ON MOTZKIN'S PROBLEM IN THE CIRCLE GROUP

PABLO CANDELA, CARLOS CATALÁ, JUANJO RUÉ, AND ORIOL SERRA

Abstract. Given a subset D of the interval $(0,1)$, if a Borel set $A \subset [0,1)$ contains no pair of elements whose difference modulo 1 is in D, then how large can the Lebesgue measure of A be? This is the analogue in the circle group of a well-known problem of Motzkin, originally posed for sets of integers. We make a first treatment of this circle-group analogue, for finite sets D of missing differences, using techniques from ergodic theory, graph theory and the geometry of numbers. Our results include an exact solution when D has two elements, at least one of which is irrational. When every element of D is rational, the problem is equivalent to estimating the independence ratio of a circulant graph. In the case of two rational elements, we give an estimate for this ratio in terms of the odd girth of the graph, which is asymptotically sharp and also recovers the classical solution of Cantor and Gordon to Motzkin's original problem for two missing differences.

1. Introduction

Many interesting developments in combinatorial number theory are related to the general problem of determining how large a subset of an abelian group can be if the set avoids certain prescribed configurations. Famous examples include Szemerédi's theorem, where the configurations in question are arithmetic progressions in sets of integers. Another notable problem of this kind, posed by T.S. Motzkin, asks how large a set of integers can be if it does not contain any pair of elements whose difference lies in a prescribed set. More precisely, given a non-empty subset D of the natural numbers $\mathbb{N}$, let us say that a set $A \subset \mathbb{Z}$ is *D-avoiding* if for every $a, a' \in A$ we have $|a - a'| \notin D$, in other words if the *difference set* $A - A = \{a - a' : a, a' \in A\}$ is disjoint from D. Let $A(N)$ denote the cardinality $|A \cap [-N, N]|$, and let $\bar{\delta}(A)$ denote the upper density of A, namely $\bar{\delta}(A) = \limsup_{N\to\infty} \frac{A(N)}{2N+1}$. Then, Motzkin's problem (posed originally for sets $A \subset \mathbb{N}$ in an unpublished problem collection; see [6]) consists in determining the following quantity, sometimes called the *Motzkin density* of D:

$$\mathrm{Md}_{\mathbb{Z}}(D) := \sup\{\bar{\delta}(A) : A \text{ is a } D\text{-avoiding subset of } \mathbb{Z}\}. \tag{1}$$

The first publication on Motzkin's problem is the paper [6] by Cantor and Gordon. Their results include a full solution for $|D| \le 2$. This involves proving that the elements of D can be assumed to be coprime, then proving that $\mathrm{Md}_{\mathbb{Z}}(D) = 1/2$ for $|D| = 1$, and then proving the following formula for $D = \{d_1, d_2\}$ with $\gcd(d_1, d_2) = 1$:

$$\mathrm{Md}_{\mathbb{Z}}(D) = \frac{\lfloor \frac{d_1+d_2}{2} \rfloor}{d_1 + d_2}. \tag{2}$$

The authors were supported by the Spanish Ministerio de Ciencia e Innovación projects MTM2017-83496-P and MTM2017-82166-P.

Motzkin's problem is still open in general. In the decades since the initial paper [6], the problem has motivated many works and various special cases have been addressed; see for instance [14, 16, 27, 30, 31, 32]. The problem also has interesting relations with other well-known topics in combinatorics and number theory, such as the fractional chromatic number of distance graphs, or the lonely runner conjecture; see for example [26] and the references therein.

There is an analogue of Motzkin's problem for any compact abelian group Z. Namely, given a non-empty set $D \subset \mathrm{Z}$, letting μ denote the Haar probability measure on Z, the problem is to determine or estimate the quantity

$$\mathrm{Md}_{\mathrm{Z}}(D) := \sup\{\mu(A) : A \subset \mathrm{Z} \text{ a Borel set with } (A-A) \cap D = \emptyset\}. \tag{3}$$

In particular, a hitherto unexplored yet natural analogue of Motzkin's problem consists in taking Z to be the circle group $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, which we shall view as the interval $[0, 1]$ with addition modulo 1, letting D be a set of real numbers in $(0, 1)$. In this paper we make a first treatment of this problem for D a finite set $\{t_1, \dots, t_r\}$.

In Section 2 we make some observations on the problem for general $r \in \mathbb{N}$, showing in particular that it can be approached using tools from ergodic theory. We illustrate this first in the "extreme" case where $D \cup \{1\}$ is linearly independent over $\mathbb{Q}$, applying the version of Rokhlin's lemma for free measure-preserving actions of $\mathbb{Z}^r$ to prove that in this case $\mathrm{Md}_{\mathbb{T}}(D) = 1/2$; see Theorem 2.4. (Different applications of Rokhlin's lemma in combinatorial number theory have been given recently in [2, 11].) The general case, where $D \cup \{1\}$ may be linearly dependent over $\mathbb{Q}$, can be approached using more general versions of Rokhlin's lemma which are applicable to free actions of *quotients* of $\mathbb{Z}^r$. In particular, the problem of determining $\mathrm{Md}_{\mathbb{T}}(D)$ can thus be transferred to a similar problem in the discrete setting of the finitely generated abelian group $\mathbb{Z}^r/\Lambda$, where Λ is the kernel of the homomorphism $\mathbb{Z}^r \to \mathbb{T}$, $n \mapsto n_1 t_1 + \dots + n_r t_r$. In this setting a natural notion of Motzkin density can be defined using Følner sequences; see Definition 2.5. We then have the following result.

Theorem 1.1. *Let $D = \{t_1, \dots, t_r\} \subset \mathbb{T}$, let Λ be the kernel of the homomorphism $\mathbb{Z}^r \to \mathbb{T}$, $n \mapsto n_1 t_1 + \dots + n_r t_r$, and let E be the image of the standard basis of $\mathbb{R}^r$ in the quotient $\mathbb{Z}^r/\Lambda$. Then $\mathrm{Md}_{\mathbb{T}}(D) = \mathrm{Md}_{\mathbb{Z}^r/\Lambda}(E)$.*

This result also holds for more general compact abelian groups; see Theorem 2.6.

Theorem 1.1 can be used as a first step in an approach towards determining $\mathrm{Md}_{\mathbb{T}}(D)$, since the corresponding Motzkin density in the discrete setting, i.e. $\mathrm{Md}_{\mathbb{Z}^r/\Lambda}(E)$, can often be simpler to determine. In this paper we pursue this approach for $r \leq 2$.

Another notable special case of the problem, at the other extreme from $D \cup \{1\}$ being linearly independent over $\mathbb{Q}$, is the case in which $D \subset \mathbb{Q}$. This reduces to the problem of determining the independence ratio of a circulant graph which we call the *associated circulant graph*. More precisely, supposing that each element of D is of the form $t_i = a_i/b_i$ with coprime positive integers $a_i < b_i$, then the subgroup $\langle D \rangle \leq \mathbb{T}$ is isomorphic to $\mathbb{Z}_N$ with $N = \mathrm{lcm}(b_1, \dots, b_r)$. The associated circulant graph is the (undirected) connected circulant graph G with vertex set $\mathbb{Z}_N$ (viewed as the set of integers $[0, N-1]$ with addition modulo N) with jumps $d_1, \dots, d_r$ where $d_i = a_i N/b_i$. Thus $x, y \in \mathbb{Z}_N$ form an edge in G if and only if $x - y = d_i$ or $-d_i$ mod N for some $i \in [r]$. Equivalently G is the Cayley graph on $\mathbb{Z}_N$ with generating set $\{d_i, -d_i : i \in [r]\}$, which we shall denote by $G = \mathrm{Cay}(\mathbb{Z}_N, \{d_1, \dots, d_r\})$. The independence ratio of G is $\frac{\alpha(G)}{N}$, where $\alpha(G)$ is the independence number of G, i.e. the maximal cardinality of an independent (or stable) set in G. As a straightforward consequence of Theorem 1.1 we have $\mathrm{Md}_{\mathbb{T}}(D) = \frac{\alpha(G)}{N}$; see Lemma 2.10. It can also be seen, using known results, that determining these independence ratios yields a solution to Motzkin's problem for finitely many missing differences in $\mathbb{Z}$, so in this sense Motzkin's problem in $\mathbb{T}$ subsumes the original problem in $\mathbb{Z}$; we detail this in Remark 2.11.

Circulant graphs are extensively treated in the combinatorics and computer science literature (in the latter they are also known as *multiple-loop networks* or *chordal rings*); see for instance [3, 5, 8, 13, 18]. However, these works study mostly other parameters than the independence ratio. Works determining the independence ratio of certain circulant graphs include [12, 23].

After these remarks on the problem for general r, and a brief solution for $r = 1$ (see Proposition 2.12), we close Section 2 and focus on the problem for $r = 2$ for the rest of the paper. Here we distinguish two cases.

In Section 3 we treat the case in which at least one element of D is irrational. Here we obtain the following exact solution (see Theorem 3.2).

Theorem 1.2. *Let $D = \{t_1, t_2\} \subset (0, 1)$ with $D \not\subset \mathbb{Q}$. If $D \cup \{1\}$ is linearly independent over $\mathbb{Q}$, then $\mathrm{Md}_{\mathbb{T}}(D) = 1/2$. Otherwise, letting m_0, m_1, m_2 be integers not all zero such that $m_0 = m_1 t_1 + m_2 t_2$ and $\gcd(m_0, m_1, m_2) = 1$, we have*

$$\mathrm{Md}_{\mathbb{T}}(D) = \frac{\lfloor k/2 \rfloor}{k}, \quad \text{where } k = |m_1| + |m_2|. \tag{4}$$

In Section 4, we focus on the case in which both elements of D are rational. This is equivalent to determining the independence ratio of circulant graphs with two jumps. We study this problem using mainly tools from the geometry of numbers. The usefulness of such tools for the analysis of circulant graphs is well-known (see for instance [5, 9, 28]), though apparently before the present work these tools had not been used to study the independence ratio.

The independence ratio of a circulant graph G is easily seen to be $1/2$ when G is bipartite, so we can assume that G contains odd cycles. The so-called "no-homomorphism lemma" from [1] yields an upper bound for $\frac{\alpha(G)}{N}$ of the form $\frac{k-1}{2k}$, where k is the *odd girth* of G, i.e. the smallest length of an odd cycle in G (see Lemma 4.1). It is then natural to examine how accurate this upper bound is as an estimate for $\frac{\alpha(G)}{N}$. In particular, the odd girth is always one of the successive minima, relative to the ℓ^1-norm, of a 2-dimensional lattice naturally associated with G; see Lemma 4.6 (the lattice in question is just the lattice Λ from Theorem 1.1 applied in this special case). This expression of the odd girth makes the estimate $\frac{k-1}{2k}$ relatively easy to compute (see Remark 4.11, where an algorithm is outlined). Regarding the accuracy of this estimate of $\frac{\alpha(G)}{N}$, we obtain the following result, showing that it is asymptotically sharp.

Theorem 1.3. *Let $D = \{t_1, t_2\} \subset \mathbb{Q} \cap (0, 1)$. Let G be the associated circulant graph, and let N be the order of G. If G is bipartite then $\mathrm{Md}_{\mathbb{T}}(D) = \frac{\alpha(G)}{N} = \frac{1}{2}$. Otherwise, letting k be the odd girth of G, we have*

$$\tfrac{k-1}{2k} \;\geq\; \mathrm{Md}_{\mathbb{T}}(D) = \tfrac{\alpha(G)}{N} \;>\; \tfrac{k-1}{2k} - (\tfrac{2}{N})^{\frac{1}{2}}. \tag{5}$$

This is obtained as an immediate consequence of the following estimate for the independence number of connected circulant graphs with two jumps (see Theorem 4.10).

Theorem 1.4. *Let $G = \mathrm{Cay}(\mathbb{Z}_N, \{d_1, d_2\})$ with $\langle d_1, d_2\rangle = \mathbb{Z}_N$, and suppose that G has odd girth k. Then*

$$\left\lfloor \tfrac{k-1}{2k} N \right\rfloor \;\geq\; \alpha(G) \;\geq\; \left\lceil \tfrac{k-1}{2k} N - \sqrt{2N} + 1 \right\rceil. \tag{6}$$

The independence ratio of a circulant graph G is equal to the reciprocal of its fractional chromatic number $\chi_f(G)$. Therefore the estimate (5) implies the following estimate for the fractional chromatic number of a connected circulant graph G of order N with 2 jumps and odd girth k:

$$\tfrac{2k}{k-1} \;\leq\; \chi_f(G) \;<\; \tfrac{2k}{k-1} + \tfrac{9}{(N/2)^{1/2}-3}. \tag{7}$$

We also study the related question of determining which graphs among such circulant graphs have independence number matching the upper bound $\lfloor \frac{k-1}{2k} N \rfloor$, though we do not settle this question fully; see Remark 4.3, Example 4.4, and Proposition 4.12.

Finally, we note that the odd girth notion enables a unification of solutions to Motzkin's problem for two missing differences across various settings, in the non-bipartite case. For example, Theorem 1.3 can be seen to imply the formula (2) of Cantor and Gordon, by expressing the formula in terms of the odd girth of the corresponding distance graph $\mathrm{Cay}(\mathbb{Z}, \{d_1, d_2\})$, and viewing the corresponding Motzkin density as the limit of independence ratios of circulant graphs $\mathrm{Cay}(\mathbb{Z}_N, \{d_1, d_2\})$. In Section 5 we detail such connections and discuss further questions.

2. Remarks on the general problem

In this section we make some initial observations on the problem of determining $\mathrm{Md}_{\mathbb{T}}(D)$ for finite D, illustrating especially how tools from ergodic theory can be applied to the problem. In particular we shall use Rokhlin's lemma for free actions of finitely generated abelian groups, which we state below after recalling some terminology.

Definition 2.1. A measure-preserving action of a countable discrete group Γ on a probability space $(X, \mathcal{X}, \mu)$ is a map $f : \Gamma \times X \to X$ such that for every $g \in \Gamma$ there is a measure-preserving map $f_g : X \to X$, with f_{id_Γ} being the identity map, and such that for every $g, h \in \Gamma$ and $x \in X$ we have $f_{g\,h}(x) = f_g(f_h(x))$. We say that such an action is *free* if for every $g, h \in \Gamma$ with $g \neq h$ we have $\mu(\{x \in X : f_g(x) = f_h(x)\}) = 0$.

Definition 2.2. Let f be a measure-preserving action of a countable discrete group Γ on a probability space $(X, \mathcal{X}, \mu)$, and let $K \subset \Gamma$. If $B \in \mathcal{X}$ is such that the sets $f_g(B)$, $g \in K$ are pairwise disjoint, then the union $\bigcup_{g \in K} f_g(B)$ is called a K*-tower* for f with *base* B.

A subset K of an abelian group Γ is said to *tile* Γ if there exists $C \subset \Gamma$ such that we have the partition $\Gamma = \bigsqcup_{c \in C} K + c$. The version of Rokhlin's lemma that we shall use is the following special case of [29, p. 58, Theorem 5].

Lemma 2.3. *Let Γ be a finitely generated abelian group and let f be a free measure-preserving action of Γ on a standard probability space $(X, \mathcal{X}, \mu)$. Let $K \subset \Gamma$ be a finite set that tiles Γ. Then for every $\varepsilon > 0$ there exists a K-tower for f of measure at least $1 - \varepsilon$.*

As a first simple example of the use of this lemma in this context, let us treat swiftly the case of Motzkin's problem in $\mathbb{T}$ where $D \cup \{1\}$ is linearly independent over $\mathbb{Q}$.

2.1. The case of linear independence of $D \cup \{1\}$ over $\mathbb{Q}$.

In this subsection we prove the following result.

Theorem 2.4. *Let D be a finite subset of $(0, 1)$ such that $D \cup \{1\}$ is linearly independent over $\mathbb{Q}$. Then $\mathrm{Md}_{\mathbb{T}}(D) = \frac{1}{2}$. Moreover, no D-avoiding Borel set $A \subset \mathbb{T}$ satisfies $\mu(A) = \frac{1}{2}$.*

In the proof we use the special case of Lemma 2.3 for free actions of $\mathbb{Z}^r$, which was given in [7, Theorem 3.1] and independently in [20, Theorem 1].

Proof. Let $D = \{t_1, \ldots, t_r\}$. Clearly $\mathrm{Md}_{\mathbb{T}}(D) \leq \frac{1}{2}$. Fix any $\varepsilon > 0$ and any odd $N \in \mathbb{N}$.

The translations by the elements $t_1, \ldots, t_r \in D$ generate a measure-preserving action f of $\mathbb{Z}^r$ on $\mathbb{T}$, namely $f(n, x) = x + n_1 t_1 + \cdots + n_r t_r \mod 1$. It follows from the linear independence of $D \cup \{1\}$ over $\mathbb{Q}$ that this action is free. By Lemma 2.3 there is a Borel set $B \subset \mathbb{T}$ that is the base of a $[0, N)^r$-tower for f of Haar probability at least $1 - \varepsilon$.

$$\text{Let } \ A = \bigsqcup_{j_1, \ldots, j_r \,\in\, [0, N-2] :\, j_1 + \cdots + j_r \text{ is even}} B + j_1 t_1 + \cdots + j_r t_r.$$

It is readily seen that $(A+t_i)\cap A=\emptyset$ for each $i\in[r]$, so A is D-avoiding. Moreover, since the translates of B in the tower have equal measure at least $(1-\varepsilon)/N^r$, and since A consists of $(N-1)^r/2$ of these sets, we have $\mu(A)\geq((N-1)^r/2)(1-\varepsilon)/N^r\geq(1-\varepsilon)(1-1/N)^r/2$. Letting $N\to\infty$ and $\varepsilon\to 0$, we deduce that $\mathrm{Md}_{\mathbb{T}}(D)\geq\frac{1}{2}$, so $\mathrm{Md}_{\mathbb{T}}(D)=\frac{1}{2}$.

To see that the supremum $1/2$ cannot be attained, suppose for a contradiction that $A\subset\mathbb{T}$ is a measurable D-avoiding set with $\mu(A)=1/2$. Since $A+t_1\subset A^c:=\mathbb{T}\setminus A$ and $\mu(A+t_1)=1/2=\mu(A^c)$, we have $\mu\big((A+t_1)\Delta A^c\big)=0$. Hence $\mu\big((A+2t_1)\Delta(A+t_1)^c\big)=0$. By the triangle inequality $\mu\big((A+2t_1)\Delta A\big)\leq\mu\big((A+2t_1)\Delta(A+t_1)^c\big)+\mu\big((A+t_1)^c\Delta A\big)=0$. Hence A is an invariant set of measure $1/2$ for the map $x\mapsto x+2t_1$, contradicting the fact that, since t_1 is irrational, this map is ergodic. $\square$

2.2. **Transference to finitely generated abelian groups.**

Given a compact abelian group Z, and $D=\{t_1,\dots,t_r\}\subset \mathrm{Z}$, we consider the lattice

$$\Lambda=\{n\in\mathbb{Z}^r: n_1t_1+\cdots+n_rt_r=0\},\tag{8}$$

that is, the kernel of the homomorphism $\mathbb{Z}^r\to\mathrm{Z}$, $n\mapsto n_1t_1+\cdots+n_rt_r$. The finitely generated abelian group $\mathbb{Z}^r/\Lambda$ then has a free action f on Z, well-defined by

$$f(n+\Lambda,x)=x+(n_1+u_1)t_1+\cdots+(n_r+u_r)t_r,\quad\text{for any } u\in\Lambda.\tag{9}$$

The main idea in the proof of Theorem 2.4 is that the Rokhlin lemma enables the problem of determining $\mathrm{Md}_{\mathbb{T}}(D)$ to be transferred to a discrete setting, where it can be easier to solve. The transference part of this approach can be carried out more generally. We establish this in Theorem 2.6 below, for a general finite set D, and not just for $\mathbb{T}$ but for any compact abelian group Z such that (Z,μ) is a standard probability space, so that Lemma 2.3 can be applied with $X=\mathrm{Z}$ and $\mathcal{X}$ the Borel σ-algebra on Z. This applicability holds if Z is metrizable (as $(\mathrm{Z},\mathcal{X})$ is then a standard Borel space [21, (4.2),(12.5)]). To avoid further technicalities, we shall assume that Z is metrizable.

Our transference result (Theorem 2.6 below) expresses the Motzkin density $\mathrm{Md}_{\mathrm{Z}}(D)$ as an analogous quantity in $\mathbb{Z}^r/\Lambda$. To detail this, we first describe a natural notion of Motzkin density in any finitely generated abelian group Γ.

For any set X we denote by $\mathcal{P}_{<\infty}(X)$ the set of all finite subsets of X. Recall that a sequence $(F_N)_{N\in\mathbb{N}}$ of sets in $\mathcal{P}_{<\infty}(\Gamma)$ is a *Følner sequence* if

$$\text{for every } g\in\Gamma \text{ we have } \lim_{N\to\infty}\frac{|F_N\Delta(g+F_N)|}{|F_N|}=0.\tag{10}$$

Definition 2.5. Let Γ be a finitely generated abelian group and let $E\subset\Gamma$. Let

$$\phi_E:\mathcal{P}_{<\infty}(\Gamma)\to\mathbb{Z}_{\geq 0},\;\; S\mapsto\max\{\,|A|: A\subset S,\ (A-A)\cap E=\emptyset\,\}.$$

Then we define

$$\mathrm{Md}_\Gamma(E) := \lim_{N\to\infty} \frac{\phi_E(F_N)}{|F_N|}, \quad \text{for any Følner sequence } (F_N)_{N\in\mathbb{N}} \text{ in } \Gamma. \tag{11}$$

Note that the function ϕ_E is monotone relative to inclusion, subadditive relative to unions, and Γ-invariant. It follows by known results that the limit in (11) exists and is independent of the choice of Følner sequence (see [25, Theorem 6.1] or [10, Proposition 2.2]).

A notion of Motzkin density in Γ can also be defined using the upper density relative to certain Følner sequences, the resulting definition being a more direct generalization of the original notion used in (1) (see Definition 2.7 and (17)). We show later in this section that for finite sets E this alternative definition agrees with (11) (see Lemma 2.8). We shall use mainly the version in (11), as it is more convenient for our arguments.

We can now state the transference result.

Theorem 2.6. *Let Z be a compact metrizable abelian group, let $D = \{t_1, \dots, t_r\} \subset \mathrm{Z}$, let Λ be the kernel of the homomorphism $\mathbb{Z}^r \to \mathrm{Z}$, $n \mapsto n_1 t_1 + \cdots + n_r t_r$, and let E be the image of the standard basis of $\mathbb{R}^r$ in the quotient $\mathbb{Z}^r/\Lambda$. Then $\mathrm{Md}_{\mathrm{Z}}(D) = \mathrm{Md}_{\mathbb{Z}^r/\Lambda}(E)$.*

Proof. Let $\Gamma = \mathbb{Z}^r/\Lambda$, let $(F_N)_{N\in\mathbb{N}}$ be a Følner sequence in Γ, and let us denote the elements of E by $e'_1, \dots, e'_r$. It follows from (10) that

$$\forall\, \delta > 0,\ \exists\, N_0,\ \forall\, N \geq N_0,\ \forall\, i \in [r],\ \ |(F_N + e'_i) \setminus F_N| \leq \delta |F_N|. \tag{12}$$

We first prove that

$$\mathrm{Md}_{\mathrm{Z}}(D) \geq \mathrm{Md}_\Gamma(E). \tag{13}$$

Fix any $\varepsilon > 0$. By (11) and (12), we can fix N such that the following properties hold: firstly there is an E-avoiding set $A' \subset F_N$ satisfying $\frac{|A'|}{|F_N|} \geq \mathrm{Md}_\Gamma(E) - \frac{\varepsilon}{4}$, and secondly for each $i \in [r]$ we have $|(F_N + e'_i) \setminus F_N| \leq \frac{\varepsilon}{4r}|F_N|$.

Let $A'' = \{g \in A' : g + E \subset F_N\}$. We have $A' \setminus A'' \subset \{g \in F_N : g + E \not\subset F_N\} \subset \bigcup_{i\in[r]} F_N \setminus (F_N - e'_i)$. This together with the properties above implies $\frac{|A''|}{|F_N|} \geq \mathrm{Md}_\Gamma(E) - \frac{\varepsilon}{2}$.

By Lemma 2.3 applied to the action f defined in (9), there is a base $B \subset \mathrm{Z}$ of an F_N-tower for f of measure at least $1 - \frac{\varepsilon}{2}$. Let $A = \bigsqcup_{g\in A''} f_g(B)$. For every $i \in [r]$, the set $A + t_i = \bigsqcup_{g'\in A''} f_{g'+e'_i}(B)$ is disjoint from A (otherwise, since $A'' + e'_i \subset F_N$, the tower property implies that $g' + e'_i = g$ for some $g, g' \in A''$, contradicting that A'' is E-avoiding). Hence $\mathrm{Md}_{\mathrm{Z}}(D) \geq \mu(A) = |A''|\,\mu(B) \geq |F_N|(\mathrm{Md}_\Gamma(E) - \frac{\varepsilon}{2})\,\frac{1-\frac{\varepsilon}{2}}{|F_N|} \geq \mathrm{Md}_\Gamma(E) - \varepsilon$. This yields (13) by letting $\varepsilon \to 0$.

We now prove that

$$\mathrm{Md}_{\mathrm{Z}}(D) \leq \mathrm{Md}_\Gamma(E). \tag{14}$$

Fix any D-avoiding Borel set $A \subset \mathrm{Z}$, and any $\varepsilon > 0$. By (11) and (12), we can fix N such that firstly $|(F_N + e_i') \setminus F_N| \leq \frac{\varepsilon}{2r}|F_N|$ for every $i \in [r]$, and secondly

$$\text{every } E\text{-avoiding set } S \subset F_N \text{ satisfies } \frac{|S|}{|F_N|} \leq \mathrm{Md}_\Gamma(E) + \frac{\varepsilon}{2}. \tag{15}$$

By Lemma 2.3, there is a base $B \subset \mathrm{Z}$ of an F_N-tower for f of measure at least $1 - \frac{\varepsilon}{2}$. We claim that there is a partition $B = \bigsqcup_{j\in[M]} B_j$ such that there is a set $A' \subset A$ (which is therefore D-avoiding) with $\mu(A') \geq \mu(A) - \frac{\varepsilon}{2}$, and with the property that for every $j \in [M]$ there is $S_j \subset F_N$ such that A' is of the form $A' = \bigsqcup_{j\in[M]} \bigsqcup_{g\in S_j} f_g(B_j)$. Before we prove this claim, let us explain how it yields (14). The D-avoiding property of A' implies that each set S_j is E-avoiding. Indeed, otherwise there would be some $j \in [M]$ and $i \in [r]$ such that there is $g' \in S_j$ with $g' + e_i' \in S_j$. But then the form of A' implies that $f_{g'+e_i'}(B_j) \subset A'$ (since $g := g' + e_i' \in S_j$) and $f_{g'+e_i'}(B_j) = f_{g'}(B_j) + t_i \subset A' + t_i$ (since $g' \in S_j$), so $A' \cap (A' + t_i) \supset f_{g'+e_i'}(B_j)$, contradicting that A' is D-avoiding. Hence each S_j is indeed E-avoiding, and then (15) implies $\frac{|S_j|}{|F_N|} \leq \mathrm{Md}_\Gamma(E) + \frac{\varepsilon}{2}$ for all $j \in [M]$. Then, using that $\sum_{j\in[M]} \mu(B_j)|F_N| = \mu\big(\bigsqcup_{g\in F_N} f_g(B)\big) \leq 1$, we have $\mu(A') \leq \sum_{j\in[M]} |S_j|\mu(B_j) \leq \mathrm{Md}_\Gamma(E) + \frac{\varepsilon}{2}$, so $\mu(A) \leq \mathrm{Md}_\Gamma(E) + \varepsilon$, and (14) follows by letting $\varepsilon \to 0$.

We now prove the claim by finding the desired partition of B and the set A'. For every $g \in F_N$, we have the partition $B^{(g)} = \{B_{g,0}, B_{g,1}\}$ of B with atoms $B_{g,1} := B \cap f_g^{-1}(A)$ and $B_{g,0} := B \setminus B_{g,1}$. The desired partition is the common refinement (or supremum) of these partitions, i.e. the partition of B whose atoms are all the intersections of the atoms of $B^{(g)}$ as g ranges in F_N. Let $B_1, \ldots, B_M$ be the atoms in this partition. Let $A' := \bigsqcup_{g\in F_N} [A \cap f_g(B)] \subset A$. Since the F_N-tower with base B has measure at least $1 - \frac{\varepsilon}{2}$, we have $\mu(A \setminus A') \leq \frac{\varepsilon}{2}$. Since $A' = \bigsqcup_{g\in F_N} f_g(B_{g,1})$, and each set $B_{g,1}$ is a union of some of the atoms B_j, it follows that A' is a union of some of the atoms of the partition $\{f_g(B_j) : j \in [M], g \in F_N\}$. Hence for every $j \in [M]$ there is a set $S_j \subset F_N$ such that $A' = \bigsqcup_{j\in[M]} \bigsqcup_{g\in S_j} f_g(B_j)$. This proves the claim and completes the proof. □

To close this subsection, we record another natural way to define the Motzkin density of a finite set in a finitely generated abelian group, in Lemma 2.8 below. This is not used in later sections of this paper, but it can be used for instance in an alternative proof of Theorem 2.6; see Remark 2.9.

Definition 2.7. Let Γ be a finitely generated abelian group. Given any set $A \subset \Gamma$, and any Følner sequence $\mathcal{F} = (F_N)_{N\in\mathbb{N}}$ in Γ, the *upper density of A relative to $\mathcal{F}$* is defined by $\overline{\delta}_{\mathcal{F}}(A) := \limsup_{N\to\infty} \frac{|A\cap F_N|}{|F_N|}$.

A Følner sequence $(F_N)_{N\in\mathbb{N}}$ in Γ is a *tiling Følner sequence* if F_N tiles Γ for every N. Such a sequence can be obtained using the fundamental result that there is a group isomorphism $\vartheta : \mathbb{Z}^d \times \Gamma' \to \Gamma$ for some finite group Γ' and $d \in \mathbb{Z}_{\geq 0}$. Indeed we can then take (for instance)

$$F_N = \vartheta([-N,N]^d \times \Gamma'). \tag{16}$$

Lemma 2.8. *Let Γ be a finitely generated abelian group, let $\mathcal{F}$ be a tiling Følner sequence in Γ, and let E be a finite subset of Γ. Then*

$$\mathrm{Md}_\Gamma(E) = \sup\{\overline{\delta}_{\mathcal{F}}(A) : A \subset \Gamma,\ (A-A)\cap E = \emptyset\}. \tag{17}$$

Proof. It is easily checked from the definitions that $\mathrm{Md}_\Gamma(E) \geq \overline{\delta}_{\mathcal{F}}(A)$ for every E-avoiding set $A \subset \Gamma$, so $\mathrm{Md}_\Gamma(E) \geq \sup\{\overline{\delta}_{\mathcal{F}}(A) : A \subset \Gamma,\ (A-A)\cap E = \emptyset\}$. We now prove that

$$\mathrm{Md}_\Gamma(E) \leq \sup\{\overline{\delta}_{\mathcal{F}}(A) : A \subset \Gamma,\ (A-A)\cap E = \emptyset\}. \tag{18}$$

Let $F_1, F_2, \ldots$ be the sets in $\mathcal{F}$, and fix any $\varepsilon > 0$. By (11), for all N sufficiently large we have $\frac{\phi_E(F_N)}{|F_N|} \geq \mathrm{Md}_\Gamma(E) - \frac{\varepsilon}{2}$, so there is an E-avoiding set $S \subset F_N$ with $\frac{|S|}{|F_N|} \geq \mathrm{Md}_\Gamma(E) - \frac{\varepsilon}{2}$. Since E is finite, it follows from (10) that for all N sufficiently large we also have $|(F_N + t)\setminus F_N| \leq \frac{\varepsilon}{2|E|}|F_N|$ for each $t \in E$. Let us now fix N with the previous two properties. The set $S' := \{g \in S : g + E \subset F_N\}$ satisfies $S \setminus S' \subset \bigcup_{t\in E} F_N \setminus (F_N - t)$, so $\frac{|S'|}{|F_N|} \geq \frac{|S|}{|F_N|} - \frac{\varepsilon}{2} \geq \mathrm{Md}_\Gamma(E) - \varepsilon$. By assumption there is a tiling $\Gamma = \bigsqcup_{c\in C} c + F_N$. It is then easily checked that $A := C + S'$ is E-avoiding. Therefore it now suffices to prove that $\overline{\delta}_{\mathcal{F}}(A) \geq \frac{|S'|}{|F_N|}$, since then $\mathrm{Md}_\Gamma(E) \leq \overline{\delta}_{\mathcal{F}}(A) + \varepsilon$, and then (18) follows by taking the supremum and letting $\varepsilon \to 0$. For each $N' \in \mathbb{N}$, let $C' = \{c \in C : c + F_N \subset F_{N'}\}$. Then $|F_{N'} \cap A| \geq |F_{N'} \cap (C' + S')| = \frac{|S'|}{|F_N|}|C' + F_N| = \frac{|S'|}{|F_N|}(|F_{N'}| - |F_{N'} \setminus (C' + F_N)|)$. Moreover, letting $T = F_N - F_N$, we have $F_{N'} \setminus (C' + F_N) \subset F_{N'} \setminus (T + F_{N'})$. Indeed, if $g \in F_{N'} \setminus (C' + F_N)$ then by the tiling we have $g = c + x$ for some $c \in C$, $x \in F_N$, and by the definition of C' we have $c + x' \notin F_{N'}$ for some $x' \in F_N$; so $g + x' - x \notin F_{N'}$. Thus we deduce that $\frac{|F_{N'}\cap A|}{|F_{N'}|} \geq \frac{|S'|}{|F_N|}\big(1 - \frac{|F_{N'}\setminus(T+F_{N'})|}{|F_{N'}|}\big)$. Applying now (10) with variable N' and every $g \in T$, we deduce that $\overline{\delta}_{\mathcal{F}}(A) = \limsup_{N'\to\infty} \frac{|F_{N'}\cap A|}{|F_{N'}|} \geq \frac{|S'|}{|F_N|}$, as required. □

Remark 2.9. Using (17), the anonymous referee provided an alternative proof of (14) (the second main part of the proof of Theorem 2.6) by applying the pointwise ergodic theorem for actions of finitely generated abelian groups. We gratefully include the argument here.

Let $E \subset \Gamma = \mathbb{Z}^r/\Lambda$ as defined in Theorem 2.6, let f be the action of Γ on Z, and let $\mathcal{F}$ be the tiling Følner sequence given by (16). Let $A \subset \mathrm{Z}$ be a Borel set with $\mu(A) > \mathrm{Md}_\Gamma(E)$. We will find a point $x \in \mathrm{Z}$ such that $A_x := \{g \in \Gamma : f_g(x) \in A\}$ satisfies $\overline{\delta}_{\mathcal{F}}(A_x) \geq \mu(A)$. Thus we will have $\overline{\delta}_{\mathcal{F}}(A_x) > \mathrm{Md}_\Gamma(E)$, implying by (17) that A_x is not E-avoiding, so that there are distinct elements $a, b \in A_x$ with $a - b \in E$. Then $f_a(x), f_b(x) \in A$, so $A - A$ contains the element $f_a(x) - f_b(x) = f_{a-b}(0) \in D$, so A is not D-avoiding. Hence $\mathrm{Md}_{\mathrm{Z}}(D) \leq \mathrm{Md}_\Gamma(E)$.

To find the set A_x, we apply the pointwise ergodic theorem for finitely generated abelian groups with the action f (for instance as a special case of [24, Theorem 1.2], noting that $\mathcal{F}$ clearly has the required property of being tempered). Thus we deduce that the averages $x \mapsto \frac{1}{|F_N|} \sum_{g \in F_N} 1_A(f_g(x))$ converge pointwise almost everywhere to an f-invariant function $\overline{1_A} \in L^1(\mu)$. We have $\int \overline{1_A}\, \mathrm{d}\mu = \int 1_A\, \mathrm{d}\mu = \mu(A)$, and it follows that the set of points $x \in \mathrm{Z}$ with $\overline{1_A}(x) \geq \mu(A)$ is not μ-null. Hence there exists $x \in \mathrm{Z}$ at which the limit of these averages is at least $\mu(A)$. This implies that $\overline{\delta}_{\mathcal{F}}(A_x) \geq \mu(A)$.

2.3. The case $D \subset \mathbb{Q}$: the independence ratio of circulant graphs.

Let us formalize the remarks, made in the introduction, about the general rational case $D \subset \mathbb{Q}$ in the circle group.

Lemma 2.10. *Let $D = \{t_1, \dots, t_r\} \subset (0,1)$, where for each $i \in [r]$ we have $t_i = a_i/b_i$ with $1 \leq a_i < b_i$ and $\gcd(a_i, b_i) = 1$. Let $N = \operatorname{lcm}(b_1, \dots, b_r)$, and let G be the connected circulant graph on $\mathbb{Z}_N$ with jumps $d_1, \dots, d_r$ where $d_i = N t_i$. Then $\mathrm{Md}_{\mathbb{T}}(D) = \frac{\alpha(G)}{N}$.*

Proof. The connectedness of G is equivalent to the elements $d_1, \dots, d_r$ generating the full group $\mathbb{Z}_N$, which is equivalent to $\gcd(d_1, \dots, d_r, N) = 1$, which in turn is equivalent to $\gcd(\frac{N}{b_1}, \dots, \frac{N}{b_r}, N) = 1$ by our assumptions. This last equality can be seen to hold using the identity $\operatorname{lcm}(b_1, \dots, b_r) = \frac{b_1 \cdots b_r}{\gcd(\pi_1, \dots, \pi_r)}$ where $\pi_i = \prod_{j \in [r] \setminus \{i\}} b_j$ for $i \in [r]$.

Using the notation in Theorem 2.6, we have $\mathrm{Md}_{\mathbb{T}}(D) = \mathrm{Md}_{\mathbb{Z}^r/\Lambda}(E)$. Letting ψ denote the homomorphism $\mathbb{Z}^r \to \mathbb{T}$, $n \mapsto n_1 t_1 + \cdots + n_r t_r$, by the first isomorphism theorem, we have $\mathbb{Z}^r/\Lambda \cong \psi(\mathbb{Z}^r)$. Denoting by $\frac{1}{N} \cdot \mathbb{Z}_N$ the subgroup of $\mathbb{T}$ of order N, we have $\psi(\mathbb{Z}^r) = \frac{1}{N} \cdot \mathbb{Z}_N$ and $\psi(e_i') = t_i = \frac{d_i}{N}$ for $i \in [r]$. It follows that $\mathrm{Md}_{\mathbb{Z}^r/\Lambda}(E) = \mathrm{Md}_{\frac{1}{N} \cdot \mathbb{Z}_N}(D) = \mathrm{Md}_{\mathbb{Z}_N}(\{d_1, \dots, d_r\})$. This last quantity equals $\frac{\alpha(G)}{N}$. Hence $\mathrm{Md}_{\mathbb{T}}(D) = \frac{\alpha(G)}{N}$. □

Remark 2.11. Lemma 2.10 shows that Motzkin's problem in $\mathbb{T}$ subsumes the problem of determining the independence ratio of circulant graphs. Let us mention that solving the latter problem in turn yields a solution to Motzkin's original problem in $\mathbb{Z}$ for finitely many missing differences. This follows from the fact that for any finite set $D \subset \mathbb{N}$, identifying $\mathbb{Z}_N$ with the integer interval $F_N = [-\frac{N}{2}, \frac{N}{2}]$ with addition mod N, we have $\lim_{N \to \infty} \mathrm{Md}_{\mathbb{Z}_N}(D) = \mathrm{Md}_{\mathbb{Z}}(D)$. This fact can be seen from (11) noting that $\lim_{N \to \infty} \frac{\phi_D(F_N)}{|F_N|} - \mathrm{Md}_{\mathbb{Z}_N}(D) = 0$, and it can also be seen from previous work: by [23, Theorem 4.1] the limit $\lim_{N \to \infty} \mathrm{Md}_{\mathbb{Z}_N}(D)$ equals the reciprocal of the fractional chromatic number of the graph $\mathrm{Cay}(\mathbb{Z}, D)$; this reciprocal in turn equals $\mathrm{Md}_{\mathbb{Z}}(D)$ [27, Theorem 1].

2.4. The case $|D| = 1$.

Proposition 2.12. *For $D = \{t\}$ with $t \in (0,1)$ we have*

$$\mathrm{Md}_{\mathbb{T}}(D) = \begin{cases} 1/2, & t \notin \mathbb{Q} \\ \lfloor N/2 \rfloor / N, & t = \frac{d}{N} \in (0,1),\ \gcd(d, N) = 1. \end{cases}$$

Proof. The case $t \notin \mathbb{Q}$ follows from Theorem 2.4. For $t = \frac{d}{N}$ with $(d, N) = 1$, we have by Lemma 2.10 that $\mathrm{Md}_{\mathbb{T}}(D)$ is the independence ratio of an N-cycle. This ratio is easily seen to equal $\lfloor N/2 \rfloor / N$ by identifying the cycle's vertex set with $[0, N-1]$, where $x, y \in [0, N-1]$ form an edge if and only if $|x - y| = 1 \bmod N$, and noting that $\{0, 2, \ldots, 2(\lfloor N/2 \rfloor - 1)\}$ is a stable set of maximal cardinality. □

3. The case $|D| = 2$, $D \not\subset \mathbb{Q}$

In this section we suppose that $D = \{t_1, t_2\} \subset (0, 1)$ where t_1, t_2 are not both rational, and we prove Theorem 1.2. Theorem 2.4 already covers the case in which $1, t_1, t_2$ are linearly independent over $\mathbb{Q}$, in other words, the case in which the lattice Λ from (8) is trivial. The case in which Λ has full rank 2 corresponds to $D \subset \mathbb{Q}$ (treated in the next section). Therefore, here it only remains to address the case in which Λ has rank 1, that is, where Λ is a non-trivial cyclic subgroup of $\mathbb{Z}^2$. We begin by describing this subgroup more explicitly in terms of the assumption in Theorem 1.2.

Lemma 3.1. *Suppose that $t_1, t_2 \in (0, 1)$ are not both rational and that $1, t_1, t_2$ are linearly dependent over $\mathbb{Q}$. Let Λ be the kernel of the homomorphism $\psi : \mathbb{Z}^2 \to \mathbb{T}$, $(n_1, n_2) \mapsto n_1 t_1 + n_2 t_2 \bmod 1$, and let $m_1, m_2 \in \mathbb{Z}$. Then (m_1, m_2) generates the cyclic group Λ if and only if there is $m_0 \in \mathbb{Z}$ such that*

$$(m_0, m_1, m_2) \in \mathbb{Z}^3 \setminus \{0\}, \quad m_0 = m_1 t_1 + m_2 t_2 \quad \text{and} \quad \gcd(m_0, m_1, m_2) = 1. \tag{19}$$

In particular, it follows that the quantity in (4) is well-defined.

Proof. If (m_1, m_2) generates Λ (i.e. $\Lambda = \mathbb{Z}(m_1, m_2)$) then in particular $(m_1, m_2) \in \Lambda$ so there is $m_0 \in \mathbb{Z}$ such that $m_0 = m_1 t_1 + m_2 t_2$ (and clearly m_1, m_2 cannot be both 0 since Λ is non-trivial); moreover $g := \gcd(m_0, m_1, m_2)$ must be 1, as otherwise $(\frac{m_1}{g}, \frac{m_2}{g})$ would be an element of $\Lambda \setminus \mathbb{Z}(m_1, m_2)$, contradicting that (m_1, m_2) generates Λ. Hence (19) holds.

To see the converse, note first that if (19) holds then $(m_1, m_2) \in \Lambda$, so $\mathbb{Z}(m_1, m_2) \subset \Lambda$ and it only remains to prove the opposite inclusion. For this, it suffices to prove the claim that every $m' = (m'_0, m'_1, m'_2) \in \mathbb{Z}^3$ satisfying $m'_0 = m'_1 t_1 + m'_2 t_2$ is an integer multiple of $m = (m_0, m_1, m_2)$. If one of t_1, t_2 is rational, say $t_1 \in \mathbb{Q}$, then by irrationality of t_2 we must have $m_2 = m'_2 = 0$, so $m'_0/m'_1 = t_1 = m_0/m_1$ and the claim is then clear. Let us therefore assume that t_1, t_2 are both irrational. We have by assumption $\begin{cases} m_0 = m_1 t_1 + m_2 t_2 \\ m'_0 = m'_1 t_1 + m'_2 t_2 \end{cases}$. Note that none of m_1, m'_1 is zero, otherwise t_2 is rational. Multiplying the first equation by m'_1, the second one by m_1, and subtracting, we deduce that $m'_0 m_1 - m_0 m'_1 = (m_1 m'_2 - m'_1 m_2) t_2$. Since t_2 is irrational, this implies that $m_1 m'_2 = m'_1 m_2$ and $m'_0 m_1 = m_0 m'_1$. The former equation implies that the vectors (m_1, m_2), (m'_1, m'_2) are linearly dependent over

$\mathbb{Q}$. Hence there are coprime non-zero integers a, b such that $a(m_1, m_2) = b(m_1', m_2')$. Using this back in the system of equations above, we deduce that $am_0 = am_1t_1 + am_2t_2 = bm_1't_1 + bm_2't_2 = bm_0'$. Hence $am = bm'$. This, combined with $\gcd(a, b) = \gcd(m_0, m_1, m_2) = 1$, implies that $|b| = 1$, and the claim follows. □

In view of Lemma 3.1 and Theorem 2.6, to complete the proof of Theorem 1.2 it now suffices to prove the following result.

Theorem 3.2. *Let Λ be a cyclic subgroup of $\mathbb{Z}^2$ generated by an element $(m_1, m_2) \in \mathbb{Z}^2 \setminus \{0\}$. Let E be the image of the standard basis $\{e_1, e_2\}$ in the quotient $\mathbb{Z}^2/\Lambda$. Then*

$$\mathrm{Md}_{\mathbb{Z}^2/\Lambda}(E) = \lfloor k/2 \rfloor / k, \quad \textit{where} \quad k = |m_1| + |m_2|. \tag{20}$$

The basic idea of the proof is that the (undirected) Cayley graph $\mathrm{Cay}(\mathbb{Z}^2/\Lambda, E)$ can be decomposed by partitioning $\mathbb{Z}^2/\Lambda$ into translates of a cycle of length k in the graph, so that $\mathrm{Md}_{\mathbb{Z}^2/\Lambda}(E)$ is then easily shown to equal the independence ratio of this cycle.

Proof. We can assume without loss of generality that $m_1 \geq 0$ and $m_2 > 0$.

Let R denote the set $\mathbb{Z}(1, -1) + [0, k-1] \times \{0\} = \{(n_1, n_2) \in \mathbb{Z}^2 : n_1 + n_2 \in [0, k-1]\}$. It is easily checked that R is a fundamental domain for the action of Λ on $\mathbb{Z}^2$. For this proof we identify $\mathbb{Z}^2/\Lambda$ as a group with R equipped with addition mod Λ (i.e. addition in $\mathbb{Z}^2$ composed with reduction mod Λ into R), and we identify E with $\{e_1, e_2\} \subset R$.

Let G be the Cayley graph on R with generating set E, i.e. with uv being an edge in G if and only if $v - u \in \{e_1, -e_1, e_2, -e_2\}$ (where the operations are in R). Let $C = C_1 \cup C_2 \subset R$ where $C_1 = \{(0, i) : i \in [0, m_2 - 1]\}$ and $C_2 = \{(i, m_2 - 1) : i \in [m_1]\}$ (if $m_1 = 0$ then $C_2 = \emptyset$). Note that the subgraph of G induced by C (denoted by $G[C]$) is a k-cycle. Note also that $R = \bigsqcup_{n \in \mathbb{Z}} C + n(1, -1)$.

We now prove that $\mathrm{Md}_{\mathbb{Z}^2/\Lambda}(E)$ is the independence ratio of $G[C]$, i.e. $\frac{\lfloor k/2 \rfloor}{k}$. For $N \in \mathbb{N}$ let $F_N = \bigsqcup_{n=-N}^{N} C + n(1, -1)$. It is easily seen that $(F_N)_{N \in \mathbb{N}}$ is a Følner sequence in R.

To see that $\mathrm{Md}_{\mathbb{Z}^2/\Lambda}(E) \geq \frac{\lfloor k/2 \rfloor}{k}$, let S be a stable subset of C of maximal size (thus $|S| = \lfloor k/2 \rfloor$) and note that S is E-avoiding. Let $A := \bigsqcup_{n \in \mathbb{Z}} S + n(1, -1) = S + \mathbb{Z}(1, -1)$. We claim that A is E-avoiding. Indeed, suppose for a contradiction that there is $x \in A$ with $x + e_i \in A$ for $i = 1$ or 2. Since A is invariant under translation by elements of $\mathbb{Z}(1, -1)$, we can suppose that $x \in S$. If $x + e_1 \in A$, then we must have $x + e_1 \in S \cup (S + (1, -1))$. This implies that $(S + e_1) \cap [S \cup (S + (1, -1))] \neq \emptyset$, which implies that $S - S$ contains e_1 or e_2, which is impossible since S is E-avoiding. If $x + e_2 \in A$, then $x + e_2 \in S \cup (S - (1, -1))$, but then $(S + e_2) \cap [S \cup (S - (1, -1))] \neq \emptyset$, which similarly contradicts that S is E-avoiding. This proves our claim. Now note that $\frac{|A \cap F_N|}{|F_N|} = \frac{|S|}{|C|} = \frac{\lfloor k/2 \rfloor}{k}$ for all N. Hence by (11) we have $\mathrm{Md}_{\mathbb{Z}^2/\Lambda}(E) \geq \frac{\lfloor k/2 \rfloor}{k}$.

To see that $\mathrm{Md}_{\mathbb{Z}^2/\Lambda}(E) \leq \frac{\lfloor k/2 \rfloor}{k}$, note that for any $\varepsilon > 0$, by (11), for some $N \in \mathbb{N}$ there exists an E-avoiding set $A \subset F_N$ such that $\frac{|A|}{|F_N|} \geq \mathrm{Md}_{\mathbb{Z}^2/\Lambda}(E) - \varepsilon$. We also have

$\frac{|A|}{|F_N|} = \frac{1}{(2N+1)k} \sum_{n=-N}^{N} |(C + n(1,-1)) \cap A|$. Now each set $A \cap (C + n(1,-1))$ is a stable set in (a translate of) the cycle $G[C]$, so this set has size at most $\lfloor k/2 \rfloor$. We deduce that $\frac{|A|}{|F_N|} \leq \frac{\lfloor k/2 \rfloor}{k}$, so $\mathrm{Md}_{\mathbb{Z}^2/\Lambda}(E) \leq \frac{\lfloor k/2 \rfloor}{k} + \varepsilon$ and the desired inequality follows letting $\varepsilon \to 0$. $\square$

4. $|D| = 2$, $D \subset \mathbb{Q}$: the independence ratio of 2-jump circulant graphs

When both elements of D are rational, it follows from Lemma 2.10 that $\mathrm{Md}_{\mathbb{T}}(D)$ is the independence ratio of a connected circulant graph with two jumps. Thus throughout this section we let G be a circulant graph $\mathrm{Cay}(\mathbb{Z}_N, \{d_1, d_2\})$ with $\gcd(N, d_1, d_2) = 1$. Our aim is to determine $\alpha(G)$.

It is well-known (and easily seen) that in this situation if G is bipartite then $\alpha(G) = \frac{N}{2}$, so from now on we assume that G is not bipartite and therefore contains an odd cycle. Recall that the odd girth of G is then the smallest length of an odd cycle in G. Then we have the following upper bound for $\alpha(G)$.

Lemma 4.1 (Odd-girth bound)**.** *Let G be a circulant graph of order N and odd girth k. Then*

$$\alpha(G) \leq \left\lfloor \tfrac{k-1}{2k} N \right\rfloor. \tag{21}$$

This is an immediate consequence of the "no homomorphism lemma" of Albertson and Collins, which we recall here; see [1, Theorem 2] and also [15, Lemma 3.3].

Lemma 4.2. *Let G be a vertex transitive graph and let H be a subgraph of G. Then $\alpha(G)/|V(G)| \leq \alpha(H)/|V(H)|$.*

Remark 4.3. The odd-girth bound (21) is attained in many cases. Note first that if G is 2-regular then d_1 equals d_2 or $-d_2$, i.e. there is just one jump of odd order N, so $\alpha(G)$ attains the odd-girth bound $\lfloor N/2 \rfloor$ in this case. If G is 3-regular (which occurs only if N is even and one of the jumps is $N/2$) then it can be seen that the odd-girth bound is attained as well, using for instance [17, Corollary 2.27]. Therefore, from now on we assume that G is 4-regular. Among 4-regular connected circulant graphs, examples attaining the odd-girth bound include those given by Gao and Zhu in [12, Theorem 7], which have jumps 1 and d_2, with d_2 sufficiently small compared to N. We establish a different family of examples in Proposition 4.12.

Let us give a simple example that does not attain the odd-girth bound.

Example 4.4. Let $G = \mathrm{Cay}(\mathbb{Z}_{24}, \{3, 4\})$. This graph has odd girth 7: an example of a 7-cycle is $\{0, 3, 6, 9, 12, 8, 4\}$, and a simple inspection shows that G contains no shorter odd cycle. The odd-girth bound here is therefore $\lfloor \frac{3}{7}\, 24 \rfloor = 10$. However, there is no stable set of size 10 in G. One way to see this is to consider the four cosets of the subgroup

$H = \langle 4 \rangle$ of order 6. If A is a stable set, then each coset of H can contain at most 3 elements. Therefore there are two ways in which A could have 10 elements in total: either by having 3 elements in three cosets and one element in the fourth coset, or by having 3 elements in two cosets and 2 elements in the other two cosets. It can be seen by inspection that A cannot be stable in any of these two ways.

While $\alpha(G)$ can be less than the odd-girth bound, the presence of short odd cycles in G seems to be the principal obstruction to having large independent sets, and this motivates trying to determine $\alpha(G)$ in terms of the odd-girth bound. We shall achieve this in an asymptotic sense by proving Theorem 1.3. To this end, we shall use the following full-rank lattice naturally associated with G (which is also the special case in this setting of the lattice from (8)):

$$\Lambda = \{x \in \mathbb{Z}^2 : x_1 d_1 + x_2 d_2 = 0 \mod N\}, \tag{22}$$

that is, the lattice Λ is the kernel of the homomorphism

$$\varphi : \mathbb{Z}^2 \to \mathbb{Z}_N,\ (x_1, x_2) \mapsto x_1 d_1 + x_2 d_2 \mod N. \tag{23}$$

Since we suppose that $\langle d_1, d_2 \rangle = \mathbb{Z}_N$, we have that φ is surjective. Note that φ is also a graph homomorphism $\mathrm{Cay}(\mathbb{Z}^2, \{e_1, e_2\}) \to G$.

The lattice Λ is useful to analyze cycles in G. In particular, short cycles are related to the successive minima λ_1, λ_2 of Λ relative to the ℓ^1-norm, namely (see [4])

$$\lambda_1 = \min\{\rho : \dim\big(\mathrm{Span}(B_\rho \cap \Lambda)\big) \geq 1\}, \quad \lambda_2 = \min\{\rho : \dim\big(\mathrm{Span}(B_\rho \cap \Lambda)\big) \geq 2\}, \tag{24}$$

where B_ρ is the ball in $\mathbb{R}^2$ centered at the origin and of radius ρ relative to the ℓ^1-norm.

Remark 4.5. The lattice in (22) is a special case of the lattice in (8). These objects, as well as the role played by short odd cycles, are some ideas unifying the various cases of Motzkin's problem treated in this paper. We say more about this in Section 5.

The following lemma shows that we can always select a convenient basis for Λ.

Lemma 4.6. *Let $G = \mathrm{Cay}(\mathbb{Z}_N, \{d_1, d_2\})$ with $\langle d_1, d_2 \rangle = \mathbb{Z}_N$, and let λ_1, λ_2 be the successive minima defined in* (24)*. Then there exist $u, v \in \Lambda$ with the following properties:*

(*i*) *$\{u, v\}$ is a basis of Λ such that $\|u\|_1 = \lambda_1$, $\|v\|_1 = \lambda_2$.*

(*ii*) *If G has odd girth k, then $k \in \{\lambda_1, \lambda_2\}$.*

Proof. Property (*i*) is a standard result (see [4, p. 204, Lemma 1]).

To see property (*ii*), note first that λ_1, λ_2 are both lengths of cycles in G. Indeed, given any $w \in \mathbb{Z}^2$ let $P(w)$ denote the path in $\mathbb{Z}^2$ that starts at the origin, then adds $e_1 = (1, 0)$ if $w_1 > 0$ (resp. $-e_1$ if $w_1 < 0$) until it reaches $(w_1, 0)$ and then adds $e_2 = (0, 1)$ if $w_2 > 0$ (resp. $-e_2$ if $w_2 < 0$) until it ends at w. Note that if w is u or v, then the map φ from (23) is injective on $P(w) \setminus \{w\}$, so that $\varphi(P(w))$ is indeed a cycle in G of length

$\|w\|_1 = \lambda_i$. Indeed, suppose for a contradiction that there exist $x, y \in P(w) \setminus \{w\}$ with $\varphi(x) = \varphi(y)$ and $\|x\|_1 < \|y\|_1$. Then $y - x \in \Lambda \setminus \{0\}$ would have $\|y - x\|_1 < \|w\|_1 \leq \lambda_2$, so $y - x$ would be in $\pm u$ (see [4, p. 204, Lemma 1]). It follows that $w = v$. Then $v - (y - x) = w - (y - x)$ is an element of $\Lambda \setminus \{0\}$ of ℓ^1-norm less than λ_2, so it is also $\pm u$. This contradicts the linear independence of u, v.

If G has odd girth k, then by translating we find a k-cycle $C = (x_0 = 0, x_1, \ldots, x_k = 0)$ in G. We can then construct a walk $\tilde{C} = (\tilde{x}_0 = 0, \tilde{x}_1, \ldots, \tilde{x}_k)$ in $\mathrm{Cay}(\mathbb{Z}^2, \{e_1, e_2\})$ such that $\varphi(\tilde{C}) = C$ (in particular φ restricted to $\tilde{C} \setminus \{\tilde{x}_k\}$ is bijective onto C). Note that $\tilde{x}_k$ is in Λ and cannot be 0, since otherwise k would be even. Hence $\|\tilde{x}_k\|_1 \geq \lambda_1$, and so $k \geq \lambda_1$. If λ_1 is odd, then we must have $k = \lambda_1$, since by the previous paragraph λ_1 is the length of an odd cycle in G, and k is the minimal such length. If λ_1 is even, then λ_2 must be odd. Indeed, otherwise for every cycle $C = (x_0 = 0, x_1, \ldots, x_{n-1}, x_n = 0)$ in G, for the walk $\tilde{C} = (\tilde{x}_0 = 0, \tilde{x}_1, \ldots, \tilde{x}_n)$ in $\mathbb{Z}^2$ satisfying $\varphi(\tilde{C}) = C$, we have that $\tilde{x}_n \in \Lambda$, so $\tilde{x}_n$ is an integer combination of u, v and therefore $\|\tilde{x}_n\|_1$ would be even. This would imply that every cycle in G has even length, contradicting that G has odd cycles. Since k cannot be the even number λ_1 and is at least the ℓ^1-norm of some non-zero element in Λ, we have $k \geq \lambda_2$, whence $k = \lambda_2$ (since λ_2 is an odd-cycle length). This proves property *(ii)*. $\square$

We shall use the basis $\{u, v\}$ to estimate $\alpha(G)$, our main objective being to prove Theorem 1.3. We begin by reformulating the bipartite case in terms of the minima from (24).

Lemma 4.7. *We have $\alpha(G) = N/2$ if and only if λ_1 and λ_2 are both even.*

Proof. We first prove the backward implication. If λ_1 and λ_2 are both even, then, as noted in the proof of Lemma 4.6, the graph G has no odd cycles, so it is bipartite and therefore $\alpha(G) = N/2$.

For the forward implication, note that if one of λ_1, λ_2 is odd then G has odd girth $k \in \{\lambda_1, \lambda_2\}$ by Lemma 4.6, so by Lemma 4.2 we have $\alpha(G) \leq \frac{k-1}{2k} N < N/2$. $\square$

Thus, to prove Theorem 1.3 we can assume that at least one of u, v has odd ℓ^1-norm.

Let $\mathcal{P}$ denote the parallelogram determined by u, v:

$$\mathcal{P} := [0,1)^2 \cdot (u, v) := \{\alpha u + \beta v : \alpha, \beta \in [0,1)\}.$$

By standard results, the Lebesgue measure of $\mathcal{P}$ is the absolute value of $\det\left(\begin{smallmatrix} u_1 & v_1 \\ u_2 & v_2 \end{smallmatrix}\right)$, which is also equal to the index $|\mathbb{Z}^2/\Lambda|$, which equals N by the first isomorphism theorem and the surjectivity of φ. Moreover, since $\mathcal{P}$ is also a fundamental domain for $\mathbb{Z}^2/\Lambda$, we have that $|\mathcal{P} \cap \mathbb{Z}^2|$ is also equal to $|\mathbb{Z}^2/\Lambda|$, so

$$|\mathcal{P} \cap \mathbb{Z}^2| = N. \tag{25}$$

The following result tells us that for each $i \in \{1, 2\}$ we can always partition a subset of $\mathbb{Z}_N$ of maximum possible size into useful translates of a cycle of length λ_i.

Lemma 4.8. *Let $G = \mathrm{Cay}(\mathbb{Z}_N, \{d_1, d_2\})$ be 4-regular with $\langle d_1, d_2\rangle = \mathbb{Z}_N$, let Λ be the associated lattice from* (22)*, and let λ_1, λ_2 be the successive minima of Λ relative to the ℓ^1-norm. Then for each $i \in \{1, 2\}$ there exists a λ_i-cycle C_i in G and $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$ such that we have the following union of pairwise disjoint translates of C_i in $\mathbb{Z}_N$:*

$$\bigsqcup_{t=0}^{\lfloor \frac{N}{\lambda_i} \rfloor - 1} \big(C_i + t(\varepsilon_1 d_1 + \varepsilon_2 d_2)\big). \tag{26}$$

The idea of the proof is that there is a lattice path in $\mathbb{Z}^2$ which represents a λ_i-cycle and has the property that, modulo Λ, one can tile a subset of $\mathcal{P} \cap \mathbb{Z}^2$ as large as possible with certain translates of this path. The images of these translates under φ then yield (26).

Proof. Let $\{u, v\}$ be the basis of Λ provided by Lemma 4.6. We prove (26) for $i = 1$; the proof for $i = 2$ is similar. Note that the operations of permuting d_1, d_2 and changing their sign all yield isomorphisms of G, and that the conclusion of the lemma is not affected by these operations. It follows that, by performing such operations if necessary, we can assume that u has both coordinates non-negative and the angle from u to v is in $(\pi, 2\pi)$ (i.e. $\det\left(\begin{smallmatrix} u_1 & v_1 \\ u_2 & v_2 \end{smallmatrix}\right) < 0$). In the resulting more specific situation, we can prove (26) with $\varepsilon_1 = -\varepsilon_2 = 1$, as follows.

We first settle the case in which one of u_1, u_2 is 0. If $u_1 = 0$, then $u_2 = \lambda_1$ is the order of d_2 in $\mathbb{Z}_N$. We then set C_1 to be the cycle $\langle d_2 \rangle$. By Minkowski's second theorem [4, p. 203, (12)] we have $\lambda_1 \lambda_2 \leq 2N$, and each λ_i is at least 3 (otherwise G is not 4-regular). Hence $\lambda_i < N$, so in particular C_1 is a proper subgroup of $\mathbb{Z}_N$. Since $\langle d_1, d_2 \rangle = \mathbb{Z}_N$, the cosets of the form $C_1 + td_1$, $t \geq 0$ cover $\mathbb{Z}_N$. Then the smallest $t \in \mathbb{N}$ such that $td_1 \in C_1$ is $t = N/\lambda_1$ (in particular $d_1 \notin C_1$). Hence (26) holds, as a particular way to write the partition of $\mathbb{Z}_N$ into cosets of C_1. A similar argument yields (26) when $u_2 = 0$.

We assume from now on that $u_1, u_2 > 0$. Let $\tilde{C}_1 = (x^{(1)} = 0, x^{(2)}, \ldots, x^{(\lambda_1)} = u - e_2)$ be the lattice path in $\mathbb{Z}^2$ of length λ_1 which starts at the origin, ends at $u - e_2$, and stays as close as possible to the line $\mathbb{R}u$ while staying below this line (i.e. $x_2^{(j)} \leq \frac{u_2}{u_1} x_1^{(j)}$ for all $j \in [\lambda_1]$). We can describe $\tilde{C}_1$ inductively as follows:

$$x^{(1)} = 0, \quad \text{and for } j \in [\lambda_1 - 1],\ x^{(j+1)} = \begin{cases} x^{(j)} + e_1, & \frac{u_2}{u_1} x_1^{(j)} - x_2^{(j)} \in [0, 1) \\ x^{(j)} + e_2, & \frac{u_2}{u_1} x_1^{(j)} - x_2^{(j)} \geq 1 \end{cases}. \tag{27}$$

We now determine the greatest positive integer s such that the homomorphism φ from (23) is injective on $\bigcup_{t=0}^{s} (\tilde{C}_1 + t(1, -1))$. First note that, for every $s \in \mathbb{N}$, there is no pair of points in this union differing by a non-zero multiple of u. Indeed, supposing that $x \in \tilde{C}_1 + i(1, -1)$ and $y \in \tilde{C}_1 + j(1, -1)$ for $j \geq i$, then y cannot be $x + u$ (let alone being $x + ru$ for any integer $r > 1$), for we have $y_2 \leq u_2 - 1 - j$, while $x_2 + u_2 \geq u_2 - i$, so $x_2 + u_2 - y_2 \geq j - i + 1 > 0$. Therefore φ is injective on $\bigcup_{t=0}^{s} \tilde{C}_1 + t(1, -1)$ if and only if no pair of points in this union differ by a lattice point of the form $au + bv$ with $a, b \in \mathbb{Z}$

and $b \neq 0$. A sufficient condition for this to hold is that every point in the union lies strictly above the line $v + \mathbb{R}u$. To ensure that this condition holds, it suffices to ensure that no point of $\tilde{C}_1 + (s, -s)$ lies on or below the line $v + \mathbb{R}u$. Let z denote the point in $\tilde{C}_1$ most distant from $\mathbb{R}u$ in the direction of $(1, -1)$, i.e. the point that maximizes the Euclidean length of the line segment parallel to $(1, -1)$ joining the point to the line $\mathbb{R}u$. Then the above condition holds if we let s be $\lfloor \sigma \rfloor$ where σ, η are the unique real solutions to $z + (\sigma, -\sigma) = v + \eta u$.

To determine z, we note that this is a point in $\tilde{C}_1$ which has maximum vertical distance to $\mathbb{R}u$. Hence $z = x^{(j+1)}$ where $x^{(j)}$ has vertical distance d to $\mathbb{R}u$ which is maximum subject to being less than 1. Thus $d = \max_{j \in [0, u_1 - 1]} \{ j \frac{u_2}{u_1} \} = 1 - \frac{\gcd(u_1, u_2)}{u_1}$, so the vertical distance from z to $\mathbb{R}u$ is $d + \frac{u_2}{u_1} = \frac{u_1 + u_2 - \gcd(u_1, u_2)}{u_1}$. The problem thus reduces to calculating σ such that $(0, -\frac{u_1 + u_2 - \gcd\{u_1, u_2\}}{u_1}) + \sigma(1, -1) \in v + \mathbb{R}u$. We obtain (using in particular that $\lambda_1 = u_1 + u_2$) that $\sigma = \frac{N}{\lambda_1} - 1 + \frac{\gcd(u_1, u_2)}{\lambda_1} > \frac{N}{\lambda_1} - 1$. Hence, setting $s = \lfloor \sigma \rfloor \geq \lfloor \frac{N}{\lambda_1} \rfloor - 1$, we conclude that φ is injective on the set $S := \bigcup_{t=0}^{s} \big(\tilde{C}_1 + t(1, -1) \big)$. It is easily seen from (27) that the translates of $\tilde{C}_1$ forming S are pairwise disjoint and by injectivity of φ the same holds for the images of these translates under φ. Letting C_1 be the cycle $\varphi(\tilde{C}_1)$ in G, we deduce (26) in this case, which completes the proof. $\square$

Using the tiling by cycles in Lemma 4.8, we can form large independent sets in G by carefully choosing a maximal independent subset in each translate of C_i in (26) except the last translate. This yields the following result.

Proposition 4.9. *Let $G = \mathrm{Cay}(\mathbb{Z}_N, \{d_1, d_2\})$ be 4-regular with $\langle d_1, d_2 \rangle = \mathbb{Z}_N$, let Λ be the associated lattice from (22), and let λ_1, λ_2 be the successive minima of Λ relative to the ℓ^1-norm. Then*

$$\alpha(G) \;\geq\; \max_{i \in \{1,2\}} \; \big(\lfloor \tfrac{N}{\lambda_i} \rfloor - 1 \big) \lfloor \tfrac{\lambda_i}{2} \rfloor. \tag{28}$$

Proof. Let $\bigsqcup_{t=0}^{s} (C_i + t(\varepsilon_1 d_1 + \varepsilon_2 d_2))$ be the partition in (26), with $s = \lfloor \frac{N}{\lambda_i} \rfloor - 1$. Let B be the independent subset of C_i of maximal size obtained by starting from 0 and picking one of every two successive elements, stopping once we have picked $\lfloor \frac{\lambda_1}{2} \rfloor$ elements. Let $A := \bigsqcup_{t=0}^{s-1} \big(B + t(\varepsilon_1 d_1 + \varepsilon_2 d_2) \big)$. It suffices to prove that A is stable, as then $\alpha(G) \geq |A| \geq s \lfloor \frac{\lambda_i}{2} \rfloor$. We prove this for $i = 1$; the proof for $i = 2$ is similar. By similar initial operations as in the previous proof, we may assume that $\varepsilon_1 = -\varepsilon_2 = 1$, $u_1, u_2 \geq 0$, and $\det\left(\begin{smallmatrix} u_1 & v_1 \\ u_2 & v_2 \end{smallmatrix} \right) < 0$.

Suppose for a contradiction that vertices $x, y \in A$ form an edge in G. Since B is stable, these vertices must lie in distinct translates of C_1. Shifting and relabeling, we can suppose that $x \in B$ and $y \in B + t'(d_1 - d_2)$ for some $t' \in [1, s-1]$.

We claim that $t' = 1$. To see this let $\tilde{C}_1$ be the $\mathbb{Z}^2$-path described in (27), and note that since φ is bijective on $\bigsqcup_{t=0}^{s} \big(\tilde{C}_1 + t(1, -1) \big)$, there are unique $\tilde{x} \in \tilde{C}_1$ and $\tilde{y} \in \tilde{C}_1 + t'(1, -1)$

with $\varphi(\tilde{x}) = x$, $\varphi(\tilde{y}) = y$. The distance in G between x and y (i.e. the length of a shortest path from x to y in G) is $\|\tilde{y} - \tilde{x}\|_{\ell^1/\Lambda} := \min_{z\in\Lambda} \|\tilde{y} - \tilde{x} - z\|_1$. Since x, y are neighbours in G, this distance is 1, so there is $z \in \Lambda$ and $w \in \{\pm e_1, \pm e_2\}$ such that $\tilde{y} = \tilde{x} + w + z$. If $t' \geq 2$ then this cannot happen with z being just a multiple of u, so z must be of the form $n_1 u + n_2 v$ for $n_1 \in \mathbb{Z}$ and $n_2 \in \mathbb{N}$. But then $\tilde{y} - w = \tilde{x} + z$ lies on or below the line $v + \mathbb{R}u$, which is impossible by construction of s since $t \leq s - 1$. This proves our claim.

Since $t' = 1$, we have $\tilde{y} \in \tilde{C}_1 + (1, -1)$, and since $\tilde{y} = \tilde{x} + w + z$, we have that $\tilde{C}_1 + (1, -1)$ overlaps mod Λ with $\tilde{C}_1 + w$. By construction of $\tilde{C}_1$, this requires w to be e_1 or $-e_2$ (since $\tilde{C}_1 - e_1$ and $\tilde{C}_1 + e_2$ clearly do not overlap with $\tilde{C}_1 + (1, -1)$). We deduce that $y = \varphi(\tilde{x} + w + z)$ equals $x + d_1$ or $x - d_2$. Since $y = b + d_1 - d_2$ for some $b \in B$, we deduce that $b = x + d_2$ or $x - d_1$, so x, b are elements of B adjacent in G, contradicting that B is stable. This proves that A is stable and completes the proof. $\square$

Since the odd girth k of G is in $\{\lambda_1, \lambda_2\}$, from (28) we deduce immediately that

$$\alpha(G) \geq \left(\lfloor \tfrac{N}{k} \rfloor - 1\right) \tfrac{k-1}{2}. \tag{29}$$

This may look close to the odd-girth bound, but the two bounds can in fact differ by as much as a fraction of N, when k is proportional to N. However, we can use (28) together with Minkowski's second theorem to obtain the following result, which implies the lower bound in (5) and thus completes the proof of Theorem 1.3.

Theorem 4.10. *Let $G = \mathrm{Cay}(\mathbb{Z}_N, \{d_1, d_2\})$ with $\langle d_1, d_2\rangle = \mathbb{Z}_N$, and suppose that G has odd girth k. Then*

$$\lfloor \tfrac{k-1}{2k} N \rfloor \;\geq\; \alpha(G) \;\geq\; \lceil \tfrac{k-1}{2k} N - \sqrt{2N} + 1 \rceil. \tag{30}$$

Proof. By (21), it suffices to prove the lower bound for $\alpha(G)$ in (30). As noted in Remark 4.3, if G is d-regular with $d < 4$ and has odd girth k, then we already know that $\alpha(G) = \lfloor \frac{k-1}{2k} N \rfloor$, so (30) holds in these cases. We therefore assume from now on that G is 4-regular.

Suppose first that $k = \lambda_1$. Then by Minkowski's second theorem we have

$$k \leq \sqrt{\lambda_1 \lambda_2} \leq \sqrt{2N}. \tag{31}$$

Therefore, in this case by (28) we have

$$\alpha(G) \geq \left(\lfloor \tfrac{N}{k} \rfloor - 1\right) \tfrac{k-1}{2} > \left(\tfrac{N}{k} - 2\right) \tfrac{k-1}{2} \geq \tfrac{k-1}{2k} N - k + 1 \geq \tfrac{k-1}{2k} N - \sqrt{2N} + 1.$$

Supposing instead that $k = \lambda_2 > \lambda_1$, then by minimality of k and the fact that λ_1 is the length of a cycle in G, we have that λ_1 must be even, so $\lambda_1 \geq 4$ (since G is 4-regular). By Minkowski's second theorem again we have $\lambda_1 \leq \sqrt{2N}$. Then by (28) we have (using that $2k \leq \lambda_1 \lambda_2 / 2 \leq N$)

$$\alpha(G) \geq \left(\lfloor \tfrac{N}{\lambda_1} \rfloor - 1\right) \tfrac{\lambda_1}{2} > \tfrac{N}{2} - \lambda_1 \geq \tfrac{k-1}{2k} N + \tfrac{N}{2k} - \sqrt{2N} \geq \tfrac{k-1}{2k} N - \sqrt{2N} + 1. \qquad \square$$

Remark 4.11. As mentioned above, from (30) we immediately deduce the asymptotically sharp estimate (5). To compute the main term $\frac{k-1}{2k}$ in this estimate, it suffices to find the vectors u, v from Lemma 4.6. This can be done using the Lagrange-Gauss reduction algorithm for the ℓ^1-norm [19], starting from any basis u', v' for Λ (for instance $u' = (\frac{d_2}{g}, -\frac{d_1}{g})$, $v' = (Na, Nb)$ where $g = \gcd(d_1, d_2)$ and $a, b \in \mathbb{Z}$ satisfy $a\frac{d_1}{g} + b\frac{d_2}{g} = 1$).

To finish this section, we consider the problem of determining for which 4-regular circulant graphs with 2 jumps the independence number matches the odd-girth bound. We give the following family of such graphs, which is naturally described in terms of the associated lattice, and which differs significantly from the family given by Gao and Zhu in [12, Theorem 7].

Proposition 4.12. *Let $G = \mathrm{Cay}(\mathbb{Z}_N, \{d_1, d_2\})$ be 4-regular with $\langle d_1, d_2\rangle = \mathbb{Z}_N$, and suppose that G has odd girth k. Let w be the basis element in $\{u, v\}$ such that $\|w\|_1 = k$. If some coordinate of w is 0, then $\alpha(G)$ equals the odd-girth bound $\frac{k-1}{2k}N$.*

Note that by permuting d_1 and d_2 if necessary, we can assume that $w_1 = 0$, so that $w = (0, k)$. In this case the subgroup $\langle d_2\rangle \le \mathbb{Z}_N$ constitutes a k-cycle C in G (and in particular k divides N). Let $w' \in \{u, v\} \setminus \{w\}$. By Lemma 4.8 we have the partition

$$\mathbb{Z}_N = \bigsqcup_{t=0}^{w'_1-1} (C + td_1),$$

with $w'_1 = N/k$. In particular $w'_1 d_1 \in C$, so there is $j \in \left[-\frac{k-1}{2}, \frac{k-1}{2}\right]$ which is the integer with least absolute value such that $w'_1 d_1 + jd_2 = 0 \mod N$. Then, since $\|w'\|_1$ is the other smallest length of a non-trivial cycle in G, it follows that $w'_2 = j$.

Proof of Proposition 4.12. We first observe that the following claim implies the conclusion of the proposition.

$$\text{There is a walk } p_0, p_1, \ldots, p_{w'_1} \text{ in } \mathrm{Cay}(\mathbb{Z}_k, \{1, -1\}) \text{ starting at 0 and ending at } w'_2. \quad (32)$$

Indeed, if (32) holds then we can construct a set $A \subset \mathbb{Z}_N$ that is stable in G and has $|A| = \frac{k-1}{2k}N$, as follows. The set $A_0 = \{0, 2d_2, 4d_2, \ldots, (k-3)d_2\} \subset C$ is stable in G and has size $\frac{k-1}{2}$ (which is maximal subject to being a stable set included in C). Then, letting $p_0, p_1, \ldots, p_{w'_1}$ be a walk as described in (32), the following set is stable of size $\frac{N}{k}\frac{k-1}{2}$:

$$A = \bigsqcup_{t=0}^{w'_1-1} A_0 + td_1 + p_t d_2.$$

We now prove the claim (32), by distinguishing two cases according to the parity of $\|w'\|_1$.

Suppose that $\|w'\|_1$ is odd. Then $w'_1 + |w'_2| = \|w'\|_1 \ge k$. Then $\frac{N}{k} = w'_1 \ge k - |w'_2|$. We can then see that there is a walk as claimed in (32), as follows. Since $w'_1 - (k - |w'_2|)$ is non-negative even, we can start the walk by alternating $+1$ and -1, setting $p_0 = 0$,

$p_1 = 1$, $p_2 = 0$, and so on up to $p_{w'_1-(k-|w'_2|)} = 0$. From here the walk becomes monotonic, adding only $+1$s (resp. -1s) to end at $p_{w'_1} = k - |w'_2| \equiv w'_2 \mod k$ if $w'_2 \in [-\frac{k-1}{2}, 0)$ (resp. $p_{w'_1} = -(k-|w'_2|) \equiv w'_2 \mod k$ if $w'_2 \in [0, \frac{k-1}{2}]$).

Suppose now that $\|w'\|_1$ is even. We claim that $w'_1 \geq |w'_2|$. Indeed, otherwise the number $w'_1 + k - |w'_2|$ is less than k, is odd (since it equals $k + \|w'\|_1 - 2|w'_2|$), and is positive (since $|w'_2| \leq \frac{k-1}{2}$). On the other hand this number is the length of an odd cycle in G. Indeed, since $w' \in \Lambda$, we have $sw'_1 d_1 + |w'_2| d_2 = 0 \mod N$ for some $s \in \{1, -1\}$. Hence, since d_2 has order k, we have $-sw'_1 d_1 + (k - |w'_2|)d_2 = 0 \mod N$, which indeed implies the existence of a cycle of length $w'_1 + k - |w'_2|$. This proves our claim. Since $w'_1 \geq |w'_2|$, we have that $w'_1 - |w'_2| = \|w'\|_1 - 2|w'_2|$ is non-negative even. We can then construct a walk as claimed in (32) as follows. We start again by alternating $+1$ and -1, setting $p_0 = 0$, $p_1 = 1$, $p_2 = 0$, and so on up to $p_{w'_1 - |w'_2|} = 0$. From here the path goes monotonically again, to end at $p_{w'_1} = w'_2$ (adding only $+1$s if $w'_2 \in [0, \frac{k-1}{2}]$ and only -1s if $w'_2 \in [-\frac{k-1}{2}, 0)$). □

5. Final remarks

As mentioned in the introduction and explained in Remark 2.11, Motzkin's problem in $\mathbb{T}$ can be seen to subsume (in its rational case $D \subset \mathbb{Q}$) the original problem in $\mathbb{Z}$. At the end of the introduction we mention a more specific instance of this, namely that the asymptotic solution to the case of two rational missing differences in $\mathbb{T}$ (i.e. Theorem 1.3) implies the classical solution (2) of Cantor and Gordon, namely $\mathrm{Md}_{\mathbb{Z}}(\{d_1, d_2\}) = \frac{\lfloor (d_1+d_2)/2 \rfloor}{d_1+d_2}$ for any coprime positive integers d_1, d_2. Let us detail this.

As explained in Remark 2.11, we have $\mathrm{Md}_{\mathbb{Z}_N}(\{d_1, d_2\}) \to \mathrm{Md}_{\mathbb{Z}}(\{d_1, d_2\})$ as $N \to \infty$. It is easily seen that if d_1, d_2 are both odd then, for N even, the circulant graph $G_N := \mathrm{Cay}(\mathbb{Z}_N, \{d_1, d_2\})$ is bipartite, while if d_1, d_2 have different parity then for large N the graph G_N has odd girth $d_1 + d_2$. Hence in all cases Theorem 1.3 indeed yields formula (2) in the limit. In particular, in the non-bipartite case, formula (2) can be written in terms of the odd girth k of $\mathrm{Cay}(\mathbb{Z}, \{d_1, d_2\})$, namely $\mathrm{Md}_{\mathbb{Z}}(\{d_1, d_2\}) = \frac{k-1}{2k}$.

Formula (4) can also be phrased in terms of the odd girth of an associated graph, namely the uncountable Cayley graph $G = \mathrm{Cay}(\mathbb{T}, \{t_1, t_2\})$. Under the assumptions of Theorem 1.2, it can be seen that if m_1, m_2 have equal parity then G is bipartite (since then every element of Λ is a multiple of (m_1, m_2) by Lemma 3.1 and therefore has even ℓ^1-norm, which implies that every cycle in G is even), and otherwise G has odd girth $k = |m_1| + |m_2|$, so that formula (4) can be written $\mathrm{Md}_{\mathbb{T}}(\{t_1, t_2\}) = \frac{k-1}{2k}$.

These connections suggest that there may be a more fundamental result, phrased in terms of the odd girth of a more general type of Cayley graph, which would imply all the above results in the case $|D| = 2$, thus shedding more light on the above connections.

It would be interesting to explore Motzkin's problem further, for instance in other compact abelian groups. In this direction there are known results in combinatorics which can be viewed as determining Motzkin densities in certain complex cases. We have for example the main result from the paper [22] by Kleitman, which can be phrased as follows.

Theorem 5.1 (Kleitman 1966)**.** *Let $k, n \in \mathbb{N}$ with $2k \leq n$. Let $G = \mathbb{Z}_2^n$, and let*

$$D = \{(x_1, \ldots, x_n) \in G : \#\{j : x_j = 1\} > 2k\}.$$

Then $\mathrm{Md}_G(D) = \frac{1}{2^n} \sum_{i=0}^{k} \binom{n}{i}$.

It would also be interesting to understand more precisely which connected circulant graphs with 2 jumps have independence number equal to the odd-girth bound (21), and more generally to refine Theorem 4.10 further. One may also consider whether, and in what form, the asymptotically sharp estimate (5) can be extended to circulant graphs with more than 2 jumps.

References

[1] M. O. Albertson, K. L. Collins, *Homomorphisms of 3-chromatic graphs*, Discrete Math. **54** (1985), 127–132.

[2] A. Avila, P. Candela, *Towers for commuting endomorphisms, and combinatorial applications.* Ann. Inst. Fourier (Grenoble) **66** (2016), no. 4, 1529-1544.

[3] J.-C. Bermond, F. Comellas, D.F. Hsu, *Distributed loop computer networks: A survey*, Journal of Parallel and Distributed Computing **24** (1995), 2–10.

[4] J. W. S. Cassels, *An introduction to the geometry of numbers*, Corrected reprint of the 1971 edition. Classics in Mathematics. Springer-Verlag, Berlin, 1997. viii + 344 pp.

[5] J.-Y. Cai, G. Havas, B. Mans, A. Nerurkar, J.-P. Seifert, I. Shparlinski, *On routing in circulant graphs*, Computing and combinatorics (Tokyo, 1999), 360–369, Lecture Notes in Comput. Sci., 1627, Springer, Berlin, 1999.

[6] D.G. Cantor, B. Gordon, *Sequences of integers with missing differences.* Journal of Combinatorial Theory (A) **14** (1973), 281–287.

[7] J. P. Conze, *Entropie d'un groupe abélien de transformations*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **25** (1972/73), 11–30.

[8] D. Coppersmith, C. K. Wong, *A combinatorial problem related to multimodule memory organizations*, J. Assoc. Comput. Mach. **21** (1974), 392–402.

[9] S. I. R. Costa, J. E. Strapasson, M. M. S. Alves, T. B. Carlos, *Circulant graphs and tessellations on flat tori*, Linear Algebra Appl. **432** (2010), no. 1, 369–382.

[10] A. H. Dooley, G. Zhang, *Local entropy theory of a random dynamical system*, Mem. Amer. Math. Soc. **233** (2015), no. 1099, vi+106 pp.

[11] G. Fiz Pontiveros, *Sums of dilates in $\mathbb{Z}_p$*, Combin. Probab. Comput. **22** (2013), no. 2, 282–293.

[12] G. Gao, X. Zhu, *Star-extremal graphs and the lexicographic product.* Discrete Math. **152** (1996), no. 1-3, 147–156.

[13] D. Gómez, J. Gutierrez, A. Ibeas, *Optimal routing in double loop networks*, Theoret. Comput. Sci. **381** (2007), no. 1-3, 68–85.

[14] S. Gupta, *Sets of integers with missing differences*, J. Combin. Theory Ser. A **89** (2000), no. 1, 55–69.

[15] G. Hahn, C. Tardif, *Graph homomorphisms: structure and symmetry*, Graph symmetry (Montreal, PQ, 1996), 107–166, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 497, Kluwer Acad. Publ., Dordrecht, 1997.

[16] N. M. Haralambis, *Sets of integers with missing differences*, J. Combin. Theory (A) **23** (1977), 22–33.

[17] R. Hoshino, *Independence polynomials of circulant graphs*, Thesis (Ph.D.)–Dalhousie University (Canada). 2008. 269 pp.

[18] F.K. Hwang, *A complementary survey on double loop networks*, Theoretical Computer Science **263** (2001) 211–229.

[19] M. Kaib, C. P. Schnorr, *The generalized Gauss reduction algorithm*, J. Algorithms **21** (1996), no. 3, 565–578.

[20] Y. Katznelson, B. Weiss, *Commuting measure preserving transformations*, Israel J. Math. **12** (1972), 161–173.

[21] A. S. Kechris, *Classical descriptive set theory*, Graduate Texts in Mathematics, **156**. Springer-Verlag, New York, 1995.

[22] D. J. Kleitman, *On a combinatorial conjecture of Erdős*, J. Combinatorial Theory 1 (1966), 209–214.

[23] K. W. Lih, D. Liu, X. Zhu, *Star-extremal circulant graphs*, SIAM J. Discrete Math. **12** (1999) 491–499.

[24] E. Lindenstrauss, *Pointwise theorems for amenable groups*. Invent. Math. **146** (2001), no. 2, 259–295.

[25] E. Lindenstrauss, B. Weiss, *Mean topological dimension*, Israel J. Math. **115** (2000), 1–24.

[26] D. Liu, *From rainbow to the lonely runner: a survey on coloring parameters of distance graphs*, Taiwanese J. Math. **12** (2008), no. 4, 851–871.

[27] D. Liu, G. Robinson, *Sequences of integers with three missing separations*, European J. Combin. **85** (2020), 11 pp.

[28] J. Marklof, A. Strömbergsson, *Diameters of random circulant graphs*, Combinatorica **33** (2013), no. 4, 429–466.

[29] D. S. Ornstein, B. Weiss, *Entropy and isomorphism theorems for actions of amenable groups*, J. Analyse Math. **48** (1987), 1–141.

[30] R. K. Pandey, *Maximal upper asymptotic density of sets of integers with missing differences from a given set*, Math. Bohem. **140** (2015), no. 1, 53–69.

[31] R. K. Pandey, A. Tripathi, *On the density of integral sets with missing differences*, Combinatorial number theory, 157–169, Walter de Gruyter, Berlin, 2009.

[32] R. K. Pandey, O. Prakash, S. Srivastava, *Motzkin's maximal density and related chromatic numbers*, Unif. Distrib. Theory **13** (2018), no. 1, 27–45.

Universidad Autónoma de Madrid and ICMAT, Ciudad Universitaria de Cantoblanco, Madrid 28049, Spain

E-mail address: pablo.candela@uam.es

Universidad Autónoma de Madrid, Ciudad Universitaria de Cantoblanco, Madrid 28049, Spain

E-mail address: carlos.cataladela@predoc.uam.es

Universitat Politècnica de Catalunya, Department of Mathematics, Barcelona 08034, Spain

E-mail address: juan.jose.rue@upc.edu

Universitat Politècnica de Catalunya, Department of Mathematics, Barcelona 08034, Spain

E-mail address: oriol.serra@upc.edu