# A SHARP INVERSE LITTLEWOOD-OFFORD THEOREM

TERENCE TAO AND VAN VU

ABSTRACT. Let  $\eta_i$ , i = 1, ..., n be iid Bernoulli random variables. Given a multiset  $\mathbf{v}$  of n numbers  $v_1, ..., v_n$ , the concentration probability  $\mathbf{P}_1(\mathbf{v})$  of  $\mathbf{v}$  is defined as  $\mathbf{P}_1(\mathbf{v}) := \sup_x \mathbf{P}(v_1\eta_1 + ... v_n\eta_n = x)$ . A classical result of Littlewood-Offord and Erdős from the 1940s asserts that if the  $v_i$  are non-zero, then this probability is at most  $O(n^{-1/2})$ . Since then, many researchers obtained better bounds by assuming various restrictions on  $\mathbf{v}$ .

In this paper, we give an asymptotically optimal characterization for all multisets  $\mathbf{v}$  having large concentration probability. This allow us to strengthen or recover several previous results in a straightforward manner.

## 1. INTRODUCTION

The purpose of this paper is to study the *Littlewood-Offord* and *inverse Littlewood-Offord* problems regarding concentration of random walks in torsion-free abelian groups. We recall some notation from [19].

**Definition 1.1** (Concentration probabilities). Let G = (G, +) be an additive group (e.g. the integers  $\mathbf{Z}$ , the complex numbers  $\mathbf{C}$ , or a vector space  $\mathbf{R}^m$ ). Let  $\mathbf{v} = (v_1, \ldots, v_n)$  be a multiset of n elements of G (allowing repetitions). For any  $0 \leq \mu \leq 1$ , we define the *lazy* random walk  $S^{\mu}(\mathbf{v})$  with steps  $\mathbf{v}$  and density  $\mu$  to be the G-valued random variable

$$S^{\mu}(\mathbf{v}) := v_1 \eta_1^{\mu} + \dots + v_n \eta_n^{\mu}$$

where the  $\eta_i^{\mu}$ 's are iid copies of the (lazy coin flip) random variable  $\eta^{\mu}$  which equals 0 with probability  $1 - \mu$  and  $\pm 1$  with probability  $\mu/2$  each. We define the *concentration probability*  $\mathbf{P}_{\mu}(\mathbf{v})$  to be the quantity

$$\mathbf{P}_{\mu}(\mathbf{v}) := \max_{a \in G} \mathbf{P}(S^{\mu}(\mathbf{v}) = a).$$
(1)

<sup>1991</sup> Mathematics Subject Classification. 11B25.

T. Tao is supported by a grant from the Macarthur Foundation.

V. Vu is supported by research grants DMS-0901216 and AFOSAR-FA-9550-09-1-0167.

Remark 1.2. We are interested in the regime when  $0 < \mu \leq 1$  is fixed and *n* is large. The most interesting case is perhaps when  $\mu = 1$ . In this case  $\eta$  is the Bernoulli random variable (fair coin flip), and  $\mathbf{P}_1(\mathbf{v})$  is the maximum multiplicity among the  $2^n$  signed sums  $\pm v_1 \pm \ldots \pm v_n$ , divided by  $2^n$ . Such probabilities appear in many situations in combinatorics and the theory of random structures, for instance in understanding the singularity probability of discrete random matrices (see e.g. [6], [16], [17], [11], [20]).

We will assume throughout this paper that G is *torsion-free*, thus  $nx \neq 0$  whenever  $x \in G$  is non-zero and n is a non-zero integer. In this case we can usually reduce to the model case  $G = \mathbf{Z}$  by means of Freiman isomorphisms (see [21, Lemma 5.25]).

Broadly speaking, we expect  $\mathbf{P}_{\mu}(\mathbf{v})$  to be large if and only if  $\mathbf{v}$  has significant additive structure. To explore this phenomenon, we ask the following two general (and closely related) questions:

- (Forward Littlewood-Offord problem) Given additive structural hypotheses on  $v_1, \ldots, v_n$ , what bounds can one give for  $\mathbf{P}_{\mu}(\mathbf{v})$ ?
- (Inverse Littlewood-Offord problem) Given bounds on  $\mathbf{P}_{\mu}(\mathbf{v})$ , what can one say about the additive structure of the  $v_1, \ldots, v_n$ ?

Let us now recall some previous results on these problems; further discussion may be found in [21, Chapter 5]. For simplicity we take  $\mu = 1$ . With no assumptions on  $\mathbf{v} = (v_1, \ldots, v_n)$ , we easily obtain the inequalities

$$2^{-n} \le \mathbf{P}_1(\mathbf{v}) \le 1$$

with the upper bound being attained precisely when all the  $v_i$  are zero, and the lower bound attained precisely when the the  $v_i$  are *dissociated* (which means that all the  $2^n$  partial sums  $\sum_{i \in A} v_i$  with  $A \subset \{1, \ldots, n\}$ are distinct). These two cases represent extreme additive structure and extreme lack of additive structure respectively.

Throughout this paper we adopt the following asymptotic notation:

**Definition 1.3** (Asymptotic notation). The asymptotic notation X = O(Y),  $X \ll Y$ ,  $Y = \Omega(X)$ , or  $Y \gg X$  denotes the bound  $X \leq CY$  for all  $n \geq C$  and some absolute constant C; we also use  $X = \Theta(Y)$  for  $X \ll Y \ll X$ . Subscripting such as  $O_d(Y)$  means that the implied constants C in the asymptotic notation are allowed to depend on d.

Littlewood and Offord [10] and then Erdős [1] were able to improve the upper bound assuming that some of the  $v_i$  were non-zero. In particular,

from the results in [1] one obtains the inequality

$$\mathbf{P}_1(\mathbf{v}) \ll n^{-1/2} \tag{2}$$

if all of the  $v_i$  are non-zero (Littlewood and Offord obtained the slightly weaker bound  $\mathbf{P}_1(\mathbf{v}) \ll n^{-1/2} \log n$ ). This bound is sharp: if  $v_1 = \ldots = v_n$ , one easily verifies that  $\mathbf{P}_1(\mathbf{v}) \gg n^{-1/2}$  (and in fact this example gives the precise maximum value of  $\mathbf{P}_1(\mathbf{v})$ .

The above result is phrased as a forward Littlewood-Offord result, but can be easily rephrased as an inverse theorem:

**Theorem 1.4** (Erdős' inverse Littlewood-Offord theorem). Let  $\mathbf{v} = (v_1, \ldots, v_n)$  be an *n*-tuple in a torsion-free additive group G. Suppose that  $\mathbf{P}_1(\mathbf{v}) \gg k^{-1/2}$  for some  $k \ge 1$ . Then all but O(k) of the  $v_1, \ldots, v_n$  are zero.

One can improve the upper bounds further by excluding the above counter-example. Indeed, from the work of Erdős and Moser [2] and then Sárközy and Szemerédi [13], the bound

$$\mathbf{P}_1(\mathbf{v}) \ll n^{-3/2} \tag{3}$$

was established if all the  $v_i$  were distinct (the earlier paper [2] establishes the slightly weaker bound  $\mathbf{P}_1(\mathbf{v}) \ll n^{-3/2} \log n$ ). Again, this result is sharp, since if one takes  $v_1, \ldots, v_n$  to be a proper arithmetic progression, one easily verifies that  $\mathbf{P}_1(\mathbf{v}) \gg n^{-3/2}$ . Later, Stanley [14], using algebraic methods, gave a very explicit bound for the optimal value of  $\mathbf{P}_1(\mathbf{v})$ .

The higher dimensional version of the problem, in which G is a vector space  $\mathbb{R}^m$ , has also attracted attention. Without the assumption that the  $v_i$ 's are different, the best result was obtained by Frankl and Füredi in [3], following earlier results by Katona [7], Kleitman [8], Griggs, Lagarias, Odlyzko and Shearer [4] and many others. However, the techniques used in these papers did not seem strong enough to recover (3). On the other hand, Halász [5], using harmonic analysis methods, managed to generalise (3), proving even stronger bounds upon forbidding more additive correlations among the  $v_i$ 's.

**Theorem 1.5** (Halasz inequality). [5], [21, Exercise 7.2.8] Let  $\mathbf{v} = (v_1, \ldots, v_n)$  be an n-tuple in a torsion-free additive group G. Let  $l \ge 1$  be an integer and let  $0 < \mu \le 1$ . Let  $R_l$  be the number of solutions of the equation

$$\epsilon_1 v_{i_1} + \dots + \epsilon_{2l} v_{i_{2l}} = 0$$

where  $\epsilon_i \in \{-1,1\}$  and  $i_1,\ldots,i_{2l}$  are (not necessarily different) elements of  $\{1,2,\ldots,n\}$ . Then

$$\mathbf{P}_{\mu}(\mathbf{v}) \ll_{l,\mu} n^{-2l-1/2} R_l.$$

It is easy to see that the l = 1 case of Theorem 1.5 implies the bound (3).

1.6. Main results. Theorem 1.5 states, roughly speaking, that if  $\mathbf{P}_{\mu}(\mathbf{v})$  is large, then there is a large amount of additive structure (in the form of short additive relations) between the  $v_i$ . Now we consider a slightly different type of additive structure, namely containment in a (symmetric) generalized arithmetic progression (or GAP); we recall this concept in Section 2. It is not hard to show that if all the  $v_i$  are contained in a GAP of bounded rank and controlled size, then the concentration probability  $\mathbf{P}_{\mu}(\mathbf{v})$  is large. More precisely, one has

**Proposition 1.7** (Forward Littlewood-Offord theorem). Let Q be a symmetric GAP in an additive group G with rank d, and let  $\mathbf{v} = (v_1, \ldots, v_n)$  be such that  $v_1, \ldots, v_n \in Q$ . Let  $0 < \mu \leq 1$ . Then we have

 $\mathbf{P}_{\mu}(\mathbf{v}) \gg_{d} |Q_{\sqrt{\mu n}}|^{-1} \gg_{d} (1+\mu n)^{-d/2} |Q|^{-1},$ 

where the dilate  $Q_t$  of Q is defined in Section 2.

We prove this easy result in Section 2; it reflects the intuition that a lazy random walk with steps in Q should mostly take values in the dilate  $Q_{O(\sqrt{\mu n})}$ . Note that this result incorporates the examples used to demonstrate that (2) and (3) are sharp. See also [20, Theorem 6.6] for a more complicated result in a similar spirit.

We now turn to the question of whether a converse to Proposition 1.7 exists. In [19], the authors showed

**Theorem 1.8** (Weak Inverse Theorem). Let  $A, \varepsilon > 0$  and  $0 < \mu \leq 1$ , and let  $\mathbf{v} = (v_1, \ldots, v_n)$  be an n-tuple in a torsion-free additive group G be such that

 $\mathbf{P}_{\mu}(v) \geq n^{-A}.$ 

Then there exists a proper symmetric GAP Q of rank d for some  $d = O_{A,\varepsilon}(1)$ , of volume  $O_{A,\mu,\varepsilon}(n^B)$  for some  $B = O_{A,\varepsilon}(1)$ , which contains all but  $O_{A,\mu,\varepsilon}(n^{1-\varepsilon})$  elements of **v** (counting multiplicity).

The reason we call Theorem 1.8 a *weak* inverse theorem because the dependence of B on A is not optimal (B is roughly  $2A^2$ ). The first main result of this paper is to obtain a sharper converse to Proposition 1.7, in which B is taken to be  $A - \frac{d}{2} + \varepsilon$ :

**Theorem 1.9** (Strong Inverse Theorem). Let  $A, \varepsilon > 0$ , and let  $\mathbf{v} = (v_1, \ldots, v_n)$  be an *n*-tuple in a torsion-free additive group G be such that

$$\mathbf{P}_{\mu}(v) \ge n^{-A}.\tag{4}$$

Then there exists a proper symmetric GAP Q of rank  $d \leq 2A$  of volume  $O_{A,\mu,\varepsilon}(n^{A-\frac{d}{2}+O_A(\varepsilon)})$ , which contains all but  $O_{A,\mu,\varepsilon}(n^{1-\varepsilon})$  elements of **v** (counting multiplicity).

Comparing this with Proposition 1.7 we see that except for epsilons, the exponent  $A - \frac{d}{2} + O_A(\varepsilon)$  here cannot be improved.

Theorem 1.9 will be deduced as the special case of the following stronger result.

**Theorem 1.10** (General Strong Inverse Theorem). Let  $d \ge 1$  be an integer and let  $0 < \varepsilon, \mu < 1$  be constants. Then there is a constant  $C_0 = C_0(d, \varepsilon, \mu)$  such that the following holds for all sufficiently large n and k with  $1 \le k < \sqrt{n}$ . Suppose that  $\mathbf{v} = (v_1, \ldots, v_n)$  is an n-tuple in a torsion-free additive group G that satisfies

$$\mathbf{P}_{\mu}(\mathbf{v}) \ge C_0 k^{-d}.\tag{5}$$

Then there exists a proper symmetric GAP Q of rank at most d-1 and volume

$$\operatorname{vol}(Q) \le \mathbf{P}_{\mu}(\mathbf{v})^{-1} k^{\varepsilon} \tag{6}$$

such that  $Q_{1/k}$  contains all but at most  $O_{d,\mu,\varepsilon}(k^2 \log k)$  of the  $v_1, \ldots, v_n$ . Furthermore, there is a positive integer  $C = C(d,\mu,\varepsilon)$  such that the steps of Q lie in  $\{v_1/C, \ldots, v_n/C\}$ .

Let us see how this theorem implies Theorem 1.9.

Proof of Theorem 1.9 assuming Theorem 1.10. Let  $A, \mu, \varepsilon, \mathbf{v}, n, G$  be as in Theorem 1.9. By shrinking  $\varepsilon$  if necessary we may assume that  $\varepsilon$  is small depending on A. We may assume that n is large depending on  $A, \mu, \varepsilon$  as the claim is trivial otherwise. Let d be the first integer larger than 2A, and let  $C_0$  be as in Theorem 1.10. For  $\varepsilon$  small and n large, we see from (4) that (5) holds for  $k := n^{1/2-\varepsilon}$ . By Theorem 1.10, we obtain a proper symmetric GAP Q of rank r at most d-1 and volume  $O(n^{A+\varepsilon})$  such that  $Q_{1/k}$  contains all but  $O(n^{1-\varepsilon})$  of the  $v_1, \ldots, v_n$ . Observe that any dimension of Q that is less than k does not contribute anything to  $Q_{1/k}$ , so by deleting these steps (and reducing the rank rof Q) we may assume that all dimensions of Q are at least as large as k. Then  $Q_{1/k}$  is a proper symmetric GAP of rank at most 2A and volume  $O_{A,\mu,\varepsilon}(k^{-r}|Q|) = O_{A,\mu,\varepsilon}(n^{A-r/2+O_A(\varepsilon)})$ , and the claim follows.  $\Box$ 

1.11. **Applications.** We now give some applications of Theorem 1.9 and Theorem 1.10. We first observe that these theorems can recover the classical bounds (2), (3) except for epsilon losses:

**Proposition 1.12.** Let  $\mathbf{v} = (v_1, \ldots, v_n)$  be an *n*-tuple in a torsion-free additive group G, and let  $\varepsilon > 0$  and  $0 < \mu < 1$ .

- (i) If all the  $v_i$  are non-zero, then  $\mathbf{P}_{\mu}(\mathbf{v}) \ll_{\mu,\varepsilon} n^{-1/2+\varepsilon}$ .
- (ii) If all the  $v_i$  are distinct, then  $\mathbf{P}_{\mu}(\mathbf{v}) \ll_{\mu,\varepsilon} n^{-3/2+\varepsilon}$ .

*Proof.* We may assume that n is large compared to  $\mu, \varepsilon$ , as the claim is trivial otherwise.

We first prove (i). Suppose for contradiction that  $\mathbf{P}_{\mu}(\mathbf{v}) \geq n^{-1/2+\varepsilon}$ . Applying Theorem 1.9 with  $A := 1/2 - \varepsilon$  we see that there exists a symmetric GAP Q of rank at most  $1 - 2\varepsilon$  which contains all but  $O_{\mu,\varepsilon}(n^{1-\varepsilon})$  of the  $v_1,\ldots,v_n$ . But rank has to be an integer, thus Q has rank zero and is therefore just  $\{0\}$ . Thus at least one of the  $v_i$  is zero, a contradiction.

Now we prove (ii). Suppose for contradiction that  $\mathbf{P}_{\mu}(\mathbf{v}) \geq n^{-3/2+\varepsilon}$ . Applying Theorem 1.9 with  $A := 3/2 - \varepsilon$  (and  $\varepsilon$  replaced by a smaller quantity  $\varepsilon'$  depending only on  $\varepsilon$ ) we see that there exists a symmetric GAP Q of rank d at most  $3-2\varepsilon$  and volume  $O_{\mu,\varepsilon}(n^{3/2-d/2-\varepsilon'})$  which contains all but  $O_{\mu,\varepsilon}(n^{1-\varepsilon'})$  of the  $v_1, \ldots, v_n$ . Since the  $v_i$  are all distinct, this forces  $|Q| \gg n$ , which forces d = 0, which forces more than one of the  $v_i$  to be zero, a contradiction. 

In a similar spirit, we obtain the following variant of Theorem 1.5, which essentially asserts that equality in Theorem 1.5 is only attained when the  $v_i$  lie in a symmetric arithmetic progression (i.e. a symmetric rank 1 GAP):

**Proposition 1.13.** Let  $n, \mathbf{v}, G, \mu, l, R_l$  be as in Theorem 1.5, and let  $0 < \delta, \varepsilon < 1/2$ . Then one of the following statements hold:

- P<sub>μ</sub>(**v**) ≪<sub>l,μ,ε,δ</sub> n<sup>-2l-1/2-δ</sup>R<sub>l</sub>.
  All but at most n<sup>1-ε</sup> of the v<sub>i</sub> lie in an symmetric arithmetic progression of length at most  $n^{2l+\delta+\varepsilon}R_l^{-1}$ .

Note that by combining this proposition with Proposition 1.7 and taking  $\delta = \varepsilon$  we obtain Theorem 1.5 up to epsilon losses.

*Proof.* By shrinking  $\varepsilon$  if necessary, we may assume  $\varepsilon$  is small depending on  $l, \delta$ . We may assume that n is large depending on  $l, \mu, \varepsilon, \delta$ , since the claim is trivial otherwise. Finally, we may assume that

$$\mathbf{P}_{\mu}(\mathbf{v}) \geq n^{-2l-1/2-\delta} R_l$$

since we are clearly done otherwise.

Applying Theorem 1.10 with  $k := n^{1/2-\varepsilon}$  and  $d = O_l(1)$  we obtain a proper symmetric GAP Q of rank  $r = O_l(1)$  and volume

$$\operatorname{vol}(Q) \ll_{\mu,l,\delta,\varepsilon} n^{2l+1/2+\delta+\varepsilon} R_l^{-1}$$

such that  $Q_{1/k}$  contains all but at most  $n^{1-\varepsilon}$  of the  $v_i$ . Arguing as in the proof of Theorem 1.9, we may assume that all dimensions of Q are at least k.

If  $r \leq 1$  then we are done, as  $Q_{1/k}$  is an arithmetic progression having the right length (one can adjust the constant  $\varepsilon$ ). Now assume for contradiction that  $r \geq 2$ . Then (if  $\varepsilon$  is small enough) we conclude

$$|Q_{1/k}| \ll_l k^{-2} \operatorname{vol}(Q) \ll_l n^{2l-\varepsilon} R_l^{-1}.$$

By relabeling we may assume that the  $v_1, \ldots, v_{\lfloor n/2 \rfloor}$  (say) lie in  $Q_{1/k}$ . Consider the  $\Theta_l(n^l)$  sums formed by taking l of these  $v_1, \ldots, v_{\lfloor n/2 \rfloor}$ ; these lie in  $Q_{l/k}$ , which has cardinality  $O_l(n^{2l-\varepsilon}R_l^{-1})$ . Applying the Cauchy-Schwarz inequality, we conclude that the number of solutions to

$$v_{i_1} + \ldots + v_{i_l} = v_{i_{l+1}} + \ldots + v_{i_{2l}}$$

with  $i_1, \ldots, i_{2l} \in \{1, \ldots, \lfloor n/2 \rfloor\}$ , is  $\gg_l n^{2l}/(n^{2l-\varepsilon}R_l^{-1}) = n^{-\varepsilon}R_l$ . On the other hand, this number is clearly bounded above by  $R_l$ , giving the required contradiction.

The rest of the paper is organized as follows. In the next two sections, we recall and prove several lemmas. The proof of Theorem 1.10 will be presented in the last two sections of the paper.

## 2. Generalized arithmetic progressions

In this section we recall the concept of a generalized arithmetic progression (GAP) and their basic properties. A detailed treatment of this topic can be found in [21, Chapter 3]. We will restrict our attention to symmetric GAPs.

**Definition 2.1** (GAPs). Let G be an additive group. A symmetric generalized arithmetic progression in G, or symmetric GAP for short, is a quadruplet  $\mathbf{Q} = (Q, N, v, d)$ , where the rank rank $(\mathbf{Q}) = d$  is a non-negative integer, the dimensions  $N = (N_1, \ldots, N_d)$  are a d-tuple of positive reals, the steps  $v = (v_1, \ldots, v_d)$  are a d-tuple of elements of G, and  $Q \subset G$  is the set

$$Q = \{\sum_{i=1}^{a} n_i v_i : n_i \in [-N_i, N_i] \forall i = 1, \dots, d\},\$$

where [a, b] denotes the set of integers between a and b inclusive. We shall often abuse notation and write Q for  $\mathbf{Q}$ . For any t > 0, we define the *dilate*  $\mathbf{Q}_t$  of  $\mathbf{Q}$  to be the GAP  $\mathbf{Q}_t := (Q_t, tN, v, d)$  formed by dilating all the dimensions by t. We say that  $\mathbf{Q}$  is *proper* if all the elements  $n_1v_1 + \ldots + n_dv_d$  for  $n_i \in [-N_i, N_i]$  are distinct. We say that Q is *t*-proper if tQ is proper.

We define the *volume* of **Q** to be  $vol(\mathbf{Q}) := \prod_{i=1}^{d} (2\lfloor N_i \rfloor + 1)$ . Note that  $|Q| \leq vol(\mathbf{Q})$ , with equality if and only if **Q** is proper.

If Q is a GAP of rank d, a simple covering argument (see [21, Lemma 3.10]) shows the doubling bounds

$$|Q_t| \ll_d (1+t)^d |Q| \tag{7}$$

for all t > 0.

Proof of Proposition 1.7. Let  $w_1, \ldots, w_d$  be the steps of Q, let  $N_1, \ldots, N_d$ be the dimensions, and let  $\phi : \mathbf{Z}^d \to G$  be the homomorphism  $\phi(a_1, \ldots, a_d) := a_1w_1 + \ldots + a_dw_d$ . By hypothesis, we can write  $v_i = \sum_{j=1}^d c_{ij}w_j$  for some integers  $-N_j \leq c_{ij} \leq N_j$ . Then we have  $S_{\mu}(\mathbf{v}) = \phi(x)$ , where  $x = (x_1, \ldots, x_d) \in \mathbf{Z}^d$  is the random variable whose coefficients are given by

$$x_j := \sum_{i=1}^n \eta_i c_{ij}$$

A simple computation shows that each  $x_j$  has mean zero and variance  $O(N_i^2 \mu n)$ , and so

$$\mathbf{E}\sum_{j=1}^{d} |x_j|^2 / N_j^2 \ll_d \mu n.$$

By Markov's inequality, we thus conclude that

$$\sum_{j=1}^{d} |x_j|^2 / N_j^2 \ll_d \mu n$$

with probability at least 1/2 (say). This implies that  $S_{\mu}(\mathbf{v}) \in Q_{O(\sqrt{\mu n})}$ with probability at least 1/2, and so by the pigeonhole principle

$$|\mathbf{P}_{\mu}(\mathbf{v})| \gg 1/|Q_{O(\sqrt{\mu n})}|$$

and the claim follows from (7).

One can easily pass from GAPs to proper GAPs by the following lemma:

**Lemma 2.2** (Embedding Lemma). [18] Let Q be a symmetric GAP of rank d in a torsion-free additive group G, and let t be a positive constant. Then there is a t-proper symmetric GAP Q' of rank at most d such that  $Q \subset Q' \subset Q_{O_{d,t}(1)}$  and  $|Q'| \ll_{d,t} |Q|$ . If Q was not already t-proper, one can take Q' to have rank at most d - 1.

*Proof.* See [18, Theorem 1.11].

Recall from the homomorphism theorems that if H, K are two finite subgroups of an abelian group G, then  $|H||K| = |H + K||H \cap K|$ . We now establish the analogous conclusion for GAPs (cf. [21, Exercise 2.4.7]):

**Lemma 2.3** (Intersection lemma). Let P and Q be symmetric GAPs in an additive group G of rank at most d, then

$$|P \cap Q||Q + P| = \Theta_d(|P||Q|). \tag{8}$$

Here of course  $Q + P := \{q + p : q \in Q, p \in P\}$  denotes the sumset of Q and P.

*Proof.* We recall the Ruzsa triangle inequality

$$|A - C||B| \le |A - B||B - C|$$

for finite non-empty sets  $A, B, C \subset G$  (see e.g. [21, Lemma 2.6]); this follows from the fact that any element a - c with  $a \in A$  and  $c \in C$  has at least b representations of the form a - c = (a - b) + (b - c) with  $b \in B$ . Applying this with  $A = P, C = Q, B = P \cap Q$  we obtain

$$|P - Q||P \cap Q| \le |P - (P \cap Q)||(P \cap Q) - Q| \le |2P||2Q$$

where we use the symmetry of P, Q. But from (7) we have  $|2P| \ll_d |P|$ ,  $|2Q| \ll_d |Q|$ , which gives the upper bound in (8).

Now we turn to the lower bound. By reducing d if necessary, we can assume that the dimensions of both P and Q are divisible by two, thus  $P = P_{1/2} - P_{1/2}$  and  $Q = Q_{1/2} - Q_{1/2}$ . Now we recall the inequality

$$|A||B| \le |(A - A) \cap (B - B)||A + B|$$

for finite non-empty  $A, B \subset G$  (cf. [21, Corollary 2.10]), which follows by combining the identity

$$|A||B| = |\{(a,b)|a \in A, b \in B\}| = \sum_{x \in A+B} |\{(a,b)|a \in A, b \in B, a+b=x\}|$$

with the inequality

$$|\{(a,b)|a \in A, b \in B, a+b=x\}| \le |(A-A) \cap (B-B)|$$

for all  $x \in G$  (which follows from the observation that if  $a, a' \in A$  and  $b, b' \in B$  are such that a + b = a' + b' = x, then a - a' = b - b' lies

#### TERENCE TAO AND VAN VU

in  $(A - A) \cap (B - B)$ ). Applying this inequality with  $A = P_{1/2}$  and  $B = Q_{1/2}$  and using (7), one obtains the claim.

## 3. ARITHMETIC ON WORDS

In this section, we recall some tools developed earlier in [19], which were used to prove Theorem 1.8 and will be useful here as well.

For our purpose, it is convenient to think of  $\mathbf{v} = (v_1, \ldots, v_n)$  as a word, obtained by concatenating the  $v_i$ :

$$\mathbf{v}=v_1v_2\ldots v_n.$$

This will allow us to perform several operations such as concatenating, truncating and repeating. For instance, if  $\mathbf{v} = v_1 \dots v_n$  and  $\mathbf{w} = w_1 \dots w_m$ , then

$$\mathbf{P}_{\mu}(\mathbf{vw}) = \max_{a \in Z} \left( \sum_{i=1}^{n} \eta_{i}^{\mu} v_{i} + \sum_{j=1}^{m} \eta_{n+j}^{\mu} w_{j} = a \right)$$

where  $\eta_k^{\mu}$ ,  $1 \leq k \leq n+m$  are i.i.d copies of  $\eta^{\mu}$ . Furthermore, we use  $\mathbf{v}^{[k]}$  to denote the concatenation of k copies of  $\mathbf{v}$ .

We will need to generalize the concentration probabilities  $\mathbf{P}_{\mu}(\mathbf{v})$  as follows. For finite non-empty set  $Q \subset G$ , define

$$\mathbf{P}_{\mu}(\mathbf{v};Q) := \sup_{a \in G} \mathbf{P}(S^{\mu}(\mathbf{v}) = a + q - q')$$
(9)

where q, q' are independently chosen uniformly at random from Q. Note that  $\mathbf{P}_{\mu}(\mathbf{v}; Q) = \mathbf{P}_{\mu}(\mathbf{v})$  if Q is a singleton set.

Since  $\mathbf{P}(a + q - q' = x) \leq 1/|Q|$  for any fixed a, q', x, a simple conditioning argument reveals the crude bound

$$\mathbf{P}_{\mu}(\mathbf{v};Q) \le 1/|Q|. \tag{10}$$

We have the following basic properties of the  $\mathbf{P}_{\mu}(\mathbf{v})$  and  $\mathbf{P}_{\mu}(\mathbf{v}; Q)$ :

**Lemma 3.1.** Let  $\mathbf{v} = v_1 \dots v_n$  be a word  $v_1, \dots, v_n$  in a torsion-free additive group G, and let  $Q \subset G$  be a finite non-empty set. Then the following properties hold.

- (i)  $\mathbf{P}_{\mu}(\mathbf{v}; Q)$  is invariant under permutations of  $\mathbf{v}$ .
- (ii) For any words  $\mathbf{v}, \mathbf{w}$

(iii) For any  $0 < \mu \leq 1$ , any  $0 < \mu' \leq \mu/4$ , and any word **v**,

$$\mathbf{P}_{\mu}(\mathbf{v};Q) \leq \mathbf{P}_{\mu'}(\mathbf{v};Q).$$

(iv) For any number  $0 < \mu \leq 1/2$  and any word  $\mathbf{v}$ ,

$$\mathbf{P}_{\mu}(\mathbf{v};Q) \leq \mathbf{P}_{\mu/k}(\mathbf{v}^{[k]};Q).$$

(v) For any number  $0 < \mu \leq 1/2$  and any words  $\mathbf{v}, \mathbf{w}_1, \ldots, \mathbf{w}_m$  we have

$$\mathbf{P}_{\mu}(\mathbf{v}\mathbf{w}_{1}\ldots\mathbf{w}_{m};Q) \leq \left(\prod_{j=1}^{m}\mathbf{P}_{\mu}(\mathbf{v}\mathbf{w}_{j}^{[m]};Q)\right)^{1/m}$$

(vi) For any number  $0 < \mu \leq 1/2$  and any words  $\mathbf{v}, \mathbf{w}_1, \ldots, \mathbf{w}_m$ , there is an index  $1 \leq j \leq m$  such that

$$\mathbf{P}_{\mu}(\mathbf{v}\mathbf{w}_{1}\ldots\mathbf{w}_{m};Q) \leq \mathbf{P}_{\mu}(\mathbf{v}\mathbf{w}_{j}^{[m]};Q).$$

*Proof.* When  $G = \mathbf{Z}$  and Q is a singleton, this is [19, Lemma 5.1]. When  $G = \mathbf{Z}$  and Q is not a singleton, the claim can be established by repeating the proof of [19, Lemma 5.1], using the Fourier identity

$$\mathbf{P}(S^{\mu}(\mathbf{v}) = a + q - q') = \int_{0}^{1} e(-at) |\mathbf{E}(e(qt))|^{2} \prod_{i=1}^{n} (1 - \mu + \mu \cos 2\pi v_{i}t) dt$$

in place of

$$\mathbf{P}(S^{\mu}(\mathbf{v}) = a) = \int_0^1 e(-at) \prod_{i=1}^n (1 - \mu + \mu \cos 2\pi v_i t) \ dt;$$

we omit the details. (Here and later, e(x) denotes  $\exp(2\pi\sqrt{-1}x)$ .) Finally, the generalization to arbitrary torsion-free G can be accomplished by using Freiman isomorphisms (see [21, Lemma 5.25]).

Note that for fixed  $0 < \mu < 1$ , a random walk  $S^{\mu}(v^{[k^2]})$  is roughly uniformly distributed on the progression  $[-k, k]v := \{jv : j \in \mathbb{Z}, -k \leq j \leq k\}$ , thanks to the central limit theorem. (Here  $v^{[k^2]}$  is the word vrepeated  $k^2$  times.) The following lemma can be viewed as a formalization of this intuition.

**Proposition 3.2** (Comparison of random walks). Let  $0 < \mu \leq 1/2$ , let  $\mathbf{v} = (v_1, \ldots, v_n)$  be a tuple in a torsion-free additive group G, let  $v_0 \in G$ , and let  $k \geq 1$ . Let Q be a symmetric GAP in Z of rank d. Then

$$\mathbf{P}_{\mu}(\mathbf{v}v_{0}^{[k^{2}]};Q) \ll_{\mu,d} \mathbf{P}_{\mu}(\mathbf{v};Q+[-k,k]v_{0}).$$

•

*Proof.* Fix  $\mu$ , d; we allow all implied constants to depend on these quantities. By definition,

$$\mathbf{P}_{\mu}(\mathbf{v}v_0^{[k^2]};Q) = \mathbf{P}(S^{\mu}(\mathbf{v}) + Xv_0 = q - q')$$

where q, q' are independent random variables uniformly distributed in Q, and  $X := \sum_{i=1}^{k^2} \xi_i^{\mu}$ . A direct computation using Stirling's formula shows that

 $\mathbf{P}(X=m) \ll k^{-1} \exp(-\Omega(|m|/k))$ 

for all  $m \in \mathbf{Z}$ , thus

$$\mathbf{P}_{\mu}(\mathbf{v}v_{0}^{[k^{2}]};Q) \ll k^{-1}\sum_{m\in\mathbf{Z}}\exp(-\Omega(|m|/k))\mathbf{P}(S^{\mu}(\mathbf{v})+mv_{0}=q-q').$$

This implies that

$$\mathbf{P}_{\mu}(\mathbf{v}v_{0}^{[k^{2}]};Q) \ll k^{-1}\sum_{m\in\mathbf{Z}}\exp(-\Omega(|m|/k))\mathbf{P}(S^{\mu}(\mathbf{v})+mv_{0}=q-q'+jv_{0}-j'v_{0})$$

where j, j' are drawn uniformly at random from [-k, k], independently of each other and of q, q'. It therefore suffices to show that

 $\mathbf{P}(S^{\mu}(\mathbf{v}) = a + q - q' + jv_0 - j'v_0) \ll \mathbf{P}_{\mu}(\mathbf{v}; Q + [-k, k]v_0)$ 

for all  $a \in G$ .

The random variable  $q + jv_0$  is supported in  $Q + [-k, k]v_0$ . If it were distributed uniformly in this set, we would be done. It is not quite uniform, nevertheless we can compare it to the uniform distribution as follows. Given any  $x \in Q + [-k, k]v_0$ , we have

$$\mathbf{P}(q+jv_0=x) = \frac{1}{|Q||[-k,k]v_0|} |Q \cap (x-[-k,k]v_0)|.$$

Since  $|A| \leq |A - A|$ , we see that

$$|Q \cap (x - [-k, k]v_0)| \le |(Q - Q) \cap ([-2k, 2k]v_0)|$$

and so by Lemma 2.3 and (7)

$$|Q \cap (x - [-k, k]v_0)| \ll \frac{|Q||[-k, k]v_0|}{|Q + [-k, k]v_0|}$$

and thus

$$\mathbf{P}(q+jv_0=x) \ll \frac{1}{|Q+[-k,k]v_0|}$$

Thus the probability distribution of  $q + jv_0$  is majorized by a constant multiple of the uniform distribution on  $Q + [-k, k]v_0$ , and the claim follows.

## 4. The Algorithm

We begin the proof of Theorem 1.10. By Lemma 3.1 we may assume that  $\mu \leq 1/2$ . Fix  $d, \varepsilon, \mu, n, k, \mathbf{v}, G$  as in that theorem; we assume that n, k are sufficiently large depending on  $d, \varepsilon, \mu$ . We let  $K \geq 1$  be a large number depending on  $d, \varepsilon, \mu$ , and then let  $C_0$  be an even larger number depending on  $d, \varepsilon, \mu, K$ . We assume that (5) holds.

In this section, we describe an algorithm which takes  $\mathbf{v}$  as input and produces, as output, a symmetric GAP Q as claimed by Theorem 1.10. A key concept is that of a *bad* element with respect to a symmetric GAP.

**Definition 4.1** (Bad element). Let  $K \ge 1$ ,  $x \in G$ , and let Q be a symmetric GAP in G. We say that x is *bad* with respect to a symmetric GAP Q if

$$|Q + [-k, k]x| \ge K|Q|$$

and *good* otherwise.

We will also need the generalized concentration probabilities  $\mathbf{P}_{\mu}(\mathbf{v}; Q)$  defined in (9). We now consider the following algorithm that generates words  $\mathbf{v}^{i}$  and symmetric GAPs  $Q_{i}$  for various  $i = 0, 1, 2, \ldots$ :

Step 0. Set  $\mathbf{v}^0 = \mathbf{v}, Q_0 := \{0\}.$ 

**Step** i + 1. Count the number of elements of  $\mathbf{v}^i$  which are bad with respect to  $Q_i$ .

Case 1. If this number is less than  $k^2$  then STOP.

Case 2. If this number is at least  $k^2$ , we can assume (without loss of generality) that the last  $k^2$  coordinates of  $\mathbf{v}^i$  are bad. Let  $\mathbf{v}^{i+1}$  be the vector obtained from  $\mathbf{v}^i$  by truncating these bad coordinates. By Lemma 3.1(vi), there is some value  $v_0$  among the bad coordinates such that

$$P_{\mu}(\mathbf{v}^{i+1}v_0^{[k^2]};Q_i) \ge \mathbf{P}_{\mu}(\mathbf{v}^i;Q_i).$$

Set  $r_i := \operatorname{rank}(Q_i)$  and  $Q'_{i+1} := Q_i + [-k, k]v_0$ , thus  $Q'_{i+1}$  is a GAP with rank  $r_i + 1$ . If  $Q'_{i+1}$  is proper, then set  $Q_{i+1} := Q'_{i+1}$ . If it is not proper, then use Lemma 2.2 to embed it into a proper symmetric GAP of rank at most  $r_i$  and volume  $O_{r_i}(|Q'_{i+1}|)$ ; Call this proper GAP  $Q_{i+1}$ . CONTINUE to Step i + 2.

Notice that by the algorithm the  $Q^i$  are symmetric GAPs at every step.

#### TERENCE TAO AND VAN VU

## 5. Analysis of the algorithm

For each i that occurs in the algorithm, we define the rank

$$r_i := \operatorname{rank}(Q_i)$$

and the potential

$$F_i := |Q_i| \mathbf{P}_{\mu}(\mathbf{v}^i; Q_i).$$

Initially we have

$$r_0 = 0; \quad F_0 = \mathbf{P}_{\mu}(\mathbf{v}) \ge C_0 k^{-d}; \quad |Q_0| = 1.$$
 (11)

We now record how  $r_i$ ,  $F_i$ , and  $Q_i$  evolve with the algorithm. We say that Step i + 1 is proper if  $Q'_{i+1}$  is proper.

**Lemma 5.1.** Let Step i + 1 be a step that occurs in the algorithm.

- (i) We have  $r_{i+1} = r_i + 1$  if Step i + 1 is proper, and  $r_{i+1} \leq r_i$  otherwise.
- (ii) We have  $|Q_{i+1}| \ge K|Q_i|$ . If Step i+1 is proper, we can improve this to  $|Q_{i+1}| \ge k|Q_i|$ .
- (iii) We have  $F_{i+1} \gg_{r_{i},\mu} KF_{i}$ . If Step i+1 is proper, we can improve this to  $F_{i+1} \gg_{r_{i},\mu} kF_{i}$ .

*Proof.* The first two claims are clear from construction. To prove the third claim, we observe from Proposition 3.2 that

$$\mathbf{P}_{\mu}(\mathbf{v}^{i+1}; Q_{i+1}) \gg_{r_i,\mu} \mathbf{P}_{\mu}(\mathbf{v}^i; Q_i);$$
(12)

the claim (iii) now follows from (ii).

**Corollary 5.2.** The algorithm has at most d - 1 proper steps, and terminates in  $O(d \log_K k)$  steps.

Proof. Suppose for contradiction that there were at least d proper steps. Let  $1 \leq i_1 < \ldots < i_d$  be the first d proper steps. By Lemma 5.1(i) and (11), the ranks  $r_i$  are bounded by d for all  $i \leq i_d$ . From Lemma 5.1(iii), we have  $F_{i_d} \geq_{d,\mu} k^d F_0$  if K is large enough; on the other hand, from (10) we have  $F_{i_d} \leq 1$ . This contradicts (11) if  $C_0$  is large enough.

Now that there are at most d-1 proper steps,  $r_i \leq d-1$  for all *i*. By Lemma 5.1(iii), we thus have  $F_{i+1} \geq \sqrt{K}F_i$  for all *i* if *K* is large enough. On the other hand, from (10) we have  $F_i \leq 1$  for all *i*. Applying (11), we conclude that the algorithm terminates in  $O(d \log_K k)$  steps as claimed.

Let  $\mathbf{v}^T$  and  $Q_T$  be the vector and GAP at the stopping time  $T = O(d \log_K k)$ .

**Lemma 5.3.**  $Q_T$  has rank at most d-1 and

$$|Q_T| \le k^{\varepsilon/2} \mathbf{P}_{\mu}(\mathbf{v})^{-1}$$

*Proof.* The rank bound follows from (11), Lemma 5.1(i) and Corollary 5.2.

As proved above,  $Q_T$  has rank at most d - 1. We next prove that it has small cardinality. Iterating (12) starting from (11), we see that

$$\mathbf{P}_{\mu}(\mathbf{v}^T; Q_T) \ge \Omega_{d,\mu}(1)^T \mathbf{P}_{\mu}(\mathbf{v}).$$

Combining this with (10) and the bound  $T = O(d \log_K k)$  we conclude

$$|Q_T| \le \exp(O_{d,\mu}(\log_K k))\mathbf{P}_{\mu}(\mathbf{v})^{-1}$$

and the claim follows by taking K sufficiently large.

By construction, all but  $O(dk^2 \log_K k) = O(k^2 \log k)$  of the  $v_1, \ldots, v_n$  are good relative to  $Q_T$ . To exploit this we use

**Lemma 5.4.** Suppose that  $x \in G$  is good relative to a symmetric GAP Q of rank r. Then there exists a proper symmetric GAP Q' of rank at most r containing Q and volume  $|Q'| \ll_{K,r} |Q|$  such that  $Cx \in Q'_{C/k}$ , where  $C \geq 1$  is an integer depending only on K and r.

Proof. The |Q||[-k, k]| sums q+jx with  $q \in Q$  and  $j \in [-k, k]$  lie in the set |Q + [-k, k]x|, which has cardinality at most K|Q| by hypothesis. By Cauchy-Schwarz, we conclude that there are  $\gg_K |Q|k^2$  quadruplets  $(q, q', j, j') \in Q \times Q \times [-k, k] \times [-k, k]$  such that q + jx = q' + j'x. By the pigeonhole principle, we conclude that the set  $A := \{j \in [-2k, 2k] : jx \in Q - Q\}$  has cardinality  $|A| \gg_K k$ . Applying a result of Sárkőzy [12] (see also [9], [15], or [21, Chapter 12]) we conclude that there exists a positive integer  $K_1 = O_K(1)$  such that the iterated sumset  $K_1A$ contains an arithmetic progression of length  $l = \Theta_K(k)$  and positive integer step  $a = O_K(1)$ . We conclude that  $[-l, l]ax \in Q_{4K_1}$ .

At present, l, a, and  $K_1$  are all dependent on x. But  $K_1$ , a are bounded by  $O_K(1)$ , and l is bounded from below by  $\Omega_K(k)$ . Thus, by taking the gcd over all possible values of a, one may assume that l, a,  $K_1$  are independent of x.

By Lemma 2.2, we can place  $Q_{4K_1}$  inside a 2-proper symmetric GAP Q' of rank at most r and volume  $O_{K,r}(|Q|)$ , thus  $[-l, l]ax \in Q'$ . Write  $N'_1, \ldots, N'_{r'}$  for the dimensions of Q'. Since Q' is 2-proper, the obvious map  $\phi : [-N'_1, N'_1] \times \ldots \times [-N'_r, N'_r] \to Q'$  is a Freiman isomorphism

of order 2 (see [21, Section 5.3]), and  $\phi^{-1}([-l, l]ax) = [-l, l]\phi^{-1}(ax)$  is also an arithmetic progression. From this we see that

$$\phi^{-1}(ax) \in [-N'_1/l, N'_1/l] \times \ldots \times [-N'_r/l, N'_r/l]$$

and thus

 $ax \in Q'_{1/l}$ 

and the claim follows.

Through the proof of this lemma, we see that all but at most  $O(k^2 \log k)$  of the  $v_i$  are such that  $Cv_i \in (Q_T)_{C/k}$ . By Lemma 2.2, we may place  $(Q_T)_C$  inside a proper symmetric GAP Q of rank at most d-1 and volume

$$|Q| \le k^{\varepsilon} \mathbf{P}_{\mu}(\mathbf{v})^{-1}$$

Since  $(Q_T)_C \subset Q'$ , we have  $(Q_T)_{C/k} \subset Q_{1/k}$ , and Theorem 1.10 follows.

Acknowledgement. We would like to thank the referees for their careful reading and useful remarks.

## References

- P. Erdős, On a lemma of Littlewood and Offord, Bull. Amer. Math. Soc. 51 (1945), 898–902.
- [2] P. Erdős, L. Moser, Elementary Problems and Solutions: Solutions: E736. Amer. Math. Monthly 54 (1947), no. 4, 229–230.
- [3] P. Frankl and Z. Füredi, Solution of the Littlewood-Offord problem in high dimensions. Ann. of Math. (2) 128 (1988), no. 2, 259–270.
- [4] J. Griggs, J. Lagarias, A. Odlyzko and J. Shearer, On the tightest packing of sums of vectors, *European J. Combin.* 4 (1983), no. 3, 231–236.
- [5] G. Halász, Estimates for the concentration function of combinatorial number theory and probability, *Period. Math. Hungar.* 8 (1977), no. 3-4, 197–211.
- [6] J. Kahn, J. Komlós, E. Szemerédi, On the probability that a random ±1 matrix is singular, J. Amer. Math. Soc. 8 (1995), 223–240.
- [7] G. Katona, On a conjecture of Erdős and a stronger form of Sperner's theorem. Studia Sci. Math. Hungar 1 1966 59–63.
- [8] D. Kleitman, On a lemma of Littlewood and Offord on the distributions of linear combinations of vectors, Advances in Math. 5 1970 155–157 (1970).
- [9] V. Lev, Optimal representations by sumsets and subset sums, J. Number Theory 62 (1997), 127–143.
- [10] J. E. Littlewood and A. C. Offord, On the number of real roots of a random algebraic equation. III. Rec. Math. [Mat. Sbornik] N.S. 12, (1943). 277–286.
- [11] M. Rudelson and R. Vershynin, The Littlewood-Offord problem and the condition number of random matrices, Advances in Mathematics 218 (2008), no 2, 600-633.
- [12] A. Sárkőzy, Finite addition theorems I, J. Num. Thy. 32 (1989), 114–130.
- [13] A. Sárkőzy and E. Szemerédi, Über ein Problem von Erdős und Moser, Acta Arithmetica, 11 (1965) 205-208.
- [14] R. Stanley, Weyl groups, the hard Lefschetz theorem, and the Sperner property, SIAM J. Algebraic Discrete Methods 1 (1980), no. 2, 168–184.

- [15] E. Szemerédi, V. Vu, Long arithmetic progressions in sumsets: thresholds and bounds, J. Amer. Math. Soc. 19 (2006), 119–169.
- [16] T. Tao and V. Vu, On random (-1,1) matrices: Singularity and Determinant, Random Structures and Algorithms 28 (2006), no 1, 1-23.
- [17] T. Tao and V. Vu, On the singularity probability of random Bernoulli matrices, Journal of the A. M. S, 20 (2007), 603-673.
- [18] T. Tao and V. Vu, John type theorems for generalized arithmetic progressions and iterated sumsets, *Advances in Mathematics* 219 (2008), no 2, 428-449.
- [19] T. Tao and V. Vu, Inverse Littlewood-Offord theorems and the condition number of random matrices, Annals of Mathematics (2) 169 (2009) no 2, 595-632.
- [20] T. Tao and V. Vu, Random matrices: The Circular Law, Communication in Contemporary Mathematics 10 (2008), 261-307.
- [21] T. Tao and V. Vu, Additive Combinatorics, Cambridge Univ. Press, 2006.

DEPARTMENT OF MATHEMATICS, UCLA, LOS ANGELES CA 90095-1555

*E-mail address*: tao@math.ucla.edu

DEPARTMENT OF MATHEMATICS, RUTGERS, PISCATAWAY, NJ 08854

E-mail address: vanvu@math.rutgers.edu-