# An elementary proof of Jin's theorem with a bound 

Mauro Di Nasso<br>Dipartimento di Matematica<br>Università di Pisa, Italy<br>dinasso@dm.unipi.it

Submitted: Oct 29, 2013; Accepted: Mar 27, 2014; Published: May 22, 2014
Mathematics Subject Classifications: 11B13, 11B05, 11B75


#### Abstract

We present a short and self-contained proof of Jin's theorem about the piecewise syndeticity of difference sets which is entirely elementary, in the sense that no use is made of nonstandard analysis, ergodic theory, measure theory, ultrafilters, or other advanced tools. An explicit bound to the number of shifts that are needed to cover a thick set is provided. Precisely, we prove the following: If $A$ and $B$ are sets of integers having positive upper Banach densities $a$ and $b$ respectively, then there exists a finite set $F$ of cardinality at most $1 / a b$ such that $(A-B)+F$ covers arbitrarily long intervals.


Keywords: Sumsets; upper Banach density; piecewise syndetic set; Jin's theorem

## 1 Introduction

A beautiful result in additive and combinatorial number theory was proved in 2001 by R. Jin [8] with the tools of nonstandard analysis, namely the property that sumsets $A+B$ are piecewise syndetic whenever $A, B \subseteq \mathbb{N}$ have positive upper Banach density. (See $\S 1$ for definitions). Researchers showed interest in that result but were not comfortable with nonstandard analysis. Several papers recently appeared where Jin's theorem was re-proved and extended by using more familiar non-elementary tools; most notably, see the proofs in $[4,1]$ by means of ergodic theory, and the ultrafilter proof in [2]. Recently, in [5] I gave a different nonstandard proof of the result, where an explicit bound to the number of shifts of $A+B$ that are needed to cover arbitrarily large intervals is given.

Here, the underlying ideas of the main constructions used in [5] are suitably translated into "standard" terms; the goal is to provide a short and elementary proof of Jin's theorem, completely from scratch. (Here, by "elementary" we mean that no use is made
of nonstandard analysis, measure theory and ergodic theory, ultrafilters, or any other advanced tool; and by "from scratch" we mean that the arguments used are self-contained, with no references to other existing results in the literature.)

Notation: By $\mathbb{N}$ we denote the set of positive integers. If not specified otherwise, lower-case letters $a, b, c, x, y, z, \ldots$ will denote integer numbers, with letters $k, n, m$ reserved for natural numbers, and upper-case letters $A, B, C, \ldots$ will denote sets of integers. By $[a, b]$ we denote intervals of integers, i.e. $[a, b]=\{x \in \mathbb{Z} \mid a \leqslant x \leqslant b\} ; A-B=\{a-b \mid$ $a \in A, b \in B\}$ is the difference set of $A$ and $B$; and $A+B=\{a+b \mid a \in A, b \in B\}$ is the sumset. With obvious notation, we shall simply write $A-z$ (or $A+z$ ) to indicate the left-ward shift $A-\{z\}$ (or the right-ward shift $A+\{z\}$, respectively).

## 2 Jin's theorem with a bound

Recall that a set $A$ of integers is thick if it covers intervals of arbitrary length, i.e. if for every $k$ there exists an interval $I=[x+1, x+k]$ of length $k$ such that $I \subseteq A ; A$ is syndetic if it has bounded gaps, i.e. if there exists $k$ such that $A \cap I \neq \emptyset$ for every interval $I$ of length $k ; A$ is piecewise syndetic if it covers arbitrarily long intervals of a syndetic set, i.e. if $A=B \cap C$ where $B$ is thick and $C$ is syndetic. Useful characterizations are the following: $A$ is syndetic if and only if $A+F=\mathbb{Z}$ for a suitable finite set $F$; and $A$ is piecewise syndetic if and only if $A+F$ is thick for a suitable finite set $F$.

A familiar notion in number theory is that of upper asymptotic density $\bar{d}(A)$ of sets of natural numbers $A \subseteq \mathbb{N}$ :

$$
\bar{d}(A)=\underset{n \rightarrow \infty}{\limsup } \frac{|A \cap[1, n]|}{n} .
$$

The (upper) Banach density $\mathrm{BD}(A)$ refines the upper density to sets of integers by considering arbitrary intervals instead of just initial intervals:

$$
\mathrm{BD}(A)=\lim _{n \rightarrow \infty}\left(\max _{x \in \mathbb{Z}} \frac{|A \cap[x+1, x+n]|}{n}\right) .
$$

Remark that the above limit always exists, and in fact the following holds: ${ }^{1}$

$$
\mathrm{BD}(A)=\inf _{n \in \mathbb{N}}\left(\max _{x \in \mathbb{Z}} \frac{|A \cap[x+1, x+n]|}{n}\right) .
$$

Trivially $\mathrm{BD}(A) \geqslant \bar{d}(A)$ for every $A \subseteq \mathbb{N}$; on the other hand, there exist sets $A \subseteq \mathbb{N}$ with $\bar{d}(A)=0$ and $\operatorname{BD}(A)=1$. Basic properties of Banach density are the following: $\mathrm{BD}(A)=1$ if and only if $A$ is thick; the family of sets with null Banach density is closed under finite unions; the Banach density is invariant under shifts, i.e. $\operatorname{BD}(A-z)=\mathrm{BD}(A)$. Although Banach density is not additive, the additivity property holds for families of shifts, i.e. $\mathrm{BD}\left(\bigcup_{i=1}^{k} A-z_{i}\right)=k \cdot \mathrm{BD}\left(A_{i}\right)$ whenever the shifts $A-z_{i}$ are pairwise disjoint.

[^0]The following general property of difference sets was first proved (but not published) by P. Erdős and Sárközy for sets of positive upper density. ${ }^{2}$
Proposition 1. If $B D(A)>0$ then $A-A$ is syndetic.
The proof consists of a pigeonhole principle argument. Since $A-A$ is symmetric around 0 , if it was not syndetic then one could pick a thick set $T \subseteq \mathbb{N}$ that does not meet $A-A$. Then one can construct a sequence $X=\left\{x_{1}<x_{2}<\ldots\right\}$ such that $x_{j}-x_{i} \in T$ for all $j>i$. The shifts $A-x_{i}$ are pairwise disjoint because $(X-X) \cap(A-A)=\emptyset$, and so we would have $\mathrm{BD}\left(\bigcup_{i=1}^{k} A-x_{i}\right)=\sum_{i=1}^{k} \mathrm{BD}\left(A-x_{i}\right)=k \cdot \mathrm{BD}(A)>1$ for sufficiently large $k$, a contradiction.

Remark that the above property does not extend to the general case $A-B$; indeed, it is not hard to find thick sets $A, B, C$ such that also their complements $A^{c}, B^{c}, C^{c}$ are thick, and $A-B \subset C$. However, Jin's theorem showed that $A-B$ is in fact syndetic on a suitable thick set.

Theorem 2 (Jin, with a bound). Let $A, B \subseteq \mathbb{Z}$ have positive upper Banach densities $B D(A)=\alpha$ and $B D(B)=\beta$, respectively. Then there exists a finite set $F$ of cardinality $|F| \leqslant 1 / \alpha \beta$ such that $(A-B)+F$ is thick (and hence $A-B$ is piecewise syndetic).

Notice that the above result includes the original Jin's Theorem about sumsets $A+B$ of sets $A, B \subseteq \mathbb{N}$, because trivially $\mathrm{BD}(B)=\mathrm{BD}(-B)$. Before giving our elementary proof, let us show that $A-B$ is thick when the two sets have sufficiently large densities.

Proposition 3. Let $A, B \subseteq \mathbb{Z}$, and assume that there exists $\alpha$ such that:

- $\sup \left\{a_{n}-\alpha \cdot n \mid n \in \mathbb{N}\right\}=+\infty$, where $a_{n}=\max _{x \in \mathbb{Z}}|A \cap[x+1, x+n]|$.
- $B D(B) \geqslant 1-\alpha$.

Then $A-B$ is thick.
Proof. Given $k$, let $m$ be such that $a_{m}-\alpha \cdot m>k$, and pick an interval $I$ of length $m$ with $a_{m}=|A \cap I|$. For every $i=1, \ldots, k$ we have that:

$$
|(A-i) \cap I| \geqslant|A \cap I|-i>\alpha \cdot m+k-i \geqslant \alpha \cdot m .
$$

Recall that $\operatorname{BD}(B)=\inf _{n} b_{n} / n$ where $b_{n}=\max \{|B \cap J| \mid J$ interval of length $n\}$. Then, by the hypothesis on $\operatorname{BD}(B)$, there exists an interval $J$ of length $m$ such that $|B \cap J|=$ $b_{m} \geqslant(1-\alpha) \cdot m$. Finally, pick $x$ such that $x+J=I$. We claim that the interval $[x+1, x+k] \subseteq A-B$; this will give the thesis because $k$ is arbitrary. For every $i=1, \ldots, k$ one has
$|(A-i) \cap I|+|(B+x) \cap I|=|(A-i) \cap I|+|B \cap J|>\alpha \cdot m+(1-\alpha) \cdot m=m=|I|$.
So, $(A-i) \cap(B+x) \cap I \neq \emptyset$, and there exist $a \in A$ and $b \in B$ such that $a-i=b+x$, and hence $x+i \in A-B$.

[^1]Notice that $\operatorname{BD}(A)>\alpha$ implies $\sup \left\{a_{n}-\alpha \cdot n \mid n \in \mathbb{N}\right\}=+\infty$, which in turn implies $\mathrm{BD}(A) \geqslant \alpha$; however, we remark that neither implication can be reversed. The fact that $A-B$ is thick whenever $\mathrm{BD}(A)+\mathrm{BD}(B)>1$ was first proved by M. Beiglböck, V. Bergelson and A. Fish in [1]; in fact, their proof actually shows the (slightly) stronger property stated in the above proposition.

The results mentioned in this section are just a hint of the rich combinatorial structure of sumsets and sets of differences, whose investigation seems still far from being completed (see e.g. the monographies $[14,13]$ ).

## 3 The elementary proof of Jin's theorem

We prove here our main Theorem 2, that was stated in the previous section. By the definition of upper Banach density, we can pick two sequences of integers $\left\langle x_{n} \mid n \in \mathbb{N}\right\rangle$ and $\left\langle y_{n} \mid n \in \mathbb{N}\right\rangle$ such that, if we let:

- $A_{n}=A \cap\left[x_{n}+1, x_{n}+n^{2}\right]$
- $B_{n}=B \cap\left[y_{n}+1, y_{n}+n\right]$
then $\lim _{n \rightarrow \infty}\left|A_{n}\right| / n^{2}=\alpha$ and $\lim _{n \rightarrow \infty}\left|B_{n}\right| / n=\beta$. As the first step in our proof, for every $n$ we shall find a suitable shift of $A_{n}$ that meets $B_{n}$ on a set whose relative density approaches $\alpha \beta$ as $n$ goes to infinity. To this end, we shall use the following inequality, obtained as a simple application of the pigeonhole principle. ${ }^{3}$

Lemma 4. Let $N, n \in \mathbb{N}, C \subseteq[1, N], D \subseteq[1, n]$. Then there exists $z$ such that

$$
\frac{|(C-z) \cap D|}{n} \geqslant \frac{|C|}{N} \cdot \frac{|D|}{n}-\frac{|D|}{N} .
$$

Proof. Let $\vartheta: \mathbb{N} \rightarrow\{0,1\}$ be the characteristic function of $C$. Then:

$$
\begin{aligned}
\sum_{x=1}^{N}\left(\sum_{d \in D} \vartheta(x+d)\right) & =\sum_{d \in D}\left(\sum_{x=1}^{N} \vartheta(x+d)\right)=\sum_{d \in D}|C \cap[d+1, N]| \\
& \geqslant \sum_{d \in D}(|C|-d) \geqslant|D| \cdot(|C|-n)
\end{aligned}
$$

By the pigeonhole principle, there must be at least one $z$ such that

$$
\frac{|(C-z) \cap D|}{n}=\frac{1}{n} \sum_{d \in D} \vartheta(z+d) \geqslant \frac{1}{n} \cdot \frac{|D| \cdot(|C|-n)}{N}=\frac{|C|}{N} \cdot \frac{|D|}{n}-\frac{|D|}{N} .
$$

[^2]For every $n$, apply the above lemma where $C=A_{n}-x_{n} \subseteq\left[1, n^{2}\right]$ and $D=B_{n}-$ $y_{n} \subseteq[1, n]$. Clearly, $|C|=\left|A_{n}\right|$ and $|D|=\left|B_{n}\right|$. Then we can pick a suitable sequence $\left\langle z_{n} \mid n \in \mathbb{N}\right\rangle$ such that

$$
\frac{\left|\left(A_{n}-x_{n}-z_{n}\right) \cap\left(B_{n}-y_{n}\right)\right|}{n} \geqslant \frac{\left|A_{n}\right|}{n^{2}} \cdot \frac{\left|B_{n}\right|}{n}-\frac{\left|B_{n}\right|}{n^{2}} .
$$

Now let:

$$
\text { - } E_{n}=\left(A_{n}-x_{n}-z_{n}\right) \cap\left(B_{n}-y_{n}\right) \subseteq[1, n] .
$$

By passing the previous inequality to the limit, we obtain $\lim _{n \rightarrow \infty}\left|E_{n}\right| / n \geqslant \alpha \beta$.
Next, we shall use a property of difference sets of a sequence of subsets of $[1, n]$, which can be seen as a refinement of Proposition 1.

Lemma 5. For $n \in \mathbb{N}$, let $E_{n} \subseteq[1, n]$. If $\lim _{n \rightarrow \infty}\left|E_{n}\right| / n=\gamma>0$, then there exists a finite set $F$ of cardinality $|F| \leqslant 1 / \gamma$ such that for every $m$ :

$$
[1, m] \subseteq\left(E_{n}-E_{n}\right)+F \text { for infinitely many } n
$$

Proof. We inductively define a finite increasing sequence $\sigma=\left\langle m_{i} \mid i=1, \ldots, k\right\rangle$. Set $m_{1}=0$. If property $(\star)$ is satisfied by $F=\{0\}$, then put $\sigma=\left\langle m_{1}\right\rangle$, and stop. Otherwise, let $m_{2} \in \mathbb{N}$ be the least counterexample. So, $\Gamma_{1}=\left\{n \mid\left[1, m_{2}-1\right] \subseteq\left(E_{n}-E_{n}\right)+m_{1}\right\}$ is infinite, but $\Lambda_{1}=\left\{n \in \Gamma_{1} \mid m_{2} \in\left(E_{n}-E_{n}\right)+m_{1}\right\}$ is finite. Notice that for every $n \in \Gamma_{1} \backslash \Lambda_{1}$ one has $\left(E_{n}+m_{1}\right) \cap\left(E_{n}+m_{2}\right)=\emptyset$. If for every $m \in \mathbb{N}$ the set of all $n \in \Gamma_{1}$ such that $[1, m] \subseteq \bigcup_{i=1}^{2}\left(E_{n}-E_{n}+m_{i}\right)$ is infinite, then put $\sigma=\left\langle m_{1}, m_{2}\right\rangle$ and stop. Otherwise, let $m_{3} \in \mathbb{N}$ be the least counterexample. So, the set $\Gamma_{2}=\left\{n \in \Gamma_{1} \mid\left[1, m_{2}-1\right] \subseteq\right.$ $\left.\bigcup_{i=1}^{2}\left(E_{n}-E_{n}+m_{i}\right)\right\}$ is infinite, but $\Lambda_{2}=\left\{n \in \Gamma_{2} \mid m_{3} \in \bigcup_{i=1}^{2}\left(E_{n}-E_{n}\right)+m_{i}\right\}$ is finite. Notice that for every $n \in \Gamma_{2} \backslash \Lambda_{2}$ one has $\left(E_{n}+m_{i}\right) \cap\left(E_{n}+m_{3}\right)=\emptyset$ for $i=1$, 2. Iterate this process. We claim that we must stop at a step $k \leqslant 1 / \gamma$. To see this, we show that whenever $m_{1}<\ldots<m_{k}$ are defined, one necessarily has $k \leqslant 1 / \gamma$. This is trivial for $k=1$, so let us assume $k \geqslant 2$.

The set $X=\Gamma_{k} \backslash\left(\Lambda_{1} \cup \ldots \cup \Lambda_{k}\right)$ is infinite, and since $X \subseteq \Gamma_{i} \backslash \Lambda_{i}$ for all $i$, the sets in the family $\left\{E_{N}+m_{i} \mid i=1, \ldots k\right\}$ are pairwise disjoint for every $N \in X$. Now, every $E_{N}+m_{i} \subseteq\left[1, N+m_{k}\right]$, and so we obtain:

$$
N+m_{k} \geqslant\left|\bigcup_{i=1}^{k}\left(E_{N}+m_{i}\right)\right|=\sum_{i=1}^{k}\left|E_{N}+m_{i}\right|=k \cdot\left|E_{N}\right| \Longrightarrow \frac{\left|E_{N}\right|}{N} \leqslant \frac{1}{k}+\frac{m_{k}}{k N} .
$$

By taking limits as $N \in X$ approaches infinity, one gets the desired inequality $\gamma \leqslant 1 / k$. Finally, observe that, by the definition of $\sigma=\left\langle m_{i} \mid i=1, \ldots, k\right\rangle$, for every $n \in \Gamma_{k}$ and for every $m \in \mathbb{N}$ we have the inclusion $[1, m] \subseteq \bigcup_{i=1}^{k}\left(E_{n}-E_{n}+m_{i}\right)$. This shows that property $(\star)$ is fulfilled by setting $F=\left\{m_{1}, \ldots, m_{k}\right\}$.

By the above lemma where $\gamma=\alpha \beta>0$, we can pick a finite set $F$ of cardinality $|F| \leqslant 1 / \alpha \beta$ and such that property $(\star)$ is satisfied by the sets

$$
E_{n}=\left(A_{n}-x_{n}-z_{n}\right) \cap\left(B_{n}-y_{n}\right) .
$$

So, for every $m$ there exists $n$ (in fact, infinitely many $n$ ) such that:

$$
[1, m] \subseteq\left(E_{n}-E_{n}\right)+F \subseteq\left(A_{n}-x_{n}-z_{n}\right)-\left(B_{n}-y_{n}\right)+F \subseteq(A-B)+F-t_{n}
$$

and hence $\left[t_{n}+1, t_{n}+m\right] \subseteq(A-B)+F$, where we denoted $t_{n}=x_{n}-y_{n}+z_{n}$. This completes the proof that $(A-B)+F$ is thick.

## 4 Final remarks and open problems

R. Jin's nonstandard proof in [8] was grounded on the following observation. Consider the set ${ }^{*} \mathbb{N}$ of nonstandard natural numbers; then a set $A \subseteq \mathbb{N}$ is piecewise syndetic if and only its nonstandard extension ${ }^{*} A \subseteq{ }^{*} \mathbb{N}$ is somewhere dense (i.e. not nowhere dense) in a suitable order-topology on ${ }^{*} \mathbb{N}$, as determined by the additive cut of (finite) natural numbers. A few years later, R. Jin's himself [9] elaborated a "standard" proof of his theorem, where the nonstandard reasonings were directly translated into the language of elementary combinatorics. Unfortunately, in this way "certain degree of intuition and motivation are lost" (ibid.), also because of the partly topological nature of the original arguments.

In a note with comments on a previous version of this paper, I.Z. Ruzsa pointed out that by similar arguments as the ones used here, an elementary proof of Jin's theorem can also be obtained by utilizing results from his 1978 paper [12]. Precisely, by referring to terminology and numbered theorems as presented there, one can proceed as follows. ${ }^{4}$ Given $A, B \subseteq \mathbb{Z}$ with positive upper Banach densities $d^{*}(A)=\alpha$ and $d^{*}(B)=\beta$, take the corresponding homogeneous systems $h_{1}(A)$ and $h_{1}(B)$. By Theorem 3, their densities as homogeneous systems - that we denote here by $\delta$ to avoid ambiguities - are the same as the original sets: $\delta\left(h_{1}(A)\right)=\alpha$ and $\delta\left(h_{1}(B)\right)=\beta$. Now consider the homogeneous system $H=h_{1}(A) \cap h_{1}(B)$ given by the intersection. By Theorem 5, $\delta(H) \geqslant \alpha \cdot \beta$ and so, by Theorem 4 , there exists a set $E$ with asymptotic density $d(E) \geqslant \delta(H)$, and such that $h_{1}(E) \subseteq H$. By a pigeonhole principle argument, it is shown that the positive density of $E$ implies the existence of a finite set $F$ with cardinality $|F| \leqslant 1 / d(E) \leqslant 1 / \alpha \beta$ and such that $(E-E)+F=\mathbb{Z}$. Now notice that, since $h_{1}(E) \subseteq h_{1}(A)$ and $h_{1}(E) \subseteq h_{1}(B)$, for every finite $G \subset E$ there exist $x, y$ such that $x+G \subset A$ and $y+G \subset B$, and hence $(x+y)+(G-G)+F \subset(A-B)+F$. Since $(E-E)+F=\mathbb{Z}$, it follows that every finite set has a shift included in $(A-B)+F$, which is therefore thick.

We close this paper by posing a couple of open questions. Recall that a family $\mathcal{F}$ of sets of integers is partition regular if it is closed under supersets and it satisfies the Ramsey property that $A \cup B \in \mathcal{F}$ implies $A \in \mathcal{F}$ or $B \in \mathcal{F}$ (three relevant examples are

[^3]given by the infinite sets, by the sets with positive upper density, and by the piecewise syndetic sets). We remark that, by exactly the same proof, the property of Lemma 5 also holds if one replaces $(\star)$ with
$(\star)_{\mathcal{F}}$
$$
\left\{n \in \mathbb{N} \mid[1, m] \subseteq\left(E_{n}-E_{n}\right)+F\right\} \in \mathcal{F}
$$
where $\mathcal{F}$ is any partition regular family of infinite sets. Can one derive a stronger version of Jin's theorem by using that stronger version of Lemma 5 ?

In $\S 1$, we recalled the property that $A-B$ is thick whenever $\mathrm{BD}(A)+\mathrm{BD}(B)>1$. Can one combine this fact with similar arguments as the ones presented in this paper, and prove interesting structural properties involving the three difference sets $A-B, A-C$, $B-C$, under the assumption that $\mathrm{BD}(A)+\mathrm{BD}(B)+\mathrm{BD}(C)>1$ ?

## References

[1] M. Beiglböck, V. Bergelson, and A. Fish. Sumset phenomenon in countable amenable groups, Adv. Math., 223:416-432, 2010.
[2] M. Beiglböck. An ultrafilter approach to Jin's theorem. Israel J. Math., 185:369-374, 2011.
[3] M. Kiyomi, T. Saitoh, and R. Uehara. Reconstruction of interval graphs. In Computing and Combinatorics, volume 5609 of Lecture Notes in Comput. Sci., pages 106-115. Springer, 2009.
[4] V. Bergelson, H. Fürstenberg, and B. Weiss. Piece-wise sets of integers and combinatorial number theory. In Topics in Discrete Mathematics, volume 26 of Algorithms Combin., pages 13-37. Springer, 2006.
[5] M. Di Nasso. Embeddability properties of difference sets. Integers. To appear.
[6] H. Fürstenberg. Recurrence in Ergodic Theory and Combinatorial Number Theory. Princeton University Press, 1981.
[7] N. Hegyvári. On iterated difference sets in groups. Period. Math. Hungar., 43:105110, 2001.
[8] R. Jin. The sumset phenomenon. Proc. Amer. Math. Soc., 130:855-861, 2002.
[9] R. Jin. Standardizing nonstandard methods for upper Banach density problems. In Unusual Applications of Number Theory (M. Nathanson, ed.), volume 64 of DIMACS Series, pages 109-124, 2004.
[10] S. Révész. On asymptotic uniform upper density in locally compact abelian groups. In Real Analysis Exchange, Summer Symposium 2011, pages 24-31.
[11] I.Z. Ruzsa. On difference-sequences. Acta Arith., XXV:151-157, 1974.
[12] I.Z. Ruzsa. On difference sets. Studia Sci. Math. Hungar., 13:319-326, 1978.
[13] I.Z. Ruzsa. Sumsets and structure. Part II of Combinatorial Number Theory and Additive Group Theory (A. Geroldinger and I.Z. Ruzsa, eds.), pages 87-210. Birkhäuser, 2009.
[14] T. Tao and V.H. Vu. Additive Combinatorics. Cambridge University Press, 2006.


[^0]:    ${ }^{1}$ This is proved by a straight application of Fekete's lemma: "Every sequence $\left\{a_{n}\right\}$ which is subadditive (i.e. $a_{n+m} \leqslant a_{n}+a_{m}$ ) converges to $\inf _{n} a_{n} / n$." Indeed, it is readily seen that $a_{n}=\max _{x \in \mathbb{Z}}|A \cap[x+1, x+n]|$ is subadditive.

[^1]:    ${ }^{2}$ This fact is mentioned in I.Z. Ruzsa's paper [11] of 1974. That result have been then generalized in several directions; see, e.g., [7] by H. Hegyvári where iterated difference sets are studied in the context of groups, and [10] by S. Révész in the context of locally compact abelian groups.

[^2]:    ${ }^{3}$ It is Lemma 5.1 of [5], but we re-prove it here to keep the paper self-contained.

[^3]:    ${ }^{4}$ The contents of I.Z. Ruzsa's note are reproduced here under his permission.

