Discrete Kakeya-type problems and small bases

Noga Alon* Boris Bukh† Benny Sudakov‡

Abstract

A subset U of a group G is called k-universal if U contains a translate of every k-element subset of G. We give several nearly optimal constructions of small k-universal sets, and use them to resolve an old question of Erdős and Newman on bases for sets of integers, and to obtain several extensions for other groups.

1 Introduction

A subset U of $\mathbb{R}^d$ is a Besicovitch set if it contains a unit-length line segment in every direction. The Kakeya problem asks for the smallest possible Minkowski dimension of a Besicovitch set. It is widely conjectured that every Besicovitch set has Minkowski dimension d. For large d the best lower bounds come from the approach pioneered by Bourgain [4] which is based on combinatorial number theory. For example, in [5] it is shown that if every set $X \subset \mathbb{Z}/p\mathbb{Z}$ containing a translate of every k-term arithmetic progression is of size at least $\Omega(N^{1-\epsilon(k)})$ with $\epsilon(k) \to 0$ as $k \to \infty$, then the Kakeya conjecture is true.

In this paper we address a related problem where instead of seeking a set containing a translate of every k-term arithmetic progression, we demand that the set contains a translate of every k-element set. We do not restrict the problem to the cyclic groups, and consider general (possibly non-abelian) groups. Given a finite group G, we call a subset U of G *k-universal* if U contains a left translate of every k-element set. More generally, we say that U is k-universal for $X \subset G$, if for any k-element set $W = \{w_1, \dots, w_k\} \subset X$ there is a $g \in G$ such that $gW = \{gw_1, \dots, gw_k\}$ is contained in U. We are interested in small k-universal sets.

Since U contains $\binom{|U|}{k}$ k-element subsets, and the orbit of a k-set under (left) multiplication by G has size at most $|G|$, it follows that $\binom{|U|}{k} \geq \binom{|G|}{k}/|G|$ for any U that is k-universal for the group G. From that it is easy to deduce that $|U| \geq \frac{1}{2}|G|^{1-1/k}$. It is natural to wonder how sharp this lower bound on the size of k-universal sets is.

Question. *Is it true that for every integer $k > 1$ there is a constant $c(k)$ such that every finite group G contains a k-universal set of size not exceeding $c(k)|G|^{1-1/k}$? If so, is there a universal constant c such that $c(k) \leq c$ for all k?*

*Schools of Mathematics and Computer Science, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv 69978, Israel and IAS, Princeton, NJ 08540, USA. Email: nogaa@tau.ac.il. Research supported in part by the Israel Science Foundation, by a USA-Israeli BSF grant, by the Hermann Minkowski Minerva Center for Geometry at Tel Aviv University and by the Von Neumann Fund.

†Department of Mathematics, Princeton University, Princeton, NJ 08544, USA. Email: bbukh@math.princeton.edu.

‡Department of Mathematics, UCLA, Los Angeles, CA 90095 and Institute for Advanced Study, Princeton, NJ. Email: bsudakov@math.ucla.edu. Research supported in part by NSF CAREER award DMS-0546523, NSF grants DMS-0355497 and DMS-0635607, by a USA-Israeli BSF grant, and by the State of New Jersey.

Efficient constructions of k-universal sets are hard to come by. For $k = 2$ the problem was solved by Kozma and Lev [11] and independently by Finkelstein, Kleitman and Leighton [8] who showed that the easy lower bound above is tight.

Theorem 1.1. *For every finite group G there is a 2-universal set $U \subset G$ of size not exceeding $c|G|^{1/2}$, where c is an absolute constant.*

Their proofs relied heavily on the classification of finite simple groups, and do not seem to generalize to constructions of k-universal sets for $k \geq 3$. However, an easy probabilistic argument produces k-universal sets with a loss of a logarithmic factor. To state the actual result, which is a bit more general, we first need to define an auxiliary notion of a non-doubling set in a group.

Definition. *A set $X \subset G$ is* non-doubling *if $XX = \{xx' : x, x' \in X\}$ has at most $3|X|$ elements.*

Note that in particular, any subgroup of a group G is non-doubling.

Theorem 1.2. *For every non-doubling set X of size $|X| > 1$ in a finite group G there is a $U \subset G$ which is k-universal for X, of size $|U| \leq 36|X|^{1-1/k} \log^{1/k}|X|$. In particular, for every finite group G there is a k-universal set U of size $|U| \leq 36|G|^{1-1/k} \log^{1/k}|G|$.*

An interesting aspect of this result is that it gets better as k gets larger. For instance, if $k \geq \log\log|G|$, then $(\log|G|)^{1/k} = O(1)$, showing that the lower bound is tight up to a constant factor for moderately large values of k. Here and everywhere in the paper the logarithms are natural (to the base $e = 2.71\ldots$). For simplicity of presentation we also assume, throughout the paper, that all groups considered here are sufficiently large.

It is possible to improve upon the probabilistic construction when the group is cyclic for any value of k, as well as for some large families of groups for fixed k.

Theorem 1.3. *a) If G is cyclic, there is a k-universal set of order at most $72|G|^{1-1/k}$.*

b) If $G = S_n$ is a symmetric group, there is a k-universal $U \subset G$ of size at most $(3k+1)!|G|^{1-1/k}$.

c) If G is Abelian, there is a k-universal $U \subset G$ of size at most $8^{k-1}k|G|^{1-1/k}$.

Moreover, many more families of groups containing k-universal sets of size $c(k)|G|^{1-1/k}$ can be constructed by using lemma 2.2 below.

We will apply these results to settle an old problem of Erdős and Newman [6] on bases for sets of integers. They studied bases for m-element subsets of $\{1, \ldots, n\}$, where a set B is a basis for A if $A \subset B + B = \{b_1 + b_2 : b_1, b_2 \in B\}$. Since $\{0\} \cup A$ is a basis for A, and there is a set X with at most $c\sqrt{n}$ elements such that $X + X \supset \{1, \ldots, n\}$ it follows that for any m-element subset of $\{1, \ldots, n\}$ there is always a basis of size $\min(c\sqrt{n}, m+1)$. Erdős and Newman showed by a counting argument, that compared the number of m-element sets with the number of possible bases of a given size, that if m is somewhat smaller than $\sqrt{n}$, say $m = O(n^{1/2-\epsilon})$, then almost no m-element set has a basis of size $o(m)$. Similarly, if m is at least $n^{1/2+\epsilon}$ almost all m-element sets require a basis of size at least $c\sqrt{n}$. However, for the borderline case when m is of the order $\sqrt{n}$ the counting argument only yielded existence of sets that need a basis of size $c\sqrt{n}\log\log n/\log n$. They asked if every m-set of size $m = \sqrt{n}$ has a basis with $o(m)$ elements. We answer their question in the affirmative not only for subsets of $\{1, \ldots, n\}$ but in a much greater generality that applies to many other groups.

A subset B of a group G is said to be a basis for $A \subset G$ if $A \subset BB = \{bb' : b, b' \in B\}$. Though the case when $G = (\mathbb{Z}, +)$ and $A \subset \{1, \ldots, n\}$ is the setting in which Erdős and Newman asked their question, it is better to think of their question in the group $G = \mathbb{Z}/n\mathbb{Z}$. On one hand, if $A, B \subset \mathbb{Z}$ and $B + B \supset A$, then the sets $B' = (B \mod n) \subset \mathbb{Z}/n\mathbb{Z}$ and $A' = (A \mod n) \subset \mathbb{Z}/n\mathbb{Z}$ satisfy $B' + B' \supset A'$. On the other hand, if $A', B' \subset \mathbb{Z}/n\mathbb{Z}$ satisfy $B' + B' \supset A'$, then thinking of A' and B' as subsets of $\{1, \ldots, n\}$ in the natural way and letting $B = B' \cup (B' - n)$ we have $B + B \supset A'$ in the group of integers. So, up to a multiplicative constant of 2 the Erdős-Newman problem is a problem about bases for subsets of $\mathbb{Z}/n\mathbb{Z}$.

The lower bound of Erdős and Newman immediately carries over to any finite group G: there is always a set A with at most $\sqrt{|G|}$ elements for which every basis is of size at least $c\sqrt{G} \log\log|G|/\log|G|$. It turns out that this bound is tight for many groups including the cyclic groups. We say that the group G of order n satisfies the EN-condition if for every $A \subset G$ of size at most $\sqrt{n}$ there is a basis B of size $|B| \leq 50\frac{\sqrt{n}\log\log n}{\log n}$.

Theorem 1.4. *If $|G| = n$ and G contains a non-doubling set X satisfying $\sqrt{n}\log^2 n \leq |X| \leq \sqrt{n}\log^{10} n$, then G satisfies the EN-condition.*

Using this theorem it is not difficult to show that many groups satisfy the EN-condition.

Corollary 1.5. *a) Every solvable (finite) group satisfies the EN-condition. Moreover, every group of order n that contains a solvable subgroup of size at least $\sqrt{n}\log^2 n$ satisfies the EN-condition. In particular every finite group of odd order satisfies this condition.*

b) Every symmetric group S_n (and every alternating group A_n) satisfies the EN-condition.

Estimating the size of the smallest possible basis for explicitly given sets is often far harder. Erdős and Newman showed that any basis for the set of squares $\{t^2 : t = 1, \ldots, n\}$ (which is a subset of $\{1, 2, \ldots, n^2\}$) is of size at least $n^{2/3-o(1)}$ for large values of n, which is an improvement over the trivial lower bound of $n^{1/2}$. They constructed a small basis for the squares, of size only $O\left(\frac{n}{\log^M n}\right)$ for any M. Wooley [1, Problem 2.8] asked about powers other than the squares. Whereas it is likely that any basis for the set of d-th powers $\{t^d : t = 1, \ldots, n\}$ is of size $\Omega(n^{1-\epsilon})$ for every $\epsilon > 0$ and $d \geq 2$, we can report only a modest improvement of the $n^{2/3-o(1)}$ lower bound of Erdős and Newman for large values of d.

Theorem 1.6. *The set $\{t^d : t = 1, \ldots, n\}$ does not have a basis of size $O(n^{3/4-\frac{1}{2\sqrt{d}}-\frac{1}{2(d-1)}-\epsilon})$ for any $\epsilon > 0$.*

The rest of this short paper is split into four sections. The first one describes several constructions of small k-universal sets. It is followed by two sections containing the results on small bases that answer the Erdős-Newman question, and the result on the bases for powers of integers. The last section contains some concluding remarks.

We will employ the following notation. For a set X we denote by X^t the t-fold Cartesian product $X \times \ldots \times X$. The notations 2^X and $\binom{X}{t}$ denote the family of all subsets of X and the family of all t-element subsets of X, respectively. For the sake of clarity, throughout the paper (including the introduction) we do not make any serious attempt to optimize the absolute constants in our statements and proofs, and omit all floor and ceiling signs whenever these are not crucial.

2 Universal sets

In this section we present several results about small k-universal sets. Recall that for any group G every such set should contain at least $\frac{1}{2}|G|^{1-1/k}$ elements. We start off with a simple probabilistic construction of k-universal sets that are only logarithmic factor larger than this lower bound.

Proof of Theorem 1.2. Let X be a subset such that $Z = XX$ has size at most $3|X|$. Let $p = \left(\frac{|X|}{2k^3 \log|X|}\right)^{-1/k}$. If $p > 1$, then $2k^3 \log|X| > |X|$, implying that $\frac{|X|}{\log|X|} < 36^k$ and therefore that $|X| \leq 36|X|^{1-1/k} \log^{1/k}|X|$. In this case there is nothing to prove, as X itself is obviously k-universal for X. Let U be a random subset of Z obtained by picking each element of Z, randomly and independently, with probability p. Fix any k-element set $S \subset X$. For any $x \in X$ the set xS is contained in Z. Note that if two sets xS and $x'S$ have a non-empty intersection, then $x' = xs_1s_2^{-1}$ for some $s_1, s_2 \in S$. This shows that each set xS intersects fewer than k^2 other sets of this form. So for every subset $X' \subset X, |X'| < |X|/k^2$ there is an element $x^* \in X$ such that x^*S is disjoint from xS for all $x \in X'$. Therefore the maximum subset $X' \subset X$ such that $\{xS\}_{x\in X'}$ are pairwise disjoint contains at least $|X'| \geq \frac{|X|}{k^2}$ elements. Fix such an X'.

For any $x \in X$ the probability that $xS \subset U$ is $p^k = \frac{2k^3\log|X|}{|X|}$. Therefore the probability that there is no $x \in X'$ such that $xS \subset U$ is

$$\left(1 - \frac{2k^3\log|X|}{|X|}\right)^{|X'|} \leq \left(1 - \frac{2k^3\log|X|}{|X|}\right)^{|X|/k^2} \leq e^{-2k\log|X|} = \frac{1}{|X|^{2k}}$$

As there are no more than $|X|^k$ k-element subset of X, the probability that U is not k-universal for X is at most $1/|X|^k \leq 1/2$.

On the other hand, $\mathbb{E}\big[|U|\big] = p|Z|$ and by Markov's inequality

$$\Pr\Big[|U| > 3p|Z|\Big] = \Pr\Big[|U| > 3\mathbb{E}\big[|U|\big]\Big] \leq \frac{1}{3}.$$

Therefore, with probability at least $1 - 1/2 - 1/3 > 0$, $|U| \leq 3p|Z|$ and it is k-universal for X. In particular, such a U exists. The theorem now follows since $|Z| \leq 3|X|$ and $(2k^3)^{1/k} \leq 4$. $\square$

Remark. From the above proof one can easily deduce that for every two subsets X, X^* of a finite group G with $|X| = |X^*|$, G contains a k-universal set U for X of size at most

$$|U| \leq 12\frac{|X^*X|\log^{1/k}|X|}{|X|^{1/k}}.$$

Thus, if a set X does not grow significantly when multiplied by some other set of the same cardinality, this estimate gives a k-universal set for X whose size is only slightly worse than the coresponding lower bound.

Proof of Theorem 1.3 part (a). If $|G| \le \exp(2^k)$, then it is easy to check that the existence of the desired k-universal set follows from theorem 1.2. Assume that $|G| \ge \exp(2^k)$. Let p be a prime and let $r = \frac{p^{k+1}-1}{p-1}$. We first construct, for any prime p, a k-universal set of size $\frac{p^k-1}{p-1} \approx r^{1-1/k}$ in $\mathbb{Z}/r\mathbb{Z}$. The construction is motivated by Singer's theorem [14].

Let $q = p^{k+1}$ and denote by F_q the finite field of q elements. Let ω be a generator of F_q^*, and think of F_q as a vector space of dimension $k+1$ over F_p. Since $\omega^r \in F_p$ and every element of F_q^* is a power of ω, every 1-dimensional subspace of F_q is of the form $w^t F_p$ with $t \in \mathbb{Z}/r\mathbb{Z}$. Since $(p^{k+1}-1)/(p-1) = r$ is also the number of 1-dimensional subspaces of F_q the map $\phi\colon t \mapsto \omega^t F_p$ is a bijection between $\mathbb{Z}/r\mathbb{Z}$ and the set of 1-dimensional subspaces. Fix any basis of F_q and consider a standard coordinate-wise scalar product on F_q. For a 1-dimensional subspace L of F_q let $L^\perp$ be the orthogonal complement of L, which is k-dimensional. Since the map $L \mapsto L^\perp$ taking a 1-dimensional space to its orthogonal complement, is a bijection, every k-dimensional subspace of F_q is of the form $\omega^t(F_p)^\perp$ for a unique $t \in \mathbb{Z}/r\mathbb{Z}$.

Let H be any subspace of F_q of dimension k. Let $X = \{\phi^{-1}(L) : L \subset H\}$ where L ranges over all 1-dimensional subspaces of H. The set X is of size $|X| = (p^k-1)/(p-1)$. Moreover, X is k-universal for $Z/r\mathbb{Z}$. Indeed if $L_1, \dots, L_k$ are any k 1-dimensional subspaces of F_q, then their span is contained in a k-dimensional subspace. Therefore there is a t such that $\omega^t L_i \subset H$ for $i = 1, \dots, k$.

If we now think of X not as a subset of $\mathbb{Z}/r\mathbb{Z}$ but of $\{1, \dots, r\}$, then $Y = X \cup \big(X + r\big)$ contains a translate of every k-element subset of $[1, (p^{k+1}-1)/(p-1)]$. Therefore for every cyclic group G of size $|G| \le p^k \le (p^{k+1}-1)/(p-1)$ there is a k-universal set of size at most $2(p^k-1)/(p-1) \le 4p^{k-1}$. By [13, Theorem 1] we know that for every $x > 1$ there is a prime p satisfying $x \le p \le x(1 + \frac{2}{\log x})$ and in particular, there is a prime p such that $|G|^{1/k} \le p \le |G|^{1/k}\big(1 + \frac{2k}{\log|G|}\big)$. Therefore every cyclic group G satisfying $|G| \ge \exp(2^k)$ contains a k-universal set of size at most

$$4|G|^{1-1/k}\left(1 + \frac{2k}{\log|G|}\right)^{k-1} \le 4\exp(2k^2/2^k) \cdot |G|^{1-1/k} < 72|G|^{1-1/k},$$

where here we used that $\exp(2k^2/2^k) < 18$ for all k, (with room to spare). $\square$

To prove the existence of small k-universal sets in any Abelian group and in S_n we need a more flexible concept than that of a k-universal set. In order to induct on the size of the group, one needs to be able to force some of the elements in a translate of a k-element to be confined to a subset of G of size much smaller than $|G|^{1-1/k}$. This prompts the following definition, which is inspired by [11].

A k-tuple of sets $U = (U_1, \dots, U_k)$ where $U_i \subset G$ is said to be universal if for any k-tuple $W = (w_1, \dots, w_k) \in G^k$ there is a $g \in G$ satisfying $gw_i \in U_i$ for $i = 1, \dots, k$. Equivalently, $(U_1, \dots, U_k)$ is a universal k-tuple if and only if $\{(u_1^{-1}u_2, \dots, u_{k-1}^{-1}u_k) : u_i \in U_i\} = G^{k-1}$. Although we will not need this equivalence here, we include a short proof that it holds. Suppose $\{(u_1^{-1}u_2, \dots, u_{k-1}^{-1}u_k) : u_i \in U_i\} = G^{k-1}$, then for a given $(w_1, \dots, w_k) \in G^k$ we can solve the system of equations

$$\begin{aligned} w_1^{-1}w_2 &= u_1^{-1}u_2, \\ &\vdots \\ w_{k-1}^{-1}w_k &= u_{k-1}^{-1}u_k, \end{aligned} \qquad u_i \in U_i \qquad \text{for } i = 1, \dots, k. \tag{1}$$

Let $g = w_1u_1^{-1}$. Since $w_iu_i^{-1} = w_{i+1}u_{i+1}^{-1}$, by induction on i it follows that $g = w_iu_i^{-1}$ for $i = 1, \dots, k$. Hence $g^{-1}w_i = u_i$ is an element of U_i. The reverse direction is similar.

If $(U_1, \dots, U_k)$ is a universal k-tuple of sets, then $\bigcup_{i=1}^k X_i$ is a k-universal set. The greater flexibility of universal k-tuples comes at a price: construction of small universal k-tuples is more involved than the construction of k-universal sets, and they are not as small.

Theorem 2.1. *For any cyclic group and real numbers $1 \le s_1, \dots, s_k \le |G|$ satisfying $\prod_{i=1}^k s_i = |G|^{k-1}$ there is a universal k-tuple $(U_1, \dots, U_k)$ satisfying $|U_i| \le 8s_i$.*

Proof. Let $t_i = |G|/s_i$. By definition, it is easy to see that $\prod_{i=1}^k t_i = |G|$. Since for every $x \ge 1$ there is a non-negative integer a for which $x/2 \le 2^a \le x$, we can select non-negative integers $p_1, \dots, p_k$ inductively one by one so that $\frac{1}{2}t_i \le 2^{p_i} \le 2t_i$ and

$$\prod_{i=1}^r t_i \le \prod_{i=1}^r 2^{p_i} \le 2\prod_{i=1}^r t_i \qquad \text{for } r = 1, \dots, k. \tag{2}$$

Indeed, having selected p_1 through p_r satisfying (2) we select p_{r+1} so that it satisfies $x/2 \le 2^{p_{r+1}} \le x$ with $x = 2t_{r+1}(\prod_{i=1}^r (t_i/2^{p_i}))$. Note that $t_{r+1} \le x \le 2t_{r+1}$, since by induction we already have that $1/2 \le \prod_{i=1}^r (t_i/2^{p_i}) \le 1$. Therefore $t_{r+1}/2 \le 2^{p_{r+1}} \le 2t_{r+1}$. Set $P = \sum_{i=1}^k p_i$, and note that $|G| = \prod_{i=1}^k t_i \le 2^P \le 2\prod_{i=1}^k t_i = 2|G|$. We will first construct a universal k-tuple of sets $(Y_1, \dots, Y_k)$ for the group $\mathbb{Z}/2^P\mathbb{Z}$ satisfying $|Y_i| = 2^{P-p_i}$.

Every element of $\mathbb{Z}/2^P\mathbb{Z}$ can be written as a P-digit long number in binary. The digits of such a number are naturally indexed from 0 to $P - 1$ according to the power of 2 that they represent. The set Y_1 consists of the numbers whose p_1 least significant digits are all zero. The set Y_2 is the set of numbers whose digits from position p_1 to $p_1 + p_2 - 1$ are all zero. In general, a number belongs to the set Y_i if all the digits from position $\sum_{j=1}^{i-1} p_i$ to $\sum_{j=1}^{i} p_i - 1$ are zero. The k-tuple $(Y_1, \dots, Y_k)$ is universal. Indeed suppose we are given any $(v_1, \dots, v_k) \in (\mathbb{Z}/2^P\mathbb{Z})^k$. To find $g \in \mathbb{Z}/2^P\mathbb{Z}$ satisfying $g + v_i \in Y_i$ we proceed in stages. First the condition $g + v_1 \in Y_1$ determines the p_1 least significant digits of g. Once these digits are fixed, whatever the choices for the remaining digits are, we will have $g + v_1 \in Y_1$. So, we can proceed to find the next p_2 digits from the condition $g + v_2 \in Y_2$, and so on until all the digits of g are determined.

Let $Z_i = \{n \in \{1, \dots, 2^P + |G|\} : n \bmod 2^P \in Y_i\}$. As $|G| \le 2^P$, for every $(v_1, \dots, v_k) \in \{1, \dots, |G|\}^k$ one can find $0 \le g < 2^P$ for which $(g + v_i) \bmod 2^P \in Y_i$ for $i = 1, \dots, k$. However, $0 < g + v_i < 2^P + |G|$ implying $g + v_i \in Z_i$. Thus the sets $U_i = Z_i \bmod |G|$ together form a universal k-tuple in $\mathbb{Z}/|G|\mathbb{Z} \cong G$. Their sizes are

$$|U_i| \le |Z_i| \le 2|Y_i| = 2\frac{2^P}{2^{p_i}} \le 4\frac{|G|}{2^{p_i}} \le 8\frac{|G|}{t_i} = 8s_i. \qquad \square$$

Next we show how one can sometimes reduce the construction of universal k-tuples for a group G to the construction of universal k-tuples for a subgroup H of G. The following definitions introduce a measure that estimates how small the universal k-tuples in a given group can be. For a group G and real numbers $1 \le s_1, \dots, s_k \le |G|$ satisfying $\prod_{i=1}^k s_i = |G|^{k-1}$ let

$$r_k(G; s_1, \dots, s_k) = \min\left\{\frac{|U_1|}{s_1} + \dots + \frac{|U_k|}{s_k} : (U_1, \dots, U_k) \text{ is a universal } k\text{-tuple}\right\}$$

and define $r_k(G)$ by

$$r_k(G) = \sup\left\{ r_k(G; s_1, \ldots, s_k) : 1 \le s_1, \ldots, s_i \le |G| \text{ and } \prod_{i=1}^{k} s_i = |G|^{k-1} \right\}.$$

By definition, for any universal k-tuple $U = (U_1, \ldots, U_k), U_i \subset G$ the set $\cup_{i=1}^{k} U_i$ is k-universal. Therefore, taking all $s_i = |G|^{1-1/k}$ we have that any finite group admits a k-universal set of size at most $r_k(G)|G|^{1-1/k}$. The theorem above implies that $r_k(G) \le 8k$ for any cyclic group. This is worse than the estimate provided by part (a) of Theorem 1.3, due to the dependence on k, but this dependence is unavoidable for this approach. Indeed, it is easy to see that for every universal k-tuple $\prod |U_i| \ge |G|^{k-1}$ and thus the arithmetic-geometric means inequality implies that $r_k(G) \ge k$ for any group G.

The heart of the inductive construction of small k-universal sets for non-cyclic groups is the following lemma.

Lemma 2.2. *Let H be a subgroup of a finite group G such that $|H| \ge |G|^{1-1/k}$. Then*

$$r_k(G) \le r_k(H).$$

Proof. Our aim is to show that $r_k(G; s_1, \ldots, s_k) \le r_k(H)$ for any choice $1 \le s_1, \ldots, s_k \le |G|$ satisfying $\prod_{i=1}^{k} s_i = |G|^{k-1}$. Fix any such choice. We claim that there is at most one index j for which $s_j < |G|/|H|$. Indeed, had there been two such indices then it would follow that $|G|^{k-1} = \prod_{i=1}^{k} s_i < \left(\frac{|G|}{|H|}\right)^2 |G|^{k-2}$ contradicting $|H|^2 \ge |H|^{\frac{k}{k-1}} \ge |G|$. Moreover there has to be an index j for which $s_j \le |H|$ or else $|G|^{k-1} = \prod_{i=1}^{k} s_i > |H|^k \ge |G|^{k-1}$. In short: there is an index j such that $s_j \le |H|$, but for all $i \ne j$ we have $s_j \ge |G|/|H|$.

Set $t_i = s_i|H|/|G|$ for $i \ne j$ and $t_j = s_j$. Then $\prod_{i=1}^{k} t_i = |H|^{k-1}$ and $1 \le t_1, \ldots, t_k \le |H|$. Let $(U_1, \ldots, U_k)$ be a universal k-tuple in H satisfying

$$\frac{|U_1|}{t_1} + \cdots + \frac{|U_k|}{t_k} \le r_k(H).$$

Let T_1 be a set of representatives of the right cosets of H in G and and let T_2 be the set of inverses of elements of T_1. Then $|T_1| = |T_2| = |G|/|H|$. Let

$$Y_i = \begin{cases} U_i T_1, & \text{if } i \ne j, \\ U_i, & \text{if } i = j. \end{cases}$$

Then, as we show below, $(Y_1, \ldots, Y_k)$ is a universal k-tuple satisfying

$$\sum_i \frac{|Y_i|}{s_i} = \sum_{i \ne j} \frac{|Y_i|}{t_i(|G|/|H|)} + \frac{|U_j|}{t_j} \le \sum_{i \ne j} \frac{|U_i||T_1|}{t_i(|G|/|H|)} + \frac{|U_j|}{t_j} = \sum_i \frac{|U_i|}{t_i},$$

which shows $r_k(G; s_1, \ldots, s_k) \le r_k(H)$. To verify that $(Y_1, \ldots, Y_k)$ is universal consider an arbitrary sequence $(w_1, w_2, \ldots, w_k) \in G^k$. For each $i \ne j$, let $t_i \in T_2$ satisfy $w_j^{-1} w_i t_i \in H$, (such a t_i exists by the defintion of T_2). Since $(U_1, \ldots, U_k)$ is a universal k-tuple for H, and as $w_j^{-1} w_j = 1$ is clearly in H, there is an $h \in H$ such that for every $i \ne j$, $h w_j^{-1} w_i t_i \in U_i$ and $h w_j^{-1} w_j \in U_j$. Define $g = h w_j^{-1}$. Then $g w_i \in U_i t_i^{-1} \subset Y_i$ for all $i \ne j$, and $g w_j \in U_j = Y_j$. Therefore $(Y_1, \ldots, Y_k)$ is universal, as needed. $\square$

To construct small k-universal sets, it therefore suffices to find a large subgroup for which one can construct small universal k-tuples. We do it for symmetric and Abelian groups.

Proof of parts (b) and (c) of Theorem 1.3. b) For $n \geq 3k$ it is easy to check that $|S_{n-1}| = (n-1)! \geq (n!)^{1-1/k} = |S_n|^{1-1/k}$. Therefore to bound $r_k(S_n)$ for all n, by the preceding lemma, it suffices to bound $r_k(S_n)$ for $n \leq 3k-1$. Since $r_k(G) \leq k|G|$ for any group, it follows that for the symmetric group $r_k(S_n) \leq k(3k-1)!$. This implies that $G = S_n$ has a k-universal set of size $kr_k(S_n)|G|^{1-1/k} < (3k+1)!|G|^{1-1/k}$.

c) We will show that $r_k(G) \leq 8^{k-1}$ for any Abelian group G. Let $G = G_1 \times \cdots \times G_t$ be an arbitrary Abelian group written as a direct product of cyclic groups. If $t \geq k$, then at least one of these cyclic groups has order $\leq |G|^{1/k}$, and the product of the remaining groups is a subgroup of G of order $\geq |G|^{1-1/k}$. Therefore by lemma 2.2 it suffices to consider only the Abelian groups with $t \leq k-1$ cyclic factors. Let $s_1, \ldots, s_k$ satisfying $\prod_{i=1}^k s_i = |G|^{k-1}$ be given. Let $(U_{r,1}, \ldots, U_{r,k})$ be a universal k-tuple for G_r with $|U_{r,i}| \leq 8s_i^{\log_{|G|}|G_r|}$ which exists by theorem 2.1 since $\prod_{i=1}^k s_i^{\log_{|G|}|G_r|} = |G_r|^{k-1}$. Let $U_i = U_{1,i} \times \cdots \times U_{t,i}$ be the Cartesian product. Then $(U_1, \ldots, U_k)$ is a universal k-tuple for G satisfying $|U_i| \leq \prod_{r=1}^t 8s_i^{\log_{|G|}|G_r|} = 8^t s_i$. $\square$

3 Small bases

In this section we show how to use universal sets to construct small bases for subsets of size $\leq \sqrt{|G|}$ of a group G.

Lemma 3.1. *For every $X \subset G$ satisfying $|X| \geq \sqrt{|G|}\log^2|G|$ there is a subset $Y \subset G$ of size $|Y| \leq s$, where $s = \frac{\sqrt{|G|}}{\log|G|}$ so that $YX = G$.*

Proof. Let $Y = \{y_1, \ldots, y_s\}$ be a random set of s (not necessarily distinct) elements, where each y_i is chosen uniformly at random from G, and all choices are independent. Clearly an element $g \in G$ does not belong to YX if and only if Y is disjoint from the set $\{gx^{-1} \mid x \in X\}$. Thus the probability that $g \in G$ does not belong to YX is $\left(1 - \frac{|X|}{|G|}\right)^s$. The expected number of elements of G that do not belong to YX is

$$|G|\left(1 - \frac{|X|}{|G|}\right)^s \leq |G|\left(1 - \frac{\log^2|G|}{\sqrt{|G|}}\right)^{\sqrt{|G|}/\log|G|} < 1$$

implying that there is a choice of Y for which $G = YX$. $\square$

With the lemma in our toolbox we are just a step away from showing that the existence of moderately sized non-doubling sets are all what is needed to construct small bases.

Proof of Theorem 1.4. Let G be a group with n elements containing a non-doubling set X of size $\sqrt{n}\log^2 n \leq |X| \leq \sqrt{n}\log^{10} n$. By the above lemma G contains a set Y of size $s = \frac{\sqrt{n}}{\log n}$ such that $YX = G$. Suppose $A \subset G$, $|A| \leq \sqrt{n}$. Partition A into disjoint subsets $A_1, \ldots, A_s$, where A_i are all members of A that lie in y_iX and do not lie in any of the previous set y_jX for $j < i$. Split each

A_i into $\lceil |A_i|/k \rceil$ pairwise disjoint sets $T_{i,j}$, each of size at most k, where $k = \frac{\log n}{30 \log\log n}$. Let U be a k-universal set for X of size at most

$$\begin{aligned} |U| &\leq 36|X|^{1-1/k} \log^{1/k} |X| \leq 36\Big(\sqrt{n}\log^{10} n\Big)^{1-1/k} \log^{1/k} n \\ &< \frac{\sqrt{n}\log^{10} n}{n^{1/2k}} = \frac{\sqrt{n}}{\log^5 n}, \end{aligned}$$

which exists by Theorem 1.2. For each set $T_{i,j}$ defined above, let $g_{i,j}$ be an element of G so that $T_{i,j} \subset g_{i,j}U$. The existence of $g_{i,j}$ follows from the fact that U is k-universal for X and the fact that A_i is contained in the shift y_iX of X. Note that the number of elements $g_{i,j}$ is

$$\sum_{i=1}^{s} \lceil |A_i|/k \rceil \leq \frac{A}{k} + s \leq \frac{\sqrt{n}}{k} + \frac{\sqrt{n}}{\log n} \leq 40\frac{\sqrt{n}\log\log n}{\log n}.$$

Finally, to complete the proof, define $B = U \cup \{g_{i,j} : 1 \leq i \leq s,\ 1 \leq j \leq \lceil |A_i|/k \rceil\}$ and note that $A \subset BB$ and $|B| \leq |U| + 40\frac{\sqrt{n}\log\log n}{\log n} < 50\frac{\sqrt{n}\log\log n}{\log n}$. $\square$

Remark: The proof actually gives a somewhat stronger result than stated in Theorem 1.4. Call a set $X \subset G$ non-expanding if there is a set $X^* \subset G$ so that $|X| = |X^*|$ and $|X^*X| \leq |X|\log|G|$. Trivially, every non-doubling set is non-expanding. Combining the estimate on the size of k-universal sets from the remark following the proof of Theorem 1.2 together with the above arguments gives the following

Theorem 3.2. *If G contains a non-expanding X satisfying $\sqrt{|G|}\log^2|G| \leq |X| \leq \sqrt{|G|}\log^{10}|G|$, then G satisfies the EN-condition.*

Lemma 3.3. *For every finite solvable group G of order m and every x satisfying $1 < x \leq m$ there is a non-doubling subset $X \subset G$ satisfying $x \leq |X| \leq 2x$.*

Proof. Let G be a finite solvable group. Then there is a normal sequence

$$\{1\} = G_k \subset G_{k-1} \subset \ldots \subset G_1 \subset G_0 = G,$$

where each G_{i+1} is a normal subgroup of G_i and all the quotients G_i/G_{i+1} are cyclic. Let i be the minimum index so that $|G_{i+1}| < x$. Let coset hG_{i+1} be a generator of G_i/G_{i+1}, put $t = \lceil \frac{x}{|G_{i+1}|} \rceil$ and define $X = h^0G_{i+1} \cup h^1G_{i+1} \cup \cdots \cup h^{t-1}G_{i+1}$. Then X is of size at least x and at most $2x$, and as $XX = h^0G_{i+1} \cup h^1G_{i+1} \cup \cdots \cup h^{2t-2}G_{i+1}$ it is non-doubling. $\square$

Having finished all the necessary preparations, we can now prove Corollary 1.5

Proof of Corollary 1.5. a) If a finite group G of order n contains a solvable subgroup of size $m \geq \sqrt{n}\log^2 n$ then, by Lemma 3.3 with $x = \sqrt{n}\log^2 n$, this subgroup contains a non-doubling set of size at least $x = \sqrt{n}\log^2 n$ and at most $2x$. Thus, by Theorem 1.4, G satisfies the EN-condition. In particular, every finite solvable group satisfies this condition, and the assertion of part (a) follows, as every group of odd order is solvable, by the Feit-Thompson theorem [7].

b) Clearly S_n contains a subgroup isomorphic to S_m for all $m < n$. Since, all ratios

$$|S_{m+1}|/|S_m| = m + 1 \leq n < \log^2(n!) = \log^2|S_n|,$$

it is easy to see that $G = S_n$ contains a subgroup whose size is between $\sqrt{|G|}\log^2|G|$ and $\sqrt{|G|}\log^4|G|$. As every subgroup is non-doubling, the result now follows from Theorem 1.4. $\square$

Remark: Corollary 1.5 can be used to show that many additional finite groups satisfy the EN condition, as they contain large solvable subgroups. In particular, this holds for all linear groups, see [12]. It seems plausible that in fact every finite group satisfies the EN-condition.

4 Bases for powers

To show that there is no small basis for the set of d'th powers, we shall use estimates on the number of representations of a number as a sum of several d'th powers. We let $P_d(n) = \{k^d : k = 1, \ldots, n\}$ be the set of the first n d'th powers.

Lemma 4.1. *If the equation*

$$x_1^d - x_2^d + \cdots + (-1)^{k+1} x_k^d = t, \tag{3}$$

has fewer than $O(B^\epsilon)$ solutions in distinct positive integers $x_1, \ldots, x_k$ not exceeding B, then $|A| = \Omega(n^{1-\frac{1+\epsilon}{k+1}})$ for any set A of positive integers for which $P_d(n) \subset A + A$.

Proof. Suppose A is an m-element set satisfying $A + A \supset P_k(n)$. Let G be a graph on the vertex set A in which for each element $p \in P_k(n)$ we choose the lexicographically first pair of elements $a, a' \in A$ whose sum is p and connect them by an edge. Clearly G contains exactly n edges. Let $a, a' \in A$ be any two vertices of the graph. Let $t = a + (-1)^{k+1} a'$. Any path with distinct edges of length k between a and a' gives a rise to a solution of (3). Indeed if $a = a_0, a_1, \ldots, a_k = a'$, then $t = (a_0 + a_1) - (a_1 + a_2) + \cdots + (-1)^{k-1}(a_{k-1} + a_k)$ is an alternating sum of d'th powers. Since each path between a and a' corresponds to a different solution of (3), it follows that every pair of vertices in G are connected by no more than $O(n^\epsilon)$ such paths of length k. As every graph on m vertices and n edges contains a non-empty subgraph with minimum degree at least n/m, the graph G contains such a subgraph, which we denote by G'. Let $a \in V(G')$ be any vertex of that graph. Then there are more than $(\frac{n}{m} - k)^k$ paths of lengths k consisting of distinct edges originating from a. By the pigeonhole principle a fraction of $1/m$ of them has the same endpoint. Thus $(\frac{n}{m} - k)^k \leq O(mn^\epsilon)$ and the lemma follows. $\square$

To give a lower bound on the size of a basis for $P_d(n)$ it therefore suffices to give good estimates on the number of solutions to (3). Heath-Brown [10, Theorem 13] proved that for $t \leq B^d$ the number of solutions to $x_1^d + x_2^d + x_3^d = t$ in positive integers x_1, x_2, x_3 is $O(B^{\frac{2}{\sqrt{d}} + \frac{2}{d-1} + o(1)})$. Inspection of the proof shows that it applies verbatim to yield the same bound on the number of solutions to $(\pm 1)x_1^d + (\pm 1)x_2^d + (\pm 1)x_3^d = t$ in non-zero integers x_1, x_2, x_3 not exceeding B. This establishes theorem 1.6.

5 Concluding remarks

The questions we consider in this paper are all special cases of the following general problem:

Universal set problem. *Given a set X, a group G that acts on X and a family $\mathcal{F} \subset 2^X$, find the minimum possible size of a set U such that for every $S \in \mathcal{F}$ there is a $g \in G$ for which $gS \subset U$.*

For example, Theorem 1.3 treats the case when $X = G$, $\mathcal{F} = \binom{G}{k}$ and G acts on X by left multiplication. Bourgain's arithmetic version of Kakeya problem is essentially the case $X = \mathbb{Z}/p\mathbb{Z}$ where $\mathcal{F}$ is the family of all k-term arithmetic progressions.

Another important special case of the above problem deals with universal graphs. For a family $\mathcal{H}$ of graphs, a graph Γ is $\mathcal{H}$-universal if, for each $H \in \mathcal{H}$, the graph Γ contains a subgraph isomorphic to H. In our language it is the universal set problem for $G = S_n$ and $X = \binom{[n]}{2}$ with G acting on X by permuting the elements of $[n]$. The universal graph problem, which deals with the minimum possible number of edges in a graph that is universal for a given family, has been studied extensively for many classes of graphs $\mathcal{H}$. For instance, if $\mathcal{H}$ is the family of all k-edge graphs, then the smallest $\mathcal{H}$-universal graph is of size $\Theta(k^2/\log^2 k)$ [2]. The problem has also been studied for other families of graphs, such as graphs of bounded degree, trees or planar graphs. The interested reader is referred to [2], [3] and the references therein.

Besides the Kakeya conjecture some other analogues of the universal set problem for infinite groups have been considered as well. For example, Haight [9] constructed a set U of real numbers of zero Lebesgue measure that contains a translate of every countable set. The results in this paper can be adapted to construct a $U \subset \mathbb{R}$ of Minkowski dimension $1 - 1/k$ containing a translate of every k-element set.

The universal set problem is certainly hard in general. It would be interesting to find suitable general conditions under which it can be solved.

Acknowledgments. We thank Roger Heath-Brown, Per Salberger and Aner Shalev for helpful discussions.

References

[1] Problems presented at the workshop on recent trends in additive combinatorics, American Institute of Mathematics, 2004, `http://www.aimath.org/WWN/additivecomb/additivecomb.pdf`.

[2] N. Alon and V. Asodi, Sparse universal graphs, *J. Comput. Appl. Math.* 142 (2002), 1–11.

[3] N. Alon and M. Capalbo, Sparse universal graphs for bounded degree graphs, *Random Structures and Algorithms* 31 (2007), 123–133.

[4] J. Bourgain, On the dimension of Kakeya sets and related maximal inequalities, *Geom. Funct. Anal.* 9 (1999), 256–282.

[5] J. Bourgain, Λ_p-sets in analysis: results, problems and related aspects, in: *Handbook of the geometry of Banach spaces, Vol. I*, North-Holland, Amsterdam, 2001, 195–232.

[6] P. Erdős and D.J. Newman, Bases for sets of integers, *J. Number Theory* 9 (1977), 420–425.

[7] W. Feit and J.G. Thompson, Solvability of groups of odd order, *Pacific J. Math.* 13 (1963), 775–1029.

[8] L. Finkelstein, D. J. Kleitman, and F. T. Leighton, Applying the classification theorem for finite simple groups to minimize pin count in uniform permutation architectures, in: *VLSI algorithms and architectures (Corfu, 1988)*, Lecture Notes in Comput. Sci. vol. 319, Springer, New York, 1988, 247–256.

[9] J.A. Haight, An F_σ semigroup of zero measure which contains a translate of every countable set, in: *Study group on analytic number theory, 1st–2nd years, 1984–1985*, Exp. No. 29, 9. Secrétariat Math., Paris, 1985. `http://www.numdam.org/item?id=TAN_1984-1985__1__A11_0`.

[10] D.R. Heath-Brown, The density of rational points on curves and surfaces, *Ann. of Math. (2)*, 155 (2002), 553–595.

[11] G. Kozma and A. Lev, Bases and decomposition numbers of finite groups, *Arch. Math. (Basel)*, 58 (1992), 417–424.

[12] A. Mann, Soluble subgroups of symmetric and linear groups, Israel J. Math 55 (1986), 162-172.

[13] J.B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers. *Illinois J. Math.* 6(1962), 64–94.

[14] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* 43 (1938), 377–385.