' \\ I_{n-1} & \end{pmatrix}&\\ =\frac{\delta_{cc',1}}{q^{n-1}}+q^{-1}\sum_{t\in\mathbb{F}^*}\psi(-st)\mathcal{J}_{\pi,\psi}\begin{pmatrix} & & -t^{-1}c' \\ & I_{n-2} & \\ tc & & \end{pmatrix}.&\quad(4\text{-}6)\end{aligned}$$

Summing (4-6) over $s\in\mathbb{F}^*$, we get

$$\begin{aligned}\sum_{s\in\mathbb{F}^*}\mathcal{J}_{\pi,\psi}\begin{pmatrix} & I_{n-1} \\ s^{-1}c & \end{pmatrix}\mathcal{J}_{\pi,\psi}\begin{pmatrix} & sc' \\ I_{n-1} & \end{pmatrix}&\\ =\frac{q-1}{q^{n-1}}\delta_{cc',1}-q^{-1}\sum_{t\in\mathbb{F}^*}\mathcal{J}_{\pi,\psi}\begin{pmatrix} & & -t^{-1}c' \\ & I_{n-2} & \\ tc & & \end{pmatrix}.&\quad(4\text{-}7)\end{aligned}$$

Multiplying (4-6) by $\psi(s)$ and summing over $s \in \mathbb{F}^*$, we get

$$\sum_{s\in\mathbb{F}^*} \mathcal{J}_{\pi,\psi}\begin{pmatrix} & I_{n-1}\\ s^{-1}c & \end{pmatrix}\mathcal{J}_{\pi,\psi}\begin{pmatrix} & sc'\\ I_{n-1} & \end{pmatrix}\psi(s)$$
$$= -\frac{\delta_{cc',1}}{q^{n-1}} + \frac{q-1}{q}\mathcal{J}_{\pi,\psi}\begin{pmatrix} & -c'\\ c & \end{pmatrix}$$
$$- q^{-1}\sum_{1\neq t\in\mathbb{F}^*} \mathcal{J}_{\pi,\psi}\begin{pmatrix} & -t^{-1}c'\\ tc & \end{pmatrix}. \quad (4\text{-}8)$$

Subtracting (4-7) from (4-8), we get the desired result. □

Remark 4.15. Using the formulas in Theorem 4.10 and its proof, one can show that if the cuspidal support of π does not contain any irreducible representation of $\mathrm{GL}_1(\mathbb{F})$, then we have a simpler formula:

$$\mathcal{J}_{\pi,\psi}\begin{pmatrix} & -c'\\ c & \end{pmatrix} = \sum_{s\in\mathbb{F}^*} \mathcal{J}_{\pi,\psi}\begin{pmatrix} & I_{n-1}\\ s^{-1}c & \end{pmatrix}\mathcal{J}_{\pi,\psi}\begin{pmatrix} & sc'\\ I_{n-1} & \end{pmatrix}\psi(s). \quad (4\text{-}9)$$

However, if the cuspidal support of π contains irreducible representations of $\mathrm{GL}_1(\mathbb{F})$, this simpler formula does not hold.

Remark 4.16. Using the expression in Theorem 4.10, we have that the expression on the right hand side of (4-9) is an exponential sum that generalizes the Friedlander–Iwaniec character sum; see [Kowalski 2015, Theorem 7.3, formula (27) and Remark 7.4]. The Friedlander–Iwaniec character sum played a role in Zhang's work on the twin prime conjecture [2014].

Appendix: Computation of $\gamma(\pi \times \pi^\vee, \psi)$ when π is cuspidal

In this appendix, we compute the Jacquet–Piatetski-Shapiro–Shalika gamma factor $\gamma(\pi \times \sigma, \psi)$ in the special case where π and σ are irreducible cuspidal representations of $\mathrm{GL}_n(\mathbb{F})$ and $\pi \cong \sigma^\vee$. We will prove the following theorem.

Theorem A.1. *Let π be an irreducible cuspidal representation of $\mathrm{GL}_n(\mathbb{F})$. Then*

$$\gamma(\pi \times \pi^\vee, \psi) = -1.$$

This was done in [Ye 2019, Corollary 4.3]. We provide another proof, since the proof in [loc. cit.] relies on results of representations of p-adic groups.

For future purposes, we will prove the following general lemma. We will show that Theorem A.1 follows from it.

We denote by $P_n \leq \mathrm{GL}_n(\mathbb{F})$ the mirabolic subgroup.

Lemma A.2. *Let G be a finite group and let $H \leq G$ be a subgroup. Suppose that H is a semidirect product of the form $H = N \rtimes \mathrm{GL}_n(\mathbb{F})$. Let $\Psi : H \to \mathbb{C}^*$ be a character which is trivial on $\mathrm{GL}_n(\mathbb{F})$. Let τ be an irreducible representation of G, such that*:

(1) $\dim \mathrm{Hom}_H(\mathrm{Res}_H \tau, \Psi) = 1$.

(2) $\dim \mathrm{Hom}_{N \rtimes P_n}(\mathrm{Res}_{N \rtimes P_n} \tau, \mathrm{Res}_{N \rtimes P_n} \Psi) = 1$.

(3) *There exists a functional $\ell \in \mathrm{Hom}_{Z_n}(\mathrm{Res}_{Z_n} \tau, \mathbb{C})$ and a vector $v_0 \in \tau$, such that*

$$\sum_{p \in Z_n \backslash P_n} \sum_{n \in N} \ell(\tau(np)v_0)\Psi^{-1}(n) = 1.$$

Then

$$\sum_{g \in Z_n \backslash \mathrm{GL}_n(\mathbb{F})} \sum_{n \in N} \ell(\tau(ng)v_0)\Psi^{-1}(n)\psi(\langle e_n g, e_1 \rangle) = -1.$$

Remark A.3. If $\mathbb{F}^* \leq H$ lies in the center of G, then (1) implies that the restriction of the central character of τ to $\mathbb{F}^* \leq H$ is trivial.

Proof. Notice that we have a containment

$$\mathrm{Hom}_H(\mathrm{Res}_H \tau, \Psi) \subset \mathrm{Hom}_{N \rtimes P_n}(\mathrm{Res}_{N \rtimes P_n} \tau, \mathrm{Res}_{N \rtimes P_n} \Psi).$$

Since both spaces are one dimensional, we have that they are equal. Denote for $v \in \tau$,

$$L(v) = \sum_{p \in Z_n \backslash P_n} \sum_{n \in N} \ell(\tau(np)v)\Psi^{-1}(n).$$

Then $L \in \mathrm{Hom}_{N \rtimes P_n}(\mathrm{Res}_{N \rtimes P_n} \tau, \mathrm{Res}_{N \rtimes P_n} \Psi)$ and $L \neq 0$ because $L(v_0) = 1$. Therefore, $L \in \mathrm{Hom}_H(\mathrm{Res}_H \tau, \Psi)$, which implies that $L(\tau(g)v) = L(v)$ for any $v \in \tau$, and any $g \in \mathrm{GL}_n(\mathbb{F})$.

Denote

$$S = \sum_{g \in Z_n \backslash \mathrm{GL}_n(\mathbb{F})} \sum_{n \in N} \ell(\tau(ng)v_0)\Psi^{-1}(n)\psi(\langle e_n g, e_1 \rangle).$$

We have

$$S = \sum_{g \in P_n \backslash \mathrm{GL}_n(\mathbb{F})} L(\tau(g)v_0)\psi(\langle e_n g, e_1 \rangle) = \sum_{g \in P_n \backslash \mathrm{GL}_n(\mathbb{F})} \psi(\langle e_n g, e_1 \rangle).$$

We decompose this sum through the center of $\mathrm{GL}_n(\mathbb{F})$

$$S = \sum_{g \in (\mathbb{F}^* \cdot P_n) \backslash \mathrm{GL}_n(\mathbb{F})} \sum_{a \in \mathbb{F}^*} \psi(\langle e_n a g, e_1 \rangle).$$

We have that for $t \in \mathbb{F}$,

$$\sum_{a \in \mathbb{F}^*} \psi(at) = \begin{cases} -1 & t \neq 0, \\ q-1 & t = 0. \end{cases}$$

Therefore, we get

$$S = (q-1) \sum_{\substack{g \in (\mathbb{F}^* \cdot P_n) \backslash \mathrm{GL}_n(\mathbb{F}) \\ \langle e_n g, e_1 \rangle = 0}} 1 - \sum_{\substack{g \in (\mathbb{F}^* \cdot P_n) \backslash \mathrm{GL}_n(\mathbb{F}) \\ \langle e_n g, e_1 \rangle \neq 0}} 1,$$

which we rewrite as

$$S = \sum_{\substack{g \in P_n \backslash \mathrm{GL}_n(\mathbb{F}) \\ \langle e_n g, e_1 \rangle = 0}} 1 - \frac{1}{|\mathbb{F}^*|} \sum_{\substack{g \in P_n \backslash \mathrm{GL}_n(\mathbb{F}) \\ \langle e_n g, e_1 \rangle \neq 0}} 1.$$

Consider the right action of $\mathrm{GL}_n(\mathbb{F})$ on $\mathbb{F}^n \setminus \{0\}$. This action is transitive. The stabilizer of e_n is the mirabolic subgroup P_n. Therefore, for $x = (x_1, \ldots, x_n) \in \mathbb{F}^n \setminus \{0\}$, we have that

$$S_x = \sum_{\substack{g \in P_n \backslash \mathrm{GL}_n(\mathbb{F}) \\ e_n g = x}} 1 = 1.$$

This implies that

$$S = \sum_{\substack{x \in \mathbb{F}^n \setminus \{0\} \\ x_1 = 0}} S_x - \frac{1}{|\mathbb{F}^*|} \sum_{\substack{x \in \mathbb{F}^n \setminus \{0\} \\ x_1 \neq 0}} S_x = (q^{n-1} - 1) - q^{n-1} = -1,$$

as required. □

We move to prove Theorem A.1.

Proof. We will use Lemma A.2 in the following setup. Let $G = \mathrm{GL}_n(\mathbb{F}) \times \mathrm{GL}_n(\mathbb{F})$, and let $H = \mathrm{GL}_n(\mathbb{F})$ embedded diagonally. Let $N = \{I_n\}$ and $\Psi = 1$.

Let π be an irreducible cuspidal representation of $\mathrm{GL}_n(\mathbb{F})$, then by Schur's lemma, the space

$$\mathrm{Hom}_{\mathrm{GL}_n(\mathbb{F})}(\pi \otimes \pi^\vee, \mathbb{C})$$

is one-dimensional. Since π is cuspidal, By [Gel'fand 1970, Theorem 2.2], the restriction of π to the mirabolic subgroup P_n is irreducible. Therefore, by Schur's lemma the space

$$\mathrm{Hom}_{P_n}(\mathrm{Res}_{P_n} \pi \otimes \mathrm{Res}_{P_n} \pi^\vee, \mathbb{C})$$

is also one-dimensional.

We take $\tau = \mathcal{W}(\pi, \psi) \otimes \mathcal{W}(\pi^\vee, \psi^{-1})$, and $\ell \colon \mathcal{W}(\pi, \psi) \otimes \mathcal{W}(\pi^\vee, \psi^{-1}) \to \mathbb{C}$ to be the functional defined on pure tensors by

$$\ell(W \otimes W') = W(I_n) \cdot W'(I_n).$$

We have that $\ell \in \mathrm{Hom}_{Z_n}(\mathrm{Res}_{Z_n} \tau, 1)$. Let $v_0 = \mathcal{J}_{\pi,\psi} \otimes \mathcal{J}_{\pi^\vee,\psi^{-1}}$.

Consider

$$\sum_{p \in Z_n \backslash P_n} \sum_{n \in N} \ell(\tau(np)v_0)\Psi^{-1}(n) = \sum_{p \in Z_n \backslash P_n} \mathcal{J}_{\pi,\psi}(p)\mathcal{J}_{\pi^\vee,\psi^{-1}}(p).$$

By [Nien 2014, Lemma 2.14], we have that if $\mathcal{J}_{\pi,\psi}(p) \neq 0$ for $p \in P_n$, then $p \in Z_n$. Therefore,

$$\sum_{p \in Z_n \backslash P_n} \mathcal{J}_{\pi,\psi}(p)\mathcal{J}_{\pi^\vee,\psi^{-1}}(p) = \sum_{p \in Z_n \backslash Z_n} \mathcal{J}_{\pi,\psi}(p)\mathcal{J}_{\pi^\vee,\psi^{-1}}(p) = 1.$$

Thus, we showed that the required properties for Lemma A.2 are satisfied.

Using Proposition 2.9, we have

$$\gamma(\pi \times \pi^\vee, \psi) = \sum_{g \in Z_n \backslash \mathrm{GL}_n(\mathbb{F})} \mathcal{J}_{\pi,\psi}(g)\mathcal{J}_{\pi^\vee,\psi^{-1}}(g)\psi(\langle e_n g^{-1}, e_1 \rangle).$$

Replacing g with g^{-1} and using Proposition 2.3, we have

$$\gamma(\pi \times \pi^\vee, \psi) = \sum_{g \in Z_n \backslash \mathrm{GL}_n(\mathbb{F})} \mathcal{J}_{\pi,\psi}(g)\mathcal{J}_{\pi^\vee,\psi^{-1}}(g)\psi(\langle e_n g, e_1 \rangle),$$

and therefore by Lemma A.2

$$\gamma(\pi \times \pi^\vee, \psi) = \sum_{g \in Z_n \backslash \mathrm{GL}_n(\mathbb{F})} \sum_{n \in N} \ell(\tau(ng)v)\Psi^{-1}(n)\psi(\langle e_n g, e_1 \rangle) = -1,$$

as required. □

References

[Atobe and Gan 2017] H. Atobe and W. T. Gan, "Local theta correspondence of tempered representations and Langlands parameters", *Invent. Math.* **210**:2 (2017), 341–415. MR Zbl

[Chai 2019] J. Chai, "Bessel functions and local converse conjecture of Jacquet", *J. Eur. Math. Soc.* (*JEMS*) **21**:6 (2019), 1703–1728. MR Zbl

[Chang 1976] B. Chang, "Decomposition of Gelfand–Graev characters of $\mathrm{GL}_3(q)$", *Comm. Algebra* **4**:4 (1976), 375–401. MR Zbl

[Curtis and Shinoda 2004] C. W. Curtis and K.-i. Shinoda, "Zeta functions and functional equations associated with the components of the Gelfand–Graev representations of a finite reductive group", pp. 121–139 in *Representation theory of algebraic groups and quantum groups*, edited by T. Shoji et al., Adv. Stud. Pure Math. **40**, Math. Soc. Japan, Tokyo, 2004. MR Zbl

[Gan and Ichino 2016] W. T. Gan and A. Ichino, "The Gross–Prasad conjecture and local theta correspondence", *Invent. Math.* **206**:3 (2016), 705–799. MR Zbl

[Gan and Savin 2012] W. T. Gan and G. Savin, "Representations of metaplectic groups I: epsilon dichotomy and local Langlands correspondence", *Compos. Math.* **148**:6 (2012), 1655–1694. MR Zbl

[Gel'fand 1970] S. I. Gel'fand, "Representations of the full linear group over a finite field", *Mat. Sb. (N.S.)* **83(125)** (1970), 15–41. MR

[Jacquet et al. 1983] H. Jacquet, I. I. Piatetskii-Shapiro, and J. A. Shalika, "Rankin–Selberg convolutions", *Amer. J. Math.* **105**:2 (1983), 367–464. MR Zbl

[Jiang et al. 2015] D. Jiang, C. Nien, and S. Stevens, "Towards the Jacquet conjecture on the local converse problem for p-adic GL_n", *J. Eur. Math. Soc. (JEMS)* **17**:4 (2015), 991–1007. MR Zbl

[Katz 1993] N. M. Katz, "Estimates for Soto–Andrade sums", *J. Reine Angew. Math.* **438** (1993), 143–161. MR Zbl

[Kondo 1963] T. Kondo, "On Gaussian sums attached to the general linear groups over finite fields", *J. Math. Soc. Japan* **15** (1963), 244–255. MR Zbl

[Kowalski 2015] E. Kowalski, "Gaps between prime numbers and primes in arithmetic progressions [after Y. Zhang and J. Maynard]", pp. 327–366 in *Journées de Géométrie Algébrique d'Orsay*, Astérisque **367-368**, Société Mathématique de France, Paris, 2015. MR Zbl

[Liu and Zhang 2022a] B. Liu and Q. Zhang, "Gamma factors and converse theorems for classical groups over finite fields", *J. Number Theory* **234** (2022), 285–332. MR Zbl

[Liu and Zhang 2022b] B. Liu and Q. Zhang, "On a converse theorem for G_2 over finite fields", *Math. Ann.* **383**:3-4 (2022), 1217–1283. MR Zbl

[Macdonald 1998] I. G. Macdonald, *Symmetric functions and orthogonal polynomials*, University Lecture Series **12**, American Mathematical Society, Providence, RI, 1998. MR Zbl

[Nien 2014] C. Nien, "A proof of the finite field analogue of Jacquet's conjecture", *Amer. J. Math.* **136**:3 (2014), 653–674. MR Zbl

[Nien 2017] C. Nien, "$n \times 1$ local gamma factors and Gauss sums", *Finite Fields Appl.* **46** (2017), 255–270. MR Zbl

[Piatetski-Shapiro 1983] I. Piatetski-Shapiro, *Complex representations of* $\mathrm{GL}(2, K)$ *for finite fields* K, Contemporary Mathematics **16**, American Mathematical Society, Providence, RI, 1983. MR Zbl

[Roditty-Gershon 2010] E.-A. Roditty-Gershon, *On gamma factors and bessel functions for representations of general linear groups over finite fields*, master's thesis, Tel Aviv University, 2010.

[Shahidi 1984] F. Shahidi, "Fourier transforms of intertwining operators and Plancherel measures for $\mathrm{GL}(n)$", *Amer. J. Math.* **106**:1 (1984), 67–111. MR Zbl

[Shahidi 1990] F. Shahidi, "A proof of Langlands' conjecture on Plancherel measures; complementary series for p-adic groups", *Ann. of Math.* (2) **132**:2 (1990), 273–330. MR Zbl

[Shinoda and Tulunay 2005] K. Shinoda and I. Tulunay, "Representations of the Hecke algebra for $\mathrm{GL}_4(q)$", *J. Algebra Appl.* **4**:6 (2005), 631–644. MR Zbl

[Silberger and Zink 2000] A. J. Silberger and E.-W. Zink, "The characters of the generalized Steinberg representations of finite general linear groups on the regular elliptic set", *Trans. Amer. Math. Soc.* **352**:7 (2000), 3339–3356. MR Zbl

[Soudry 1979] D. Soudry, "On gamma functions of pairs over finite fields", unpublished note, 1979.

[Ye 2019] R. Ye, "Rankin–Selberg gamma factors of level zero representations of GL_n", *Forum Math.* **31**:2 (2019), 503–516. MR Zbl

[Ye and Zelingher 2020] R. Ye and E. Zelingher, "Exterior square gamma factors for cuspidal representations of GL_n: finite field analogs and level-zero representations", *Israel J. Math.* **240**:2 (2020), 889–934. MR Zbl

[Ye and Zelingher 2021] R. Ye and E. Zelingher, "Epsilon factors of representations of finite general linear groups", *J. Number Theory* **221** (2021), 122–142. MR Zbl

[Zelingher 2023] E. Zelingher, "On values of the Bessel function for generic representations of finite general linear groups", *Adv. Math.* **434** (2023), art. id. 109314. MR Zbl

[Zhang 2014] Y. Zhang, "Bounded gaps between primes", *Ann. of Math.* (2) **179**:3 (2014), 1121–1174. MR Zbl

Received 16 Jan 2023. Revised 1 Sep 2023.

DAVID SOUDRY:

soudry@tauex.tau.ac.il
School of Mathematical Sciences, Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel

ELAD ZELINGHER:

eladz@umich.edu
Department of Mathematics, University of Michigan, Ann Arbor, MI, United States

msp

Essential Number Theory
Vol. 2, No. 1, 2023
https://doi.org/10.2140/ent.2023.2.83

Sur la conjecture de Tate pour les diviseurs

Bruno Kahn

On montre que la conjecture de Tate en codimension 1 sur un corps de type fini résulte de la même conjecture pour les surfaces sur son sous-corps premier. En caractéristique positive, ceci est dû à de Jong–Morrow sur $\mathbb{F}_p$ et à Ambrosi pour la réduction à $\mathbb{F}_p$. Nous montrons cette dernière réduction d'une manière différente, qui fonctionne aussi en caractéristique zéro. Sur $\mathbb{Q}$, la réduction aux surfaces se fait par un argument facile reposant sur le théorème (1, 1) de Lefschetz.

We prove that the Tate conjecture in codimension 1 over a finitely generated field follows from the same conjecture for surfaces over its prime subfield. In positive characteristic, this is due to de Jong–Morrow over $\mathbb{F}_p$ and to Ambrosi for the reduction to $\mathbb{F}_p$. We give a different proof than Ambrosi's, which also works in characteristic 0; over $\mathbb{Q}$, the reduction to surfaces follows from a simple argument using Lefschetz's (1, 1) theorem.

Introduction

La conjecture de Tate est l'une des plus célèbres en géométrie arithmétique : formulée dans [Tate 1965], elle prédit que l'application classe de cycle l-adique

$$\mathrm{cl}^i_X : CH^i(X) \otimes \mathbb{Q}_l \to H^{2i}(X_{k_s}, \mathbb{Q}_l(i))^{\mathrm{Gal}(k_s/k)} \tag{1}$$

(voir [SGA $4\frac{1}{2}$ 1977]) est surjective pour tout entier $i \geq 0$ et toute variété projective lisse X sur un corps k de type fini, de caractéristique différente de l et de clôture séparable k_s. Elle a été démontrée dans de nombreux cas particuliers, mais reste ouverte en général même pour $i = 1$. Pour un exposé détaillé qui reste largement d'actualité, je renvoie à [Tate 1994] (voir aussi [Li et Zhang 2022]).

Il est connu que pour $i = 1$, la conjecture de Tate pour les corps premiers implique cette même conjecture en général : en caractéristique zéro cela se déduit du théorème de spécialisation des groupes de Néron–Severi dû à Yves André [1996, théorème 5.2 (3); Ambrosi 2018, § 1.3.3], et en caractéristique positive cela résulte d'un théorème d'Emiliano Ambrosi [2018, Theorem 1.2.1]. Ambrosi démontre

MSC2020 : 14C25.
Mots-clefs : Tate conjecture, divisors.

plus : la conjecture de Tate en codimension i sur les corps finis l'implique pour tous les corps de type fini de caractéristique positive, sous une hypothèse de semi-simplicité qui résulte de la conjecture de Tate quand $i = 1$. Sa preuve, étendant au cas d'un corps fini un argument d'André en caractéristique zéro [1996, §5.1], utilise le théorème global des cycles invariants de Deligne et la cyclicité du groupe de Galois absolu de $\mathbb{F}_p$.

L'objet de cette note est d'offrir une démonstration plus élémentaire de cette réduction (uniquement pour $i = 1$), qui fonctionne uniformément en toute caractéristique : inspirée de la preuve de [Kahn 1998, Theorem 8.32 (a)], elle consiste à étendre la conjecture de Tate aux variétés lisses *ouvertes* (théorème 6). Cette idée, due originellement à Jannsen [1990], permet de remplacer avantageusement le recours au théorème global des cycles invariants par une simple utilisation du critère de dégénérescence des suites spectrales de Deligne [1968; 1994]. Un argument élémentaire de correspondances permet par ailleurs de se débarrasser aisément du problème de semi-simplicité qui apparaît aussi chez Jannsen (lemme 2 et proposition 3).

D'après de Jong (non publié) et Morrow [2019], la conjecture de Tate pour $i = 1$ en caractéristique positive se réduit même au cas des surfaces sur un corps fini (cette dernière conjecture étant par ailleurs équivalente à la conjecture de Birch et Swinnerton-Dyer pour les variétés abéliennes sur les corps de fonctions d'une variable sur k, voir remarque 9). La même chose est vraie en caractéristique zéro (théorème 8), en utilisant le théorème (1,1) de Lefschetz via les théorèmes de comparaison cohomologiques.

English introduction

The famous Tate conjecture, which predicts that the l-adic cycle class map (1) is surjective for smooth projective varieties X over finitely generated fields k, was formulated in [Tate 1965], but remains open up to now, even though it has been proven in important special cases [Tate 1994; Li et Zhang 2022]. This is so even for $i = 1$.

In this case, the Tate conjecture over prime fields implies the conjecture over any finitely generated field by work of Emiliano Ambrosi [2018, Theorem 1.2.1 and §1.3.3]. In characteristic 0, the argument uses Yves André's specialisation theorem [1996, théorème 5.2 (3)] for the Néron–Severi group, while in positive characteristic, Ambrosi's proof relies in particular on the cyclicity of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.

The aim of this note is to offer a simple proof of this reduction, which works uniformly in all characteristics (proposition 7). It is however special to codimension 1, while Ambrosi's argument also works (in positive characteristic) in any codimension i under a semisimplicity hypothesis which follows from Tate's conjecture if $i = 1$.

There are two ideas: the first is to get rid of the semisimplicity issue by a simple argument of correspondences (lemme 2), and the second is to extend the Tate conjecture for divisors from smooth projective to (all) smooth varieties (théorème 6). This idea goes back to Jannsen [1990]; its point is that it allows us to replace Ambrosi's use of Deligne's global invariant cycles theorem (an argument going back to André in characteristic 0 [1996, § 5.1]) by the degeneracy of the l-adic Leray spectral sequence, also due to Deligne. This is a reformulation of the arguments given in [Kahn 1998, proof of Theorem 8.32 (a)], specialised to codimension 1 (see also [Kahn 2002, Theorem 3.4]); the first idea is new.

When $k = \mathbb{F}_p$, a theorem of de Jong (unpublished) and Morrow [2019] even reduces the Tate conjecture for divisors to surfaces. (This case is in turn equivalent to the Birch and Swinnerton-Dyer conjecture for abelian varieties over global fields of positive characteristic, see remarque 9.) Over $\mathbb{Q}$, the same reduction holds (théorème 8): the proof involves the Lefschetz (1,1) theorem via the cohomological comparison theorems.

1. Notations

Soient k un corps et X une k-variété lisse. Soient k_s une clôture séparable de k et l un nombre premier différent de $\operatorname{car} k$. On note $H^j(X, i) := H^j(X_{k_s}, \mathbb{Q}_l(i))$; de même pour la cohomologie à supports. On note $\mathrm{cl}_X^i : CH^i(X) \otimes \mathbb{Q}_l \to H^{2i}(X, i)$ la classe de cycle, et simplement cl_X pour cl_X^1.

2. Une rétraction

Supposons X projective de dimension d. Pour $i \leq d$, choisissons une base $(\bar{Z}^1, \ldots, \bar{Z}^r)$ du groupe $N^i(X)_{\mathbb{Q}}$ des cycles de codimension i à coefficients rationnels sur X modulo l'équivalence numérique, et notons $(\bar{Z}_1, \ldots, \bar{Z}_r)$ la base duale dans $N_i(X)_{\mathbb{Q}}$, de sorte que $\langle \bar{Z}^i, \bar{Z}_j \rangle = \delta_{ij}$ [1]. Relevons les $\bar{Z}^i$ et $\bar{Z}_i$ en des classes de cycle $Z^i \in CH^i(X)_{\mathbb{Q}}$, $Z_i \in CH_i(X)_{\mathbb{Q}}$. Soit

$$e = \sum_a Z^a \times Z_a \in CH^d(X \times X)_{\mathbb{Q}},$$

vu comme correspondance algébrique, où $\times$ est le cross-produit des cycles (cf. la démonstration de [Kahn et al. 2007, Proposition 7.2.3]).

Lemme 1. *On a $e^2 = e$.*

Démonstration. Pour $Z, Z' \in CH^i(X)$ et $T, T' \in CH_i(X)$, on a l'identité

$$(Z \times T) \circ (Z' \times T') = \langle Z', T \rangle Z \times T'$$

1. Rappelons que $N^i(X)_{\mathbb{Q}}$ et $N_i(X)_{\mathbb{Q}}$ sont des $\mathbb{Q}$-espaces vectoriels de dimension finie [Fulton 1998, Example 19.1.4, p. 375], mis en dualité par l'accouplement d'intersection.

dans l'anneau des correspondances de Chow $CH^d(X \times X)$, où $\langle\ ,\ \rangle$ est le produit d'intersection : cela résulte immédiatement de la définition de la composition des correspondances [Fulton 1998, Definition 16.1.1, p. 305]. □

Lemme 2. *Soit V le sous-espace vectoriel de* $\mathrm{Im}\,\mathrm{cl}^i_X$ *engendré par les Z^a. L'action de e sur $H^{2i}(X, i)$ définit une rétraction G-équivariante de l'inclusion $V \hookrightarrow H^{2i}(X, i)$. En particulier, si $i = 1$, elle définit une rétraction de* cl_X.

Démonstration. Soit $x \in H^{2i}(X, i)$. Pour $(Z, T) \in CH^i(X) \times CH_i(X)$, on a

$$(Z \times T)^* x = <x, \mathrm{cl}_i(T)> \mathrm{cl}^i(Z)$$

où $<\ ,\ >$ est l'accouplement de Poincaré, cf. [Fulton 1998, Definition 16.1.2, p. 307]. Cela montre que $e(H^{2i}(X, i)) \subset V$, et aussi que sa restriction à ce sous-espace est l'identité.

Le cas $i = 1$ résulte du théorème de Matsusaka [1957] (équivalences homologique et numérique coïncident en codimension 1). □

3. Passage aux variétés lisses ouvertes

Supposons k de type fini, et X seulement lisse. On s'intéresse à l'extension suivante de la conjecture de Tate :

- $T(X)$: l'homomorphisme « classe de diviseur » $\mathrm{cl}_X : \mathrm{Pic}(X) \otimes \mathbb{Q}_l \to H^2(X, 1)^G$, où $G = \mathrm{Gal}(k_s/k)$, est surjectif.
- $T(k) : T(X)$ pour toutes les k-variétés lisses X.

Aux notations près, cette conjecture est due à Jannsen [1990, Conjecture 7.3, p. 109], qui l'étend même aux variétés singulières (avec l'homologie de Borel–Moore). Dans [Jannsen 1990, Theorem 7.10 (b), p. 114], il la réduit au cas des variétés projectives lisses sous une hypothèse de semi-simplicité (b), en bas de [Jannsen 1990, p. 113]) qui n'est pas connue en général même pour H^2. Le but de cette section est de faire cette réduction (théorème 6) en évitant l'hypothèse de semi-simplicité grâce à la proposition 3 ci-dessous. Bien sûr, ceci ne marche que pour les cycles de codimension 1!

Dans la suite, on note

$$H^2_{\mathrm{tr}}(X, 1) = \mathrm{Coker}\,\mathrm{cl}_X\,.$$

Proposition 3. *Pour X projective lisse, $T(X)$ équivaut à $H^2_{\mathrm{tr}}(X, 1)^G = 0$.*

Démonstration. L'implication $H^2_{\mathrm{tr}}(X, 1)^G = 0 \Longrightarrow T(X)$ est évidente. L'autre résulte du lemme 2. □

Lemme 4. *Soit $f : X' \to X$ un morphisme fini et plat de k-variétés lisses. Alors $T(X') \Longrightarrow T(X)$.*

Démonstration. En effet, $f^* : H^2(X, 1) \to H^2(X', 1)$ admet la rétraction G-équivariante $(1/\deg(f))f_*$, et ces deux homomorphismes commutent avec les homomorphismes correspondants entre $\mathrm{Pic}(X) \otimes \mathbb{Q}_l$ et $\mathrm{Pic}(X') \otimes \mathbb{Q}_l$ via cl_X et $\mathrm{cl}_{X'}$. □

Proposition 5. (*a*) *Soit U un ouvert de X. Alors $T(U) \Longrightarrow T(X)$.*

(*b*) *La réciproque est vraie si X est projective.*

Démonstration. (a) Notons que cl_X se factorise par $\mathrm{NS}(X) \otimes \mathbb{Q}_l$ où $\mathrm{NS}(X)$ est le groupe de Néron–Severi de X. Soit $Z = X - U$ (structure réduite). On a un diagramme commutatif aux lignes exactes

$$\begin{array}{ccccccc} \bigoplus\limits_{x \in Z \cap X^{(1)}} \mathbb{Q}_l & \longrightarrow & \mathrm{NS}(X) \otimes \mathbb{Q}_l & \longrightarrow & \mathrm{NS}(U) \otimes \mathbb{Q}_l & \longrightarrow & 0 \\ \downarrow & & \downarrow{\scriptstyle \overline{\mathrm{cl}}_X} & & \downarrow{\scriptstyle \overline{\mathrm{cl}}_U} & & \\ H^2_Z(X, 1) & \xrightarrow{\delta} & H^2(X, 1) & \longrightarrow & H^2(U, 1) & \longrightarrow & H^3_Z(X, 1) \end{array} \tag{2}$$

où la ligne du bas est la suite exacte de cohomologie à supports et la flèche verticale de gauche est surjective (en fait bijective) par semi-pureté [SGA $4\frac{1}{2}$ 1977, proposition 2.2.6 et rappel 2.2.8]. On en déduit un nouveau diagramme commutatif aux lignes exactes

$$\begin{array}{ccccccc} \bigoplus\limits_{x \in Z \cap X^{(1)}} \mathbb{Q}_l & \longrightarrow & \mathrm{NS}(X) \otimes \mathbb{Q}_l & \longrightarrow & \mathrm{NS}(U) \otimes \mathbb{Q}_l & \longrightarrow & 0 \\ \downarrow & & \downarrow{\scriptstyle \overline{\mathrm{cl}}_X} & & \downarrow{\scriptstyle \overline{\mathrm{cl}}_U} & & \\ 0 & \longrightarrow & \mathrm{Im}\,\delta & \longrightarrow & H^2(X, 1)^G & \longrightarrow & H^2(U, 1)^G \end{array} \tag{3}$$

où la flèche verticale de gauche est surjective. L'assertion résulte alors d'une petite chasse aux diagrammes.

(b) Supposons d'abord k parfait. D'après (a), on peut choisir U aussi petit qu'on veut. Prenons $Z = X - U$ assez gros pour contenir des diviseurs $D_1, \ldots, D_r$ dont les classes engendrent $\mathrm{NS}(X)$. Alors $\mathrm{NS}(U) = 0$ et il faut montrer que $H^2(U, 1)^G = 0$. Or le diagramme (2) montre que la suite

$$\mathrm{NS}(X) \otimes \mathbb{Q}_l \xrightarrow{\overline{\mathrm{cl}}_X} H^2(X, 1) \to H^2(U, 1) \to H^3_Z(X, 1)$$

est exacte. Avec la notation de la proposition 3, on a donc une suite exacte

$$0 \to H^2_{\mathrm{tr}}(X, 1)^G \to H^2(U, 1)^G \to H^3_Z(X, 1)^G.$$

Si $T(X)$ est vrai, le terme de gauche est nul par cette proposition. Il reste à voir que le terme de droite l'est également. Soit Z' la réunion du lieu singulier de Z et

de ses composantes irréductibles de codimension supérieure ou égale à 2 dans X : la suite exacte de cohomologie à supports

$$0 \simeq H^3_{Z'}(X, 1) \to H^3_Z(X, 1) \to H^3_{Z-Z'}(X - Z', 1) \simeq H^1(Z - Z', 0),$$

où le premier isomorphisme est par semi-pureté et le second par pureté [SGA $4\frac{1}{2}$ 1977, rappel 2.2.8], montre que $H^3_Z(X, 1)^G$ s'injecte dans $H^1(Z - Z', 0)^G$. Mais ce dernier groupe est trivial, car $H^1(Z - Z', 0)$ est mixte de poids supérieur ou égal à 1 [Deligne 1980, corollaire 3.3.5][2].

L'argument ci-dessus utilise implicitement le fait que les composantes irréductibles de codimension 1 de Z sont génériquement lisses. Pour obtenir ceci quand k est imparfait, il suffit de passer à une extension radicielle finie convenable de k, ce qui ne change ni $H^2(X, 1)$, ni $\mathrm{Pic}(X) \otimes \mathbb{Q}_l$, ni G. □

Théorème 6. *$T(X)$ est vrai pour les k-variétés lisses de dimension d si et seulement s'il est vrai pour les k-variétés projectives lisses de dimension d.*

Démonstration. Soit X lisse de dimension d. Choisissons une immersion ouverte dense $X \hookrightarrow X_0$ où X_0 est propre. D'après [de Jong 1996, Theorem 4.1], on peut trouver une altération $\pi : \tilde{X} \to X_0$ avec $\tilde{X}$ projective lisse et π génériquement fini. Soit $U \subset X$ un ouvert tel que $\pi_{|\pi^{-1}(U)}$ soit fini et plat.

Supposons $T(\tilde{X})$ vrai. Par la proposition 5(b), $T(\pi^{-1}(U))$ est vrai. D'après le lemme 4, $T(U)$ est donc vrai, et enfin $T(X)$ est vrai par la proposition 5(a). □

4. Changement de corps de base

Proposition 7. *Soit K/k une extension de corps de type fini. Alors $T(k) \iff T(K)$.*

Démonstration. En quatre étapes ; les deux premières et la dernière sont bien connues et valables en toute codimension ; elles sont rappelées pour la clarté de l'exposition. Pour plus de précision, on note ici $G_K = \mathrm{Gal}(K_s/K)$.

(1) Soit X lisse sur K, connexe et de corps des constantes L. Comme X est lisse, L/K est séparable. Je dis que, avec des notations évidentes, $T(X/K) \iff T(X/L)$. En effet, le G_K-module $H^2(X/K, 1)$ est induit du G_L-module $H^2(X/L, 1)$, donc $H^2(X/K, 1)^{G_K} \xrightarrow{\sim} H^2(X/L, 1)^{G_L}$.

(2) L'énoncé est vrai si K/k est finie séparable. En effet, $\Longrightarrow$ résulte immédiatement de (1). Pour $\Longleftarrow$, on se ramène à K/k galoisienne en considérant sa clôture galoisienne ; si X est lisse sur k, $T(X_K)$ implique alors $T(X)$ en prenant les invariants sous $\mathrm{Gal}(K/k)$.

2. Au moins sur un corps fini, ce dernier point peut se déduire plus élémentairement du théorème antérieur de A. Weil pour les courbes [1948, n° 48], en utilisant le fait que $H^1(Z-Z', 0)$ est isomorphe au module de Tate rationnel de la variété d'Albanese de $Z - Z'$ via un morphisme d'Albanese.

(3) Soit k_0 le sous-corps premier de K ; montrons que $T(k_0) \Longrightarrow T(K)$. Il suffit grâce au théorème 6 de montrer que $T(k_0)$ implique $T(X)$ pour toute K-variété projective lisse X. L'argument est une version simplifiée de celle de [Kahn 1998, Theorem 8.32 (a)].

On peut supposer X connexe. Soit L son corps des constantes, et soit k_1 la fermeture algébrique de k_0 dans L. Puisque k_1 est parfait, l'extension L/k_1 est régulière ; choisissons-en un k_1-modèle lisse S. Quitte à remplacer S par un ouvert, étendons X en un S-schéma projectif lisse $f : \mathcal{X} \to S$. Notant $\bar{S} = S \otimes_{k_1} k_s$, on a la suite spectrale de Leray (de $\mathbb{Q}_l[\![G_{k_1}]\!]$-modules)

$$E_2^{p,q} = H^p(\bar{S}, R^q f_* \mathbb{Q}_l(1)) \Longrightarrow H^{p+q}(\mathcal{X}, 1).$$

D'après [Deligne 1968] (voir aussi [Deligne 1994]), le choix d'une section hyperplane lisse $\mathcal{Y}/S$ de $\mathcal{X}/S$ et le théorème de Lefschetz difficile [Deligne 1980, théorème 4.1.1] font dégénérer cette suite spectrale, montrant aussi que la filtration sur l'aboutissement est scindée [3]. En particulier, l'homomorphisme « edge » $H^2(\mathcal{X}, 1) \to E_2^{0,2} = H^2(X, 1)^{\pi_1(\bar{S})}$ admet une section G_{k_1}-équivariante ; par conséquent, $H^2(\mathcal{X}, 1)^{G_{k_1}} \to H^2(X, 1)^{G_L}$ est *surjectif* ; en effet, $G_L \to \pi_1(S)$ est surjectif puisque S est géométriquement connexe. Avec les notations de (1), on a donc $T(\mathcal{X}/k_0) \Longrightarrow T(\mathcal{X}/k_1) \Longrightarrow T(X/L) \Longrightarrow T(X/K)$. (Noter que k_1/k_0 est séparable puisque k_0 est parfait.)

(4) Finalement, montrons que $T(K) \Longrightarrow T(k_0)$, ce qui terminera la démonstration. Soit, comme ci-dessus, k_1 la fermeture algébrique de k_0 dans K. Donnons-nous une k_0-variété projective lisse X ; rappelons que $\mathrm{NS}(X_{k_1}) \otimes \mathbb{Q}_l \to \mathrm{NS}(X_K) \otimes \mathbb{Q}_l$ est bijectif (c'est vrai en général pour les classes de cycles modulo l'équivalence algébrique, voir par exemple [Kahn 2018, proposition 5.5] et sa preuve). Ceci montre que $T(X_K) \Longrightarrow T(X_{k_1})$; mais d'autre part $T(X_{k_1}) \Longrightarrow T(X)$ par (2). □

Théorème 8. *Soit k_0 le sous-corps premier de k. Alors $T(S)$ pour toutes les surfaces projectives lisses S sur k_0 implique $T(k)$.*

Démonstration. D'après la proposition 7, on se ramène à $k = k_0$. Si $k = \mathbb{Q}$, soit X une variété projective lisse connexe de dimension $d \geq 2$, de corps des constantes k_1. D'après le point (1) de la preuve de la proposition 7, on peut remplacer $\mathbb{Q}$ par k_1. Choisissons un plongement complexe $k_1 \hookrightarrow \mathbb{C}$. Par les théorèmes de comparaison, l'équivalence homologique l-adique pour $X \otimes_{k_1} \bar{\mathbb{Q}}$ coïncide avec la même pour $X \otimes_{k_1} \mathbb{C}$, qui coïncide avec l'équivalence homologique pour la cohomologie de Betti ; notons $A^i_{\mathrm{hom}}(\bar{X})$ les quotients correspondants. Choisissons un k_1-plongement projectif $X \hookrightarrow \mathbb{P}^N$, d'où un faisceau très ample L ; le théorème de Lefschetz fort (pour la cohomologie de Betti) implique que $\bigcup c_1(L)^{d-2} : A^1_{\mathrm{hom}}(\bar{X}) \to A^{d-1}_{\mathrm{hom}}(\bar{X})$

3. Le résultat précis de [Deligne 1968, proposition 2.4] ou de [Deligne 1994, §2 ou §3] est que $Rf_*\mathbb{Q}_l$ est isomorphe à $\bigoplus_{i \geq 0} R^i f_* \mathbb{Q}_l[-i]$ dans la catégorie dérivée.

est injectif, et même *bijectif* grâce au théorème (1,1) de Lefschetz [Lieberman 1968, preuve de Corollary 1]. Comme $A^*_{\mathrm{hom}}(X) \xrightarrow{\sim} A^*_{\mathrm{hom}}(\overline{X})^{\mathrm{Gal}(\bar{\mathbb{Q}}/k_1)}$, on a aussi un isomorphisme $\bigcup c_1(L)^{d-2} : A^1_{\mathrm{hom}}(X) \xrightarrow{\sim} A^{d-1}_{\mathrm{hom}}(X)$. Mais, si $i : S \hookrightarrow X$ est une surface (lisse, connexe) ample donnée par le théorème de Bertini, cet isomorphisme se factorise en

$$A^1_{\mathrm{hom}}(X) \xrightarrow{i^*} A^1_{\mathrm{hom}}(S) \xrightarrow{i_*} A^{d-1}_{\mathrm{hom}}(X)$$

et de même pour l'isomorphisme correspondant $H^2(X, 1) \xrightarrow{\sim} H^{2d-2}(X, d-1)$, de manière compatible aux classes de cycles. Une petite chasse aux diagrammes montre alors que $T(S) \Longrightarrow T(X)$.

Si $k = \mathbb{F}_p$, Morrow se ramène d'abord au cas $\dim X \leq 3$ par le théorème de Lefschetz faible pour la cohomologie l-adique [Freitag et Kiehl 1988, Corollary I.9.4, p. 106] et pour le groupe de Picard [SGA 2 2005, corollaire 4.9 (b)], puis au cas d'une surface dans [Morrow 2019, Theorem 4.3]. Le premier point est un peu délicat, comme me l'a fait remarquer Juan Felipe Castro Cárdenas : il n'est pas clair que, pour le groupe de Picard, Lefschetz faible soit vrai pour les diviseurs *réduits*, en l'absence du théorème d'annulation de Kodaira (cf. [SGA 2 2005, remarque 4.10] [4]). Néanmoins, l'argument de la preuve de [Morrow 2019, Theorem 4.3] pour réduire le cas de la dimension 3 à celui de la dimension 2 marche aussi bien, et même mieux, pour réduire le cas de la dimension $d+1$ à celui de la dimension d quand $d \geq 3$: dans ce cas, toutes les inclusions horizontales du diagramme de la page 3495 sont des égalités. □

Remarque 9. D'après [Lichtenbaum et al. 2022], la conjecture $T(S)$ pour les surfaces S sur un corps fini k est équivalente à la conjecture de Birch et Swinnerton-Dyer pour les jacobiennes de courbes sur les corps de fonctions d'une variable K/k. Cette dernière implique la même conjecture pour toute variété abélienne A définie sur K : en effet, ladite conjecture est équivalente à la finitude de la composante l-primaire $Ш(K, A)\{l\}$ du groupe de Tate–Chafarevitch $Ш(K, A)$ [Schneider 1982; Kato et Trihan 2003]. Si $i : C \hookrightarrow A$ est une courbe ample, l'homomorphisme $i_* : J(C) \to A$ est surjectif (Weil, voir [Murre 1990, Lemma 2.3]), donc il existe $\sigma : A \to J(C)$ tel que $i_* \circ \sigma$ soit la multiplication par un entier $n > 0$, d'où $nШ(K, A) \subset i_* Ш(K, J(C))$. Mais on sait que $Ш(K, A)\{l\}$ est de cotype fini, donc la finitude de $Ш(K, J(C))\{l\}$ implique celle de $Ш(K, A)\{l\}$.

À ce stade, il est obligatoire de terminer avec la question évidente :

Question A. Peut-on réduire le cas de caractéristique zéro à celui de la caractéristique positive?

4. Note ajoutée pendant la correction des épreuves : ce problème a maintenant été résolu dans la preuve du lemme 3 de [Kahn 2023].

Par changement de base propre et lisse et par le théorème de Tchebotariov, cette question est équivalente à la suivante :

Question B. Soit S une $\mathbb{Q}$-surface projective lisse, et soit $\alpha \in H^2(S, 1)$. Supposons que, pour (presque) tout nombre premier p de bonne réduction, la spécialisation de α en p soit algébrique. Est-ce que α est algébrique?

Bibliographie

[Ambrosi 2018] E. Ambrosi, "A note on the behaviour of the Tate conjecture under finitely generated field extensions", *Pure Appl. Math. Q.* **14**:3-4 (2018), 515–527. MR Zbl

[André 1996] Y. André, "Pour une théorie inconditionnelle des motifs", *Inst. Hautes Études Sci. Publ. Math.* 83 (1996), 5–49. MR Zbl

[Deligne 1968] P. Deligne, "Théorème de Lefschetz et critères de dégénérescence de suites spectrales", *Inst. Hautes Études Sci. Publ. Math.* 35 (1968), 259–278. MR Zbl

[Deligne 1980] P. Deligne, "La conjecture de Weil, II", *Inst. Hautes Études Sci. Publ. Math.* 52 (1980), 137–252. MR Zbl

[Deligne 1994] P. Deligne, "Décompositions dans la catégorie dérivée", pp. 115–128 dans *Motives* (Seattle, WA, 1991), édité par U. Jannsen et al., Proc. Sympos. Pure Math. **55.1**, Amer. Math. Soc., Providence, RI, 1994. MR Zbl

[Freitag et Kiehl 1988] E. Freitag et R. Kiehl, *Étale cohomology and the Weil conjecture*, Ergebnisse der Math. (3) **13**, Springer, 1988. MR Zbl

[Fulton 1998] W. Fulton, *Intersection theory*, 2e éd., Ergebnisse der Math. (3) **2**, Springer, 1998. MR Zbl

[Jannsen 1990] U. Jannsen, *Mixed motives and algebraic K-theory*, Lecture Notes in Mathematics **1400**, Springer, 1990. MR Zbl

[de Jong 1996] A. J. de Jong, "Smoothness, semi-stability and alterations", *Inst. Hautes Études Sci. Publ. Math.* 83 (1996), 51–93. MR Zbl

[Kahn 1998] B. Kahn, "A sheaf-theoretic reformulation of the Tate conjecture", prépublication, 1998. arXiv math/9801017

[Kahn 2002] B. Kahn, "The Geisser–Levine method revisited and algebraic cycles over a finite field", *Math. Ann.* **324**:3 (2002), 581–617. MR Zbl

[Kahn 2018] B. Kahn, "Motifs et adjoints", *Rend. Semin. Mat. Univ. Padova* **139** (2018), 77–128. MR Zbl

[Kahn 2023] B. Kahn, "Some remarks on the smash-nilpotence conjecture", prépublication, 2023. arXiv 2311.14362

[Kahn et al. 2007] B. Kahn, J. P. Murre et C. Pedrini, "On the transcendental part of the motive of a surface", pp. 143–202 dans *Algebraic cycles and motives*, *Vol.* 2, édité par J. Nagel et C. Peters, London Math. Soc. Lecture Note Ser. **344**, Cambridge Univ. Press, 2007. MR Zbl

[Kato et Trihan 2003] K. Kato et F. Trihan, "On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$", *Invent. Math.* **153**:3 (2003), 537–592. MR Zbl

[Li et Zhang 2022] C. Li et W. Zhang, "A note on Tate's conjectures for abelian varieties", *Essent. Number Theory* **1**:1 (2022), 41–50. MR Zbl

[Lichtenbaum et al. 2022] S. Lichtenbaum, N. Ramachandran et T. Suzuki, "The conjectures of Artin–Tate and Birch–Swinnerton-Dyer", *Épijournal Géom. Algébrique* **6** (2022), article n° 7. MR Zbl

[Lieberman 1968] D. I. Lieberman, "Numerical and homological equivalence of algebraic cycles on Hodge manifolds", *Amer. J. Math.* **90** (1968), 366–374. MR Zbl

[Matsusaka 1957] T. Matsusaka, "The criteria for algebraic equivalence and the torsion group", *Amer. J. Math.* **79** (1957), 53–66. MR Zbl

[Morrow 2019] M. Morrow, "A variational Tate conjecture in crystalline cohomology", *J. Eur. Math. Soc.* (*JEMS*) **21**:11 (2019), 3467–3511. MR Zbl

[Murre 1990] J. P. Murre, "On the motive of an algebraic surface", *J. Reine Angew. Math.* **409** (1990), 190–204. MR Zbl

[Schneider 1982] P. Schneider, "Zur Vermutung von Birch und Swinnerton-Dyer über globalen Funktionenkörpern", *Math. Ann.* **260**:4 (1982), 495–510. MR Zbl

[SGA 2 2005] A. Grothendieck, "Application aux schémas algébriques projectifs", exposé XII, p. 109–134 dans *Cohomologie locale des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux* (Séminaire de Géométrie Algébrique du Bois Marie 1962), Documents Mathématiques (Paris) **4**, Soc. Math. France, Paris, 2005.

[SGA $4\frac{1}{2}$ 1977] A. Grothendieck et P. Deligne, "La classe de cohomologie associée à un cycle", pp. 129–153 dans *Cohomologie étale* (Séminaire de Géométrie Algébrique du Bois Marie), édité par P. Deligne, Lecture Notes in Math. **569**, Springer, 1977. MR Zbl

[Tate 1965] J. T. Tate, "Algebraic cycles and poles of zeta functions", pp. 93–110 dans *Arithmetical Algebraic Geometry* (West Lafayette, IN, 1963), édité par O. F. G. Schilling, Harper & Row, New York, 1965. MR Zbl

[Tate 1994] J. Tate, "Conjectures on algebraic cycles in l-adic cohomology", pp. 71–83 dans *Motives* (Seattle, WA, 1991), édité par U. Jannsen et al., Proc. Sympos. Pure Math. **55.1**, Amer. Math. Soc., Providence, RI, 1994. MR Zbl

[Weil 1948] A. Weil, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Ind. **1064**, Hermann et Cie, Paris, 1948. MR Zbl

Received 25 May 2022. Revised 1 Feb 2023.

BRUNO KAHN:

bruno.kahn@imj-prg.fr
IMJ-PRG, CNRS, Paris, France

msp

Essential Number Theory
Vol. 2, No. 1, 2023
https://doi.org/10.2140/ent.2023.2.93

Ranks of matrices of logarithms of algebraic numbers, I
The theorems of Baker and Waldschmidt–Masser

Samit Dasgupta

Let $\mathscr{L}$ denote the $\mathbb{Q}$-vector space of logarithms of algebraic numbers. In this expository work, we provide an introduction to the study of ranks of matrices with entries in $\mathscr{L}$. We begin by considering a slightly different question; namely, we present a proof of a weak form of Baker's theorem. This states that a collection of elements of $\mathscr{L}$ that is linearly independent over $\mathbb{Q}$ is in fact linear independent over $\overline{\mathbb{Q}}$. Next we recall Schanuel's conjecture and prove Ax's analogue of it over $\mathbb{C}((t))$.

We then consider arbitrary matrices with entries in $\mathscr{L}$ and state the structural rank conjecture, concerning the rank of a general matrix with entries in $\mathscr{L}$. We prove the theorem of Waldschmidt and Masser, which provides a lower bound, giving a partial result toward the structural rank conjecture. We conclude by stating a new conjecture that we call the matrix coefficient conjecture, which gives a necessary condition for a square matrix with entries in $\mathscr{L}$ to be singular.

1. Introduction

At the 1900 International Congress of Mathematicians, David Hilbert presented 23 open problems that have continued to serve as an inspiration for generations of mathematicians, including the following question:

MSC2020: 11J81.
Keywords: transcendence theory, Baker's theorem, Ax's theorem, Waldschmidt's theorem, Masser's theorem.

Hilbert's 7th problem. Let $a, b \in \overline{\mathbb{Q}}$, with $a \neq 0, 1$ and $b \notin \mathbb{Q}$. Is the value a^b necessarily transcendental?

A proof that Hilbert's question has an affirmative answer was given independently by Gelfond (1934) and Schneider (1935). The Gelfond–Schneider theorem can be stated equivalently as follows. Let

$$\mathscr{L} = \{x \in \mathbb{C} \mid e^x \in \overline{\mathbb{Q}}\}$$

denote the $\mathbb{Q}$-vector space of logarithms of algebraic numbers.

Theorem 1.1 (Gelfond–Schneider). *If two elements of $\mathscr{L}$ are linearly dependent over $\overline{\mathbb{Q}}$, then they are linearly dependent over $\mathbb{Q}$.*

A fantastic breakthrough was achieved by Alan Baker [1966; 1967a; 1967b], when he generalized from two to an arbitrary number of elements of $\mathscr{L}$.

Theorem 1.2 (Baker). *If $n \geq 1$ elements of $\mathscr{L}$ are linearly dependent over $\overline{\mathbb{Q}}$, then they are linearly dependent over $\mathbb{Q}$.*

In fact, Baker proved an effective refinement of this result giving a strong lower bound on the magnitude of any algebraic linear combination of elements of $\mathscr{L}$ that are linearly independent over $\mathbb{Q}$. Here we will present a proof of a version of Baker's theorem that is slightly weaker than Theorem 1.2.

We next shift our focus from a single linear form in logarithms to arbitrary matrices with entries in $\mathscr{L}$. Such matrices appear very naturally in number theory. For example, the regulator of a number field is the determinant of such a matrix, and this expression appears in the class number formula for the zeta function of the number field. Generalizations appear in Stark's conjectures for the leading terms of L-functions, and p-adic avatars appear in the study of p-adic L-functions. The question of the ranks of such matrices is therefore an important question, with Leopoldt's conjecture and the Gross–Kuz'min conjecture being important special cases in Iwasawa theory (these are discussed in Section 4B).

The primary conjecture about the ranks of matrices with entries in $\mathscr{L}$ is the *structural rank conjecture*. In applications, it is often useful to consider the $\mathbb{Q}$-vector space spanned by $\mathscr{L}$ and $\mathbb{Q}$, which we denote by $\mathscr{L} + \mathbb{Q}$. Given an $m \times n$ matrix M with entries in any field of characteristic 0, we define the structural rank of M as follows. Choose a $\mathbb{Q}$-basis $\{\ell_1, \ldots, \ell_r\}$ for the entries of M, and write $M = \sum_{i=1}^{r} \ell_i M_i$, with $M_i \in M_{m\times n}(\mathbb{Q})$. Write $M_x = \sum_{i=1}^{r} x_i M_i$, where the x_i are indeterminates. Then M_x is an $m \times n$ matrix with entries in the field of rational functions $F = \mathbb{Q}(x_1, \ldots, x_n)$. We define the *structural rank* of M to be the rank of M_x over F. One checks that this definition is independent of the basis $\{\ell_i\}$ chosen.

Conjecture 1.3 (structural rank conjecture). *The rank of any $M \in M_{m\times n}(\mathscr{L} + \mathbb{Q})$ is equal to the structural rank of M.*

The "über conjecture" in the transcendence theory of special values of logarithms and exponentials of algebraic numbers is the following conjecture of Schanuel. We write $\mathrm{trd}_{\mathbb{Q}}$ for the transcendence degree over $\mathbb{Q}$.

Conjecture 1.4. *Let $y_1, \dots, y_n \in \mathbb{C}$ be $\mathbb{Q}$-linearly independent. Then*

$$\mathrm{trd}_{\mathbb{Q}}\, \mathbb{Q}(y_1, \dots, y_n, e^{y_1}, \dots, e^{y_n}) \geq n.$$

In particular, if $y_1, \dots, y_n \in \mathscr{L}$ are $\mathbb{Q}$-linearly independent, then

$$\mathrm{trd}_{\mathbb{Q}}\, \mathbb{Q}(y_1, \dots, y_n) = n. \tag{1}$$

It is perhaps not surprising that the special case of Schanuel's conjecture given in (1) implies the structural rank conjecture; however, an elegant theorem of Roy [1995] is that the converse is also true:

Theorem 1.5 (Roy). *The structural rank conjecture is equivalent to the special case of Schanuel's conjecture given in* (1)*.*

Theorem 1.5 is proven in Section 4. For more on the structural rank conjecture and Schanuel's conjecture, see [Waldschmidt 2023]. The strongest unconditional evidence toward the structural rank conjecture is the following theorem of Waldschmidt [1981] and Masser [1981]:

Theorem 1.6 (Waldschmidt and Masser). *Let $M \in M_{m\times n}(\mathscr{L})$. Suppose that*

$$\mathrm{rank}(M) < \frac{mn}{m+n}.$$

Then there exist $P \in \mathrm{GL}_m(\mathbb{Q})$ and $Q \in \mathrm{GL}_n(\mathbb{Q})$ such that

$$PMQ = \begin{pmatrix} M_1 & 0 \\ M_2 & M_3 \end{pmatrix},$$

where the 0 block has dimension $m' \times n'$ with $m'/m + n'/n > 1$.

Intuitively, Theorem 1.6 states that, if the rank of $M = (\log(x_{ij}))$ is very small, then the underlying algebraic numbers x_{ij} satisfy a large number of multiplicative relations. In certain situations we can show that such relations do not exist, and hence we must have $\mathrm{rank}(M) \geq mn/(m+n)$. The six exponentials theorem (Theorem 4.2) is an example of a special case of the Waldschmidt–Masser theorem.

Transcendence results have many important applications in algebraic number theory. Especially in Iwasawa theory, it is the p-adic analogues of these statements that are most relevant. For example, Leopoldt's conjecture concerns the rank of the matrix of p-adic logarithms of a basis of units in a number field F. The p-adic analogue of the Waldschmidt–Masser theorem provides the strongest evidence for this conjecture. For instance, for a totally real field F one deduces that the rank of the Leopoldt matrix is at least half the expected one. We prove the p-adic version

of the Waldschmidt–Masser theorem in Section 5, since the archimedean case is studied more often in the literature, and discuss applications in Section 5A.

The paper is organized as follows. In Section 2, we prove Baker's theorem on the linear independence of logarithms of algebraic numbers. In Section 3, we prove Ax's theorem on the function field analogue of Schanuel's conjecture. In Section 4, we discuss the structural rank conjecture, explaining its connection to important conjectures in Iwasawa theory and proving Roy's Theorem 1.5. In Section 5, we prove the Waldschmidt–Masser theorem and give applications. In the concluding Section 6, we state a new conjecture, called the matrix coefficient conjecture, which attempts to answer the question: what can be said about a square matrix M with entries in $\mathscr{L}$ when it does not have full rank? Our conjecture is not as strong as the structural rank conjecture (and hence is perhaps more tractable), but still has important arithmetic implications.

2. Baker's theorem

Before giving an outline of the proof of Baker's theorem, let us discuss how one could hope to deduce the *conclusion* of the theorem. We are given algebraic numbers $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}^*$, complex numbers x_i such that $e^{x_i} = \alpha_i$, and a linear dependence

$$\beta_1 x_1 + \cdots + \beta_n x_n = 0 \tag{2}$$

with $\beta_i \in \overline{\mathbb{Q}}$. We will show that this implies the existence of integers $\lambda_1, \ldots, \lambda_n$, not all zero, such that

$$\alpha_1^{\lambda_1} \alpha_2^{\lambda_2} \cdots \alpha_n^{\lambda_n} = 1. \tag{3}$$

This implies that the x_i, together with the complex number $2\pi i$, are linearly dependent over $\mathbb{Q}$. Therefore, the mildly weaker version of Baker's theorem that we will prove is the following:

Theorem 2.1. *If $x_1, \ldots, x_n, 2\pi i \in \mathscr{L}$ are linearly independent over $\mathbb{Q}$, then $x_1, \ldots, x_n$ are linearly independent over $\overline{\mathbb{Q}}$.*

It does not take much work beyond the methods that we will present to remove $2\pi i$ and prove the version of Baker's theorem stated in Theorem 1.2 above (see [Baker 1967a]). However, to simplify the exposition and highlight the main points, we have included $2\pi i$ in our proof of Theorem 2.1.

Now, how does one deduce the existence of the λ_i from the existence of the β_i? It may be enticing to try to prove that the λ_i can be taken equal to the β_i, i.e., that the β_i are rational (or, more generally, that the λ_i can somehow be extracted from the β_i in a direct way). However, in practice a more indirect approach is effective.

Theorem 2.2. *Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}^*$. Suppose there exists a nonzero polynomial*

$$f(t_1, \ldots, t_n) \in \mathbb{C}[t_1, \ldots, t_n]$$

of degree $\leq L$ *in each variable* t_i *such that*

$$f(\alpha_1^z, \ldots, \alpha_n^z) = 0$$

for $z = 1, 2, \ldots, (L+1)^n$. *Then there exist integers* $\lambda_1, \ldots, \lambda_n$, *not all zero, such that*

$$\alpha_1^{\lambda_1}\alpha_2^{\lambda_2}\cdots\alpha_n^{\lambda_n} = 1.$$

Proof. Consider the square matrix M whose rows are indexed by the integers

$$z = 1, \ldots, (L+1)^n$$

and whose columns are indexed by the tuples $\lambda = (\lambda_1, \ldots, \lambda_n)$ of integers with $0 \leq \lambda_i \leq L$, with corresponding matrix entry

$$\alpha^{\lambda z} := \alpha_1^{\lambda_1 z}\cdots\alpha_n^{\lambda_n z}. \tag{4}$$

The existence of the polynomial f is equivalent to the existence of a column vector v such that $Mv = 0$. Indeed, the components of v are precisely the coefficients of f.

The existence of a nonzero f therefore implies that $\det(M) = 0$. But M is the Vandermonde matrix associated to the elements $\alpha^\lambda = \alpha_1^{\lambda_1}\cdots\alpha_n^{\lambda_n}$ as the tuple λ ranges over all $(L+1)^n$ possibilities. The vanishing of the determinant therefore implies the existence of two distinct tuples λ and λ' such that $\alpha^\lambda = \alpha^{\lambda'}$. We therefore have $\alpha^{\lambda-\lambda'} = 1$, as desired. □

Baker's theorem therefore amounts to using (2) to construct an *auxiliary polynomial* f that satisfies the conditions of Theorem 2.2. We first summarize Baker's ingenious method to do this:

(1) The Dirichlet box principle is a method of using the pigeonhole principle to construct a polynomial f with certain prescribed zeroes. One can apply this to the elements α^z appearing in the statement of Theorem 2.2. Of course, the result will not produce a polynomial with enough zeroes (i.e., we may find zeroes for $z = 1, \ldots, A$ for some A, but A will be less than $(L+1)^n$). Baker's clever insight is that the condition (2) allows us to ensure that a certain number of *derivatives* of f also have zeroes corresponding to these values of z.

(2) Baker then proves a complex analytic lemma, which is a quantitative strengthening of the classical Schwarz's lemma that shows that the vanishing of f and many of its derivatives implies a strong upper bound on the size of f and half as many of its derivatives, but for B times as many integers z (for some $B > 1$ depending on parameters we will make precise later).

(3) Using the fact that the α_i and β_i are algebraic, Baker deduces that these bounded values (i.e., the values of f and many of its derivatives for $z = 1, \ldots, AB$) must actually be 0. The basic concept is that an integer of absolute value less

than 1 must vanish; a generalization of this elementary statement to algebraic numbers of bounded degree and height is applied.

(4) Armed with more vanishing, one may now go back to step (2) and once again show that half as many derivatives are small for another factor of B times as many values of z. Baker iterates this procedure N times until $AB^N > (L+1)^n$, thereby showing that the auxiliary polynomial f has enough zeroes to apply Theorem 2.2.

In the rest of this section we will describe these steps in detail.

2A. ***Construction of auxiliary polynomial.*** For each α_i, let c_i denote the leading coefficient of the integral minimal polynomial of α_i, and let d denote the maximum degree of any α_i.

Lemma 2.3. *There exist integers $a_{i,j,s}$ such that, for each integer $j \geq 0$, we have*

$$(c_i\alpha_i)^j = \sum_{s=0}^{d-1} a_{i,j,s}\alpha_i^s.$$

Proof. For notational simplicity, we remove the index i. So we consider $\alpha \in \overline{\mathbb{Q}}$ with degree at most d, and let c denote the leading coefficient of the integral minimal polynomial of α. Then there exist integers $b_0, \ldots, b_{d-1}$ such that

$$c\alpha^d = b_{d-1}\alpha^{d-1} + \cdots + b_1\alpha + b_0. \tag{5}$$

We prove the result by induction on j. The base cases $0 \leq j < d$ are clear. For $j \geq d$ we assume by induction that there are integers $a_{j-1,s}$ such that

$$(c\alpha)^{j-1} = \sum_{s=0}^{d-1} a_{j-1,s}\alpha^s.$$

Multiplying by $c\alpha$, we obtain

$$(c\alpha)^j = \left(\sum_{s=0}^{d-2} c \cdot a_{j-1,s}\alpha^{s+1}\right) + a_{j-1,d-1}(c\alpha^d). \tag{6}$$

Plugging in (5) for $c\alpha^d$ on the right of (6), we obtain the desired expression

$$(c\alpha)^j = \sum_{s=0}^{d-1} a_{j,s}\alpha^s,$$

where

$$a_{j,s} = \begin{cases} a_{j-1,d-1}b_0 & \text{if } s = 0, \\ a_{j-1,d-1}b_s + c \cdot a_{j-1,s-1} & \text{if } 1 \leq s \leq d-1. \end{cases}$$

□

Let

$$f(t) = \sum_{\lambda=(\lambda_1,\ldots,\lambda_n)} p_\lambda t^\lambda := \sum_\lambda p_\lambda t_1^{\lambda_1} \cdots t_n^{\lambda_n}$$

be a polynomial of degree $\le L$ in each variable t_i. Let the c_i and $a_{i,j,s}$ be as in Lemma 2.3. Writing $c = (c_1, \ldots, c_n)$ and recalling the notation (4), we calculate

$$\begin{aligned}(c_1 \cdots c_n)^{Lz} f(\alpha^z) &= (c_1 \cdots c_n)^{Lz} \sum_\lambda p_\lambda \alpha^{\lambda z} \\ &= \sum_\lambda p_\lambda c^{Lz-\lambda z} (c\alpha)^{\lambda z} \\ &= \sum_\lambda p_\lambda c^{Lz-\lambda z} \prod_{i=1}^{n} \sum_{s=0}^{d-1} (\alpha_i)^s a_{i,\lambda_i z,s} \\ &= \sum_{s_1,s_2,\ldots,s_n=0}^{d-1} \alpha^s \sum_\lambda p_\lambda c^{L-\lambda z} \prod_{i=1}^{n} a_{i,\lambda_i z,s}.\end{aligned}$$

We can therefore force $f(\alpha^z) = 0$ by imposing integer linear conditions on the coefficients p_λ, namely that, for each z, we have

$$\sum_\lambda p_\lambda c^{L-\lambda z} \prod_{i=1}^{n} a_{i,\lambda_i z,s} = 0. \tag{7}$$

This observation allows for the initial construction of an auxiliary polynomial f using the following lemma of Siegel [1929], often known as "Dirichlet's box principle":

Lemma 2.4 (Siegel). *Let $N > 2M > 0$ be integers, and let $A = (a_{i,j})$ be an $M \times N$ matrix of integers such that $|a_{i,j}| < H$ for all i and j. There is a nonzero vector $b \in \mathbb{Z}^N$ such that $Ab = 0$ and each coordinate of b has absolute value less than $2NH$.*

Proof. Consider all vectors $b \in \mathbb{Z}^N$ with coordinates of absolute value $\le NH$. There are $(2NH+1)^N > (2NH)^N$ such vectors. For each such b, each coordinate of Ab has size at most $(NH)^2$. The total number of possible vectors Ab is less than $(2(NH)^2)^M$. Since $N > 2M$, the pigeonhole principle implies that two distinct b must give the same value of Ab. Their difference gives the desired vector. □

Applying Siegel's lemma to the system of linear equations in (7) will not produce enough zeroes for Theorem 2.2. Indeed, we have not yet used the assumption (2)! A key trick noticed by Baker is that it will suffice to have f and sufficiently many of its derivatives vanish. The precise statement is given below:

Theorem 2.5. *The following holds for every sufficiently large parameter h. Let*

$$L = \lceil h^{2-1/(4n)} \rceil.$$

There exists a polynomial

$$f(t) = \sum_{\lambda} p_\lambda t^\lambda \in \mathbb{Z}[t_1, \ldots, t_n]$$

of degree $\leq L$ in each variable t_i such that $|p_\lambda| < e^{h^3}$ for each λ and such that the complex analytic function of one variable $z \in \mathbb{C}$ defined by

$$\phi(z) = \sum_{\lambda} p_\lambda e^{z(\lambda_1 x_1 + \cdots + \lambda_n x_n)} \tag{8}$$

satisfies

$$\phi^{(m)}(z) = 0 \quad \text{for } m = 0, \ldots, h^2 - 1 \text{ and } z = 1, \ldots, h.$$

Proof. Note that $\phi(z)$ has been defined so that $\phi(z) = f(\alpha^z) = f(\alpha_1^z, \ldots, \alpha_n^z)$ for integers z. After dividing the linear dependence (2) by $-\beta_n$ (reordering if necessary to ensure this is nonzero) and renaming the coefficients, we can write

$$x_n = \beta_1 x_1 + \cdots + \beta_{n-1} x_{n-1}$$

with $\beta_i \in \overline{\mathbb{Q}}$. We then have

$$\phi(z) = \sum_{\lambda} p_\lambda e^{z[(\lambda_1 + \lambda_n \beta_1) x_1 + \cdots + (\lambda_{n-1} + \lambda_n \beta_{n-1}) x_{n-1}]}. \tag{9}$$

Note that $\phi^{(m)}(z)$ is the same sum as for $\phi(z)$, but with the term indexed by λ multiplied by

$$((\lambda_1 + \lambda_n \beta_1) x_1 + \cdots + (\lambda_{n-1} + \lambda_n \beta_{n-1}) x_{n-1})^m.$$

Expanding this out, it suffices to show that

$$\sum_{\lambda} p_\lambda \alpha^{\lambda z} (\lambda_1 + \lambda_n \beta_1)^{m_1} \cdots (\lambda_{n-1} + \lambda_n \beta_{n-1})^{m_{n-1}} = 0 \tag{10}$$

for all tuples of nonnegative integers satisfying

$$m_1 + \cdots + m_{n-1} = m.$$

Let d be the degree of the number field generated by all the α_i and β_i. Let c_i denote the leading coefficient in the integral minimal polynomial of α_i. By Lemma 2.3, for every nonnegative integer j, there exist integers $a_{i,j,s}$ such that

$$(c_i \alpha_i)^j = \sum_{s=0}^{d-1} a_{i,j,s} \alpha_i^s.$$

Let d_i and $b_{i,j,s}$ play the same role for the β_i.

The expression (10) will vanish if

$$\sum_{\mu_1=0}^{m_1}\cdots\sum_{\mu_{n-1}=0}^{m_{n-1}}\sum_{\lambda_1,\ldots,\lambda_n=0}^{L} p_\lambda\Bigg(\prod_{i=1}^{n} c_i^{Lz-\lambda_i z}a_{i,\lambda_i z,s_i}\Bigg) \times\Bigg(\prod_{j=1}^{n-1}\binom{m_j}{\mu_j}(d_j\lambda_j)^{m_j-\mu_j}\lambda_n^{\mu_j}b_{j,\mu_j,t_j}\Bigg)$$

vanishes for all tuples $(s_1,\ldots,s_n)$ and $(t_1,\ldots,t_{n-1})$ with $0\le s_i, t_i < d$.

How many linear equations is this in the coefficients p_λ we are searching for? We want vanishing for $0\le m < h^2$ and $1\le z\le h$. Hence, the number of such equations is at most

$$M = (h^2)^{n-1}hd^{2n-1} = h^{2n-1}d^{2n-1}.$$

Note that d and n are fixed but we are free to make h as large as we want.

The number of variables p_λ is $(L+1)^n$, so, to ensure this is bigger than $2M$ when h is large, we let $L=\lceil h^{2-1/(4n)}\rceil$, as in the statement of the theorem. Finally, we bound the size of the coefficients. An easy induction shows that there is a constant C, depending only on the α_i and β_i, such that

$$|a_{i,j,s}|\le C^j,\quad |b_{i,j,t}|\le C^j.$$

Therefore, for some constant K depending only on the α_i, β_i and n, we have

$$\prod_{i=1}^{n}|c_i^{Lz-\lambda_i z}a_{i,\lambda_i z,s_i}|\le K^{Lz}\le K^{Lh}$$

and, similarly,

$$\prod_{j=1}^{n-1}\left|\binom{m_j}{\mu_j}(d_j\lambda_j)^{m_j-\mu_j}\lambda_n^{\mu_j}b_{j,\mu_j,t_j}\right|\le K^{h^2\log(h)}.$$

By Siegel's lemma, there is a nontrivial solution in integers p_λ such that

$$|p_\lambda|\le 2K^{Lh+h^2\log(h)}(L+1)^n \ll e^{h^3}. \qquad \square$$

2B. ***Baker's lemma.*** In this section we present a complex analytic lemma of Baker, strengthening the classical Schwarz' lemma. This will allow us to bound the sizes of f and many of its derivatives for a multiple B of the A values of z at which we ensured vanishing of our auxiliary polynomial f.

Lemma 2.6. *Let $f:\mathbb{C}\to\mathbb{C}$ be an entire function, let $\epsilon>0$, and let A, B, C, T and U be large positive integers such that*

$$\tfrac{1}{2}\epsilon C > \frac{2T+UAB}{A(\log A)^{1/2}}+\frac{UBA^{\epsilon}}{\log A}. \tag{11}$$

Suppose that:

- $|f(z)| \leq e^{T+U|z|}$ *for* $z \in \mathbb{C}$.
- $f^{(t)}(z) = 0$ *for* $t = 0, \ldots, C-1$ *and* $z = 1, 2, \ldots, A$.

Then

$$|f(z)| \leq e^{-(T+Uz)(\log A)^{1/2}} \quad \text{for } z = 1, \ldots, AB.$$

Proof. The function

$$h(z) = \frac{f(z)}{(z-1)^C \cdots (z-A)^C}$$

is entire by the second assumption. By the maximum modulus principle on the circle of radius $A^{1+\epsilon}B$ around the origin, we have, for $|z| \leq AB$,

$$|h(z)| \leq \max_{|w|=A^{1+\epsilon}B} |h(w)|;$$

hence,

$$|f(z)| \leq \max_{|w|=A^{1+\epsilon}B} |f(w)| \cdot \max_{|w|=A^{1+\epsilon}B} \left| \frac{(z-1)(z-2)\cdots(z-A)}{(w-1)(w-2)\cdots(w-A)} \right|^C.$$

Now

$$\left| \frac{(z-1)(z-2)\cdots(z-A)}{(w-1)(w-2)\cdots(w-A)} \right| \leq \frac{(AB)^A}{(A^{1+\epsilon/2}B)^A} = e^{-(\epsilon/2)A\log A},$$

where the inequality holds since

$$\frac{AB+i}{A^{1+\epsilon}B-i} \leq A^{-\epsilon/2}$$

for all $i = 1, \ldots, A$. Meanwhile,

$$|f(w)| \leq e^{T+UA^{1+\epsilon}B}.$$

Our goal is to show that $|f(z)| \leq e^{-(T+UAB)(\log A)^{1/2}}$, so it suffices to show that

$$-\tfrac{1}{2}\epsilon AC \log A + (T + UA^{1+\epsilon}B) \leq -(T+UAB)(\log A)^{1/2}.$$

It is easy to see that this is implied by the assumption of the lemma,

$$\tfrac{1}{2}\epsilon C > \frac{2T+UAB}{A(\log A)^{1/2}} + \frac{UBA^{\epsilon}}{\log A}. \qquad \square$$

Let us now apply Baker's lemma to our auxiliary polynomial and its derivatives. With $\phi(z)$ as in (8) and (9), we have

$$\phi^{(m)}(z) = \sum_{m_i} \binom{m}{m_1, \ldots, m_{n-1}} \prod_{i=1}^{n-1} x_i^{m_i} f_{m_1,\ldots,m_{n-1}}(z),$$

where

$$f_{m_1,\dots,m_{n-1}}(z) = \sum_{\lambda} p_\lambda \alpha^{\lambda z}(\lambda_1 + \lambda_n\beta_1)^{m_1}\cdots(\lambda_{n-1}+\lambda_n\beta_{n-1})^{m_{n-1}}. \tag{12}$$

It is clear from this last expression that

$$|f_{m_1,\dots,m_{n-1}}(z)| < K^{h^3+L|z|} \tag{13}$$

for a suitable constant K depending only on n, the α_i and the β_i. Indeed, the p_λ are bounded by e^{h^3}. The m_i and λ_i are bounded by h^2. We choose the constant K so that the inequality (13) holds with the α_i or β_i replaced by any of their conjugates as well.

We would like to apply Baker's lemma on each of the functions $f_{m_1,\dots,m_{n-1}}(z)$ with

$$T = h^3\log K, \quad U = L\log K, \quad C = \tfrac{1}{2}h^2, \quad A = h, \quad B = h^{1/(8n)}, \quad \epsilon = \frac{1}{8n}.$$

We suppose that the constants K and h have been chosen so that the values T, U, A, B and C are integers. The first condition on $f_{m_1,\dots,m_{n-1}}(z)$ necessary to apply Baker's lemma is precisely the inequality (13). For the second condition, we note that the t-th derivative of $f_{m_1,\dots,m_{n-1}}(z)$ for $m_1+\cdots+m_{n-1} \le \frac{1}{2}h^2$ and $t \le \frac{1}{2}h^2 - 1$ is a linear combination of $f_{m'_1,\dots,m'_{n-1}}(z)$ with $m'_1+\cdots+m'_{n-1} \le h^2-1$. This gives the desired vanishing for $z = 1,\dots,h$ by the construction of the polynomial f in Theorem 2.5.

Furthermore, with our selection of parameters, the required inequality (11) reads

$$\frac{h^2}{32n} > \frac{2(\log K)h^3 + (\log K)h^{2-1/(4n)}\cdot h\cdot h^{1/(8n)}}{h(\log h)^{1/2}} + \frac{(\log K)h^{2-1/(4n)}\cdot h^{1/(8n)}\cdot h^{1/(8n)}}{\log h},$$

which is easily seen to hold for h large. We may therefore apply Baker's lemma to $f_{m_1,\dots,m_{n-1}}(z)$. This yields

$$|f_{m_1,\dots,m_{n-1}}(z)| < K^{-(h^3+Lz)(\log h)^{1/2}} \tag{14}$$

for $m_1+\cdots+m_{n-1} \le \frac{1}{2}h^2$ and $z = 1,\dots,h^{1+1/(8n)}$.

2C. ***Discreteness of algebraic integers.*** We apply the following elementary basic principle:

Lemma 2.7. *Suppose that $a \in \overline{\mathbb{Q}}$ such that da is an algebraic integer for some positive integer d. Suppose that $|a| < \epsilon$ for some positive real number ϵ and that every conjugate $\sigma(a)$ satisfies $|\sigma(a)| < M$ for some positive real number M. Finally, suppose that $[\mathbb{Q}(\alpha):\mathbb{Q}] \le n$ and that $\epsilon M^{n-1}d^n < 1$. Then $a = 0$.*

Proof. We bound the norm of the algebraic integer da:

$$|\mathrm{N}_{\mathbb{Q}(a)/\mathbb{Q}}(da)| = \prod_{\sigma:\mathbb{Q}(a)\hookrightarrow\mathbb{C}} |\sigma(da)| \le d^n|a| \cdot \prod_{\sigma\neq 1} |\sigma(a)| \le d^n \epsilon M^{n-1} < 1.$$

An integer of absolute value less than 1 must be 0. Hence, $\mathrm{N}_{\mathbb{Q}(a)/\mathbb{Q}}(da) = 0$, so $a = 0$. □

We apply Lemma 2.7 to each of the algebraic numbers $f_{m_1,\dots,m_{n-1}}(z)$ defined in (12) for

$$m_1 + \cdots + m_{n-1} \le \tfrac{1}{2}h^2, \quad z = 0, 1, \dots, h^{1+1/(8n)}.$$

In (14) we showed that

$$|f_{m_1,\dots,m_{n-1}}(z)| < \epsilon := K^{-(h^3+Lz)(\log h)^{1/2}}. \tag{15}$$

We also saw in (13) that

$$|\sigma(f_{m_1,\dots,m_{n-1}}(z))| < M := K^{h^3+Lz} \tag{16}$$

for each σ. It is easy to see from its definition that the denominator of $f_{m_1,\dots,m_{n-1}}(z)$ can be cleared by an integer of size at most

$$d := K^{h^2+Lz}, \tag{17}$$

after making K larger if necessary depending only on the α_i and β_i.

The inequality $\epsilon M^{n-1} d^n < 1$ is then easily seen to hold for h large because of the extra factor $(\log h)^{1/2}$ in the exponent of (15), so we conclude that

$$f_{m_1,\dots,m_{n-1}}(z) = 0$$

for $m_1 + \cdots + m_{n-1} \le \frac{1}{2}h^2$ and $z = 0, 1, \dots, h^{1+1/(8n)}$.

2D. ***Bootstrapping.*** We repeat the process described above, in the k-th iteration using Baker's lemma on the functions $f_{m_1,\dots,m_{n-1}}(z)$ with $m_1 + \cdots + m_{n-1} \le h^2/2^{k+1}$ with the parameters

$$T = h^3 \log K, \quad U = L \log K, \quad C = \frac{h^2}{2^{k+1}},$$
$$A = h^{1+k/(8n)}, \quad B = h^{1/(8n)}, \quad \epsilon = \frac{1}{8n}.$$

We assume that K and h had been chosen initially so that the quantities above are integers. In the k-th iteration we obtain that

$$|f_{m_1,\dots,m_{n-1}}(z)| < K^{-(h^3+Lz)\left(\log(h+k/(8n))\right)^{1/2}}$$

for

$$m_1 + \cdots + m_{n-1} \le \frac{h^2}{2^{k+1}}, \quad z = 0, 1, \dots, h^{1+(k+1)/(8n)}.$$

The quantities in (16) and (17) do not change, so again Lemma 2.7 implies that the values $f_{m_1,\dots,m_{n-1}}(z)$ vanish. We may therefore move on to the next k.

Each iteration multiplies the number of zeroes by $B = h^{1/(8n)}$. After $16n^2$ iterations we will obtain more than h^{2n} zeroes. Since $L = h^{2-1/(4n)}$ and h is large, we have

$$h^{2n} > (L+1)^n,$$

so the polynomial $f = f_{0,0,\dots,0}$ satisfies the conditions of Theorem 2.2. Therefore, there exist integers $\lambda_1, \dots, \lambda_n$, not all zero, such that

$$\alpha_1^{\lambda_1} \cdots \alpha_n^{\lambda_n} = 1.$$

This completes the proof of Baker's theorem.

3. Ax's theorem

Moving on from linear forms in elements of $\mathscr{L}$ to arbitrary polynomials, we remind the reader of Schanuel's conjecture, which was stated in the introduction:

Schanuel's conjecture. *Let $y_1, \dots, y_n \in \mathbb{C}$ be $\mathbb{Q}$-linearly independent. Then*

$$\operatorname{trd}_{\mathbb{Q}} \mathbb{Q}(y_1, \dots, y_n, e^{y_1}, \dots, e^{y_n}) \geq n.$$

While little is known about this conjecture, we have the following function field analogue, proved by James Ax [1971]:

Theorem 3.1 (Ax). *Let $y_1, \dots, y_n \in t\mathbb{C}[\![t]\!]$ be $\mathbb{Q}$-linearly independent. Then*

$$\operatorname{trd}_{\mathbb{C}(t)} \mathbb{C}(t)(y_1, \dots, y_n, e^{y_1}, \dots, e^{y_n}) \geq n.$$

In this section we prove Ax's theorem. The section is self-contained and may be skipped by readers not interested in the function field setting. Before proceeding, we note simply the tool that is available in the function field setting that is not available in the classical setting: there is a derivative operator on $\mathbb{C}((t))$, and elements of the form e^y satisfy $(e^y)' = y'e^y$.

3A. *Derivations.*

Definition 3.2. Let A be a commutative ring and B a commutative A-algebra. An A-derivation of B into a B-module M is an A-linear map

$$D : B \to M$$

such that

$$D(ab) = aD(b) + D(a)b, \quad a, b \in B, \tag{18}$$

where we view M as both a left and right B-module since B is commutative.

There is a pair $(d = d_{B/A}, \Omega_{B/A})$ of a B-module $\Omega_{B/A}$ and an A-derivation

$$d : B \to \Omega_{B/A}$$

that is universal in the sense that any A-derivation $D : B \to M$ can be obtained by composing $d_{B/A}$ with a B-module homomorphism $\Omega_{B/A} \to M$. The module of *Kähler differentials* $\Omega_{B/A}$ is defined as the quotient of the free B-module generated by formal generators db for each $b \in B$ by the relations $da = 0$ for $a \in A$, $d(b+b') = db + db'$, and $d(bb') = b \cdot db' + b' \cdot db$. The universal derivation $d_{B/A} : B \to \Omega_{B/A}$ is defined by $d_{B/A}(b) = db$.

Lemma 3.3. *Let F/K be field extension and $x \in F$ separable algebraic over K. Then $dx = 0$ in $\Omega_{F/K}$.*

Proof. Let $f(t) \in K[t]$ be the minimal polynomial of x. Then

$$0 = d(f(x)) = f'(x)dx.$$

Since x is separable, $f'(x) \neq 0$, so $dx = 0$. □

Meanwhile, if $F(t)$ denotes the function field in one variable over the field F, we have that $\Omega_{F(t)/F}$ is the 1-dimensional $F(t)$-vector space generated by dt, with $d(f(t)) = f'(t)dt$.

Lemma 3.4. *Let $K \subset F \subset L$ be fields of characteristic 0. Let $D : F \to F$ be a K-derivation. Then D can be extended to a K-derivation $L \to L$.*

Proof. For $f \in F[t]$, let f^D denote the polynomial where D has been applied to the coefficients of f. We show how to extend the derivation d. Let $z \in L$ with $z \notin F$. If z is algebraic over F, let $p(x)$ be its minimal polynomial. Define

$$u = -\frac{p^D(z)}{p'(z)}, \quad \widetilde{D}(g(z)) = g^D(z) + g'(z)u. \tag{19}$$

If z is transcendental over F, we define

$$\widetilde{D}(g(z)) = g^D(z) + g'(z)u \tag{20}$$

for any $u \in L$. We leave it to the reader to check that setting $\widetilde{D}|_F = D$ and using (19) or (20) to extend to $F(z)$ yields a derivation $\widetilde{D}$. Now one uses Zorn's lemma on pairs (D', F'), where F' is a field such that $K \subset F' \subset L$ and D' is a derivation extending D, to extend D all the way to L. □

Corollary 3.5. *Let $K \subset L$ be fields of characteristic 0. Then*

$$\dim_L \Omega_{L/K} = \operatorname{trd}_K L.$$

More generally, if $K \subset F \subset L$, then

$$\dim_L (L \cdot d_{L/K}(F)) = \operatorname{trd}_K F.$$

Proof. Let $\{f_1, \ldots, f_n\}$ be a transcendence basis for F/K. Suppose that

$$\sum_{i=1}^{n} a_i d_{L/K} f_i = 0$$

with $a_i \in L$. By the universal property of $d_{L/K}$, we have

$$\sum_{i=1}^{n} a_i D(f_i) = 0$$

for any K-derivation $D_i : L \to L$. Therefore, if we show that for each i there exists a K-derivation $D_i : L \to L$ such that $D_i(f_j) = \delta_{ij}$, then we obtain $a_i = 0$ for all i. This yields the linear independence of the $d_{L/K} f_i$ over L.

The existence of the D_i follows from the proof of Lemma 3.4. We can first extend the 0 derivation on K to $K(f_i)$ by setting $z = f_i$ and $u = 1 - f_i$ in (20), and then inductively extend to $K(f_1, \ldots, f_n)$ by setting $z = f_j$ and $u = -f_j$ for $j \neq i$. Finally, we extend D_i to L using Lemma 3.4 once more. □

3B. ***Derivation on Kähler differentials.*** Let A be a commutative ring and B an A-algebra. Let $D : B \to B$ be a derivation such that $D(A) \subset A$. There exists an A-linear map

$$D^1 : \Omega_{B/A} \to \Omega_{B/A}$$

satisfying

$$D^1(f\,dg) = (Df)dg + f\,d(Dg). \tag{21}$$

We leave the verification of this to the reader, but we note that a more general fact is true. If we consider the graded algebra of differentials

$$\Omega^*_{B/A} = \bigoplus_{n=0}^{\infty} \bigwedge^n_B \Omega_{B/A},$$

then the differential $D : B \to B$ extends to a graded derivation

$$D^* : \Omega^*_{B/A} \to \Omega^*_{B/A}$$

satisfying (18), where the 0th graded piece is D and the 1st graded piece is D^1. In our proof of Ax's theorem, we will only need the map D^1, but let us note that the rule (21) generalizes: for any $f \in B$ and $\omega \in \Omega_{B/A}$, we have

$$D^1(f\omega) = (Df)\omega + f D^1(\omega). \tag{22}$$

Proofs of these facts may be found in the references given in [Ax 1971, page 255].

Lemma 3.6. *Let $y \in t\mathbb{C}[\![t]\!]$, $z = e^y$, and let $D : \mathbb{C}((t)) \to \mathbb{C}((t))$ be a $\mathbb{C}$-derivation of the form $D(f(t)) = f'(t) \cdot g(t)$ for some fixed $g(t) \in \mathbb{C}((t))$. Then*

$$D^1(dy - z^{-1}dz) = 0$$

in $\Omega_{\mathbb{C}((t))/\mathbb{C}}$.

Proof. A direct computation with the definition (21) shows that, in general, we have

$$D^1(dy - z^{-1}dz) = d(Dy - z^{-1}Dz).$$

Yet, when $z = e^y$, the term $Dy - z^{-1}Dz$ vanishes for the derivation $D(f(t)) = f'(t) \cdot g(t)$. □

Lemma 3.7. *Let $K \subset L$ be fields and $D : L \to L$ a derivation such that* $\ker D = K$. *Then the map*

$$L \otimes_K \ker D^1 \to \Omega_{L/K}, \quad f \otimes \omega \mapsto f\omega,$$

is injective.

Proof. Suppose there exist

$$f_1, \ldots, f_n \in L^*, \quad \omega_1, \ldots, \omega_n \in \ker D^1$$

such that

$$\sum_{i=1}^{n} f_i \otimes \omega_i \mapsto 0, \quad \text{i.e., } \sum_{i=1}^{n} f_i\omega_i = 0. \tag{23}$$

Scale so that $f_1 = 1$. If all the f_i lie in K, then

$$\sum_{i=1}^{n} f_i \otimes \omega_i = 1 \otimes \sum_{i=1}^{n} f_i\omega_i = 1 \otimes 0 = 0,$$

so we are done. Suppose this is not the case and take the minimal such vanishing linear combination. By minimality, we can assume that the ω_i are linearly independent over L. Apply D^1 to the expression (23). Using (22), we find

$$0 = \sum_{i=1}^{n}((Df_i)\omega_i + f_i D^1(\omega_i)) = \sum_{i=1}^{n}(Df_i)\omega_i,$$

where the second equality holds since $\omega_i \in \ker D^1$. By the linear independence of the ω_i over L, we see that $Df_i = 0$ for all i and hence, by assumption, $f_i \in K$ for all i. □

The following is a technical algebraic lemma that will allow us to reduce to the setting of function fields of curves:

Lemma 3.8. *Let $K \subsetneq L$ be an extension of fields with K relatively algebraically closed in L (i.e., if $\alpha \in L$ and α is algebraic over K, then $\alpha \in K$). Let*

$$W = \{F : K \subset F \subset L,\ \mathrm{trd}_F\, L = 1,\ F \text{ relatively algebraically closed in } L\}.$$

Then

$$\bigcap_{F \in W} F = K.$$

Proof. Let $t \in L$ with $t \notin K$. We need to show there exists $F \in W$ such that $t \notin F$. Since K is relatively algebraically closed in L, the element t is transcendental over K.

Choose a transcendence basis for L/K consisting of t and a set B of elements not in $K(t)$. Let F be the relative algebraic closure of $K(B)$ in L, i.e.,

$$F = \{x \in L \mid x \text{ algebraic over } K(B)\}.$$

Then $F \in W$, since L is algebraic over $F(t)$. Since $t \notin F$, this completes the proof. □

In some sense, the following lemma is the main engine of Ax's proof:

Lemma 3.9. *Let L/K be fields of characteristic 0. Denote by dL the K-subspace of $\Omega_{L/K}$ spanned by df for $f \in L$. Denote by dL/L the $\mathbb{Z}$-submodule of $\Omega_{L/K}$ spanned by $f^{-1}df$ for $f \in L^*$. Then the canonical map of K-vector spaces*

$$K \otimes_{\mathbb{Z}} dL/L \to \Omega_{L/K}/dL, \quad k \otimes \frac{df}{f} \mapsto \frac{k}{f} df, \tag{24}$$

is injective, where $\Omega_{L/K}/dL$ denotes the quotient of $\Omega_{L/K}$ by the K-subspace spanned by df for $f \in L$.

Proof. Choose an element

$$\sum_{i=1}^{n} k_i \otimes f_i^{-1} df_i \tag{25}$$

in the kernel of the map (24), with n minimal. By minimality, the k_i are linearly independent over $\mathbb{Q}$. We will show that each f_i lies in $\overline{K}_L$, the relative algebraic closure of K in L. By Lemma 3.3, this will imply $df_i = 0$, giving the desired injectivity.

If $L = \overline{K}_L$, there is nothing to prove. Otherwise, let $F \in W$, with W as in Lemma 3.8. So $K \subset F \subset L$, $\mathrm{trd}_F\, L = 1$, and $\overline{F}_L = F$. Since the element (25) lies in the kernel of (24), we have

$$\sum_{i=1}^{n} k_i f_i^{-1} df_i = \sum_{i=1}^{m} k_i' df_i' \tag{26}$$

for some $f_i' \in L^*$ and $k_i' \in K$. Now, we would like to use properties of function fields of curves, but, unfortunately, we do not know that L is finitely generated over F. To this end, we consider a field L' generated over F by the f_i, the f_i', and by any elements used in any relations in $\Omega_{L/K}$ used to obtain (26). The field L' then still has transcendence degree 1 over F, and is finitely generated over F. We may therefore identify L' with the function field of a smooth projective algebraic curve over F. Furthermore, equation (26) still holds in $\Omega_{L'/K}$ by construction, and so it holds also in $\Omega_{L'/F}$.

Points P on this curve correspond to valuations

$$\mathrm{ord}_P : (L')^* \to \mathbb{Z}.$$

Associated to P we also have a residue map

$$\mathrm{res}_P : \Omega_{L'/F} \to F.$$

The residue and valuation maps satisfy the following well-known properties. For all $g \in (L')^*$, we have

$$\mathrm{res}_P(g^{-1}dg) = \mathrm{ord}_P(g), \quad \mathrm{res}_P(dg) = 0.$$

Applying res_P to (26), we get

$$\sum_{i=1}^{n} k_i \,\mathrm{ord}_P(f_i) = 0.$$

By $\mathbb{Q}$-linear independence of the k_i, we obtain $\mathrm{ord}_P(f_i) = 0$ for all P and i. But a function on a smooth projective curve with no zeroes or poles must be constant, and hence $f_i \in F$ for all i. Since this holds for all F, we have by Lemma 3.8 that $f_i \in \overline{K}_L$. □

We can now complete the proof of Ax's theorem.

Proof of Theorem 3.1. Let $y_1, \ldots, y_n \in t\mathbb{C}[\![t]\!]$ and write $z_i = e^{y_i} \in \mathbb{C}[\![t]\!]$. Let

$$L = \mathbb{C}(y_1, \ldots, y_n, z_1, \ldots, z_n).$$

It suffices to show that, if $\mathrm{trd}_{\mathbb{C}} L \leq n$, then $y_1, \ldots, y_n$ are $\mathbb{Q}$-linearly dependent. Suppose $\mathrm{trd}_{\mathbb{C}} L \leq n$. Then, by Corollary 3.5, the differentials

$$\omega_i = dy_i - z_i^{-1}dz_i \in \Omega_{L/\mathbb{C}}$$

for $i = 1, \ldots, n$ together with dy_1 must be linearly dependent over L, so

$$\sum_{i=1}^{n} f_i\omega_i + g\,dy_1 = 0 \tag{27}$$

with $f_i, g \in L$ not all zero. Note that, if $y_1'(t) = 0$, then y_1 is a constant, and since $y_1 \in t\mathbb{C}[\![t]\!]$ we would get $y_1 = 0$. Then the y_i are trivially linearly dependent; so we may assume hereafter that $y_1'(t) \neq 0$. Define a $\mathbb{C}$-derivation

$$D : L \to L, \quad D(f(t)) = \frac{f'(t)}{y_1'(t)}.$$

By Lemma 3.6, we have $D^1(\omega_i) = 0$. Furthermore, a direct computation shows

$$D^1(dy_1) = d(Dy_1) = d(1) = 0.$$

Therefore, we have that

$$\sum f_i \otimes \omega_i + g \otimes dy_1 \in \ker((L \otimes_{\mathbb{C}} \ker D^1) \to \Omega_{L/\mathbb{C}}).$$

By Lemma 3.7, we may assume $f_i, g \in \mathbb{C}$.

Rewrite the equation $\sum f_i\omega_i + g dy_1 = 0$ in the form

$$\sum_{i=1}^{n} f_i \cdot (-z_i^{-1} dz_i) = -\sum_{i=1}^{n} f_i dy_i - g dy_1.$$

Lemma 3.9 implies that either all $f_i = 0$, or the $z_i^{-1}dz_i$ are $\mathbb{Q}$-linearly dependent. In the first case, from (27) and the fact that the f_i and g are not all zero, we would get $dy_1 = 0$. Hence, y_1 is a constant, and, as noted earlier, this implies that $y_1 = 0$. Therefore, we suppose we are in the second case, say

$$\sum \frac{m_i(dz_i)}{z_i} = 0$$

with $m_i \in \mathbb{Z}$ not all zero. This implies

$$d\left(\frac{\prod z_i^{m_i}}{\prod z_i^{m_i}}\right) = 0,$$

so $\prod z_i^{m_i} = e^{\sum m_i y_i}$ is a constant. By considering constant terms, this constant must be 1. Therefore,

$$\sum m_i y_i = 0,$$

giving the desired linear dependence of the y_i over $\mathbb{Q}$. □

4. The structural rank conjecture

We now return to the classical setting over $\mathbb{C}$, rather than the function field setting, and move on to consider matrices of elements of $\mathscr{L}$. The simplest case of 2×2 matrices leads to the following *four exponentials conjecture*:

Conjecture 4.1. *Let $M \in M_{2\times 2}(\mathscr{L})$. Then* $\det(M) = 0$ *only if the rows or columns of M are linearly dependent over $\mathbb{Q}$.*

This conjecture was first stated in print by Schneider [1957], though versions had been considered over the previous two decades by Selberg, Siegel, Alaoglu and Erdős [1944], and others (precise statements by Selberg and Siegel do not appear in the literature, but see [Waldschmidt 2023] for a discussion of their consideration of this problem). The four exponentials conjecture remains wide open. As an example, Waldschmidt [2023] points out the following elementarily stated open question, a positive answer for which would follow from the four exponentials conjecture: let t be a real number such that 2^t and 3^t are integers; does it follow that t is a nonnegative integer?

The strongest theoretical evidence for the conjecture is the following *six exponentials theorem*:

Theorem 4.2. *Let $M \in M_{2\times 3}(\mathscr{L})$. Then* $\operatorname{rank}(M) < 2$ *only if the rows or columns of M are linearly dependent over $\mathbb{Q}$.*

The six exponentials theorem was proven independently by Lang [1966] and Ramachandra [1968a; 1968b]. See Waldschmidt's delightful personal account [2023] for details and references on the history of the four exponentials conjecture and the six exponentials theorem.

The six exponentials theorem follows as a special case of the theorem of Waldschmidt and Masser that we will discuss later (see Section 5A). A naive generalization of the four exponentials conjecture to matrices of arbitrary dimension does not hold — in general, matrices may have lower than maximal rank even if the rows and columns are linearly independent over $\mathbb{Q}$. As an example, note that

$$\det \begin{pmatrix} x & z & 0 \\ 0 & y & -x \\ y & 0 & z \end{pmatrix} = 0.$$

Therefore, if we substitute for x, y and z any elements of $\mathscr{L}$ that are linearly independent, then we obtain a matrix of rank < 3 whose rows and columns are linearly independent over $\mathbb{Q}$. Examples such as these motivate the *structural rank conjecture*, which was stated precisely in the introduction. The matrix above has structural rank equal to 2.

4A. ***The p-adic setting.*** Most statements in transcendence theory have analogues in the p-adic setting. As we will describe below, these analogues are particularly important in Iwasawa theory. Let p be a prime number, and let $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}}_p$ denote the completion of the algebraic closure of $\mathbb{Q}_p$. The statements below work equally well over $\mathbb{Q}_p$, but working with $\mathbb{C}_p$ provides extra generality. We normalize the

p-adic absolute value on $\mathbb{C}_p$ in the usual way: $|p| = p^{-1}$. There exists a p-adic logarithm and a p-adic exponential function

$$\log_p : \{x \in \mathbb{C}_p : |x-1| < 1\} \to \mathbb{C}_p, \quad \exp_p : \{x \in \mathbb{C}_p : |x| < p^{-1/(p-1)}\} \to \mathbb{C}_p \tag{28}$$

defined by the usual power series

$$\log_p(1-x) = -\sum_{n=1}^{\infty} \frac{x^n}{n}, \quad \exp_p(x) = \sum_{n=1}^{\infty} \frac{x^n}{n!}.$$

The functions $\log_p$ and $\exp_p$ are injective group homomorphisms on the domains given in (28). The p-adic logarithm extends uniquely to a continuous homomorphism

$$\log_p : \{x \in \mathbb{C}_p : |x| = 1\} \to \mathbb{C}_p$$

since every $x \in \mathbb{C}_p$ with $|x| = 1$ satisfies $|x^n - 1| < 1$ for an appropriate positive integer n, and we may define $\log_p(x) = (1/n)\log_p(x^n)$. Next we extend $\log_p$ to a continuous homomorphism

$$\log_p : \mathbb{C}_p^* \to \mathbb{C}_p$$

by fixing Iwasawa's (noncanonical) choice $\log_p(p) = 0$. The kernel of $\log_p$ on $\mathbb{C}_p^*$ then consists of elements of the form $p^a \cdot u$, where $a \in \mathbb{Q}$ and u is a root of unity.

We define the $\mathbb{Q}$-vector space of p-adic logarithms of algebraic numbers,

$$\mathscr{L}_p = \{\log_p(x) \mid x \in \overline{\mathbb{Q}}^*\} \subset \mathbb{C}_p.$$

The p-adic version of Baker's theorem was proved by Brumer [1967] following Baker's method.

Theorem 4.3 (Baker and Brumer). *Let $y_1, \ldots, y_n \in \mathscr{L}_p$ be linearly independent over $\mathbb{Q}$. Then $y_1, \ldots, y_n$ are linearly independent over $\overline{\mathbb{Q}}$.*

Similarly, there are natural analogues of Schanuel's conjecture and the structural rank conjecture in the p-adic setting. To be precise we state the latter of these:

Conjecture 4.4 (p-adic structural rank conjecture). *Let*

$$M \in M_{m\times n}(\mathscr{L}_p + \mathbb{Q}) \subset M_{m\times n}(\mathbb{C}_p).$$

The rank of M is equal to the structural rank of M.

4B. ***Applications in number theory.*** Statements in transcendence theory have important applications in algebraic number theory. In this section, we describe two important conjectures in Iwasawa theory that are special cases of the p-adic structural rank conjecture. These conjectures are our personal motivation for this study.

4B1. *Leopoldt's conjecture.* Fix a prime p and an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$.

Conjecture 4.5 (Leopoldt's conjecture). *Let F be a number field of degree n over $\mathbb{Q}$ and let $\sigma_1, \dots, \sigma_n$ denote the embeddings $F \hookrightarrow \overline{\mathbb{Q}}$. Let $\{u_1, \dots, u_r\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}_F^*/\mu(F)$. Let*

$$M = (\log_p \sigma_j(u_i)) \in M_{r\times n}(\mathscr{L}_p).$$

Then $\operatorname{rank}_{\mathbb{C}_p}(M) = r$.

Proposition 4.6. *The p-adic structural rank conjecture implies Leopoldt's conjecture.*

Proof. The important point here is that the archimedean analogue of the statement of Leopoldt's conjecture is known to be true; this is the classical nonvanishing of the regulator of a number field. More precisely, if we fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and let $N = \big(\log|\sigma_j(u_i)|\big)$, where the absolute value denotes the usual absolute value on $\mathbb{C}$, then we have

$$\operatorname{rank}_{\mathbb{C}}(N) = r.$$

This is proved using the fact that $\log|\cdot|$ takes values in the ordered field $\mathbb{R}$ (whereas $\log_p$ does not). For this reason, the p-adic statement lies far deeper than the archimedean one.

The field $\mathbb{Q}(x_1, \dots, x_k)$ appearing in the definition of the structural rank provides a bridge between the p-adic and complex settings, with the p-adic structural rank conjecture doing most of the heavy lifting.

Let $\{c_1, \dots, c_k\} \subset \{\sigma_j(u_i)\}$ be such that $\{\log_p(c_i)\}$ is a $\mathbb{Q}$-basis for the $\mathbb{Q}$-vector space spanned by the $\log_p(\sigma_j(u_i))$. Write

$$M = (\log_p \sigma_j(u_i)) = \sum_{i=1}^{k} M_i \log_p(c_i)$$

with $M_i \in M_{r\times n}(\mathbb{Q})$. The p-adic structural rank conjecture implies that

$$\begin{aligned}
\operatorname{rank}_{\mathbb{C}_p} M &= \operatorname{rank}_{\mathbb{Q}(x_1,\dots,x_k)}\left(\sum_{i=1}^{k} M_i x_i\right) \\
&\geq \operatorname{rank}_{\mathbb{C}}\left(\sum_{i=1}^{k} M_i \log|c_i|\right) \\
&= \operatorname{rank}_{\mathbb{C}}\big(\log|\sigma_j(u_i)|\big) \qquad (29) \\
&= r.
\end{aligned}$$

Hence, $\operatorname{rank}_{\mathbb{C}_p} M \geq r$, and so we must have equality. Note that in the equality (29), we are implicitly using the fact that, if $u_i \in \overline{\mathbb{Q}}^*$ are p-adic units and $m_i \in \mathbb{Z}$ are

integers, then

$$\sum m_i \log_p(u_i) = 0 \implies \prod u_i^{m_i} \text{ is a root of unity} \implies \sum m_i \log|u_i| = 0. \quad \square$$

Let us describe two applications of Leopoldt's conjecture.

Algebraic (*Iwasawa theory*). By class field theory, Leopoldt's conjecture implies that the maximal pro-p abelian extension of F unramified outside p has $\mathbb{Z}_p$-rank equal to $r_2 + 1$, where $2r_2$ is the number of embeddings $F \hookrightarrow \mathbb{C}$ with image not contained in $\mathbb{R}$. See for example the exercises in [Neukirch 1999, page 394].

Analytic (*p-adic L-functions*). Let F be a totally real field, so

$$r = \operatorname{rank} \mathcal{O}_F^* = [F : \mathbb{Q}] - 1.$$

There is a p-adic analogue of the classical Dedekind zeta function of F, denoted by $\zeta_{F,p}$. A theorem of Colmez [1988] states that

$$\lim_{s \to 1} (s-1)\zeta_{F,p}(s) = (*)R_p(F), \tag{30}$$

where

$$R_p(F) = \pm \det\bigl(\log_p(\sigma_j(u_i))_{i,j=1,\dots,r}\bigr) \tag{31}$$

and $(*)$ denotes a specific nonzero algebraic number, which we do not describe precisely here. Note that, since there are $r+1$ embeddings σ_j, the last one has been excluded in the definition of $R_p(F)$. Which embedding is excluded, as well as the ordering of the remaining embeddings, only affects the determinant in (31) up to sign; the unspecified $\pm$ in (31) includes an orientation (a sign) that makes the product independent of choices.

Colmez's formula (30) is a p-adic "class number formula". It implies that $\zeta_{F,p}(s)$ has a pole at $s = 1$ if and only if Leopoldt's conjecture for (F, p) holds.

4B2. *The Gross–Kuz'min conjecture.* There is an analogue of Leopoldt's conjecture due independently to Gross and Kuz'min concerning p-adic L-functions at $s = 0$ rather than $s = 1$. Unlike the case of classical L-functions, there is no functional equation for p-adic L-functions relating the values at 0 and 1.

We refer the reader to [Gross 1981] for details about the Gross–Kuz'min conjecture beyond what we write below. To state the conjecture, let H be a CM field and H^+ its maximal totally real subfield. Let

$$U_p^- = \{u \in H^* : |u|_w = 1 \text{ for all } w \nmid p\}.$$

Here w ranges over all places of H that do not divide p, including the archimedean ones. Then $\operatorname{rank}(U_p^-) = r$, where r is the number of primes of H^+ above p that split completely in H.

Let X_p denote the $\mathbb{C}_p$-vector space with basis indexed by the places of H above p. Let c denote the nontrivial element of $\mathrm{Gal}(H/H^+)$, i.e., c is complex conjugation. Let X_p^- denote the largest quotient of X_p on which c acts as -1. Then X_p^- has dimension r. We define two maps

$$\ell_p, o_p : U_p^- \to X_p^-.$$

The coordinate of $o_p(u)$ at the component corresponding to a place $\mathfrak{P}$ of H is $\mathrm{ord}_{\mathfrak{P}}(u)$, and the coordinate of $\ell_p(u)$ is $\log_p(\mathrm{N}_{H_{\mathfrak{P}}/\mathbb{Q}_p}(u))$. We extend ℓ_p and o_p to $\mathbb{C}_p$-linear maps

$$U_p^- \otimes \mathbb{C}_p \to X_p^-.$$

It is not hard to show using Dirichlet's unit theorem that o_p is an isomorphism, and we define

$$R_p^-(H) = \det(\ell_p \circ o_p^{-1}).$$

Conjecture 4.7 (Gross–Kuz'min). *We have* $R_p^-(H) \neq 0$.

A proof similar to the proof of Proposition 4.6 shows that the p-adic structural rank conjecture implies the Gross–Kuz'min conjecture (one uses ord_p in place of $\log|\cdot|$). Once again there are algebraic and analytic interpretations of this conjecture.

Algebraic (*Iwasawa theory*). By class field theory, the Gross–Kuz'min conjecture implies a bound on the growth of the p-parts of class groups of fields in the cyclotomic $\mathbb{Z}_p$-extension of H. See [Federer and Gross 1981, Proposition 3.9] for details.

Analytic (*p-adic L-functions*). Let χ denote the nontrivial character of $\mathrm{Gal}(H/H^+)$. Then one knows that

$$\mathrm{ord}_{s=0} L_p(\chi\omega, s) \geq r.$$

This follows for odd p by work of Wiles [1990]; an alternative proof using the Eisenstein cocycle that works for all p was given in [Charollois and Dasgupta 2014; Spiess 2014] using an argument of Spiess. In joint work with Darmon and Pollack then with Kakde and Ventullo [Dasgupta et al. 2011; 2018], we proved that

$$L_p^{(r)}(\chi\omega, 0) = (*)R_p^-(H),$$

where $(*)$ is a specific nonzero rational number. This is a p-adic class number formula at $s = 0$. Therefore, $L_p(\chi\omega, s)$ has a zero of order exactly r at $s = 0$ if and only if the Gross–Kuz'min conjecture is true.

4B3. *Representation-theoretic considerations.* Retaining the setting of the Gross–Kuz'min conjecture, suppose now that H contains a totally real field F such that

H/F is Galois. Let $G = \mathrm{Gal}(H/F)$. For any representation M of G over $\mathbb{C}_p$, and character χ of an irreducible representation V, let M^χ denote the χ-isotypic component of M (i.e., the span of the subrepresentations of M isomorphic to V).

Then

$$U_p^- = \bigoplus_\chi U_p^\chi, \quad X_p^- = \bigoplus_\chi X_p^\chi,$$

where the sums range over the characters χ of irreducible representations V of G on which c acts as -1. The maps ℓ_p and o_p also decompose as sums of maps

$$\ell_p^\chi, o_p^\chi : U_p^\chi \to X_p^\chi.$$

We define

$$R_p^\chi(H) = \det(\ell_p^\chi \circ (o_p^\chi)^{-1}).$$

We then have

$$R_p^-(H) = \prod_\chi R_p^\chi(H). \tag{32}$$

Now, for χ as above,

$$r_p^\chi := \dim_{\mathbb{C}_p} U_p^\chi = \dim_{\mathbb{C}_p} X_p^\chi = \sum_{\mathfrak{p}\mid p} \dim_{\mathbb{C}_p} V^{G_\mathfrak{p}},$$

where the sum ranges over the primes of F above p, $G_\mathfrak{p} \subset G$ denotes the decomposition group of a prime of H above $\mathfrak{p}$, and $V^{G_\mathfrak{p}}$ denotes the maximal subspace of V invariant under $G_\mathfrak{p}$. When $r_p^\chi = 1$, the regulator $R_p^\chi(H)$ is a $\overline{\mathbb{Q}}$-linear combination of p-adic logarithms of algebraic numbers. As pointed out in Proposition 2.13 of Gross [1981], the nonvanishing of $R_p^\chi(H)$ follows from the theorem of Brumer and Baker (Theorem 4.3) in this case.

Theorem 4.8. *If $r_p^\chi = 1$, then $R_p^\chi(H) \neq 0$.*

There is a particular case when *every* $r_p^\chi \leq 1$. If F contains only one prime above p (for example $F = \mathbb{Q}$), and G is abelian (so every V has dimension 1), then clearly $r_p^\chi \leq 1$. Combining Theorem 4.8 with the factorization (32), we obtain:

Corollary 4.9. *Let F be a totally real field with exactly one prime above p, and let H be a CM abelian extension of F. Then the Gross–Kuz'min conjecture holds for H.*

A similar analysis holds for Leopoldt's conjecture, and one obtains:

Theorem 4.10 [Brumer 1967, Theorem 2]. *Leopoldt's conjecture holds for abelian extensions of $\mathbb{Q}$.*

4C. ***A theorem of Roy.*** Damien Roy has proven a number of beautiful results in transcendence theory. We prove one of these now.

Theorem 4.11 (Roy). *The structural rank conjecture is equivalent to the special case of Schanuel's conjecture that states that, if* $y_1, \ldots, y_n \in \mathscr{L}$ *are* $\mathbb{Q}$*-linearly independent, then*

$$\operatorname{trd}_{\mathbb{Q}} \mathbb{Q}(y_1, \ldots, y_n) = n.$$

Similarly, the p-adic structural rank conjecture is equivalent to the p-adic version of the special case of Schanuel's conjecture, but we will content ourselves with the archimedean setting here. Theorem 4.11 is proven in [Roy 1995].

One direction of Roy's theorem is relatively elementary.

Lemma 4.12. *The special case of Schanuel's conjecture implies the structural rank conjecture.*

Proof. We assume the special case of Schanuel's conjecture. We first consider a matrix M with entries in $\mathscr{L}$. Let $M = \sum M_i c_i$ with $M_i \in M_{m\times n}(\mathbb{Q})$ and $c_i \in \mathscr{L}$ linearly independent over $\mathbb{Q}$. Write

$$M_x = \sum M_i x_i \in M_{m\times n}(\mathbb{Q}(x_1, \ldots, x_n))$$

and let $r = \operatorname{rank}(M_x)$. Let J_x be an $r \times r$ submatrix of M_x such that

$$\det(J_x) = P(x_1, \ldots, x_n) \neq 0$$

in $\mathbb{Q}[x_1, \ldots, x_n]$. The determinant of the corresponding submatrix of M is equal to $P(c_1, \ldots, c_n)$ and hence cannot vanish since the c_i are algebraically independent, by the special case of Schanuel's conjecture. Therefore, $\operatorname{rank}(M) \geq r$. Of course, it is clear that $\operatorname{rank}(M) \leq r$, so we get equality.

Now assume M has entries in $\mathscr{L} + \mathbb{Q}$, but not in $\mathscr{L}$. There are two cases.

Case 1: 1 is not in the $\mathbb{Q}$-linear span of the entries of M. The $\mathbb{Q}$-basis for this span can be taken to have the form $\{1 + c_1, c_2, \ldots, c_n\}$, where $c_i \in \mathscr{L}$. It is easy to check that the c_i must be $\mathbb{Q}$-linearly independent, and hence, by the special case of Schanuel's conjecture, they are algebraically independent. The same is therefore true of $\{1 + c_1, c_2, \ldots, c_n\}$. The previous proof then applies to this basis.

Case 2: 1 is in the $\mathbb{Q}$-linear span of the entries of M. We may take a $\mathbb{Q}$-basis of this span of the form $\{c_0 = 1, c_1, \ldots, c_n\}$, where $c_i \in \mathscr{L}$ for $i \geq 1$. We proceed as before. Write

$$M = \sum_{i=0}^{n} M_i c_i, \quad M_x = \sum_{i=0}^{n} M_i x_i.$$

Let $r = \operatorname{rank}(M_x)$ and J_x an $r \times r$ submatrix of M_x with

$$\det(J_x) = P(x_0, \ldots, x_n) \neq 0.$$

The determinant of the corresponding submatrix J of M is $P(1, c_1, \ldots, c_n)$. Since P is a nonzero homogeneous polynomial of degree r, its specialization $P(1, x_1, \ldots, x_n)$ is also nonzero, so $\det(J) = P(1, c_1, \ldots, c_n) \neq 0$ by the algebraic independence of the c_i. Therefore, $\operatorname{rank}(M) \geq r$, as desired. □

The main content of the converse is in the following lemma:

Lemma 4.13. *Let k be a commutative ring and let $P \in k[x_1, \ldots, x_n]$. There exists a square matrix N with entries in*

$$k + kx_1 + \cdots + kx_n$$

such that $\det(N) = P$.

Let us for the moment take the lemma for granted and prove Roy's theorem.

Proof of Theorem 4.11. Assume the structural rank conjecture. Suppose $c_1, \ldots, c_n \in \mathscr{L}$ are linearly independent over $\mathbb{Q}$ and that $P(c_1, \ldots, c_n) = 0$ for some nonzero $P \in \mathbb{Q}[x_1, \ldots, x_n]$. As in Lemma 4.13, let N be a square matrix with entries in $\mathbb{Q} + \mathbb{Q}x_1 + \cdots + \mathbb{Q}x_n$ such that $\det(N) = P$.

Let M be the matrix N with x_i replaced by c_i. We then have $\det(M) = 0$. Note that the matrix M_x in the structural rank conjecture is the homogenization of the matrix N, with entries in $\mathbb{Q}x_0 + \mathbb{Q}x_1 + \cdots + \mathbb{Q}x_n$. We are using here that the c_i are $\mathbb{Q}$-linearly independent from 1, since e is transcendental. The conjecture implies that $\det(M_x) = 0$, whence $\det(N) = 0$ by specializing $x_0 = 1$, a contradiction. □

It remains now to prove Lemma 4.13. We first remark that this lemma is actually the starting point of an important avenue of research in theoretical computer science, where the lemma is usually attributed to Valiant [1979]. There are well-known efficient algorithms for calculating the determinant of a matrix, so expressing a general polynomial as a determinant gives an algorithm for efficiently calculating values of a polynomial. The minimal dimension of a matrix necessary to express a given polynomial as a determinant is known as the *determinantal complexity* of the polynomial. The study of the growth of determinantal complexity in families of polynomials is a topic with an extensive literature.

We follow Roy's proof of Lemma 4.13. We will prove the more general statement that, given any matrix $N \in M_{m\times m}(P_d)$, there exists a matrix $N' \in M_{m'\times m'}(P_1)$ such that $\det(N) = \det(N')$. Lemma 4.13 is the case where we start with an element $N \in P_d$, which we view as a 1×1 matrix. The advantage of the more general statement is that it may be proven by induction on d. We need to establish two sublemmas. The first establishes that, given a matrix $N \in M_{m\times m}(P_d)$, we may write it as a product of matrices with entries in spaces $P_{d'}$ with $d' < d$. The matrices that arise in the proof are not necessarily square, and this is resolved by the second lemma.

Lemma 4.14. *For a nonnegative integer d, let $P_d \subset k[x_1, \ldots, x_n]$ denote the k-subspace of polynomials of total degree $\leq d$. Given $N \in M_{m\times m}(P_d)$ with $d \geq 1$, there exists an integer s and matrices*

$$A \in M_{m\times s}(P_{d-1}), \quad B \in M_{s\times m}(P_1)$$

such that $N = AB$.

Proof. Let $N = (a_{i,j})$ with $a_{i,j} \in P_d$. We can write

$$a_{i,j} = \sum_{\ell=1}^{n} c_{i,j,\ell} x_\ell + c_{i,j,n+1}$$

with $c_{i,j,\ell} \in P_{d-1}$ for $1 \leq \ell \leq n+1$. Let

$$c_{i,j} = (c_{i,j,\ell}) \in M_{1\times(n+1)}(P_{d-1}), \quad x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \\ 1 \end{pmatrix} \in M_{(n+1)\times 1}(P_1).$$

Define

$$A = (c_{i,j}) \in M_{m\times m(n+1)}(P_{d-1}), \quad B = x \otimes 1_{m\times m} \in M_{(n+1)m\times m}(P_1).$$

Then one calculates that $N = AB$. □

The matrices A and B in Lemma 4.14 are not square, so we cannot recursively apply the lemma. This is resolved by the following observation:

Lemma 4.15. *Let $A \in M_{m\times s}$, $B \in M_{s\times m}$. Then*

$$\det(AB) = \det \begin{pmatrix} I_s & B \\ -A & 0 \end{pmatrix},$$

where the matrix on the right is square of dimension $m + s$.

Proof. We simply note that

$$\begin{pmatrix} I_s & 0 \\ A & I_m \end{pmatrix} \begin{pmatrix} I_s & B \\ -A & 0 \end{pmatrix} \begin{pmatrix} I_s & -B \\ 0 & I_m \end{pmatrix} = \begin{pmatrix} I_s & 0 \\ 0 & AB \end{pmatrix}$$

and take determinants of both sides. □

We can now prove our main lemma.

Proof of Lemma 4.13. As indicated above, we will show by induction on d that, for any matrix $N \in M_{m\times m}(P_d)$, there exists a matrix $N' \in M_{m'\times m'}(P_1)$ such that $\det(N) = \det(N')$.

The base case $d = 1$ is trivial. For $d > 1$ we use Lemma 4.14 to write $N = AB$ with $A \in M_{m\times s}(P_{d-1})$ and $B \in M_{s\times m}(P_1)$. Lemma 4.15 then yields $\det(N) = \det(N')$ with $N' \in M_{(m+s)\times(m+s)}(P_{d-1})$. The induction is now complete.

The lemma is the case where we start with a 1×1 matrix in P_d. □

5. The theorem of Waldschmidt and Masser

To our knowledge, the strongest general unconditional result toward the structural rank conjecture is Theorem 1.6 of Waldschmidt and Masser, stated in the introduction. For the sake of variety, we will prove the p-adic version of the conjecture in this section, though the proof of the archimedean version is essentially the same (both versions are proven in [Waldschmidt 1981]). The statement of the p-adic version is exactly the same as the archimedean one, with $\mathscr{L}$ replaced by $\mathscr{L}_p$.

Theorem 5.1 (Waldschmidt and Masser). *Let m and n be positive integers and let $M \in M_{m\times n}(\mathscr{L}_p)$. Suppose that*

$$\operatorname{rank}(M) < \frac{mn}{m+n}.$$

Then there exist $P \in \mathrm{GL}_m(\mathbb{Q})$ and $Q \in \mathrm{GL}_n(\mathbb{Q})$ such that

$$PMQ = \begin{pmatrix} M_1 & 0 \\ M_2 & M_3 \end{pmatrix},$$

where the 0 block has dimension $m' \times n'$ with $m'/m + n'/n > 1$.

5A. ***Applications.*** Let us first state some applications of the complex and p-adic Waldschmidt–Masser theorems. The six exponentials theorem, which had been proven earlier in the 1960s, is a corollary of the Waldschmidt–Masser theorem.

Proof of Theorem 4.2. The case where $M = 0$ is trivial. Therefore suppose $M \in M_{2\times 3}(\mathscr{L})$ has rank 1. Since $1 < \frac{6}{5}$, the Waldschmidt–Masser theorem implies that, after a rational change of basis on the left and right, the matrix M has the block matrix form

$$PMQ = \begin{pmatrix} M_1 & 0 \\ M_2 & M_3 \end{pmatrix},$$

where the 0 block has dimension 1×2 or 2×1. In the first case, our matrix has the form

$$PMQ = \begin{pmatrix} * & 0 & 0 \\ * & * & * \end{pmatrix}.$$

Such a matrix has rank 1 only if it has the form

$$PMQ = \begin{pmatrix} 0 & 0 & 0 \\ * & * & * \end{pmatrix} \quad \text{or} \quad PMQ = \begin{pmatrix} * & 0 & 0 \\ * & 0 & 0 \end{pmatrix}.$$

In the first case, we see that PM has the same shape, which says that the rows of M are linearly dependent over $\mathbb{Q}$. In the second case, we see that MQ has the same shape, which says that the columns of M are linearly dependent over $\mathbb{Q}$. The case where the original block of zeroes has dimension 2×1 is similar. □

In the case of a square matrix, the Waldschmidt–Masser theorem simplifies to the following:

Corollary 5.2. *Let $M \in M_{n\times n}(\mathscr{L})$ or $M_{n\times n}(\mathscr{L}_p)$. Suppose that* $\operatorname{rank}(M) < \frac{1}{2}n$. *Then there exist P, $Q \in \mathrm{GL}_n(\mathbb{Q})$ such that*

$$PMQ = \begin{pmatrix} M_1 & 0 \\ M_2 & M_3 \end{pmatrix} \quad (\textit{block matrix})$$

where the 0 *block has dimension $m \times m'$ with $m + m' > n$.*

Corollary 5.3. *The Leopoldt regulator matrix and the Gross–Kuz'min regulator matrix have rank at least half their expected ranks.*

Proof. Let r be the expected rank of the Leopoldt matrix. Let

$$M' = \left(\log|\sigma_j(u_i)|\right)_{i,j=1,\dots,r}$$

be an $r \times r$ submatrix of the *archimedean* regulator with $\det(M') \neq 0$. Let

$$M = (\log_p \sigma_j(u_i))_{i,j=1,\dots,r}$$

be the corresponding submatrix of the Leopoldt matrix.

If the rank of the Leopoldt matrix is less than $\frac{1}{2}r$, the same is true for M. The Waldschmidt–Masser theorem then implies that there exist P, $Q \in \mathrm{GL}_r(\mathbb{Q})$ such that PMQ has an upper right 0 block with dimension $m \times m'$, where $m + m' > r$. But then $PM'Q$ has this same property. This implies that $\det(M') = 0$, a contradiction.

The same proof works for Gross's regulator, using ord_p instead of $\log|\cdot|$. □

5B. ***Auxiliary polynomial.*** As in the proof of Baker's theorem, the Waldschmidt–Masser theorem is proven by constructing, under the assumptions of the theorem, a suitable auxiliary polynomial whose existence implies the conclusion of the theorem. Waldschmidt's result is that the auxiliary polynomial exists, and Masser's theorem is that this polynomial gives the desired conclusion. Let us describe this in greater detail.

We have $M = (a_{i,j})$ with $a_{i,j} = \log_p(x_{i,j}) \in \mathscr{L}_p$. Here $x_{i,j} \in \overline{\mathbb{Q}}^*$. After scaling M if necessary, we may assume that $|x_{i,j} - 1|_p < 1$. For $i = 1, \dots, m$, let

$$x_i = (x_{i,j})_{j=1,\dots,n} \in (\overline{\mathbb{Q}}^*)^n \subset (\mathbb{C}_p^*)^n.$$

Let $X = \langle x_1, x_2, \dots, x_m \rangle \subset (\overline{\mathbb{Q}}^*)^n$ be the subgroup generated by the x_i. For each positive integer N, define

$$X(N) = \left\{ \prod_{i=1}^{m} x_i^{a_i} \;\middle|\; a_i \in \mathbb{Z},\ 0 \le a_i \le N \right\}.$$

For a polynomial P in several variables, we write $\deg(P)$ for the total degree of P.

Theorem 5.4 [Waldschmidt 1981]. *Suppose* $r = \operatorname{rank}(M) < mn/(m+n)$. *There exists* $\epsilon > 0$ *such that, for all* N *sufficiently large, there exists a nonzero* $P \in \mathbb{Z}[t_1, \ldots, t_n]$ *such that* $\deg(P) < N^{m/n-\epsilon}$ *and* $P(x) = 0$ *for all* $x \in X(N)$.

Waldschmidt's theorem is the "transcendence" part of Theorem 1.6. Masser's theorem, which is a purely algebrogeometric statement, takes the existence of an auxiliary polynomial P as above and deduces the relations necessary to give the desired result about the original matrix M. We will describe the statement of Masser's theorem precisely in a moment, but first let us comment about the numerology concerning the auxiliary polynomial in the statement of Theorem 5.4. We can view the existence of a polynomial with prescribed zeroes as a system of linear equations in the coefficients of the polynomial. Each zero gives one such linear equation. If the $x_{i,j}$ are generic, the size of $X(N)$ is $(N+1)^m$. A polynomial of degree $< d$ has fewer than d^n coefficients. Therefore, if the $x_{i,j}$ are generic, we expect that we would require $d^n \geq (N+1)^m$ for a polynomial to exist, so, in particular, $d > N^{m/n}$. For this reason, the existence of the auxiliary polynomial P in Theorem 5.4 does not hold for generic $x_{i,j}$.

Let us now state Masser's theorem precisely. Let k be a field of characteristic 0, let $(x_{i,j}) \in M_{m\times n}(k^*)$. Define X and $X(N)$ as above. Define a pairing

$$\mathbb{Z}^m \times \mathbb{Z}^n \to k^*, \quad \langle (a_i), (b_j) \rangle = \prod_{i,j} x_{i,j}^{a_i b_j}.$$

Theorem 5.5 [Masser 1981]. *Let* $N > 0$ *and suppose there exists* $P \in k[t_1, \ldots, t_n]$ *such that* $\deg(P) < (N/n)^{m/n}$ *and* $P(x) = 0$ *for all* $x \in X(N)$. *Then there exist subgroups* $A \subset \mathbb{Z}^m$ *and* $B \subset \mathbb{Z}^n$ *of ranks* m' *and* n', *respectively, with* $\langle A, B \rangle = 1$ *and* $m'/m + n'/n > 1$.

Theorems 5.4 and 5.5 combine to give Theorem 5.1. In the remainder of this section, we prove these two theorems.

5C. ***Waldschmidt's theorem.*** We will give two proofs of Waldschmidt's theorem.

5C1. *Proof* 1 *of Waldschmidt's theorem.* Our first proof is similar in spirit to Waldschmidt's original proof. For simplicity, we will assume $x_{i,j} \in \mathbb{Z}$ and $x_{i,j} \equiv 1 \pmod{p}$. Standard techniques (scaling by an integer to obtain algebraic integers, and taking norms to obtain integers) allow one to handle the general case, but we would like to avoid the extra notation required.

Let r denote the rank of the matrix $M \in M_{m\times n}(\mathbb{Z}_p)$. After reordering columns if necessary, we can assume that the last $n-r$ columns of M are in the $\mathbb{Z}_p$-linear span of the first r columns. Then, for each $i > r$, there exist $\lambda_{i,1}, \ldots, \lambda_{i,r} \in \mathbb{Z}_p$ such that, if $z = (z_1, \ldots, z_n) \in X$, we have

$$z_i = z_1^{\lambda_{i,1}} z_2^{\lambda_{i,2}} \cdots z_r^{\lambda_{i,r}} \quad \text{for } i > r. \tag{33}$$

To make sense of the right-hand side of this equality, note that, for $\lambda \in \mathbb{Z}_p$, the function

$$t^\lambda = (1 + (t-1))^\lambda = \sum_{i=0}^{\infty} \binom{\lambda}{i} (t-1)^i \tag{34}$$

is a convergent power series in $t-1$. Hence, if $t \in 1 + p\mathbb{Z}_p$, then (34) converges in $\mathbb{Z}_p$.

Our goal is to find a polynomial $P \in \mathbb{Z}[t_1, \ldots, t_n]$ such that $P(z) = 0$ for $z \in X(N)$. Define $u_i = t_i - 1$ and consider the canonical map

$$\varphi : \mathbb{Z}[t_1, \ldots, t_n] \to \mathbb{Z}_p[\![u_1, \ldots, u_n]\!]/(t_i - t_1^{\lambda_{i,1}} \cdots t_r^{\lambda_{i,r}})_{i=r+1}^n \cong \mathbb{Z}_p[\![u_1, \ldots, u_r]\!]. \tag{35}$$

The elements in the quotient in (35) are interpreted as power series in the u_i via (34).

Fix a positive integer c. Define φ_c to be the composition of φ with the canonical reduction

$$\mathbb{Z}_p[\![u_1, \ldots, u_r]\!] \to (\mathbb{Z}/p^c\mathbb{Z})[\![u_1, \ldots, u_r]\!]/(u_1^c, \ldots, u_r^c). \tag{36}$$

If a polynomial $P \in \mathbb{Z}[t_1, \ldots, t_n]$ satisfies $\varphi_c(P) = 0$, then $P(z)$ will be divisible by p^c for any $z \in X$. Indeed, $\varphi(P)(z) = P(z)$ is well defined for $z \in X$, since the kernel of φ vanishes on X. Next, it is clear that $\varphi(P)(z) \pmod{p^c}$ depends only on the coefficients of $\varphi(P)$ modulo p^c. Finally, we note that

$$z_i \equiv 1 \pmod{p} \implies u_i \equiv 0 \pmod{p} \implies u_i^c \equiv 0 \pmod{p^c}.$$

Now, the ring on the right in (36) is finite. The total number of monomials in $u_1, \ldots, u_r$ modulo $(u_1^c, \ldots, u_r^c)$ is c^r, so the total number of possible values of these coefficients mod p^c is

$$(p^c)^{c^r} = p^{c^{r+1}}.$$

Therefore, by the pigeonhole principle, if we have a subset of $\mathbb{Z}[t_1, \ldots, t_n]$ of size greater than $p^{c^{r+1}}$, then some two elements of the subset, say P_1 and P_2, will have equal image under φ_c, and the difference $P = P_1 - P_2$ will satisfy $P(z) \equiv 0 \pmod{p^c}$ for all $z \in X$.

We will take the subset of all polynomials with degree in each variable less than some constant d with coefficients that are nonnegative integers less than p^h for some constant h. The size of this subset is p^{hd^n}, and hence the condition that we want is

$$hd^n > c^{r+1}. \tag{37}$$

Now, we also want to use the principle of "discreteness of the integers" discussed in the proof of Baker's theorem to ensure that the condition $P(z) \equiv 0 \pmod{p^c}$ for $z \in X(N)$ implies that $P(z) = 0$. For this, we need a crude bound on $|P(z)|$ (the archimedean absolute value). Suppose that A is an upper bound on $|x_{i,j}|$. Then, for

each $z = (z_1, \ldots, z_n) \in X(N)$, we have $|z_i| < A^{Nm}$. Therefore, each monomial in the evaluation of $P(z)$ has absolute value at most $p^h A^{Ndmn}$, and in total we obtain

$$|P(z)| < d^n p^h A^{Ndmn}.$$

Therefore, if

$$d^n p^h A^{Ndmn} < p^c, \tag{38}$$

then we indeed have the implication

$$P(z) \equiv 0 \pmod{p^c} \implies P(z) = 0.$$

To prove the theorem, we set $d = \lfloor N^{m/n-\epsilon}/n \rfloor$, so that the constructed polynomial P will have degree less than $N^{m/n-\epsilon}$, as required. We search for parameters h and c such that both (37) and (38) hold. Not surprisingly, these inequalities are pulling in the opposite direction — the first says that h is large relative to c, and the second says that h is small relative to c. For N large, the two inequalities will be satisfied if

$$h \cdot N^{m-n\epsilon} \gg c^{r+1}, \quad c > k \log N + h + k' N^{(m+n)/n-\epsilon}$$

for the appropriate constants k and k'.

If we set $c = N^{(m+n)/n+\epsilon}$ and $h = cN^{-\delta}$ for a small $\delta > 0$, then it is clear that the second inequality will hold for N sufficiently large. Plugging these parameters into the first inequality yields

$$m - \delta > \left(\frac{m}{n} + 1 + \epsilon\right) r.$$

It is clear that we can choose small positive δ and ϵ satisfying this inequality if

$$m > \left(\frac{m}{n} + 1\right) r, \quad \text{i.e., } r < \frac{mn}{m+n}.$$

This completes the proof.

5C2. *Proof 2 of Waldschmidt's theorem.* For our second proof, we will return to the completely general case, i.e., we do not assume that $x_{i,j} \in \mathbb{Z}$, only that $x_{i,j} \in \overline{\mathbb{Q}}^*$. Our motivation in giving the second proof is that it introduces an important topic in transcendence theory not discussed earlier, namely the theory of *interpolation determinants* pioneered by Michel Laurent. Laurent [1991] gave a new proof of the six exponentials theorem using his new theory. The basic idea is that we will view the existence of the desired polynomial P as the solution of a linear system of equations in the coefficients of the polynomial, and show that the associated determinant vanishes.

Again we will construct a polynomial P such that the degree in each variable is less than $d = \lfloor N^{m/n-\epsilon}/n \rfloor$ and such that $P(z) = 0$ for all $z \in X(N)$. Consider the matrix whose rows are indexed by our desired zeroes $z \in X(N)$, and columns are

indexed by the exponents

$$y \in \mathbb{Z}^n(d-1) = \{(y_1, \ldots, y_n) \mid 0 \leq y_i \leq d-1\}$$

of the monomials of our desired polynomial,

$$L = (z^y) \in M_{(N+1)^m \times d^n}(\mathbb{C}_p).$$

It suffices to show that $\operatorname{rank}(L) < N^{m-n\epsilon}/n^m < d^n$, as then any nonzero vector in its kernel will be the coefficients of our desired polynomial. Of course, by making ϵ smaller, we can ignore the constant n^m, since $N^\epsilon \gg n^m$ for N large.

We state without proof the following elementary interpretation of the rank of a matrix:

Lemma 5.6. *Let k be a field and suppose that a matrix*

$$(a_{i,j}) \in M_{m \times n}(k)$$

has rank equal to r. Then there exist vectors

$$\beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_n \in k^r$$

such that $a_{i,j} = \langle \beta_i, \gamma_j \rangle$.

In our situation, we have $M = \log_p(x_{i,j}) \in M_{m \times n}(\mathbb{C}_p)$ with rank r. We write

$$\log_p(x_{i,j}) = \langle \beta_i, \gamma_j \rangle \quad \text{for } \beta_i, \gamma_j \in \mathbb{C}_p^r.$$

Without loss of generality, we can scale all the β_i and γ_j to assume all their coordinates have absolute value $< p^{-1}$. (This just scales the matrix M, which affects neither the assumptions nor conclusions of the theorem.)

If $z = \prod_{i=1}^m x_i^{\ell_i}$ for $\ell \in \mathbb{Z}^m$, then, for $y \in \mathbb{Z}^n$, we have

$$z^y = \exp\left\langle \sum \beta_i \ell_i, \sum \gamma_j y_j \right\rangle.$$

Next we will require a p-adic Schwarz' lemma. For a positive integer d and real $R > 0$, define

$$B_d(R) = \{(z_1, \ldots, z_d) : |z_i| \leq R \text{ for all } i\} \subset \mathbb{C}_p^d.$$

For analytic $f : B_d(R) \to \mathbb{C}_p$, define

$$|f|_R = \max_{z \in B_d(R)} |f(z)|. \tag{39}$$

Lemma 5.7. *Suppose that $f : B_1(R) \to \mathbb{C}_p$ is analytic and has a zero of order at least n at $z = 0$. Then, for any $0 < R' < R$, we have*

$$|f|_{R'} \leq \left(\frac{R}{R'}\right)^{-n} |f|_R.$$

Proof. Let $g(z) = f(z)/z^n$. This is analytic on $B_1(R)$ since f has a zero of order at least n at $z = 0$. For any $z \in B_1(R')$, we have

$$|f(z)| \le (R')^n |g(z)| \le (R')^n |g|_R = \left(\frac{R'}{R}\right)^n |f|_R.$$

The last equality uses the p-adic maximal modulus principle, which states that the maximum in (39) is achieved on the boundary $|z| = R$. See [Cherry 2009, Theorem 1.4.1] or [Stansifer 2012, Theorem 7] for a proof of this analytic fact. □

Now we present Laurent's main theorem on interpolation determinants.

Theorem 5.8 (Laurent). *Let $0 < R' < R$ and let $f_1, \dots, f_d$ be analytic functions*

$$B_r(R) \to \mathbb{C}_p.$$

Let $z_1, \dots, z_d \in B_r(R')$. Then $L = \det(f_j(z_i))$ satisfies

$$|L| \le \left(\frac{R}{R'}\right)^{-\Theta_r(d)} \prod_{i=1}^{d} |f_i|_R,$$

where, for d sufficiently large relative to r,

$$\Theta_r(d) > \frac{r}{6e} d^{(r+1)/r}. \tag{40}$$

Proof. Define $\Delta(z) = \det(f_j(z_i z))$, which is analytic on $|z| \le R/R'$. We will show that $\Delta(z)$ has a zero of order at least $\Theta_r(d)$ at $z = 0$ for some combinatorial function Θ_r satisfying (40), which we will define in a moment. The result then follows from Schwarz' lemma:

$$|L| = |\Delta(1)| \le \left(\frac{R}{R'}\right)^{-\Theta_r(d)} |\Delta|_{R/R'}$$

using the trivial upper bound

$$|\Delta|_{R/R'} \le \prod_{i=1}^{d} |f_i|_R.$$

(Note that, in the complex case, we would need a factor of $d!$ on the right, but, in the nonarchimedean setting, this factor is not required because of the strong triangle inequality.)

Write each f_i as a power series in the variables $u_1, \dots, u_r \in \mathbb{C}_p$. By multilinearity of the determinant, it suffices to consider the case $f_j(u) = u^{v_j} = u_1^{v_{1j}} u_2^{v_{2j}} \cdots u_r^{v_{rj}}$ for nonnegative integers v_{ij}. Then

$$\Delta(z) = z^{\sum_j \|v_j\|} \det(z_i^{v_j}),$$

where $\|v_j\| = v_{j1} + v_{j2} + \cdots + v_{jr}$. If any two tuples v_j are equal, this determinant vanishes and $\Delta(z)$ is identically 0. If not, then the order of vanishing is at least

$$\Theta_r(d) := \min\left\{ \sum_{j=1}^{d} \|v_j\| \;\middle|\; v_1, \ldots, v_d \in (\mathbb{Z}^{\geq 0})^r \text{ with } v_i \neq v_j \text{ if } i \neq j \right\}.$$

For example, $\Theta_1(d) = \frac{1}{2}d(d-1)$. For a proof of the combinatorial inequality (40), see [Waldschmidt 1992, Lemma 4.3]. □

We can now apply Laurent's theorem to complete the proof of Waldschmidt's theorem. We want to show that any square submatrix $L' = (z_i^y)$ of L of dimension $d^n \approx N^{m-n\epsilon}$ has vanishing determinant, where

$$z_1, \ldots, z_d \in X(N), \quad y \in \mathbb{Z}^n(d-1), \quad d = \lfloor N^{m/n-\epsilon} \rfloor.$$

As explained earlier, the entries of the matrix L' can be written in the form $\exp\left(\left\langle \sum \beta_i \ell_i, \sum \gamma_i y_i \right\rangle\right)$ with $\ell \in \mathbb{Z}^m(N)$ corresponding to z. For each y we have the function

$$f_y(u_1, \ldots, u_r) = \exp\left(\left\langle u, \sum \gamma_i y_i \right\rangle\right)$$

We apply Laurent's theorem on interpolation determinants with $R = 1$ and $R' = 1/p$. We find

$$|L'| \leq C^{-N^{(m-n\epsilon)(r+1)/r}},$$

where $C > 1$ is a constant.

Now we want to put a bound on the archimedean absolute value of L'. Let

$$A = \max_{i,j} |x_{i,j}|_\infty.$$

Then $|z^y|_\infty \leq A^{N \cdot N^{(m/n)-\epsilon} n}$. Therefore,

$$|L'|_\infty \leq (N^{m-n\epsilon})! \cdot D^{N^{(m/n)+1+m-(n+1)\epsilon}}.$$

The factorial is dominated by the other term and can be ignored. Scaling to obtain integrality just scales D. The same is true for taking norm from the field generated by the $x_{i,j}$ down to $\mathbb{Q}$ in order to obtain an element of $\mathbb{Z}$.

Therefore, we will have $L' = 0$ if

$$C^{N^{(m-n\epsilon)(r+1)/r}} > D^{N^{(m/n)+1+m-(n+1)\epsilon}}.$$

Of course, for this inequality to hold for large N, the precise values of C and D do not matter; all that matters is that we have the corresponding inequality of exponents.

It therefore suffices to have

$$(m - n\epsilon)\frac{r+1}{r} > \frac{m}{n} + 1 + m - (n+1)\epsilon.$$

This simplifies to

$$\frac{1}{r} > \frac{m+n}{mn} + \frac{\epsilon}{m}\left(\frac{n-r}{r}\right).$$

There exists $\epsilon > 0$ satisfying this inequality if and only if

$$r < \frac{mn}{m+n}.$$

This gives the desired vanishing of $\det(L')$ and completes the second proof of Waldschmidt's theorem.

5D. ***Masser's theorem.*** We conclude this section by proving Masser's theorem, stated in Theorem 5.5 above. This is a purely algebrogeometric statement that does not involve the logarithm or exponential functions. In particular, we work over an arbitrary field k of characteristic 0. Recall the notation established in Section 5B. We let the group $X \subset (k^*)^n$ act on the polynomial ring $R = k[t_1, \ldots, t_n]$ by

$$z \cdot f = f(z_1 t_1, z_2 t_2, \ldots, z_n t_n).$$

Recall that the subgroup X is generated by elements $x_1, \ldots, x_m$. If $a \in \mathbb{Z}^m$, we write $x^a = \prod_{i=1}^m x_i^{a_i} \in X$. For a prime ideal $\mathfrak{p} \subset R$, let

$$\mathrm{Stab}_X(\mathfrak{p}) = \{a \in \mathbb{Z}^m \mid x^a \cdot \mathfrak{p} = \mathfrak{p}\}.$$

Before delving into the proof, it is instructive to consider the simplest case, $n = m = 2$. We let $N > 0$ and suppose there exists $P \in k[t_1, t_2]$ such that $\deg(P) < N$ and $P(x) = 0$ for all $x \in X(2N)$. We want to show that either

(A) there is a nonzero $a \in \mathbb{Z}^2$ such that $x^a = (1, 1)$ (this corresponds to $m' = 1$ and $n' = 2$), or

(B) there exists a nonzero $b \in \mathbb{Z}^2$ such that $z^b = z_1^{b_1} z_2^{b_2} = 1$ for all $z \in X$ (this corresponds to $m' = 2$ and $n' = 1$).

We factor P into a product $\prod P_i$ of irreducibles of $k[t_1, t_2]$. We can assume that none of the P_i are monomials, since monomials have no zeroes in $(k^*)^2$. We will first show that, if any P_i satisfies $\mathrm{rank}\big(\mathrm{Stab}_X((P_i))\big) = 2$, then we are in the second case above. This follows from Lemma 5.9 below, but it is relatively easy to see in this case explicitly. Indeed, if $t_1^{a_1} t_2^{a_2}$ is a monomial occurring in P_i, then the equation $zP_i = \lambda P_i$ for $z \in X$ and $\lambda \in k^*$ yields

$$z_1^{a_1} z_2^{a_2} = \lambda.$$

Letting $t_1^{a_1'} t_2^{a_2'}$ be some other monomial occurring in P_i (recall we may assume that P_i is not a monomial) we get a similar equation; dividing these two cancels λ, so we obtain

$$z_1^{b_1} z_2^{b_2} = 1,$$

where $b_i = a_i - a_i'$ for $i = 1, 2$ are not both zero. If $\operatorname{rank}\big(\operatorname{Stab}_X((P_i))\big) = 2$, then this holds for all z in a finite-index subgroup of X, so, replacing (b_1, b_2) by an appropriate multiple, we are in case (B).

Therefore, we are left to consider the case where each irreducible factor P_i of P satisfies $\operatorname{rank}\big(\operatorname{Stab}_X((P_i))\big) \leq 1$. In this case, we will show that there is a polynomial of the form

$$Q = \sum_{i=1}^{k} a_i (z_i \cdot P),$$

where $a_i \in \mathbb{Z}$ and $z_i \in X(N)$, such that P and Q are relatively prime. Let us first explain why this completes the proof. Since P vanishes on $X(2N)$, each polynomial $z \cdot P$ with $z \in X(N)$ vanishes on $X(N)$; hence, the polynomial Q vanishes on $X(N)$. Therefore, both P and Q vanish on $X(N)$. The set $X(N)$ has size $(N+1)^2$ *unless* we are in case (A) above. But $\deg Q \leq \deg P < N$, and the polynomials are coprime, so we would obtain a contradiction to Bézout's theorem if these polynomials had $(N+1)^2$ common zeroes. We must therefore be in case (A).

To see the existence of the polynomial Q, we first show that, for each irreducible polynomial P_i, there exists z_i such that $z_i^{-1} \cdot P_i$ does not divide P, or, equivalently, P_i does not divide $z_i \cdot P$. This is established by counting. Since $\operatorname{rank}_X((P_i)) \leq 1$, there are at least $N+1$ distinct ideals among the set $(z^{-1} \cdot P_i)$ as z ranges over $X(N)$. See Lemma 5.12 below for a proof. But P has degree less than N, which is a bound on the number of irreducible factors, so some $z^{-1} \cdot P_i$ must not be a factor of P. With these z_i in hand, the existence of the linear combination Q is an easy inductive argument using the pigeonhole principle; see Lemma 5.13 below.

We now return to the general case. Recall that the *height* $\operatorname{ht}(\mathfrak{p})$ of a prime ideal $\mathfrak{p}$ is the largest integer r such that there exists a chain of distinct prime ideals

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_r = \mathfrak{p}.$$

Lemma 5.9. *Let $\mathfrak{m} = (t_1 - 1, \ldots, t_n - 1)$. Let $\mathfrak{p} \subset \mathfrak{m}$ be a prime of height n' and let $A = \operatorname{Stab}_X(\mathfrak{p})$. There exists a subgroup $B \subset \mathbb{Z}^n$ of rank $\geq n'$ such that $\langle A, B \rangle_X = 1$.*

Proof. Let $B = \{y \in \mathbb{Z}^n \mid \langle A, y \rangle_X = 1\}$. Choose $Z \subset \mathbb{Z}^n$ such that

$$\mathbb{Q}^n = \mathbb{Q}B \oplus \mathbb{Q}Z.$$

We want to show that $s := \operatorname{rank}(Z) \leq n - n'$. Let $\{z_1, \ldots, z_s\}$ be a basis for Z. Write $z_i = (z_{i,1}, \ldots, z_{i,n})$.

For $i = 1, \ldots, s$, let $u_i = \prod_{j=1}^{n} t_j^{z_{i,j}} \in R' = k[t_1^{\pm 1}, \ldots, t_n^{\pm 1}]$. Since

$$\operatorname{trd}_k \operatorname{Frac}(R'/\mathfrak{p}R') = n - n',$$

if $s > n - n'$ then there exists a nonzero polynomial Q with coefficients in k such that $Q(u_1, \ldots, u_s) \in \mathfrak{p}R'$. Suppose this is the case, and write $Q(u_1, \ldots, u_s)$ as a polynomial $Q'(t_1, \ldots, t_n) \in \mathfrak{p}R'$.

For any $a \in A$, we have $x^a \cdot Q' \in \mathfrak{p}R'$, so

$$Q'(x^a t) \in \mathfrak{p}R' \subset \mathfrak{m}R' \implies Q'(x^a) = 0 \implies Q(\langle a, z_1\rangle_X, \ldots, \langle a, z_s\rangle_X) = 0.$$

Fix a and apply this with a replaced by da, as $d = 0, 1, \ldots$. Using the Vandermonde trick from Baker's theorem, we find that some $\mathbb{Z}$-linear combination of the z_i is orthogonal to a. More precisely, we have $\langle a, w\rangle_X = 1$ for some

$$w \in S = \left\{ \sum_{i=1}^{s} w_i z_i \neq 0 \;\middle|\; |w_i| \leq \deg(Q) \right\}.$$

Therefore,

$$A = \bigcup_{w \in S} w^{\perp}.$$

But A is a finitely generated free abelian group and cannot be written as a finite union of proper subgroups. Therefore, there exists $w \in S$ such that $\langle A, w\rangle = 1$. But then $w \in B$, contradicting $w \in Z$. Therefore, $s \leq n - n'$, as desired. □

Given Lemma 5.9, our task now is to show the existence of a prime ideal $\mathfrak{p}$ with height n' such that $\operatorname{rank}(\operatorname{Stab}_X(\mathfrak{p})) = m'$, where $m'/m + n'/n > 1$. This is provided by the following theorem:

Theorem 5.10. *Let $N > 0$ and suppose there exists*

$$P \in k[t_1, \ldots, t_n]$$

such that $\deg(P) < (N/n)^{m/n}$ and $P(x) = 0$ for all $x \in X(N)$. Then there exists a prime ideal $\mathfrak{p} \subset \mathfrak{m}$ of height n' such that

$$\operatorname{rank}(\operatorname{Stab}_X(\mathfrak{p})) = m', \quad \text{where } frm'/m + \frac{n'}{n} > 1.$$

Lemma 5.9 and Theorem 5.10 combine to give Theorem 5.5. We will prove the contrapositive of Theorem 5.10. For each $1 \leq n' \leq n$, let $m' = m'_{n'}$ be the maximal rank of $\operatorname{Stab}_X(\mathfrak{p})$ as $\mathfrak{p}$ ranges over the primes contained in $\mathfrak{m}$ with height equal to n'. If any $m' = m$, then $m'/m + n'/n = 1 + n'/n > 1$, so we are done. Therefore, assume that every $m' < m$ and define

$$\eta_{n'} = \frac{n'}{m - m'}.$$

Note that

$$\eta_{n'} > \frac{n}{m} \iff \frac{m'}{m} + \frac{n'}{n} > 1. \tag{41}$$

Theorem 5.10 will arise as a corollary of the following statement:

Theorem 5.11. *Let $f \in R$ have degree D and let*

$$N = D^{\eta_1} + D^{\eta_2} + \cdots + D^{\eta_n}.$$

There exists $z \in X(N)$ such that $f(z) \neq 0$.

Theorem 5.11 implies Theorem 5.10. Indeed, if each $\eta_{n'}$ for $1 \leq n' \leq n$ satisfies $\eta_{n'} \leq n/m$, then Theorem 5.11 implies that there exists $z \in X(n \deg(P)^{n/m})$ such that $P(z) \neq 0$. But, by assumption, $n \deg(P)^{n/m} < N$, yielding a contradiction to the assumption $P(z) = 0$ for all $z \in X(N)$. Therefore, some $\eta_{n'}$ is larger than n/m, giving the desired result by (41).

The proof of Theorem 5.11 requires significant commutative algebra. We first establish some notation. Let

$$\mathfrak{M} = \bigcup_{z \in X(N)} z \cdot \mathfrak{m}, \quad S_{\mathfrak{M}} = R - \mathfrak{M}.$$

The set $S_{\mathfrak{M}}$ is multiplicatively closed. For an ideal $\mathfrak{a} \subset R$, define

$$\mathfrak{a}^* = (S_{\mathfrak{M}}^{-1}\mathfrak{a}) \cap R \supset \mathfrak{a}.$$

Note that, for a prime ideal $\mathfrak{p} \subset R$, we have $\mathfrak{p}^* = \mathfrak{p}$ if and only if $\mathfrak{p} \subset z \cdot \mathfrak{m}$ for some $z \in X$, and $\mathfrak{p}^* = R$ otherwise. Indeed, if $\mathfrak{p}^* \neq \mathfrak{p}$, then there exists $t/s \in (S_{\mathfrak{M}}^{-1}\mathfrak{p}) \cap R$ such that $t/s \notin \mathfrak{p}$. Write $t/s = g \in R$ with $g \notin \mathfrak{p}$. Since $t = gs \in \mathfrak{p}$ and $\mathfrak{p}$ is prime, this implies that $s \in \mathfrak{p}$. Since $s \in S_{\mathfrak{M}}$, we conclude that $\mathfrak{p} \not\subset \mathfrak{M}$, and hence $\mathfrak{p} \not\subset z \cdot \mathfrak{m}$ for any $z \in X(N)$. Furthermore, in this case, we have $s/s = 1 \in \mathfrak{p}^*$, so $\mathfrak{p}^* = R$. Now, all of these steps are clearly reversible, except possibly "$\mathfrak{p} \not\subset \mathfrak{M}$ implies $\mathfrak{p} \not\subset z \cdot \mathfrak{m}$ for all $z \in X(N)$". The inverse (equivalently, converse) of this statement reads "$\mathfrak{p} \subset \mathfrak{M}$ implies $\mathfrak{p} \subset z \cdot \mathfrak{m}$ for some $z \in X(N)$". This is precisely the prime avoidance lemma. This completes the proof of our claim about $\mathfrak{p}^*$.

We next recall some definitions from commutative algebra. An *associated prime* of an ideal $\mathfrak{a} \subset R$ is a prime ideal $\mathfrak{p}$ such that there exists an R-module injection $R/\mathfrak{p} \hookrightarrow R/\mathfrak{a}$. (The associated primes play the role of the irreducible factors in our simplified proof for $n = m = 2$.) An ideal $\mathfrak{a} \subset R$ is called *unmixed of height r* if all its associated prime ideals have height r.

Next we recall the definitions of *dimension* and *degree* of an ideal of R and some of the basic properties of these functions. Let $R_0 = k[t_0, \ldots, t_n]$. For $f \in R$, let $f_0 \in R_0$ denote the homogenization of f, defined by padding each monomial of f with the correct power of t_0 to obtain a homogeneous polynomial of degree $\deg(f)$. For an ideal $\mathfrak{a} \subset R$, let $\mathfrak{a}_0$ denote the homogeneous ideal generated by f_0 for $f \in \mathfrak{a}$. Then $R_0/\mathfrak{a}_0$ is a graded R_0-module.

There is a polynomial

$$H_{\mathfrak{a}}(t) = a_d t^d + \cdots + a_0 \in \mathbb{Q}[x],$$

called the *Hilbert polynomial* of $\mathfrak{a}$, such that

$$H_{\mathfrak{a}}(i) = \dim_k(i\text{-th graded piece of } R_0/\mathfrak{a}_0)$$

for i sufficiently large. We define the dimension and degree of $\mathfrak{a}$, respectively, by

$$d(\mathfrak{a}) = d, \quad \ell(\mathfrak{a}) := \tilde{\ell}(R_0/\mathfrak{a}_0) := a_d \cdot d!.$$

These are both integers. They satisfy the following properties:

- $\ell((f))$ is the degree of f in the usual sense.
- If $\mathfrak{a} \subset \mathfrak{b}$ and $\mathrm{ht}(\mathfrak{a}) = \mathrm{ht}(\mathfrak{b})$, then $\ell(\mathfrak{a}) \geq \ell(\mathfrak{b})$.
- If $\mathfrak{a}$ and $\mathfrak{b}$ are unmixed of height r, then so is $\mathfrak{a} \cap \mathfrak{b}$, and

$$\ell(\mathfrak{a} \cap \mathfrak{b}) \leq \ell(\mathfrak{a}) + \ell(\mathfrak{b}).$$

Note that from this it follows that, if $\mathfrak{a}$ is unmixed, then the number of associated primes of $\mathfrak{a}$ is $\leq \mathfrak{l}(\mathfrak{a})$. To see this, we note that there is a *primary decomposition* $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i$, where $\{\sqrt{\mathfrak{q}_i}\}$ is the set of associated primes.

We can now begin the proof of Theorem 5.11. Let $f \in R$ have degree D and let

$$N_r = D^{\eta_1} + \cdots + D^{\eta_{r-1}} \quad \text{for } 1 \leq r \leq n+1.$$

We will inductively construct f_r, a $\mathbb{Z}$-linear combination of elements in $X(N_r) \cdot f$ such that $\mathfrak{a}_r = (f_1, \ldots, f_r)$ satisfies the following: either $\mathfrak{a}_r^* = R$, or $\mathfrak{a}_r^*$ is unmixed of height r and degree at most D^r.

This will give the theorem: for $r = n+1$, $\mathfrak{a}_r^*$ cannot have height $n+1$, so $\mathfrak{a}_r^* = R$, which implies $\mathfrak{a}_r \not\subset \mathfrak{M}$. In particular, $f_i \notin \mathfrak{m}$ for some i, so, if $f_i = \sum d_j(z_j \cdot f)$ with $d_j \in \mathbb{Z}$ and $z_j \in X(N_{n+1})$, then $f(z_j) \neq 0$ for some z_j, as desired.

Base case: Take $f_1 = f$ and $\mathfrak{a}_1 = (f)$. Then $\mathfrak{a}_1^* = (f^*)$, where f^* is the quotient of f by any irreducible factors not lying in $\mathfrak{M}$. If $f^* \neq 1$, then (f^*) is unmixed of height 1 by Krull's principal ideal theorem, and has degree $\leq D = \deg(f)$.

Inductive step: Suppose $r \geq 2$ and that we have constructed $f_1, \ldots, f_{r-1}$. If $\mathfrak{a}_{r-1}^* = R$, then we can take $f_r = f$. We have $\mathfrak{a}_r^* = R$, and we are done. Therefore, we suppose that $\mathfrak{a}_{r-1}^*$ is unmixed of height $r-1$ and degree at most D^{r-1}. The construction of f_r is slightly elaborate in this case, so let us outline the steps:

(1) For any associated prime $\mathfrak{p}$ of $\mathfrak{a}_{r-1}^*$, show by counting that there exists $a \in \mathbb{Z}^m(D^{\eta_{r-1}})$ such that $x^{-a}\mathfrak{p}$ is not associated to $\mathfrak{a}_{r-1}^*$, i.e., that $\mathfrak{p}$ is not associated to $x^a\mathfrak{a}_{r-1}^*$.

(2) Show that this implies there exists $1 \leq i \leq r-1$ such that $x^a f_i \notin \mathfrak{p}$.

(3) Show that this implies there exists a $\mathbb{Z}$-linear combination f_r of these $x^a f_i$ that does not lie in any $\mathfrak{p}$ associated to $\mathfrak{a}_{r-1}^*$.

(4) Letting $\mathfrak{a}_r = (\mathfrak{a}_{r-1}, f_r)$, show that $\mathfrak{a}_r^* = R$ or $\mathfrak{a}_r^*$ is unmixed of height r.

It is perhaps worth pointing out here that the fourth point above is precisely the reason that associated primes appear in this proof — the key fact is that, if an element f_r does not lie in any prime associated to $\mathfrak{a}_{r-1}^*$, then the height of $\mathfrak{a}_r^* = (\mathfrak{a}_{r-1}, f_r)^*$ goes up by one (or $\mathfrak{a}_r^* = R$). Let us now carry out the four steps above:

(1) Let $\mathfrak{p}$ be associated to $\mathfrak{a}_{r-1}^*$. Then $\mathfrak{p} \subset \mathfrak{M}$, so $\mathfrak{p} \subset z \cdot \mathfrak{m}$ for some $z \in X$, so $z^{-1} \cdot \mathfrak{p} \subset \mathfrak{m}$. By definition, $\operatorname{rank}(\operatorname{Stab}_X(z^{-1} \cdot \mathfrak{p})) \leq m'_{r-1}$, whence $\operatorname{rank}(\operatorname{Stab}_X(\mathfrak{p})) \leq m'_{r-1}$.

Lemma 5.12. *Let T be a positive integer. Let $\mathbb{Z}^m(T)$ denote the set of tuples $(a_1, \ldots, a_m) \in \mathbb{Z}^m$ with $0 \leq a_i \leq T$ for each i. If $H \subset \mathbb{Z}^m$ is a subgroup of rank h, then the image of $\mathbb{Z}^m(T)$ in $\mathbb{Z}^m/H$ has size at least $(T+1)^{m-h}$.*

Before proving the lemma, we first note that it implies that the image of $\mathbb{Z}^m(D^{\eta_{r-1}})$ in $\mathbb{Z}^m/\operatorname{Stab}_X(\mathfrak{p})$ has size at least

$$(\lfloor D^{\eta_{r-1}} \rfloor + 1)^{m-m'_{r-1}} > (D^{\eta_{r-1}})^{m-m'_{r-1}} = D^{r-1}.$$

Now, the number of primes associated to $\mathfrak{a}_{r-1}^*$ is at most its degree $\ell(\mathfrak{a}_{r-1}^*) \leq D^{r-1}$. Therefore, there exists $a \in \mathbb{Z}^m(D^{\eta_{r-1}})$ such that $x^{-a}\mathfrak{p}$ is not an associated prime of $\mathfrak{a}_{r-1}^*$. Equivalently, $\mathfrak{p}$ is not an associated prime of $x^a\mathfrak{a}_{r-1}^*$. This completes the first step.

Proof of Lemma 5.12. Choose $m-h$ elements of the canonical basis of $\mathbb{Z}^m$ that generate a subgroup B such that $H \cap B = \{0\}$. Then the canonical map from $\mathbb{Z}^m$ to $\mathbb{Z}^m/H$ is injective when restricted to B. The result follows since $B \cap \mathbb{Z}^m(T)$ contains exactly $(T+1)^{m-h}$ elements. □

(2) Since $\mathfrak{p}$ and $x^a\mathfrak{a}_{r-1}^*$ are unmixed of the same height $r-1$, but $\mathfrak{p}$ is not associated to $x^a\mathfrak{a}_{r-1}^*$, it follows that $x^a\mathfrak{a}_{r-1}^* \not\subset \mathfrak{p}$. This implies $x^a\mathfrak{a}_{r-1} \not\subset \mathfrak{p}$ since $\mathfrak{p}^* = \mathfrak{p}$. Since

$$\mathfrak{a}_{r-1} = (f_1, \ldots, f_{r-1}),$$

this implies there exists $1 \leq i \leq r-1$ such that $x^a f_i \notin \mathfrak{p}$.

(3) The third step follows from a general lemma:

Lemma 5.13. *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be prime ideals of R and let*

$$f_1, \ldots, f_s \in R$$

such that $f_i \notin \mathfrak{p}_i$. Then there exists a $\mathbb{Z}$-linear combination of the f_i that does not lie in any $\mathfrak{p}_i$.

Proof. Induction on s. In the base case $s = 1$, there is nothing to prove. For $s > 1$, suppose that g is a $\mathbb{Z}$-linear combination of $f_1, \ldots, f_{s-1}$ that does not lie in $\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-1}$. If $g \notin \mathfrak{p}_s$, then we can simply take g and we are done. So suppose $g \in \mathfrak{p}_s$.

Consider all linear combinations $f_s + ag$ with $a \in \mathbb{Z}$. For each a, consider the set $S_a \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-1}\}$ consisting of the $\mathfrak{p}_i$ such that $f_s + ag \in \mathfrak{p}_i$. There are 2^{s-1} possible subsets S_a. By the pigeonhole principle, if we take $a = 0, \ldots, 2^{s-1}$, then there must exist distinct a and $'$ such that $S_a = S_{a'}$. But, if $f_s + ag$ and $f_s + a'g \in \mathfrak{p}_i$ for $1 \leq i \leq s-1$, then $(a - a')g \in \mathfrak{p}_i$, whence $g \in \mathfrak{p}_i$ (since k has characteristic 0), a contradiction. Therefore, $f_s + ag \notin \mathfrak{p}_i$ for $i \leq s-1$.

Also, $f_s \notin \mathfrak{p}_s$ but $g \in \mathfrak{p}_s$ implies $f_s + ag \notin \mathfrak{p}_s$. Therefore, $f_s + ag$ is the desired linear combination. □

We can now complete step (3): We conclude that there is a $\mathbb{Z}$-linear combination f_r of the $x^a f_i$ (where $1 \leq i \leq r-1$ and $a \in \mathbb{Z}^m(D^{\eta_{r-1}})$) such that f_r does not lie in any associated prime of $\mathfrak{a}^*_{r-1}$.

(4) The fourth step will follow from the following lemma:

Lemma 5.14. *Let $\mathfrak{a} \subset R$ be unmixed of height $r-1$ and suppose $f \in R$ is not contained in any of the primes associated to $\mathfrak{a}$. Let $\mathfrak{b} = \mathfrak{a} + (f)$. Then either $\mathfrak{b} = R$ or $\mathfrak{b}$ has height r. In the latter case, $\ell(\mathfrak{b}) \leq \ell(\mathfrak{a}) \cdot \deg f$.*

Proof. Let $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ be a minimal primary decomposition and let $\mathfrak{p}_i$ be the radical of $\mathfrak{q}_i$. If $\mathfrak{p}_i + (f) = R$ for all i, then, for each i, there exists an element of the form $1 - gf \in \mathfrak{p}_i$, and hence an element of the form $(1-gf)^j \in \mathfrak{q}_i$. The product of these lies in $\mathfrak{a}$. This product is congruent to 1 modulo f, so $1 \in \mathfrak{b} = (\mathfrak{a}, f)$. Therefore, assume that there exists some $\mathfrak{p} = \mathfrak{p}_i$ such that $\mathfrak{p} + (f) \neq R$.

By Krull's principal ideal theorem, the image $\bar{\mathfrak{b}}$ of $\mathfrak{b}$ in $R/\mathfrak{p}$ has height 1. The inverse image of any associated prime of $\bar{\mathfrak{b}} \subset R/\mathfrak{p}$ in R is a prime of height $(r-1)+1 = r$. Therefore, the height of $\mathfrak{b}$ is at most r and, since $\mathfrak{b} \supset \mathfrak{a}$, the height is at least $r-1$.

But, if the height of $\mathfrak{b}$ is $r-1$, then it has some associated prime $\mathfrak{p}'$ of height $r-1$. But $\mathfrak{p}' \supset \mathfrak{b} \supset \mathfrak{a}$. As $\mathfrak{a}$ is unmixed of height $r-1$, this implies that $\mathfrak{p}'$ is an associated prime of $\mathfrak{a}$. But $f \in \mathfrak{p}'$ and we assumed f was not contained in any associated primes of $\mathfrak{a}$. This is a contradiction, so we must have that the height of $\mathfrak{b}$ is r.

To conclude, we note that $(\mathfrak{a} + (f))_0 \supset \mathfrak{a}_0 + (f)_0$; hence,

$$\ell(\mathfrak{b}) = \tilde{\ell}(R_0/\mathfrak{b}_0) \leq \tilde{\ell}\big(R_0/(\mathfrak{a}_0 + (f)_0)\big) = \tilde{\ell}(R_0/\mathfrak{a}_0) \cdot \deg(f) = \ell(\mathfrak{a}) \cdot \deg(f).$$

The second-to-last equality requires explanation. Firstly, f_0 is not contained in any of the associated primes of $\mathfrak{a}_0$ since f is not contained in any of the associated primes of $\mathfrak{a}$. This implies that multiplication by f_0 is injective on $R_0/\mathfrak{a}_0$. This multiplication map has degree equal to $\deg(f)$ and cokernel equal to $R_0/(\mathfrak{a}_0 + (f_0))$, whence

$$H_{\mathfrak{a}_0 + (f_0)}(t + \deg(f)) = H_{\mathfrak{a}_0}(t + \deg(f)) - H_{\mathfrak{a}_0}(t).$$

This yields $\tilde{\ell}\big(R_0/(\mathfrak{a}_0 + (f)_0)\big) = \tilde{\ell}(R_0/\mathfrak{a}_0) \cdot \deg(f)$, as desired. □

We can now complete step (4). We have $\mathfrak{a}_r = \mathfrak{a}_{r-1} + (f_r)$. Let $\mathfrak{b} = \mathfrak{a}^*_{r-1} + (f_r)$. Then $\mathfrak{a}^*_r \supset \mathfrak{b}$, and Lemma 5.14 implies that either $\mathfrak{b} = R$ or $\mathfrak{b}$ has height r and $\ell(\mathfrak{b}) \leq D^{r-1} \cdot D = D^r$.

If $\mathfrak{b} = R$ then of course $\mathfrak{a}^*_r = R$, so assume the latter case holds. Let $\mathfrak{p}$ be an associated prime of $\mathfrak{a}^*_r$. Then $\mathrm{ht}(\mathfrak{p}) \geq \mathrm{ht}(\mathfrak{a}^*_r) \geq r$. We want to show equality. We know $\mathfrak{p} \subset \mathfrak{m}'$, where $\mathfrak{m}' = z\mathfrak{m}$ for some $z \in X(N)$. We can work in the localization $R_{\mathfrak{m}'}$, which is a regular local ring. The ideal $\mathfrak{a}_r R_{\mathfrak{m}'}$ is generated by r elements, so Krull's height theorem implies it has height at most r; hence, it has height exactly r. Therefore it is unmixed of height r and hence the same is true of the associated prime $\mathfrak{p}$.

Finally, $\mathfrak{a}^*_r \supset \mathfrak{b}$ and both are unmixed of height r so $\ell(\mathfrak{a}^*_r) \leq \ell(\mathfrak{b}) \leq D^r$. This completes the proof of step (4), and of Theorem 5.11.

6. The matrix coefficient conjecture

Both the assumption and the conclusion of the Waldschmidt–Masser theorem are quite strong. For instance, in the case of a square matrix of dimension n with entries in $\mathscr{L}$ or $\mathscr{L}_p$, one assumes that the rank of the matrix is less than $\frac{1}{2}n$ and one concludes that, after a rational change of basis on both sides, one can arrange a large block of zeroes, precisely a block of dimension $m' \times n'$, where $m' + n' > n$.

We would like a statement that is more sensitive, and gives a "rational" condition whenever the rank is not full. Such a statement is necessary if one wants to prove Leopoldt's conjecture, rather than the partial result given in Corollary 5.3.

To this end, we have formulated with Mahesh Kakde the following conjecture. The name *matrix coefficient conjecture* is inspired by the theory of automorphic representations, where expressions of the form $w^t M v$ are called matrix coefficients.

Conjecture 6.1 (Dasgupta and Kakde). *Let M be a square matrix of dimension n with entries in $\mathscr{L}$ or $\mathscr{L}_p$. If $\det(M) = 0$, then there exist nonzero vectors $w, v \in \mathbb{Q}^n$ such that $w^t M v = 0$.*

Despite its simplicity, Conjecture 6.1 remains quite deep: in the case $n = 2$, it is easily seen to be equivalent to the four exponentials conjecture. We have proven the following about the matrix coefficient conjecture:

- Conjecture 6.1 is implied by the structural rank conjecture.
- The version of Conjecture 6.1 over $\mathscr{L}_p$ implies both Leopoldt's conjecture and the Gross–Kuz'min conjecture.

We have also developed a strategy to study Conjecture 6.1 using auxiliary polynomials, but unfortunately the construction of the necessary polynomials remains a mystery. Our hope is that Conjecture 6.1 may be more tractable than the structural

rank conjecture. We will prove the results stated above and explore Conjecture 6.1 further in forthcoming work.

Acknowledgements

I would like to extend a great thanks to Damien Roy, who provided a detailed reading of an earlier draft of this paper and made many helpful suggestions that greatly improved the exposition. I would also like to thank Mahesh Kakde, my collaborator with whom I learned this material, as well as Michel Waldschmidt for helpful discussions. We are very grateful to Adam Harper [2010], whose exposition we follow for Baker's theorem, and to Eric Stansifer [2012], whose exposition was very influential for our discussion of the Waldschmidt–Masser theorem. Finally, we thank the referees for very helpful comments.

This note arose out of a topics course that I taught online at Duke University during Spring 2020, and I thank those attending the course for lively discussions.

References

[Alaoglu and Erdős 1944] L. Alaoglu and P. Erdős, "On highly composite and similar numbers", *Trans. Amer. Math. Soc.* **56** (1944), 448–469. MR Zbl

[Ax 1971] J. Ax, "On Schanuel's conjectures", *Ann. of Math.* (2) **93** (1971), 252–268. MR Zbl

[Baker 1966] A. Baker, "Linear forms in the logarithms of algebraic numbers", *Mathematika* **13** (1966), 204–216. MR Zbl

[Baker 1967a] A. Baker, "Linear forms in the logarithms of algebraic numbers, II", *Mathematika* **13** (1967), 102–107. MR Zbl

[Baker 1967b] A. Baker, "Linear forms in the logarithms of algebraic numbers, III", *Mathematika* **13** (1967), 220–228. MR Zbl

[Brumer 1967] A. Brumer, "On the units of algebraic number fields", *Mathematika* **14** (1967), 121–124. MR Zbl

[Charollois and Dasgupta 2014] P. Charollois and S. Dasgupta, "Integral Eisenstein cocycles on $\mathbf{GL}_n$, I: Sczech's cocycle and p-adic L-functions of totally real fields", *Camb. J. Math.* **2**:1 (2014), 49–90. MR Zbl

[Cherry 2009] W. Cherry, "Lectures on non-Archimedean function theory", lecture notes, *Advanced school on p-adic analysis and applications*, Abdus Salam International Centre for Theoretical Physics, 2009. arXiv 0909.4509

[Colmez 1988] P. Colmez, "Résidu en $s = 1$ des fonctions zêta p-adiques", *Invent. Math.* **91**:2 (1988), 371–389. MR Zbl

[Dasgupta et al. 2011] S. Dasgupta, H. Darmon, and R. Pollack, "Hilbert modular forms and the Gross–Stark conjecture", *Ann. of Math.* (2) **174**:1 (2011), 439–484. MR Zbl

[Dasgupta et al. 2018] S. Dasgupta, M. Kakde, and K. Ventullo, "On the Gross–Stark conjecture", *Ann. of Math.* (2) **188**:3 (2018), 833–870. MR Zbl

[Federer and Gross 1981] L. J. Federer and B. H. Gross, "Regulators and Iwasawa modules", *Invent. Math.* **62**:3 (1981), 443–457. MR Zbl

[Gross 1981] B. H. Gross, "p-adic L-series at $s = 0$", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28**:3 (1981), 979–994. MR Zbl

[Harper 2010] A. Harper, "A version of Baker's theorem on linear forms in logarithms", preprint, 2010, available at https://warwick.ac.uk/fac/sci/maths/people/staff/harper/bakernotes.pdf.

[Lang 1966] S. Lang, *Introduction to transcendental numbers*, Addison-Wesley, Reading, MA, 1966. MR Zbl

[Laurent 1991] M. Laurent, "Sur quelques résultats récents de transcendance", pp. 209–230 in *Journées arithmétiques* (Luminy, 1989), edited by G. Lachaud, Astérisque **198–200**, Soc. Math. France, Paris, 1991. MR Zbl

[Masser 1981] D. W. Masser, "On polynomials and exponential polynomials in several complex variables", *Invent. Math.* **63**:1 (1981), 81–95. MR Zbl

[Neukirch 1999] J. Neukirch, *Algebraic number theory*, Grundl. Math. Wissen. **322**, Springer, 1999. MR Zbl

[Ramachandra 1968a] K. Ramachandra, "Contributions to the theory of transcendental numbers, I", *Acta Arith.* **14** (1968), 65–72. MR Zbl

[Ramachandra 1968b] K. Ramachandra, "Contributions to the theory of transcendental numbers, II", *Acta Arith.* **14** (1968), 73–88. MR Zbl

[Roy 1995] D. Roy, "Points whose coordinates are logarithms of algebraic numbers on algebraic varieties", *Acta Math.* **175**:1 (1995), 49–73. MR Zbl

[Schneider 1957] T. Schneider, *Einführung in die transzendenten Zahlen*, Springer, 1957. MR Zbl

[Siegel 1929] C. L. Siegel, "Über einige Anwendungen diophantischer Approximationen", *Abh. Preuß. Akad. Wisse.. Phys.-Math. Kl.* **1** (1929), 1–70. Reprinted as pp. 81–138 in *On some applications of Diophantine approximations*, edited by U. Zannier, Quad./Monogr. **2**, Ed. Norm., Pisa, 2014. MR Zbl

[Spiess 2014] M. Spiess, "Shintani cocycles and the order of vanishing of p-adic Hecke L-series at $s = 0$", *Math. Ann.* **359**:1-2 (2014), 239–265. MR Zbl

[Stansifer 2012] E. Stansifer, *Leopoldt's conjecture for abelian and non-abelian cases*, Master's thesis, ALGANT Erasmus Mundus, Universitá degli Studi di Milano, 2012, available at https://algant.eu/documents/theses/stansifer.pdf.

[Valiant 1979] L. G. Valiant, "Completeness classes in algebra", pp. 249–261 in *Conference record of the eleventh annual ACM symposium on theory of computing* (Atlanta, GA, 1979), edited by M. J. Fischer et al., ACM, New York, 1979. MR

[Waldschmidt 1981] M. Waldschmidt, "Transcendance et exponentielles en plusieurs variables", *Invent. Math.* **63**:1 (1981), 97–127. MR Zbl

[Waldschmidt 1992] M. Waldschmidt, *Linear independence of logarithms of algebraic numbers*, IMS Report **116**, Institute of Mathematical Sciences, Madras, 1992. MR Zbl

[Waldschmidt 2023] M. Waldschmidt, "The four exponentials problem and Schanuel's conjecture", pp. 579–592 in *Mathematics going forward*: *collected mathematical brushstrokes*, edited by J.-M. Morel and B. Teissier, Lecture Notes in Math. **2313**, Springer, 2023. MR Zbl

[Wiles 1990] A. Wiles, "The Iwasawa conjecture for totally real fields", *Ann. of Math.* (2) **131**:3 (1990), 493–540. MR Zbl

Received 2 Mar 2023. Revised 12 Dec 2023.

SAMIT DASGUPTA:

dasgupta@math.duke.edu
Department of Mathematics, Duke University, Durham, NC, United States

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the submission page.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles are usually in English or French, but articles written in other languages are welcome.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not refer to bibliography keys. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and a Mathematics Subject Classification for the article, and, for each author, affiliation (if appropriate) and email address.

Format. Authors are encouraged to use LaTeX and the standard amsart class, but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should normally be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages — Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc. — allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@msp.org with as many details as you can about how your graphics were generated.

Bundle your figure files into a single archive (using zip, tar, rar or other format of your choice) and upload on the link you been provided at acceptance time. Each figure should be captioned and numbered so that it can float. Small figures occupying no more than three lines of vertical space can be kept in the text ("the curve looks like this:"). It is acceptable to submit a manuscript with all figures at the end, if their placement is specified in the text by means of comments such as "Place Figure 1 here". The same considerations apply to tables.

White Space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

ESSENTIAL NUMBER THEORY

2023 vol. 2 no. 1