Combinatorics, Probability and Computing (2024), **33**, pp. 484–486
doi:10.1017/S0963548324000051

ARTICLE

Sharp bounds for a discrete John's theorem

Peter van Hintum[1] and Peter Keevash[2]

[1]New College, University of Oxford, Oxford, UK and [2]Mathematical Institute, University of Oxford, Oxford, UK
Corresponding author: Peter van Hintum; Email: peter.vanhintum@new.ox.ac.uk

(Received 25 September 2023; revised 30 January 2024; accepted 2 February 2024; first published online 5 March 2024)

Abstract
Tao and Vu showed that every centrally symmetric convex progression $C \subset \mathbb{Z}^d$ is contained in a generalized arithmetic progression of size $d^{O(d^2)}\#C$. Berg and Henk improved the size bound to $d^{O(d\log d)}\#C$. We obtain the bound $d^{O(d)}\#C$, which is sharp up to the implied constant and is of the same form as the bound in the continuous setting given by John's theorem.

Keywords: Convex progression; generalised arithmetic progression; John's theorem
2020 MSC Codes: Primary: 52C07; Secondary: 52A27

1. Introduction

A classical theorem of John [2] shows that for any centrally symmetric convex set $K \subset \mathbb{R}^d$, there exists an ellipsoid E centred at the origin so that $E \subset K \subset \sqrt{d}E$. This immediately implies that there exists a parallelotope P so that $P \subset E \subset K \subset \sqrt{d}E \subset dP$. In the discrete setting, quantitative covering results are of great interest in Additive Combinatorics, a prominent example being the Polynomial Freiman–Ruzsa Conjecture, which asks for effective bounds on covering sets of small doubling by convex progressions. In this context, a natural analogue of John's theorem in $\mathbb{Z}^d$ would be covering centrally symmetric convex progressions by generalised arithmetic progressions. Here, a d-dimensional *convex progression* is a set of the form $K \cap \mathbb{Z}^d$, where $K \subset \mathbb{R}^d$ is convex and a d-dimensional *generalised arithmetic progression* (d-GAP) is a translate of a set of the form $\left\{\sum_{i=1}^d m_i a_i : 1 \leq m_i \leq n_i\right\}$ for some $n_i \in \mathbb{N}$ and $a_i \in \mathbb{Z}^d$.

Tao and Vu [4, 5] obtained such a discrete version of John's theorem, showing that for any origin-symmetric d-dimensional convex progression $C \subset \mathbb{Z}^d$ there exists a d-GAP P so that $P \subset C \subset O(d)^{3d/2} \cdot P$, where $m \cdot P := \left\{\sum_{i=1}^m p_i : p_i \in P\right\}$ denotes the iterated sumset. Berg and Henk [1] improved this to $P \subset C \subset d^{O(\log(d))} \cdot P$. Our focus will be on the covering aspect of these results, that is, minimising the ratio $\#P'/\#C$, where P' is a d-GAP covering C. This ratio is bounded by $d^{O(d^2)}$ by Tao and Vu and by $d^{O(d\log d)}$ by Berg and Henk. We obtain the bound $d^{O(d)}$, which is optimal.

Theorem 1.1. *For any origin-symmetric convex progression $C \subset \mathbb{Z}^d$, there exists a d-GAP P containing C with $\#P \leq O(d)^{3d}\#C$.*

Corollary 1.2. *For any origin-symmetric convex progression $C \subset \mathbb{Z}^d$ and linear map $\phi : \mathbb{R}^d \to \mathbb{R}$, there exists a d-GAP P containing C with $\#\phi(P) \leq O(d)^{3d}\#\phi(C)$.*

The optimality of Theorem 1.1 is demonstrated by the intersection of a ball B with a lattice L. Moreover, Lovett and Regev [3] obtained a more emphatic negative result, disproving the GAP analogue of the Polynomial Freiman–Ruzsa Conjecture, by showing that by considering a random lattice L one can find a convex d-progression $C = B \cap L$ such that any $O(d)$-GAP P with $\#P \leq \#C$ has $\#(P \cap C) < d^{-\Omega(d)}\#C$. Our result can be viewed as the positive counterpart that settles this line of enquiry, showing that indeed $d^{\Theta(d)}$ is the optimal ratio for covering convex progressions by GAPs.

2. Proof

We start by recording two simple observations and a proposition on a particular basis of a lattice, known as the Mahler Lattice Basis.

Observation 2.1. *Given an origin-symmetric convex set $K \subset \mathbb{R}^d$, there exists a origin-symmetric parallelotope Q and an origin-symmetric ellipsoid E so that $\frac{1}{d}Q \subset E \subset K \subset \sqrt{d}E \subset Q$, so in particular $|Q| \leq d^d|K|$.*

This is a simple consequence of John's theorem.

Observation 2.2. *Let $X, X' \in \mathbb{R}^{d\times d}$ be so that the rows of X and X' generate the same lattice of full rank in $\mathbb{R}^d$. Then $\exists T \in GL_n(\mathbb{Z})$ so that $TX = X'$.*

This can be seen by considering the Smith Normal Form of the matrices X and X'.

Proposition 2.3 (Corollary 3.35 from [4]). *Given a lattice $\Lambda \subset \mathbb{R}^d$ of full rank, there exists a lattice basis $v_1, \ldots, v_d$ of Λ so that $\prod_{i=1}^d \|v_i\|_2 \leq O(d^{3d/2}) \det(v_1, \ldots, v_d)$.*

With these three results in mind, we prove the theorem.

Proof of Theorem 1.1. By passing to a subspace if necessary, we may assume that C is full-dimensional. Write $C = K \cap \mathbb{Z}^d$ where $K \subset \mathbb{R}^d$ is origin-symmetric and convex. Use Observation 2.1 to find a parallelotope $Q \supset K$ so that $|Q| \leq d^d|K|$. Let the defining vectors of Q be $u_1, \ldots, u_d$, that is, $Q = \left\{\sum_i \lambda_i u_i : \lambda_i \in [-1, 1]\right\}$. Write u_i^j for the j-th coordinate of u_i and write U for the matrix $\left(u_i^j\right)$ with rows u^j and columns u_i.

Consider the lattice Λ generated by the vectors u^j (these are the vectors formed by the j-th coordinates of the vectors u_i). Using Proposition 2.3 find a basis $v^1, \ldots, v^d$ of Λ so that $\prod_{j=1}^d ||v^j||_2 \leq O\left(d^{3d/2}\right) \det\left(v^1, \ldots, v^d\right)$. Write v_i^j for the i-th coordinate of v^j and write $V := \left(v_i^j\right)$. By Observation 2.2, we can find $T \in GL_n(\mathbb{Z})$ so that $TU = V$, so that $Tu_i = v_i$ for $1 \leq i \leq d$ and $T(\mathbb{Z}^d) = \mathbb{Z}^d$.

Write $Q' := T(Q) = \left\{\sum_i \lambda_i v_i : \lambda_i \in [-1, 1]\right\}$ and consider the smallest axis aligned box $B := \prod_i [-a_i, a_i]$ containing Q'. Note that $a_j \leq \sum_i |v_i^j| = ||v^j||_1 \leq \sqrt{d}||v^j||_2$. Hence, we find

$$|B| = 2^d \prod_{i=1}^{d} a_i \leq 2^d \prod_{j=1}^{d} \sqrt{d}||v^j||_2 \leq O(d)^{2d} \det\left(v^1, \ldots, v^d\right) = O(d)^{2d} \det(v_1, \ldots, v_d) = O(d)^{2d}|Q'|.$$

Now we cover C by a d-GAP P, constructed by the following sequence:

$$C = K \cap \mathbb{Z}^d \subset Q \cap \mathbb{Z}^d = T^{-1}(Q') \cap \mathbb{Z}^d \subset T^{-1}(B) \cap \mathbb{Z}^d = T^{-1}\left(B \cap \mathbb{Z}^d\right) =: P.$$

It remains to bound $\#P$. As C is full-dimensional each $a_i \geq 1$, so

$$\#P = \#\left(B \cap \mathbb{Z}^d\right) \leq 2^d|B| \leq O(d)^{2d}|Q'| = O(d)^{2d}|Q| \leq O(d)^{3d}|K| \leq O(d)^{3d}\#C,$$

https://doi.org/10.1017/S0963548324000051 Published online by Cambridge University Press

where the last inequality follows from Minkowski's First Theorem (see for instance equation (3.14) in [4]). □

Proof of Corollary 1.2. Let $m := \max_{x\in\mathbb{Z}} \#(\phi^{-1}(x) \cap C)$ and note that $\#\phi(C) \geq \#C/m$. Analogously, let $m' := \max_{x\in\mathbb{Z}} \#(\phi^{-1}(x) \cap P)$ so that $m' \geq m$. By translation, we may assume that m' is achieved at $x = 0$. Note that for any $x = \phi(p)$ with $p \in P$ and $p' \in P \cap \phi^{-1}(0)$ we have $p + p' \in P + P$ with $\phi(p + p') = x$, so $\#\big(\phi^{-1}(x) \cap (P + P)\big) \geq m'$. We conclude that

$$\#\phi(P) \leq \#(P+P)/m' \leq 2^d \#P/m \leq O(d)^{3d} \#C/m \leq O(d)^{3d} \#\phi(C).$$ □

References

[1] Berg, S. L. and Henk, M. (2019) Discrete analogues of John's theorem. *Moscow J. Comb. Number Theory* **8**(4) 367–378.
[2] John, F. (1948) Extremum problems with inequalities as subsidiary conditions. In *Studies and Essays, Presented to R. Courant on his 60th Birthday,*. New York: Interscience, pp. 187–204.
[3] Lovett, S. and Regev, O. (2017) A counterexample to a strong variant of the Polynomial Freiman-Ruzsa Conjecture in Euclidean space. *Discrete Anal.* **8** 379–388.
[4] Tao, T. and Vu, V. (2006) *Additive Combinatorics*. Cambridge University Press, Vol. 105.
[5] Tao, T. and Van, V. (2008) John-type theorems for generalized arithmetic progressions and iterated sumsets. *Adv. Math.* **219**(2) 428–449.

Cite this article: van Hintum P and Keevash P (2024). Sharp bounds for a discrete John's theorem. *Combinatorics, Probability and Computing* **33**, 484–486. https://doi.org/10.1017/S0963548324000051