ACTA ARITHMETICA
153.1 (2012)

An equivalent of Kronecker's theorem for powers of an algebraic number and structure of linear recurrences of fixed length

by

Nevio Dubbini and Maurizio Monge (Pisa)

1. Introduction. The classical Kronecker theorem in diophantine approximation, in one of its different versions, says that if $\theta_1, \dots, \theta_m \in \mathbb{R}$ are linearly independent over $\mathbb{Q}$ then $(t\theta_1, \dots, t\theta_m)$ is dense modulo 1. This means, denoting by

$$\pi_m : \mathbb{R}^m \to \mathbb{R}^m/\mathbb{Z}^m = \mathbb{T}^m$$

the canonical projection, that $\{\pi_m(t\theta_1, \dots, t\theta_m) : t \in \mathbb{R}\}$ is dense in $\mathbb{T}^m$.

In this paper we estimate how much this results fails when the θ_i are not all linearly independent, but of a special form. In particular, we give an estimate, uniformly in m, when the θ_i are powers of an algebraic number α, or more generally when they satisfy a general linear recurrence relation with characteristic polynomial $A(x)$ of degree d, a condition which is automatically satisfied if $\theta_i = \alpha^{i-1}$ and $A(x)$ is the minimal integral polynomial of α. We say that a sequence $\theta_1, \theta_2, \dots$ is a recurrence sequence determined by the polynomial $a_d x^d + \dots + a_1 x + a_0$ when $\sum_{i=0}^{d} \theta_{i+j} a_i = 0$ for each $j > 1$.

Before stating our main result, we give the definition of ϵ-density and recall the notion of Mahler measure.

1.1. ϵ-density. For $\epsilon > 0$ and a positive integer m, let $I_\epsilon = [-\epsilon/2, \epsilon/2]^m$ be the cube with edge length ϵ centred at the origin, and let $C_\epsilon = \pi_m(I_\epsilon) \subseteq \mathbb{T}^m$ be its projection on the torus.

Definition. A subset $S \subseteq \mathbb{T}^m$ is *ϵ-dense* if $S + C_{\bar\epsilon} = \mathbb{T}^m$ for each $\bar\epsilon > \epsilon$, or equivalently if $S + C_\epsilon$ is dense. A subset $T \subseteq \mathbb{R}^m$ is ϵ-dense if $T + I_{\bar\epsilon} = \mathbb{R}^m$ whenever $\bar\epsilon > \epsilon$, or equivalently if $T + I_\epsilon$ is dense.

2010 *Mathematics Subject Classification*: Primary 11K06, 11K60; Secondary 11G50, 11H31.
Key words and phrases: Kronecker theorem, epsilon density, recurrence sequence, density modulo 1, algebraic dynamics, Mahler measure, p-adic, Toeplitz matrix.

DOI: 10.4064/aa153-1-2

Alternatively, it is possible to consider on $\mathbb{T}^m$ the distance $d_\infty(x,y)$ defined as the infimum of the ∞-distance $|\tilde{x}-\tilde{y}|_\infty$ over all representatives $\tilde{x},\tilde{y}\in\mathbb{R}^m$ of x,y. Since for each $\rho>0$ the $\rho/2$-neighborhood of S with respect to $d_\infty(\cdot,\cdot)$ is precisely $S+C_\rho$, we see that S is ϵ-dense if and only if its $\bar{\epsilon}/2$-neighborhood is the whole $\mathbb{T}^m$ for each $\bar{\epsilon}>\epsilon$ (or, equivalently, if its $\epsilon/2$-neighborhood is dense).

1.2. Mahler measure. Let $A(x)=\sum_{i=0}^d a_ix^i=a_d\prod_{i=1}^d(x-\alpha_i)$ be a polynomial with complex coefficients such that $a_0\neq 0$. The *Mahler measure* of $A(x)$ is defined as

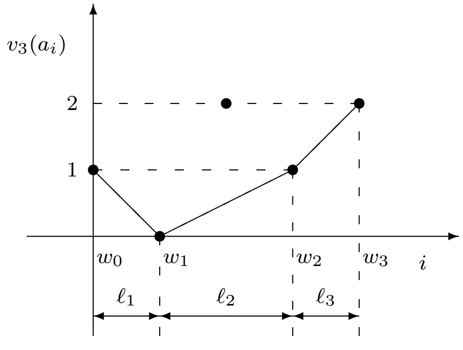
$$M(A)=M(A(x))=|a_d|\prod_{i=1}^d\max\{1,|\alpha_i|\}.$$

It is a notion of complexity that for the minimal polynomial of a rational number p/q with $(p,q)=1$ reduces to $\max(|p|,|q|)$. Furthermore, each coefficient a_i can be written as the sum of $\binom{d}{i}$ products of some elements among $a_d,\alpha_1,\dots,\alpha_d$, each taken at most once, and we have $a_i\leq\binom{d}{i}M(A)$ for $i=0,\dots,d$.

1.3. Newton polygon. For a prime p let $v_p(\cdot)$ be the p-adic valuation, and let us recall that the *Newton polygon* of an integral primitive polynomial $A(x)$ is the boundary of the polygon in $\mathbb{R}^2$ obtained as the upper convex envelope of the points with coordinates

$$(0,v_p(a_0)),(1,v_p(a_1)),\dots,(d,v_p(a_d)).$$

Suppose that the polygon has r edges with different slopes which connect the consecutive pairs of points $(w_k,v_p(a_{w_k}))$ for $0=w_0<w_1<\dots<w_r=d$, let $\ell_k=w_k-w_{k-1}$ be the length of the horizontal projection of the kth edge, and let $\sigma_k=(v_p(a_{w_k})-v_p(a_{w_{k-1}}))/\ell_k$ be its slope. We have $\sigma_i<\sigma_j$ whenever $1\leq i<j\leq d$.



Newton polygon of $A(x)=9x^4-3x^3-9x^2-2x+3$ for $p=3$

We will consider a splitting field K of $A(x)$ over the field $\mathbb{Q}_p$ of p-adic numbers, and we extend the p-adic valuation and absolute value to K. As usual, we write $\mathcal{O}_K$ for the integral closure of $\mathbb{Z}_p$ in K, which is the local ring formed by the elements having non-negative valuation, with maximal ideal $\mathfrak{m}$ generated by the uniformizer π. As is well known, the polynomial $A(x)$ has precisely ℓ_k roots with p-adic valuation equal to $-\sigma_k$ for $1 \le k \le r$.

1.4. Main results. We now state our main results:

THEOREM 1. *Let $m, d > 0$ be positive integers, and let $\theta_1, \dots, \theta_m$ be real numbers such that $\theta_1, \dots, \theta_d$ are linearly independent over $\mathbb{Q}$, and the remaining $\theta_{d+1}, \dots, \theta_m$ are inductively defined by the linear recurrence relation induced by a primitive integral polynomial $A(x)$ of degree d and with non-zero constant coefficient. Then*

$$S_\theta = S_{\theta,m} = \{\pi_m(t\theta_1, \dots, t\theta_m) : t \in \mathbb{R}\} \subseteq \mathbb{T}^m$$

is ϵ-dense for all

$$\epsilon \ge \min\left\{\frac{1}{M(A(x/2))}, \frac{2^d}{M(A(2x))}\right\}.$$

In other terms, if ϵ is as stated, then for arbitrary real numbers $x_1, \dots, x_m$ it is possible to find a real number t and integers $p_1, \dots, p_m$ such that

$$x_i \le t\theta_i - p_i \le x_i + \epsilon \quad \text{for } 1 \le i \le m.$$

The θ_i can clearly be taken to be the powers α^{i-1} of a real algebraic number α, and $A(x)$ the minimal integral polynomial of α. But for each primitive integral polynomial $A(x)$ the allowed θ_i are any 'sufficiently generic' recurrence sequence determined by $A(x)$, provided that $\theta_1, \dots, \theta_d$ are linearly independent over $\mathbb{Q}$.

We remark for convenience that

$$\min\left\{\frac{1}{M(A(x/2))}, \frac{2^d}{M(A(2x))}\right\} \le \frac{2^{[d/2]}}{M(A(x))},$$

giving an estimate in terms of the Mahler measure of $A(x)$; this inequality will also be proved later.

Fixing the recurrence sequence $\theta_1, \theta_2, \dots$ and varying m, the best ϵ_m such that $S_{\theta,m}$ is ϵ_m-dense is initially equal to 0 by Kronecker's theorem, because $S_{\theta,m}$ is dense for $m \le d$, and then increases with m, since $S_{\theta,m}$ is a projection of $S_{\theta,m'}$ for $m < m'$. Theorem 1 gives an upper bound for the sequence ϵ_m; a lower bound for the limit will be given in Theorem 2 below.

Some computational evidence actually makes us propose the following

CONJECTURE 1. *In Theorem 1 we have ϵ-density for all $\epsilon \ge 1/M(A(x))$.*

The conjecture is supported by the apparent connection of the above problem with algebraic dynamics (see [5]): as is well known, the toral automorphism determined by the companion matrix of the polynomial $A(x)$ has topological entropy equal to $M(A(x))$, a quantity controlling the growth of orbits (which are recurrence sequences connected to $A(x)$). The ϵ-density considered here is rather about how well the orbits in the toral dynamical system can approximate a generic sequence modulo 1, but there may still be some connection between the two questions.

This conjectured optimal density coefficient is not very far from what is obtained in Theorem 1. Such a result would be optimal because of the following lower bound for the ϵ-density, for large m:

Theorem 2. *Let $\theta_1, \theta_2, \ldots$ and $A(x)$ be as in Theorem* 1. *Then for each $\epsilon < 1/M(A(x))$ the set $S_{\theta,m}$ is not ϵ-dense for sufficiently large m.*

Should it be possible to prove, for some $\epsilon > 1$, that $S_{\theta,m}$ is ϵ-dense for all recurrence sequences θ such that the corresponding $A(x)$ is not a cyclotomic polynomial, then a positive solution of Lehmer's problem [5, Chap. 1] would follow. This is because the existence of a sequence of polynomials with Mahler measure approaching 1 from above would be automatically ruled out.

During the proof of Theorem 2 a result about the structure of the module of linear recurrences of fixed length is obtained. In particular, fixing a prime p, denoting by $\Lambda_m^{(p)} \subset \mathbb{Z}_p^m$ the module of linear recurrences of length m in $\mathbb{Z}_p$ determined by $A(x)$, and keeping the notation of §1.3 for the Newton polygon of $A(x)$, we have

Theorem 3. *For each prime p there exists a unique basis of $\Lambda_m^{(p)}$ such that the $d \times m$ matrix $M = (M_{i,j})$ having the basis vectors as rows satisfies:*

(1) *The submatrix $(M_{i,j})_{1\le i\le d,\,1\le j\le d}$ (resp. $(M_{i,j})_{1\le i\le d,\,m-d+1\le j\le m}$) is block upper (resp. lower) triangular, with blocks $B_1, \ldots, B_r$ (resp. $C_1, \ldots, C_r$) on the diagonal; the number r of blocks is equal to the number of edges of the Newton polygon of $A(x)$, and B_k and C_k are square matrices of size equal to the length ℓ_k of the kth side of the polygon for each $1 \le k \le r$.*

(2) *Let $1 \le s \le r$ be the smallest integer such that $\sigma_s \ge 0$ (or, alternatively, $\sigma_s > 0$). Then $B_1, \ldots, B_{s-1}, C_s, \ldots, C_r$ are identity matrices, C_k has determinant with valuation $-\sigma_k \ell_k (m-d)$ for $1 \le k \le s-1$, and B_k has determinant with valuation $\sigma_k \ell_k (m-d)$ for $s \le k \le r$.*

(3) *Moving t steps to the right from the element $M_{j,j} = 1$ on the diagonal of the kth identity block B_k for $1 \le k \le s-1$ (resp. to the left from an $M_{j+m-d,j} = 1$ on the diagonal of the identity block C_k for $s \le k \le r$) we find an element with p-adic valuation at least $-t\sigma_k$ (resp. at least $t\sigma_k$).*

In other words, the matrix M can be taken of the following form:

$$\left(\begin{array}{cccccccc|c|cccccccc}
\boxed{1} & & \cdots & & & & & & \cdots & \boxed{C_0} & & & & & & & \\
& \boxed{1} & & \cdots & & & & & \cdots & & \boxed{C_1} & & & & & 0 & \\
& & \ddots & & & & & & & & & \ddots & & & & & \\
& & & \boxed{1} & & \cdots & & & \cdots & & \cdots & & \boxed{C_{s-1}} & & & & \\
& & & & \boxed{B_s} & & \cdots & & \cdots & & & \cdots & & \boxed{1} & & & \\
& & & & & \ddots & & & & & & & & & \ddots & & \\
& 0 & & & & & \boxed{B_{r-1}} & & \cdots & & & & & \cdots & & \boxed{1} & \\
& & & & & & & \boxed{B_r} & \cdots & & & & & & \cdots & & \boxed{1}
\end{array}\right)$$

and the behaviour of the p-adic valuation on the rows is controlled by the slope of the segments of the Newton polygon of $A(x)$.

For instance, if $A(x) = 9x^4 - 3x^3 - 9x^2 - 2x + 3$ and we take $p = 3$, then for recurrence length $m = 10$ the matrix M is

$$\begin{pmatrix}
\boxed{1} & \frac{480}{887} & \frac{4203}{16853} & \frac{3861}{33706} & \frac{2511}{33706} & \frac{243}{16853} & \boxed{\frac{729}{33706}} & 0 & 0 & 0 \\
0 & \frac{-7722}{887} & \frac{-5049}{16853} & \frac{-3339}{33706} & \frac{-76419}{33706} & \frac{33378}{16853} & \frac{-51543}{33706} & 1 & 0 & 0 \\
0 & \frac{729}{887} & \frac{-44658}{16853} & \frac{42822}{16853} & \frac{-27306}{16853} & \frac{19179}{16853} & \frac{3489}{16853} & 0 & 1 & 0 \\
0 & 0 & 0 & \boxed{\frac{729}{1078}} & \frac{243}{1078} & \frac{405}{539} & \frac{675}{1078} & \frac{423}{539} & 48/49 & \boxed{1}
\end{pmatrix}.$$

All denominators are prime to 3, the 3-adic valuations are

$$\begin{pmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & \infty & \infty & \infty \\
\infty & 3 & 3 & 2 & 2 & 1 & 3 & 0 & \infty & \infty \\
\infty & 6 & 3 & 3 & 2 & 2 & 1 & \infty & 0 & \infty \\
\infty & \infty & \infty & 6 & 5 & 4 & 3 & 2 & 1 & 0
\end{pmatrix},$$

and these valuations increase from left to right in the first row, slowly increase from right to left in the second and third rows, and increase from right to left in the last row.

2. Preliminaries. For a complex polynomial $A(x) = a_dx^d + \cdots + a_1x + a_0$ with $a_d, a_0 \neq 0$ let us define, for each $\ell \geq 1$, the rectangular $\ell \times (\ell + d)$ matrix

$$[\![A]\!]_\ell \stackrel{\text{def}}{=} \begin{pmatrix}
a_0 & a_1 & \ldots & a_d & & & & \\
& a_0 & a_1 & \ldots & a_d & & & \\
& & a_0 & a_1 & \ldots & a_d & & \\
& & & \ddots & & \ddots & \ddots & \\
& & & & a_0 & a_1 & \ldots & a_d
\end{pmatrix}.$$

$[\![A]\!]_\ell$ is also the multiplication matrix for sections of power series by the polynomial $A(x)$, in the sense that if

$$F(x) = \sum_{i=0}^{\infty} f_i x^i, \qquad G(x) = \sum_{i=0}^{\infty} g_i x^i$$

are complex power series such that $G(x) = A(x) \cdot F(x)$, then

$$(g_{d+\ell-1}, \dots, g_{d+1}, g_d)^\top = [\![A]\!]_\ell \cdot (f_{d+\ell-1}, \dots, f_{d+1}, f_d, \dots, f_0)^\top,$$

indeed the range of the coefficients with index $0, 1, \dots, d+\ell-1$ of $F(x)$ uniquely determines the coefficients with index $d, d+1, \dots, d+\ell-1$ of $G(x)$.

Moreover, if $A(x)$ factors as

$$A(x) = B(x)C(x), \qquad B(x) = \sum_{i=0}^{s} b_i x^i, \qquad C(x) = \sum_{i=0}^{t} c_i x^i,$$

then we have

$$[\![A]\!]_\ell = [\![B]\!]_\ell \cdot [\![C]\!]_{\ell+s} = [\![C]\!]_\ell \cdot [\![B]\!]_{\ell+t},$$

as is easy to verify, observing that multiplying a power series by $A(x)$ and discarding the lowest d coefficients gives the same result as multiplying first by $C(x)$ and discarding the lowest t coefficients, and then by $B(x)$ and discarding the lowest s coefficients (and vice versa).

For each polynomial $A(x)$ and positive integer m we will also need the lower triangular $m \times m$ matrix

$$\{A\}_m \overset{\text{def}}{=} \begin{pmatrix} a_d & & & & & & \\ a_{d-1} & a_d & & & & & \\ \vdots & \vdots & \ddots & & & & \\ a_0 & a_1 & \dots & a_d & & & \\ & a_0 & a_1 & \dots & a_d & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_0 & a_1 & & a_d \end{pmatrix}.$$

Note that $[\![A]\!]_\ell$ is embedded in $\{A\}_{\ell+d}$ as the last ℓ rows. Similarly to the previous case, if $A(x) = B(x)C(x)$, then $\{A\}_m = \{B\}_m\{C\}_m$. In particular, if $C(x)$ splits into linear factors as

$$C(x) = \prod_{i=1}^{t} (x - \gamma_i),$$

we have

$$\{C\}_m = \prod_{i=1}^{t} \{x - \gamma_i\}_m.$$

3. Proof of Theorem 1. We will first show the inequality implicitly stated in Theorem 1:

Proposition 1. *Let $A(x)$ be a polynomial. Then*

$$\min\left\{ \frac{1}{M(A(x/2))}, \frac{2^d}{M(A(2x))} \right\} \le \frac{2^{[d/2]}}{M(A(x))}.$$

Proof. We have

$$M(A(x/2)) = \frac{|a_d|}{2^d} \prod_{j=1}^{d} \max\{1, |2\alpha_j|\} = |a_d| \prod_{j=1}^{d} \max\{1/2, |\alpha_j|\},$$

while

$$\begin{aligned} 2^{-d} M(A(2x)) &= |a_d| \prod_{j=1}^{d} \max\{1, |\alpha_j/2|\} \\ &= |a_0| \prod_{j=1}^{d} \max\{|\alpha_j^{-1}|, 1/2\} = M(\tilde{A}(x/2)), \end{aligned}$$

where we denoted by $\tilde{A}(x)$ the conjugate polynomial $\sum_{i=0}^{d} a_i x^{d-i}$.

We have $M(A(x/2)) \ge 2^{-[d/2]} M(A(x))$ if $A(x)$ has at least $d/2$ roots ≥ 1 in absolute value, while $2^{-d} M(A(2x)) \ge 2^{-[d/2]} M(A(x))$ if $A(x)$ has at least $d/2$ roots ≤ 1 in absolute value. Since at least one of these conditions must hold, the proposition is proven. ∎

Proof of Theorem 1. From Kronecker's approximation theorem [3, pp. 53–54] the set $S_{\theta,m}$ is dense in the closed subgroup of the torus consisting of the elements satisfying the same integral relations as the $\theta_1, \ldots, \theta_m$.

Let $A(x) = \sum_{i=0}^{d} a_d x^d = a_d \prod_{i=1}^{d} (x - \alpha_i)$ be the primitive integral polynomial defining the recurrence sequence $\theta_1, \theta_2, \ldots$. If $k_0, \ldots, k_{m-1}$ is an integral linear relation satisfied by the θ_i (that is, $\sum_{i=1}^{m} k_{i-1}\theta_i = 0$), and $K(x) = \sum_{i=0}^{m-1} k_i x^i$ is the corresponding polynomial, we can consider the remainder $R(x) = \sum_{i \ge 0} r_i x^i$ of the division of $K(x)$ by $A(x)$. It is a polynomial of degree $\le d - 1$ and its coefficients $r_0, r_1, \ldots$ still define a linear relation among the θ_i. But $\theta_1, \ldots, \theta_d$ are linearly independent over $\mathbb{Q}$, so $R(x)$ must be zero.

Consequently, $K(x)$ must be a multiple of $A(x)$ in $\mathbb{Q}[x]$, and thus in $\mathbb{Z}[x]$ by the Gauss lemma, $A(x)$ being primitive. This shows that for $\ell = m - d$

the rows of the matrix $[\![A]\!]_\ell$ generate the $\mathbb{Z}$-module of integral relations of $\theta_1, \dots, \theta_m$.

The closure of $S_{\theta,m}$ is thus the projection on $\mathbb{T}^m$ of the hyperplane

$$P = P(A) = \{v \in \mathbb{R}^m : [\![A]\!]_\ell \cdot v = 0\},$$

the kernel of the linear map $[\![A]\!]_\ell : \mathbb{R}^m \to \mathbb{R}^\ell$.

Its inverse image under the projection π_m is $P + \mathbb{Z}^m$, and since we just showed that the sublattice of $\mathbb{Z}^m$ generated by the rows of the matrix $[\![A]\!]_\ell$ is the saturated sublattice of integral linear relations of $\theta_1, \dots, \theta_m$, we conclude that $P + \mathbb{Z}^m$ is also equal to

$$Q = Q(A) = \{v \in \mathbb{R}^m : [\![A]\!]_\ell \cdot v \in \mathbb{Z}^\ell\}.$$

Indeed, the $\mathbb{Z}$-linear map $[\![A]\!]_\ell : \mathbb{Z}^m \to \mathbb{Z}^\ell$ must be surjective (this is true a fortiori as the above lattice is saturated, but it can also be seen directly considering the $\ell \times \ell$ minors modulo p for each prime p [4, Lemma 2, Chap. 1], which have gcd 1 because $A(x)$ is primitive). Now, $P + \mathbb{Z}^m \subseteq Q$ clearly, and for each vector $w \in Q$ there exists $z \in \mathbb{Z}^m$ such that $[\![A]\!]_\ell \cdot w = [\![A]\!]_\ell \cdot z$, and consequently $v = w - z$ is in P, so $w = v + z \in P + \mathbb{Z}^m$.

We are now reduced to proving that $Q(A)$ is ϵ-dense in $\mathbb{R}^m$ for each ϵ satisfying the inequality stated in the theorem. Applying the involution

$$(x_1, x_2, \dots, x_{m-1}, x_m) \mapsto (x_m, x_{m-1}, \dots, x_2, x_1)$$

to $Q(A)$ we obtain a set which clearly has the same ϵ-density properties as $Q(A)$, and which is $Q(\tilde{A})$, where $\tilde{A}(x)$ is the conjugate polynomial $\tilde{A}(x) = a_0 x^d + \dots + a_{d-1}x + a_d$. Consequently, we can just prove that $Q(A)$ is ϵ-dense for

$$\epsilon \geq 1/M(A(x/2)) = \Big(|a_d| \prod_{i=1}^{d} \max\{1/2, |\alpha_i|\}\Big)^{-1},$$

and the ϵ-density for $\epsilon \geq 2^d/M(A(2x)) = 1/M(\tilde{A}(x/2))$ will follow from the same estimate applied to $Q(\tilde{A})$.

To do so, note first that $Q = Q(A)$ is ϵ-dense if and only if the image of $I_\epsilon = I_{\epsilon,m} = [-\epsilon/2, \epsilon/2]^m$ via the map $\pi_\ell \circ [\![A]\!]_\ell$ is the whole $\mathbb{T}^\ell$. Indeed, Q is ϵ-dense if and only if every vector $v \in \mathbb{R}^m$ is contained in $Q + I_\epsilon$, and

$$\begin{aligned} &\Leftrightarrow\ (v + I_\epsilon) \cap Q \neq \emptyset\ \forall v \in \mathbb{R}^m \\ &\Leftrightarrow\ (w + [\![A]\!]_\ell \cdot I_\epsilon) \cap \mathbb{Z}^\ell \neq \emptyset\ \forall w \in \mathbb{R}^\ell, \end{aligned}$$

by applying the matrix $[\![A]\!]_\ell$ to the expression, and denoting by $[\![A]\!]_\ell \cdot I_\epsilon$ the image of I_ϵ under the map $[\![A]\!]_\ell$. This passage must be justified because the matrix $[\![A]\!]_\ell$ does not have rank m, but since Q contains *all* the vectors that are mapped to $\mathbb{Z}^\ell$, the first intersection will be non-empty whenever the second one is (the other direction is trivial).

We will now factor $A(x)$ as a product of polynomials $B(x), C(x) \in \mathbb{R}[x]$, with a consequent factorization of $[\![A]\!]_\ell$, and prove two different estimates for each of the two factors $B(x)$ and $C(x)$. We will select *a posteriori* the factorization providing the best compound estimate.

So, let $B(x) = \sum_{i=0}^{s} b_i x_i$ and $C(x) = \sum_{i=0}^{t} c_i x_i$ with $A(x) = B(x)C(x)$, and recall the induced matrix factorization $[\![A]\!]_\ell = [\![B]\!]_\ell [\![C]\!]_{\ell+s}$. To prove that

$$\pi_\ell \circ [\![A]\!]_\ell = \pi_\ell \circ [\![B]\!]_\ell \circ [\![C]\!]_{\ell+s}$$

is surjective from $I_{\epsilon,m}$ to $\mathbb{T}^\ell$, we can just prove that $\pi_\ell \circ [\![B]\!]_\ell$ is surjective from $I_{\delta,\ell+s}$ for some δ, and that $[\![C]\!]_{\ell+s} \cdot I_{\epsilon,m}$ contains $I_{\delta,\ell+s}$. We anticipate that $C(x)$ will be chosen monic and with all roots < 1 in absolute value.

3.1. Estimate for $B(x)$**.** We can take $\delta = 1/b_0$. Let us show that the image of the cube $I_{\delta,\ell+s}$ under $[\![B]\!]_\ell$ assumes each value modulo $\mathbb{Z}^\ell$, starting with an arbitrary $v = (v_1, \ldots, v_\ell) \in \mathbb{R}^\ell$ and building inductively a vector $w = (w_1, \ldots, w_{\ell+s})$ in $I_{\delta,\ell+s}$ such that $[\![B]\!]_\ell \cdot w - v \in \mathbb{Z}^\ell$. Suppose that $w \in I_{\delta,\ell+s}$ is such that the components with index $> i$ of $[\![B]\!]_\ell \cdot w - v$ are in $\mathbb{Z}$, and observe that while w_i varies in the interval $[-\delta/2, \delta/2]$, the ith component of $[\![B]\!]_\ell \cdot w$ varies in an interval of width $b_0\delta = 1$, while all components with index $> i$ of $[\![B]\!]_\ell \cdot w$ stay fixed. Consequently, we can select w_i in $[-\delta/2, \delta/2]$ to ensure that all components with index $\geq i$ of $[\![B]\!]_\ell \cdot w - v$ are in $\mathbb{Z}$. Repeating this procedure we construct a w with the required properties and our claim follows.

3.2. Estimate for $C(x)$**.** If $C(x) = \sum_{i=0}^{t} c_i x^i = \prod_{i=1}^{t}(x - \gamma_i)$, we prove that it is possible to take

$$\epsilon = \delta \prod_{i=1}^{t} \frac{1}{1 - |\gamma_i|}$$

as follows. Rather than working with $[\![C]\!]_{\ell+s}$ we work with the non-singular square matrix $\{C\}_m$; if we prove that the image of $I_{\epsilon,m}$ under $\{C\}_m$ contains $I_{\delta,m}$ our claim will follow, since the image under $[\![C]\!]_m$ is just the projection on the last $\ell + s$ coordinates of the image under $\{C\}_m$.

Now, rather than proving that the image of $I_{\epsilon,m}$ under $\{C\}_m$ contains $I_{\delta,m}$, it is easier to prove that the image of $I_{\delta,m}$ under $\{C\}_m^{-1}$ is contained in $I_{\epsilon,m}$. In particular, $\{C\}_m$ factors as

$$\{C\}_m = \prod_{i=1}^{t} \{x - \gamma_i\}_m,$$

and the inverse of a matrix of the form $\{x - \gamma\}_m$ for $\gamma \in \{\gamma_i\}_{1 \leq i \leq t}$ is easily computed as

$$\begin{pmatrix} 1 & & & & & \\ -\gamma & 1 & & & & \\ & -\gamma & 1 & & & \\ & & -\gamma & \ddots & & \\ & & & \ddots & 1 & \\ & & & & -\gamma & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & & & & & \\ \gamma & 1 & & & & \\ \gamma^2 & \gamma & 1 & & & \\ \gamma^3 & \gamma^2 & \gamma & \ddots & & \\ \vdots & & \vdots & \ddots & 1 & \\ \gamma^{m-1} & \gamma^{m-2} & \dots & \gamma^2 & \gamma & 1 \end{pmatrix}.$$

This shows that if a (possibly complex) vector $v = (v_1, \dots, v_m)$ has all components with absolute value $\leq \rho$ for some $\rho > 0$, the vector w obtained by applying the matrix $\{x - \gamma\}_m^{-1}$ will have components of the form

$$w_{r+1} = \sum_{i=0}^{r} \gamma^i v_{r+1-i}$$

for some $0 \leq r < m$, and their absolute value can be estimated as

$$\Big|\sum_{i=0}^{r} \gamma^i v_{r+1-i}\Big| \leq \sum_{i=0}^{r} |\gamma^i| \cdot |v_{r+1-i}| \leq \sum_{i=0}^{r} |\gamma^i| \rho \leq \frac{1}{1 - |\gamma|}\rho.$$

Since ρ is arbitrary, applying iteratively $\{x - \gamma_i\}_m^{-1}$ for $i = 1, \dots, t$ we find that the set of complex vectors with all components $< \delta$ in absolute value is mapped by $\{C\}_m^{-1}$ to complex vectors whose components have absolute value at most ϵ. Consequently, $I_{\delta,m}$ is mapped into $I_{\epsilon,m}$, since $\{C\}_m^{-1}$ is a matrix with real entries.

3.3. Conclusion. Let $A(x) = B(x)C(x)$ be a real factorization of $A(x)$, with

$$B(x) = \sum_{i=0}^{s} b_i x^i = a_d \prod_{i=1}^{s} (x - \beta_i), \qquad C(x) = \sum_{i=0}^{t} c_i x^i = \prod_{i=1}^{t} (x - \gamma_i),$$

and with $C(x)$ monic with all roots < 1 in absolute value. The above estimate shows that Q is ϵ-dense for

$$\epsilon \geq \frac{1}{|a_d|} \prod_{i=0}^{s} \frac{1}{|\beta_i|} \cdot \prod_{i=1}^{t} \frac{1}{1 - |\gamma_i|},$$

and consequently for

$$\epsilon \geq \frac{1}{|a_d|} \prod_{i=0}^{d} \min\left\{\frac{1}{|\alpha_i|}, \frac{1}{1 - |\alpha_i|}\right\} = \Big(|a_d| \prod_{i=1}^{d} \max\{|\alpha_i|, 1 - |\alpha_i|\}\Big)^{-1},$$

because we can take as γ_i precisely the α_i with absolute value $\leq 1/2$, and as β_i the remaining roots of $A(x)$ (note that $C(x)$ will have real coefficients).

Since this last expression is clearly not greater than $1/M(A(x/2))$, the proof is complete. ∎

Remark 1. While Theorem 1 gives an ϵ providing ϵ-density for S_m which is good for each m, and by Theorem 2 this ϵ cannot be smaller than $1/M(A)$, a remark on the dependence on m of the best possible constant ϵ_m should be added. Discarding the $m \le d$ for which S_m is dense and hence $\epsilon_m = 0$, for $m = d+1$ the matrix $[\![A]\!]_{d+1}$ is $(a_0, a_1, \ldots, a_d)$ and since we must have $[\![A]\!]_{d+1} \cdot I_\epsilon + \mathbb{Z} = \mathbb{R}$, ϵ should be at least

$$\frac{1}{\sum_{i=0}^d |a_i|} \ge \frac{1}{\sum_{i=0}^d \binom{d}{i} M(A)} = \frac{1}{2^d M(A)}.$$

Consequently, the first non-trivial example already requires a constant of the order of $1/M(A)$, up to a constant depending only on d.

4. Integral linear recurrences of fixed length. In this section we prove Theorem 3; it will be proved in full strength for its independent interest, even if only a small corollary is required to prove Theorem 2. All conclusions obtained in $\mathbb{Z}_p$ can be lifted to $\mathbb{Z}$ with arbitrary approximation with respect to the p-adic absolute value.

Let $A(x) = \sum_{i=0}^d a_i x^i$ be a primitive integral polynomial of degree d with $a_0 \neq 0$, and for $m > d$ let Λ_m be the $\mathbb{Z}$-module of integral vectors in $\mathbb{Z}^m$ forming a recurrence sequence determined by $A(x)$. It is also the module of integral vectors in the kernel of the matrix $[\![A]\!]_{m-d}$, so it has rank d. The $\mathbb{Z}_p$-module $\Lambda_m \otimes_{\mathbb{Z}} \mathbb{Z}_p$ over the ring $\mathbb{Z}_p$ of p-adic integers is clearly equal to the set of vectors in $\mathbb{Z}_p^m$ annihilated by $[\![A]\!]_{m-d}$ and will be denoted by $\Lambda_m^{(p)}$.

Proof of Theorem 3. Let $N = (N_{i,j})$ be the rational $d \times m$ matrix obtained by putting $N_{i,j} = \delta_{ij}$ for $1 \le i,j \le d$, and inductively defining the remaining elements in each row to form a linear recurrence determined by $A(x)$. We prove that the square matrix $N_\xi = (N_{i,\xi_j})_{1\le i,j\le d}$ is non-singular for $\xi = (1, 2, \ldots, w, m-d+w+1, \ldots, m)$, for all $w = w_0, \ldots, w_r$ which are the ordinate of a vertex of the Newton polygon of $A(x)$.

If $A(x)$ has distinct roots $\alpha_1, \ldots, \alpha_d$ the matrix N is given by $V^{-1} \cdot L$, where

$$V = (\alpha_i^{j-1})_{1\le i,j\le d}, \qquad L = (\alpha_i^{j-1})_{1\le i\le d,\, 1\le j\le m}.$$

To obtain a formula for the determinant of N_ξ valid for general α_i, let us work over $\mathbb{C}$ and suppose for a moment that $(1/a_d)A(x) = \prod_{i=1}^d (x - \alpha_i)$ where the α_i are algebraically independent over $\mathbb{C}$. The determinant of $N_\xi = (N_{i,\xi_j})_{1\le i,j\le d}$ is equal to the determinant of $L_\xi = (L_{i,\xi_j})_{1\le i,j\le d}$ divided by $\det V$, and this turns out to be the Schur function s_λ (see [10]) associated to the partition λ defined as $\lambda_{d-1+i} = \xi_i - i + 1$ for $1 \le i \le d$, evaluated at $\alpha_1, \ldots, \alpha_d$. Applying the definition of N by linear recurrence, note that the entries of N are polynomial functions in the elementary symmetric functions of the α_i, and hence polynomials in the α_i, and the determinant of each submatrix is a polynomial function of the α_i as well. For α_i varying outside of the closed algebraic set defined by $\prod_{i>j}(\alpha_i - \alpha_j) = 0$, the determinant of N_ξ is equal to the polynomial $s_\lambda(\alpha_1, \ldots, \alpha_d)$, and consequently that expression will hold for each value of the α_i.

If ξ is defined as above, λ has precisely $d - w$ parts all equal to $m - d$, and its conjugate partition λ' is formed by $m-d$ parts equal to $d-w$. Recall now Jacobi–Trudi's identity

$$s_\lambda = \det\,(e_{\lambda'_i - i + j})_{1 \le i,j \le k},$$

where the e_i's are the elementary symmetric functions, which holds for each k no smaller than the number of parts of λ'. We are reduced to proving that a matrix of the form $(e_{d-w-i+j})_{1 \le i,j \le m-d}$ is non-singular. After evaluation at the roots we have $e_i = (-1)^i a_{d-i}/a_d$, and flipping the sign of rows and columns of even index we can consider the determinant of

$$U = (a_{w+i-j})_{1 \le i,j \le m-d}$$

possibly up to sign, and discarding a factor a_d^{-m+d}. Note that all entries on the diagonal are equal to a_w.

If $w = w_0 = 0$ (resp. $w = w_r = d$) then the matrix is lower (resp. upper) triangular with $a_w \neq 0$ on the diagonal, and consequently non-singular. Suppose $w = w_k$ for some $1 < k < r$, let $\rho \in K$ be an element with p-adic valuation equal to σ_k, and let R be the diagonal matrix with $1, \rho, \rho^2, \ldots, \rho^{m-d-1}$ on the diagonal. The matrix

$$\frac{1}{a_w} R^{-1} \cdot U \cdot R = \left(\frac{a_{w+i-j}\rho^{j-i}}{a_w} \right)_{1 \le i,j \le m-d}$$

has all entries in $\mathcal{O}_K$, and is upper unitriangular when reduced modulo $\mathfrak{m}$ because it has all 1's on the diagonal, and starting from a_w the p-adic valuation increases at a rate higher than σ_k.

Consequently, N_ξ is non-singular, and we can consider the matrix $Q = N_\xi^{-1} \cdot N$. We deduce that the matrix M must be unique: indeed, assume for contradiction that M' has the same properties, and suppose that the ith rows differ. If $(v_j)_{1 \le j \le m}$ is the difference vector of those rows we must have $v_j = 0$ unless $w_k < j \le m - d + w_k$ for some k, and taking $w = w_k$ we see that (v_j) cannot be a linear combination of the rows of Q. But Q has rank d, and the existence of (v_j) would imply that the module $\Lambda_m \otimes_{\mathbb{Z}} \mathbb{Q}$ of linear recurrences has rank $> d$, which is absurd.

Suppose now that $w = w_k$ with $1 \le k < s$, so that the slope σ_k is ≤ 0 by the definition of s. We show that all entries in the rows with indices

$w_{k-1}+1,\dots,w_k-1,w_k$ are integers, and that the valuation of $Q_{i,j}$ for $w_{k-1}<i\le w_k$ and $j\ge i$ is at least $-\sigma_k(j-i)$.

In fact, let ρ have valuation equal to σ_k and consider the polynomial

$$B(x)=\sum_{i=0}^{d}\frac{\rho^{w-i}a_i}{a_w}x^i=\sum_{i=0}^{d}b_ix^i\in\mathcal{O}_K[x].$$

Note that the Newton polygon of $B(x)$ is obtained from the Newton polygon of $A(x)$ by subtracting the linear affine function $f(x)=\sigma_k(x-w)+v_p(a_w)$, and the kth side of the Newton polygon is moved to lie on the horizontal axis. In particular, the coefficients $b_{w_{k-1}}$ and b_{w_k} of $B(x)$ are $\not\equiv 0 \bmod \mathfrak{m}$, but $b_i\equiv 0 \pmod{\mathfrak{m}}$ for $i<w_{k-1}$ or $i>w_k$.

On the other hand, for each $w_{k-1}<i\le w_k$ the vector $(\rho^{j-i}Q_{i,j})_{1\le j\le m}$ is a linear recurrence determined by $B(x)$, and we claim that all entries are in $\mathcal{O}_K$. Indeed, suppose this is not the case, and multiply its entries by the smallest power of the uniformizer π required to make all entries in $\mathcal{O}_K$. Some entry will be in $\mathcal{O}_K\setminus\mathfrak{m}$, but the first $\ell_k=w_k$ entries will be in $\mathfrak{m}$. When reduced modulo $\mathfrak{m}$, the subvector $(\rho^{j-i}Q_{i,j})_{w_{k-1}<j\le m-d+w_k}$ is a recurrence determined by the polynomial

$$C(x)=\sum_{i=0}^{\ell_k}\overline{b_{w_{k-1}+i}}\,x^i=\sum_{i=0}^{\ell_k}c_ix^i\in(\mathcal{O}_K/\mathfrak{m})[x].$$

This recurrence of order ℓ_k in $\mathcal{O}_K/\mathfrak{m}$ is supposed to have non-zero entries, while the first ℓ_k entries are zero. This is absurd, and the claim on the integrality of the $w_{k-1}+1,\dots,w_k-1,w_k$ is proved.

The matrix $(\rho^{j-i}Q_{i,j})_{w_{k-1}<i\le w_k,\,m-d+w_{k-1}<j\le m-d+w_k}$ is invertible, because modulo $\mathfrak{m}$ it is obtained as the $(m-d)$th power of the companion matrix

$$\begin{pmatrix} 0 & & & & -c_0/c_{\ell_k}\\ 1 & 0 & & & -c_1/c_{\ell_k}\\ & 1 & 0 & & -c_2/c_{\ell_k}\\ & & \ddots & \ddots & \vdots\\ & & & 1 & -c_{\ell_k-1}/c_{\ell_k}\end{pmatrix}$$

of $C(x)$, which is invertible. Hence $(Q_{i,j})_{w_{k-1}<i\le w_k,\,m-d+w_{k-1}<j\le m-d+w_k}$, which is obtained by conjugating it with the diagonal matrix with diagonal $1,\rho,\dots,\rho^{\ell_k-1}$ and multiplying by $\rho^{-(m-d)}$, has the same valuation as $\rho^{-\ell_k(m-d)}$, i.e. equal to $-\sigma_k\ell_k(m-d)$.

In this way we have built the rows from $w_{k-1}+1$ to w_k of M, and proved that $C_k=(Q_{i,j})_{w_{k-1}<i\le w_k,\,m-d+w_{k-1}<j\le m-d+w_k}$ has determinant with valuation $-\sigma_k\ell_k(m-d)$, while $B_k=(Q_{i,j})_{w_{k-1}<i,j\le w_k}$ is the identity. For $s\le k\le r$ we can clearly proceed in a symmetrical way, taking C_k

equal to the identity and proceeding on the left of C_k towards B_k, which will have determinant equal to $\sigma_k \ell_k(m-d)$.

The matrix we have built by selecting at each step the rows with indices from $w_{k-1}+1$ to w_k of Q clearly satisfies all requirements for M. Furthermore all rows are linearly independent, so the module they generate over $\mathbb{Z}_p$ has rank d.

To prove that the rows of M generate all of $\Lambda_m^{(p)}$ observe that they generate a $\mathbb{Z}_p$-module contained in $\Lambda_m^{(p)}$, and suppose the containment is strict. A basis of $\Lambda_m^{(p)}$ can be obtained by left multiplication by a matrix B with determinant in $\mathbb{Q}_p \setminus \mathbb{Z}_p$. However the matrix $M_\xi = (M_{i,\xi_j})_{1\le i,j\le d}$ for $\xi = (1,\ldots,w_s, m-d+w_s+1,\ldots,m)$ has determinant 1, and $B \cdot M_\xi$ (and consequently $B \cdot M$) would not have coefficients in $\mathbb{Z}_p$, which is absurd. ∎

Let us now turn to the $\mathbb{Z}$-module Λ_m again. If E is a finitely generated $\mathbb{Z}$-module and $F \subseteq E$ a submodule with index n, then the index of $F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ in $E \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is precisely the largest power of p dividing n.

Let $\Theta_m \subseteq \mathbb{Z}^d \times \mathbb{Q}^{m-d}$ be $\mathbb{Z}$-module of linear recurrences determined by $A(x)$ such that the first d coordinates are in $\mathbb{Z}$, and similarly let $\Theta_m^{(p)} = \Theta_m \otimes_{\mathbb{Z}} \mathbb{Z}_p$. The matrix N in the proof of Theorem 1 is clearly a $\mathbb{Z}$-basis of Θ_m.

For each prime p the matrix M is $M_\xi \cdot N$ where $M_\xi = (M_{i,\xi_j})_{1\le i,j\le d}$ and $\xi = (1,\ldots,d)$, and as is immediately verified, $\det M_\xi$ has the same p-adic valuation as a_d^{m-d}, because for $s \le k \le r$, $\det B_k$ has valuation $\sigma_k \ell_k(m-d) = (v_p(a_{w_k}) - v_p(a_{w_{k-1}}))(m-d)$.

Consequently, $(\Theta_m^{(p)} : \Lambda_m^{(p)})$ is equal to the largest power of p dividing a_d^{m-d}, for each p. We have proved:

Corollary 1. *The module Λ_m has index $|a_d|^{m-d}$ in Θ_m.*

5. Proof of Theorem 2. Before providing the proof of Theorem 2, let us recall a few facts of linear algebra. Let $\langle\cdot,\cdot\rangle$ be the standard inner product on $\mathbb{R}^n$, and $u_1,\ldots,u_k \in \mathbb{R}^n$ for $k \le n$. The Gram matrix of the u_i is the $k \times k$ matrix defined as

$$G(u_1,\ldots,u_k) = (\langle u_i, u_j\rangle)_{1\le i,j\le k},$$

and its determinant can be geometrically interpreted as the square of the volume of the parallelepiped formed by the vectors u_i. If the u_i can be completed with $u_{k+1},\ldots,u_n \in \mathbb{R}^n$ to a basis of $\mathbb{R}^n$, and $v_1,\ldots,v_n \in \mathbb{R}^n$ are such that they form a pair of biorthonormal bases, then we have

$$G(u_1,\ldots,u_n)G(v_1,\ldots,v_n) = I$$

(see [8, §66.2, p. 66-6]). Since $G(u_1,\ldots,u_k)$ is a minor of $G(u_1,\ldots,u_n)$ and its cofactor is $G(v_{k+1},\ldots,v_n)$, if the $u_1,\ldots,u_n$ form a parallelepiped of volume 1 (and consequently $G(u_1,\dots,u_n)$ has determinant 1) we have

$$\det G(u_1,\dots,u_k) = \det G(v_{k+1},\dots,v_n).$$

This follows from the properties of compound matrices (see [6, Chap. 1, §4, p. 21, equation (33) in particular]) related to what is sometimes also called "Jacobi's theorem" [7, §14.16].

We will also need the following technical lemma about the asymptotic behaviour of the determinant of a perturbed Toeplitz matrix that arises as the Gram matrix of particular sets of vectors (see Bump–Diaconis [2], Tracy–Widom [11] and Lyons [9] for general results on this topic). Let $B(x)$ be a real polynomial of degree d, and let $(B_i)_{1\le i\le \ell}$ be the row vectors of the matrix $[\![B]\!]_\ell$. Let $f_1,\dots,f_q$ be a finite set of vectors in $\mathbb{R}^d$, which will also be considered as vectors in $\mathbb{R}^{d+\ell}$ with all extra coordinates 0.

Lemma 1. *We have*

$$\det G(f_1,\dots,f_q,B_1,\dots,B_\ell) = \mathcal{O}(M^{2\ell})$$

for each $M > M(B)$.

Proof. Let us start by showing that

$$\det G(B_1,\dots,B_\ell) = \mathcal{O}(M^{2\ell})$$

for each $M > M(B)$. The determinant of a banded Hermitian Toeplitz matrix can be easily estimated via Trench's formula [1, Theorem 2.10, p. 41]. Let $C(x) = \sum_{j=-r}^{s} c_j x^j$ be a Laurent polynomial, and let $g_n(z)$ be the row

$$g_n(z) = (1, z, z^2, \dots, z^{r-1}, z^{n+r}, z^{n+r+1}, \dots, z^{n+r+s-1}).$$

Let $\xi_1,\dots,\xi_k$ be the distinct roots of $C(x)$, and let $\mu_1,\dots,\mu_k$ be their multiplicities. Define G_n as the determinant of the $(r+s)\times(r+s)$ matrix Γ_n whose first μ_1 rows are $g_n(\xi_1), g_n'(\xi_1),\dots,g_n^{(\mu_1-1)}(\xi_1)$, whose next μ_2 rows are $g_n(\xi_2), g_n'(\xi_2),\dots,g_n^{(\mu_2-1)}(\xi_2)$, and so on.

Then $G_0 \neq 0$, and putting $D_{n-1}(C) = \det(c_{i-j})_{0\le i,j\le n-1}$ we have (by Trench's formula)

$$D_{n-1}(C) = (-1)^{ns} c_s^n \frac{G_n}{G_0} \qquad \text{for every } n \ge 1.$$

Applying the formula to $C(x) = B(x)B(x^{-1})$ and $n = \ell$, we just have to show that $c_s^n G_n = \mathcal{O}(M^n)$ for each $M > M(C) = M(B)^2$, for some $K(M)$. But the determinant of the $(r+s)\times(r+s)$ matrix Γ_n can be expanded as a sum of monomials in the ξ_i having polynomials in n as coefficients, where in each monomial, ξ_i appears with exponent smaller than $(n+r+s)\mu_i$. Consequently, by estimating each monomial the determinant is $\le P(n) M(c_s^{-1}C)^{n+r+s}$ for some polynomial $P(n)$ in n. Therefore $c_s^n G_n = \mathcal{O}(M^n)$ for each $M > M(C)$, as required.

Now we know from Bump–Diaconis [2] that a minor of a Toeplitz matrix obtained by deleting the first r columns and a fixed set of rows, i.e. of the form $D_{n-1}^{\lambda}(C) = \det(c_{\lambda_i - i + j})_{1\le i,j\le n}$ for some fixed partition $\lambda = (\lambda_1, \lambda_2, \dots)$, is asymptotic for $n \to \infty$ to $K \cdot D_{n-1}(C)$ for some constant K. On the other hand, let us expand the determinant of the matrix

$$(G_{i,j})_{1\le i,j\le q+\ell} = G(f_1, \dots, f_q, B_1, \dots, B_\ell)$$

along the first $p \ge d + q$ columns: the expression obtained is a sum of the form

$$\sum_{i_1<\dots<i_p} \det(G_{i_u,v})_{1\le u,v\le p} \cdot C_{1\dots p}^{i_1\dots i_p}(G),$$

where $\det(G_{i_u,v})$ is non-zero only for a finite number of choices of the rows $i_1, \dots, i_p$, while for $i_1, \dots, i_p$ fixed the cofactor $C_{1\dots p}^{i_1\dots i_p}(G)$ is ± 1 times a determinant of the form $D_{n-1}^{\lambda}(C)$, where $C(x) = B(x)B(x^{-1})$ and λ is a partition depending only in the $i_1, \dots, i_p$. Consequently, the expansion is a sum of a fixed number of terms that are $\mathcal{O}(M^{2\ell})$ for each $M > M(B)$, and hence is $\mathcal{O}(M^{2\ell})$ too. ■

We also require the following lemma, which provides for $m = \ell + d$ a basis of the d-dimensional lattice Λ_m of vectors in $\mathbb{Z}^m$ killed by $[\![A]\!]_\ell$ (i.e. form a linear recurrence determined by $A(x)$) which has good properties with respect to the Gramian:

Lemma 2. *There exist for each m a basis $\omega_1, \dots, \omega_d$ of the lattice Λ_m such that*

$$G(\omega_{r_1}, \dots, \omega_{r_p}) \le K \cdot M^{2m}$$

for each subset of the ω_i and for each $M > M(A)$, with some constant K independent of m.

Proof. To construct the required basis, let $\zeta_1, \dots, \zeta_d \in \mathbb{Q}^m$ be such that the jth coordinate of ζ_i is δ_{ij} for $1 \le i, j \le d$, and define the remaining coordinates by the linear recurrence determined by $A(x)$. The ζ_i are clearly a basis of the $\mathbb{Z}$-module Θ_m of vectors in $\mathbb{Z}^d \times \mathbb{Q}^\ell$ killed by $[\![A]\!]_\ell$, and by Corollary 1 we have $(\Theta_m : \Lambda_m) = |a_d|^\ell$. Consequently, a basis (ω_i) of Λ_m can be obtained by applying to (ζ_i) a matrix $W = (W_{i,j})_{1\le i,j\le d}$ with determinant $|a_d|^\ell$. Changing it by left multiplication with an element of $SL(d, \mathbb{Z})$ we can take W in Hermite normal form [8, §23.2, pp. 23-6, 23-7], that is, upper triangular and with $|W_{i,j}| \le |W_{j,j}|$ whenever $i < j$.

We show that we can bound the Gramian of a subset of the ω_i in terms of the Gramians of all subsets of the ζ_i and the determinant of $(W_{i,j})$. Indeed, let $\omega_{r_1}, \dots, \omega_{r_p}$, for $1 \le p \le d$ and $1 \le r_1 < \dots < r_p \le d$, be a subset of the ω_i. The quantity $\sqrt{G(\omega_{r_1}, \dots, \omega_{r_p})}$ is the volume of the parallelepiped formed by the ω_{r_i} and is also equal to

$$\sup_{\phi\in\Phi_p} \phi(\omega_{r_1},\dots,\omega_{r_p}),$$

where Φ_p is the subset of the exterior power $\Lambda_p^*(\mathbb{R}^m)$ defined by

$$\Phi_p = \{n_1\wedge\dots\wedge n_p : n_1,\dots,n_p \in \mathbb{R}^m \text{ orthonormal}\},$$

with $\mathbb{R}^m$ identified with its dual through $\langle\cdot,\cdot\rangle$. This can now be estimated as

$$\begin{aligned}
&\sup_{\phi\in\Phi_p} \phi\Big(\sum_{j=1}^d W_{r_1,j}\zeta_j,\dots,\sum_{j=1}^d W_{r_p,j}\zeta_j\Big)\\
&\quad= \sup_{\phi\in\Phi_p} \sum_{1\le s_1,\dots,s_p\le d} \phi(W_{r_1,s_1}\zeta_{s_1},\dots,W_{r_p,s_p}\zeta_{s_p})\\
&\quad\le \sum_{1\le s_1,\dots,s_p\le d} \sup_{\phi\in\Phi_p} W_{r_1,s_1}\cdots W_{r_p,s_p}\cdot\phi(\zeta_{s_1},\dots,\zeta_{s_p})\\
&\quad\le \sum_{1\le s_1,\dots,s_p\le d} |W_{s_1,s_1}\cdots W_{s_p,s_p}|\cdot \sup_{\phi\in\Phi_p}\phi(\zeta_{s_1},\dots,\zeta_{s_p})\\
&\quad\le \det(W_{i,j})\cdot \sum_{1\le s_1,\dots,s_p\le d} \sup_{\phi\in\Phi_p}\phi(\zeta_{s_1},\dots,\zeta_{s_p}),
\end{aligned}$$

and since we can discard the summands where $s_i = s_j$ for some $i\ne j$, and $(W_{i,j})$ is upper triangular and with integral entries, the above is

$$\le \det(W_{i,j})\cdot d^p\cdot \max_{1\le s_1<\dots<s_p\le d}\sqrt{G(\zeta_{s_1},\dots,\zeta_{s_p})}.$$

Now let $B(x) = a_d^{-1}A(x)$ (so that $M(B) = |a_d^{-1}|M(A)$), and let $(B_i)_{1\le i\le\ell}$ be the row vectors of the rational matrix $[\![B]\!]_\ell$. The matrix $[\![B]\!]_\ell$ can be completed to a square matrix with determinant 1 by inserting the row vectors $e_1,\dots,e_d$ of the standard basis $(e_i)_{1\le i\le m}$ of $\mathbb{R}^m$, and the ζ_i are dual to the e_i in the basis $e_1,\dots,e_d,B_1,\dots,B_\ell$ with respect to the standard scalar product $\langle\cdot,\cdot\rangle$. Consequently, if $\zeta_{r_1},\dots,\zeta_{r_p}$, for $1\le r_1<\dots<r_p\le d$, are a subset of the ζ_i and $1\le s_1<\dots<s_q\le d$ is the complementary set of indices in $1,\dots,d$, the Gram determinant of $\zeta_{r_1},\dots,\zeta_{r_p}$ is the same as that of $e_{s_1},\dots,e_{s_q},B_1,\dots,B_\ell$, which is $\mathcal{O}(N^{2\ell})$ for each $N > M(B)$ by Lemma 1. Therefore the Gram determinant of the ω_{r_i} can be estimated by $K|a_d|^{2\ell}N^{2\ell}$ for some constant K, and hence by $KM^{2\ell} = K'M^{2m}$ for each $M > M(A)$. ∎

Proof of Theorem 2. As in the proof of Theorem 1, put $\ell = m-d$, and set

$$Q = Q(A) = \{v\in\mathbb{R}^m : [\![A]\!]_\ell\cdot v\in\mathbb{Z}^\ell\}.$$

Let $\omega_1,\dots,\omega_d\in\mathbb{Z}^m$ be any basis of the d-dimensional lattice Λ_m of vectors in $\mathbb{Z}^m$ which are killed by $[\![A]\!]_\ell$ (i.e. form a linear recurrence determined by $A(x)$), and let $e_1, \ldots, e_m$ be the standard basis of $\mathbb{R}^m$.

Suppose for contradiction that $\bar{\epsilon} < \epsilon < 1/M(A(x))$ and Q is $\bar{\epsilon}$-dense, independently of m. Since $\epsilon > \bar{\epsilon}$ we have $\pi_m(Q + [0,\epsilon]^m) = \mathbb{T}^m$, and since Q is the union of integral translates of the parallelepiped formed by $\omega_1, \ldots, \omega_d$, the map $\pi_m : \mathbb{R}^m \to \mathbb{T}^m$ must be surjective on the parallelepiped Π formed by the combinations with coefficients in $[0,1]$ of the vectors $\epsilon e_1, \ldots, \epsilon e_m, \omega_1, \ldots, \omega_d$.

The map π_m locally preserves the volume, and the image of Π is all $\mathbb{T}^m$, so the volume of Π must be ≥ 1. But this volume can be computed as the sum of the volumes of the parallelepipeds formed by all choices of m vectors among $\epsilon e_1, \ldots, \epsilon e_m, \omega_1, \ldots, \omega_d$. Note that the volume of the parallelepiped formed by, say, $\epsilon e_{s_1}, \ldots, \epsilon e_{s_q}, \omega_{r_1}, \ldots, \omega_{r_p}$ with $p+q=m$ is not greater than

$$\epsilon^q \sqrt{G(\omega_{r_1}, \ldots, \omega_{r_p})} \leq \epsilon^{m-d} \sqrt{G(\omega_{r_1}, \ldots, \omega_{r_p})},$$

since $q \geq m-d$ and $\epsilon \leq 1$. The total number of such parallelepipeds is $\binom{m+d}{m}$, and if we take a basis ω_i of Λ_m via Lemma 2, the volume of Π can be estimated as

$$\mathrm{Vol}(\Pi) \leq \sqrt{K} \binom{m+d}{m} \epsilon^{m-d} M^m.$$

In particular, this tends to 0 as $m \to \infty$ if M is chosen such that $M(A) < M < 1/\epsilon$, which is possible since we assumed $\epsilon < 1/M(A)$. ∎

Acknowledgements. We wish to thank Roberto Dvornicich for offering kind support and advice during our work, and for providing us with the motivation to improve the second part of the paper. We would also like to thank Albrecht Böttcher and Samuele Mongodi for their help in looking for references, and Lisa Beck for reading the manuscript.

References

[1] A. Böttcher and S. M. Grudsky, *Spectral Properties of Banded Toeplitz Matrices*, SIAM, Philadelphia, PA, 2005.

[2] D. Bump and P. Diaconis, *Toeplitz minors*, J. Combin. Theory Ser. A 97 (2002), 252–271.

[3] J. W. S. Cassels, *An Introduction to Diophantine Approximation*, Cambridge Tracts in Math. 45, Cambridge Univ. Press, New York, 1957.

[4] —, *An Introduction to the Geometry of Number*, 2nd printing, corrected, Springer, Berlin, 1971.

[5] G. Everest and T. Ward, *Heights of Polynomials and Entropy in Algebraic Dynamics*, Springer, London, 1999.

[6] F. R. Gantmacher, *The Theory of Matrices, Vol. 1*, Chelsea Publ., New York, 1959.

[7] I. S. Gradštejn, I. M. Ryžik, A. Jeffrey, and D. Zwillinger, *Tables of Integrals, Series, and Products*, Academic Press, 2000.

[8] L. Hogben, R. A. Brualdi, A. Greenbaum, and R. Mathias, *Handbook of Linear Algebra*, CRC Press, 2007.

[9] R. Lyons, *Szegö limit theorems*, Geom. Funct. Anal. 13 (2003), 574–590.

[10] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, 2nd ed., Oxford Univ. Press, New York, 1995.

[11] C. A. Tracy and H. Widom, *On the limit of some Toeplitz-like determinants*, SIAM J. Matrix Anal. Appl. 23 (2002), 1194–1198.

Nevio Dubbini
Interdepartmental Research Center "E. Piaggio"
Via Diotisalvi 2
56126 Pisa, Italy
E-mail: nevio.dubbini@for.unipi.it

Maurizio Monge
Scuola Normale Superiore di Pisa
Piazza dei Cavalieri, 7
56126 Pisa, Italy
E-mail: maurizio.monge@sns.it

Received on 8.2.2010
and in revised form on 20.8.2011 (6301)