

# The stability of finite sets in dyadic groups

by

TOM SANDERS (Oxford)

**1. Introduction and results.** Arithmetic stability is a concept introduced by Terry and Wolf [TW19] which quickly leads to many lines of questions. It is the purpose of this note to highlight one such line.

Formally, suppose that  $G$  is an Abelian group and  $A \subset G$ . For  $k \in \mathbb{N}$  we say  $A$  has the  *$k$ -order property (in  $G$ )* if there are vectors  $s, t \in G^k$  such that  $s_i + t_j \in A$  if and only if  $i \leq j$  (we say that  $s$  and  $t$  *witness* the  $k$ -order property), and it is  *$k$ -stable* if it does not have the  $k$ -order property.

The definition of the  $k$ -order property is inspired by the model-theoretic order property of formulas [She71, Definition 2.2]. Indeed, in the setup of [She71], the formula  $x + y \in A$  has the order property if and only if  $A$  has the  $k$ -order property for all  $k \in \mathbb{N}$ .

The model-theoretic stability of a formula has many equivalent definitions (see [She71, §2]), one of which is the negation of the order property. (Hence the terminology above.) It also extends to theories; a simple example of a stable theory is the theory of  $(G, +, 0)$  when  $G$  is a direct sum of a divisible group and a group of bounded order [Mac71, Theorem 1] <sup>(1)</sup>.

The problem of determining when stability is preserved under the adjoining of a predicate was opened up in [CZ01], and the particular case of adjoining sets of integers as unary predicates to the theory of  $(\mathbb{Z}, +, 0)$  has been pursued recently in [PS18, Con18, Con19]. Adjoining the natural numbers makes the theory unstable, and the present work might be seen as part of a quantitative investigation into whether there are subsets of dyadic groups that behave as badly as the naturals do in the integers.

---

2010 *Mathematics Subject Classification*: Primary 11B30.

*Key words and phrases*: stability, order property, additive combinatorics, Ruzsa modelling, polynomial method.

Received 1 November 2018; revised 24 May 2019.

Published online 18 October 2019.

<sup>(1)</sup> And the fact that totally transcendental theories are stable.

We say that sets  $S$  and  $T$  *witness* the  $k$ -order property if there is an enumeration of  $S$  as  $s_1, \dots, s_k$  and  $T$  as  $t_1, \dots, t_k$  such that  $s$  and  $t$  witness the  $k$ -order property. It is useful to observe that if  $s, t \in G^k$  witness the  $k$ -order property in  $A$  and  $\sigma$  and  $\tau$  are permutations of  $\{1, \dots, k\}$  such that  $s' := (s_{\sigma(i)})_i$  and  $t' := (t_{\tau(j)})_j$  also witness the  $k$ -order property in  $A$ , then  $\sigma$  and  $\tau$  are both the identity permutation <sup>(2)</sup>. In particular, if  $s, t \in G^k$  witness the  $k$ -order property then the  $s_i$ s are all distinct (and similarly for the  $t_j$ s); and if sets  $S$  and  $T$  witness the  $k$ -order property then the associated enumerations are unique.

We begin with the following simple proposition.

**PROPOSITION 1.1.** *Suppose that  $A \subset G$  has size  $N$ . Then  $A$  is  $(N + 1)$ -stable.*

*Proof.* Suppose that  $s$  and  $t$  witness the  $k$ -order property in  $G$ . Since the  $t_j$ 's are distinct,  $\{s_1 + t_j : 1 \leq j \leq k\}$  is a set of  $k$  elements contained in  $A$ , so  $k \leq N$ , and the result is proved. ■

In some groups this is best possible.

**PROPOSITION 1.2.** *Suppose that  $A$  is an arithmetic progression of length  $N$  in  $\mathbb{Z}$ . Then  $A$  is not  $N$ -stable.*

*Proof.* Write  $A = \{x, x + d, \dots, x + (N - 1)d\}$ , and let  $s_i := x - \text{id}$  and  $t_i = \text{id}$  for  $1 \leq i \leq N$ . A simple check shows  $s, t \in \mathbb{Z}^N$  witness the  $N$ -order property (cf. [Sis18, Lemma 6.3]). ■

Given this we ask what happens in groups not containing long arithmetic progressions. The dyadic group  $\mathbb{F}_2^\infty$  (the direct sum of  $\mathbb{F}_2$  with itself countably many times) is the prototypical example of such a group. Its study has been tremendously useful in additive combinatorics, and we refer the reader to the survey [Gre05] by Green and the sequel [Wol15] by Wolf for more information.

**THEOREM 1.3.** *There is  $c > 0$  such that every  $A \subset \mathbb{F}_2^\infty$  of size  $N$  is  $O(N^{1-c})$ -stable.*

[TW19, Example 3] shows that  $c$  cannot be improved past  $1/2$ ; we shall develop this to give the following.

**PROPOSITION 1.4.** *There is  $c > 0$  such that for all  $N \in \mathbb{N}$  there is a set  $A \subset \mathbb{F}_2^\infty$  of size  $N$  that is not  $\Omega(N^{1/2+c})$ -stable.*

---

<sup>(2)</sup> Indeed, since  $\tau$  is a surjection and  $s$  and  $t$  witness the  $k$ -order property, the set  $\{\tau(j) : s_{\sigma(i)} + t_{\tau(j)} \in A\}$  has size  $k + 1 - \sigma(i)$ . On the other hand, since  $s'$  and  $t'$  witness the  $k$ -order property, the set  $\{j : s_{\sigma(i)} + t_{\tau(j)} \in A\} = \{j : s'_i + t'_j \in A\}$  has size  $k + 1 - i$ . Since  $\tau$  is a bijection,  $k + 1 - \sigma(i) = k + 1 - i$  and so  $\sigma(i) = i$ ; the same arguments work for  $\tau$ .

Before turning to the proofs we make two remarks. First, the notion of stability is of interest in the papers [TW19, TW18] of Terry and Wolf when a set has small stability, and it is not clear to us whether our work, which sits at the other end of the scale, genuinely gets at mathematically significant issues.

Secondly, it may well be that there is a rather more direct combinatorial argument and allied lower-bound construction that significantly simplifies and strengthens the work here; certainly we do not know how to rule out such a possibility.

**2. Proofs.** Our proof of Theorem 1.3 decouples into two parts. We begin with the ‘modelling’ part.

**LEMMA 2.1.** *Suppose that  $A \subset \mathbb{F}_2^\infty$  has the  $k$ -order property,  $|A| \leq Kk$ , and  $1 \leq l < \frac{1}{4}k$  is an integer with  $l = \eta k$ . Then there is a natural number  $n$  and a set  $A' \subset \mathbb{F}_2^n$  with  $2^n = O(\eta^{-10} K^{15} k)$  that has the  $(k - 2l + 1)$ -order property.*

It is tremendously tempting to note that the Balog–Szemerédi–Gowers theorem [TV06, Theorem 2.29] applies to show that if  $A \subset \mathbb{F}_2^\infty$  has the  $k$ -order property (witnessed by sets  $S$  and  $T$ ) and  $|A| \leq Kk$  then there are sets  $S' \subset S$  and  $T' \subset T$  with  $|S'|, |T'| = \Omega(k)$  and  $|S' + T'| = O(K^3 k)$ . While this seems very well suited, in fact we shall find it easier to proceed directly.

*Proof of Lemma 2.1.* Let  $s, t \in (\mathbb{F}_2^\infty)^k$  witness the  $k$ -order property in  $A$ , and let  $G$  be the group generated by  $A \cup \{t_1, \dots, t_k, s_1, \dots, s_k\}$  (which is finite) and recall that the  $s_i$ ’s and  $t_j$ ’s are distinct. Put

$$\begin{aligned} S' &:= \{s_i : 1 \leq i \leq l\}, & S^+ &:= \{s_i : l \leq i \leq k - l\}, \\ T' &:= \{t_j : k - l \leq j \leq k\}, & T^+ &:= \{t_j : l \leq j \leq k - l\}. \end{aligned}$$

It follows that

$$|S'|, |T'| \geq l, \quad |S^+|, |T^+| \geq k - 2l \quad \text{and} \quad S' + T^+, S' + T', S^+ + T' \subset A.$$

The Ruzsa triangle inequality [TV06, Lemma 2.6] then gives

$$\begin{aligned} |S^+ + T^+| &\leq \frac{|S^+ + T'| \cdot |T' + T^+|}{|-T'|} = \frac{|S^+ + T'| \cdot |T' - T^+|}{|T'|} \\ &\leq \frac{|S^+ + T'| \cdot |T' + S'| \cdot |-S' - T^+|}{|T'| \cdot |-S'|} = \frac{|S^+ + T'| \cdot |T' + S'| \cdot |S' + T^+|}{|T'| \cdot |S'|} \\ &\leq \eta^{-2} K^3 k \leq 2\eta^{-2} K^3 \min\{|T^+|, |S^+|\}. \end{aligned}$$

We now follow the proof of [GR07, Proposition 6.1]. Let  $n \in \mathbb{N}$  be the smallest positive integer for which there is a homomorphism  $\phi : G \rightarrow \mathbb{F}_2^n$  such that  $\phi$

restricted to  $S^+ + T^+$  is injective. Such a map exists since  $S^+ + T^+$  is finite, so projection onto the (finite) group it generates is an example.

Suppose there is some  $x \in \mathbb{F}_2^n \setminus (\phi(S^+) - \phi(S^+) + \phi(T^+) - \phi(T^+))$ . Let  $\theta : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^{n-1}$  be a homomorphism with  $\ker \theta = \{0, x\}$ . Then  $\theta \circ \phi : G \rightarrow \mathbb{F}_2^{n-1}$  is a homomorphism, and so by minimality of  $n$  there are elements  $s, s' \in S^+$  and  $t, t' \in T^+$  such that

$$\theta \circ \phi(s + t) = \theta \circ \phi(s' + t') \quad \text{and} \quad s + t \neq s' + t'.$$

It follows that

$$\phi((s + t) - (s' + t')) \in \ker \theta = \{0, x\}.$$

Since  $s + t \neq s' + t'$ , we see that  $\phi(s) + \phi(t) - \phi(s') - \phi(t') = x$ , which contradicts how  $x$  was chosen. It follows that

$$2^n = |\phi(S^+) - \phi(S^+) + \phi(T^+) - \phi(T^+)|.$$

Let  $\emptyset \neq Z \subset T^+$  be such that  $|Z|^{-1}|S^+ + Z|$  is minimal possible:

$$\frac{|S^+ + Z|}{|Z|} = \min \left\{ \frac{|S^+ + Z'|}{|Z'|} : \emptyset \neq Z' \subset Z \right\},$$

and similarly for  $\emptyset \neq W \subset S^+$ . By [Pet12, Proposition 2.1] (and the fact that  $-A = A$  for all sets in  $G$  and  $\phi$  is injective on  $S^+ + T^+$ ) we see that

$$\begin{aligned} 2^n &= |\phi(S^+) - \phi(S^+) + \phi(T^+) - \phi(T^+)| \\ &= \frac{|S^+ - S^+ + T^+ - T^+ + \ker \phi|}{|\ker \phi|} = \frac{|2S^+ + 2T^+ + \ker \phi|}{|\ker \phi|} \\ &\leq \frac{|2S^+ + 2T^+ + Z + W + \ker \phi|}{|\ker \phi|} \leq (2\eta^{-2}K^3)^4 \frac{|Z + W + \ker \phi|}{|\ker \phi|} \\ &\leq (2\eta^{-2}K^3)^4 \frac{|S^+ + T^+ + \ker \phi|}{|\ker \phi|} \leq 2^4 \eta^{-10} K^{15} k. \end{aligned}$$

Finally, let

$$A' := \{\phi(s_i + t_j) : l \leq i \leq j \leq k - l\},$$

and let  $s', t' \in (\mathbb{F}_2^m)^{k-2l+1}$  be defined by

$$s'_i := \phi(s_{l+i-1}) \quad \text{and} \quad t'_j := \phi(t_{l+j-1}) \quad \text{for } 1 \leq i, j \leq k - 2l + 1.$$

Since  $\phi$  is injective, we see that  $s'_i + t'_j \in A'$  if and only if  $s_{l+i-1} + t_{l+j-1} \in A$ , which is true if and only if  $l + i - 1 \leq l + j - 1$ , which in turn is true if and only if  $i \leq j$ . We conclude that  $A'$  has the  $(k - 2l + 1)$ -order property. ■

The second ingredient is the following.

LEMMA 2.2. *There is  $c > 0$  such that every  $A \subset \mathbb{F}_2^n$  is  $O(2^{n(1-c)})$ -stable.*

We shall use the polynomial method from the work of Croot, Lev and Pach [CLP17], though we follow the sequel [EG17] by Ellenberg and Gijswijt.

We write  $S_n$  for the  $\mathbb{F}_2$ -vector space of maps  $\mathbb{F}_2^n \rightarrow \mathbb{F}_2$ ; put

$$M_n^d := \left\{ \mathbb{F}_2^n \rightarrow \mathbb{F}_2 : x \mapsto \prod_{i \in I} x_i : I \subset [n] \text{ has } |I| \leq d \right\},$$

so that  $M_n^d$  is linearly independent; let  $S_n^d$  be the subspace of  $S_n$  with  $M_n^d$  as a basis; and write  $M_n := M_n^n$  for the basis of monomials for  $S_n$ , so

$$\dim S_n^d = \sum_{r=0}^d \binom{n}{r} = \sum_{r=n-d}^n \binom{n}{r}.$$

This can be estimated using  $H$ , the binary entropy function—we refer to [MS77, §11, Chapter 10] for the relevant estimate <sup>(3)</sup>.

*Proof of Lemma 2.2.* Suppose that  $k$  is maximal such that  $A$  has the  $k$ -order property;  $s, t \in (\mathbb{F}_2^n)^k$  witness the  $k$ -order property in  $A$ ; and write  $S := \{s_i : 1 \leq i \leq k\}$  and  $T := \{t_j : 1 \leq j \leq k\}$ . Suppose that there are elements  $1 \leq i, j \leq k$  such that  $s_i + t_i = s_j + t_j$ . Without loss of generality we have  $i \leq j$  and hence (since  $2 \cdot t_i = 0_{\mathbb{F}_2^n}$  and  $-t_j = t_j$ )

$$(2.2) \quad s_j + t_i = s_j - t_i = s_i - t_j = s_i + t_j \in A.$$

It follows that  $i = j$ , and so  $\{s_i + t_i : 1 \leq i \leq k\}$  is a set of  $k$  distinct elements; write  $A_0$  for this set.

The remainder of the proof follows that of [EG17, Theorem 4] very closely. Let  $p \in (1/2, 1]$  be a constant to be optimised later with  $np$  an odd integer, and suppose that  $k \geq 2^{H(p)n+1}$ . Write  $d := np - 1$  (which is an even integer), and so by (2.1),

$$\frac{1}{2}k \geq 2^{H(p)n} \geq \sum_{r=d+1}^n \binom{n}{r} = 2^n - \sum_{r=0}^d \binom{n}{r}.$$

Writing  $V := S_n^d \cap \{F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 : F(x) = 0_{\mathbb{F}_2} \text{ for all } x \in \neg A\}$  and rearranging the above we get

$$\dim V \geq \sum_{r=0}^d \binom{n}{r} - |\neg A| \geq |A| - \frac{1}{2}k.$$

Let  $P \in S_n^d$  be a polynomial that is  $0_{\mathbb{F}_2}$  on  $\neg A$  and of maximal support and write  $\Sigma$  for the support of  $P$ . If  $|\Sigma| < \dim V$  then there would be some  $Q \in V$  not identically  $0_{\mathbb{F}_2}$  with  $Q(x) = 0_{\mathbb{F}_2}$  for all  $x \in \Sigma$ , so that  $Q + P$

---

<sup>(3)</sup> For completeness:  $H : [0, 1] \rightarrow \mathbb{R}; p \mapsto -p \log_2 p - (1-p) \log_2 (1-p)$  with the usual conventions that  $H(0) = H(1) = 0$ , and [MS77, Lemma 8, §11, Chapter 10] tells us that

$$(2.1) \quad \sum_{r=pn}^n \binom{n}{r} \leq 2^{H(p)n} \quad \text{whenever } p \in (1/2, 1] \text{ and } pn \in \mathbb{Z}.$$

would have larger support. We conclude that the support of  $P$  has size at least  $|A| - \frac{1}{2}k$  and so includes at least half of  $A_0$ .

Write  $I := \{1 \leq i \leq k : P(s_i + t_i) \neq 0_{\mathbb{F}_2}\}$ , so that  $|I| \geq \frac{1}{2}k$ . The matrix  $(P(s + t))_{s \in S, t \in T}$  includes the rows  $(P(s_i + t_j))_{j=1}^k$  for  $i \in I$ . If  $i \in I$  then  $P(s_i + t_i) \neq 0_{\mathbb{F}_2}$  and  $P(s_i + t_j) = 0_{\mathbb{F}_2}$  for all  $1 \leq j < i$ , and so the rows generate a space of dimension at least  $|I|$ , and hence

$$\text{rk}_{\mathbb{F}_2}(P(s + t))_{s \in S, t \in T} \geq \frac{1}{2}k.$$

On the other hand (as in [EG17, (1)]) there are constants  $c_{m,m'} \in \mathbb{F}_2$  such that

$$\begin{aligned} P(x + y) &= \sum_{m, m' \in M_n^d : \deg mm' \leq d} c_{m, m'} m(x) m'(y) \\ &= \sum_{m \in M_n^{d/2}} m(x) F_m(y) + \sum_{m' \in M_n^{d/2}} F_{m'}(x) m'(y) \quad \text{for all } x, y \in \mathbb{F}_2^n. \end{aligned}$$

It follows from (2.1) again that

$$\begin{aligned} \text{rk}_{\mathbb{F}_2}(P(s + t))_{s \in S, t \in T} &\leq 2 \dim S_n^{d/2} \leq 2 \sum_{r=0}^{d/2} \binom{n}{r} = 2 \sum_{r=n-d/2}^n \binom{n}{r} \\ &\leq 2^{1+H(1-p/2+1/(2n))n}, \end{aligned}$$

and since  $H$  is decreasing on  $[1/2, 1]$ , we conclude that

$$k \leq \max\{2^{H(p)n+1}, 2^{H(1-p/2)n+2}\}.$$

We get the result on putting  $p := 2/3 + O(n^{-1})$ , so that  $H(p) = H(1 - p/2) + o(1)$ . ■

It may be worth noting that (2.2) is a special case of a more general fact. Suppose that  $s, t \in (\mathbb{F}_2^\infty)^k$  witness the  $k$ -order property in  $A$  and consider the  $\mathbb{F}_2^\infty$ -valued matrix  $M$  with  $M_{ij} := s_i + t_j$ . If  $1 \leq i \leq j < i' \leq j' \leq k$  are such that  $M_{ij} = M_{i'j'}$ , then

$$M_{i'j} = s_{i'} + t_j = s_i + M_{ij} + t_{j'} + M_{i'j'} = M_{ij'} + 2M_{ij} = M_{ij'},$$

which contradicts the fact that  $1_A(M_{i'j}) = 0 \neq 1 = 1_A(M_{ij'})$ . Put another way, we have  $M_{ij} \neq M_{i'j'}$  whenever  $1 \leq i \leq j < i' \leq j' \leq k$ . One might hope that this condition alone requires  $M$  to take many different values (and hence  $A$  to be large compared with  $k$ ). However, it is possible to construct a matrix satisfying this property (and having distinct values in every row and column) using  $O(k \log k)$  distinct elements.

Our argument is very similar to the arguments of Dvir and Edelman [DE19] who apply the Croot–Lev–Pach method to examine the rigidity [Val77, Definition, §6] of certain random matrices. The matrix we have to

consider is the ‘all-ones’ upper triangular matrix and as it happens the rigidity of this has been explicitly calculated in [PV91, Theorem 1]. It is very natural to imagine more can be made of this structure.

With these two lemmas we can prove our main result.

*Proof of Theorem 1.3.* Suppose that  $A$  has the  $k$ -order property. Let  $K := N/k$  and apply Lemma 2.1 with  $l := \lfloor k/4 \rfloor$  to get  $n \in \mathbb{N}$  and a set  $A' \subset \mathbb{F}_2^n$  that has the  $\frac{1}{2}k$ -order property where  $2^n \leq O(K^{15}k)$ . Then apply Lemma 2.2 to  $A'$  to get an absolute  $c_0 \in (0, 1)$  such that  $\frac{1}{2}k = O(K^{15(1-c_0)}k^{1-c_0})$ . The result follows with  $c = c_0/(15 - 14c_0)$ . ■

The extension of Theorem 1.3 to groups of bounded exponent seems interesting, though there the constant  $c$  would have to depend on the exponent since Proposition 1.2 extends from integers to any Abelian group if we add the hypothesis  $|A + A| = 2|A| - 1$ .

The proof of Lemma 2.1 extends easily, as does much of the proof of Lemma 2.2. In particular, the Croot–Lev–Pach method has been extended to groups of bounded exponent (see e.g. [BC<sup>+</sup>17, proof of Theorem A]). However, (2.2) relies on working in characteristic 2 and this would need to be replaced in the more general setting.

It remains to prove Proposition 1.4; we shall show the following explicit version.

**PROPOSITION 2.3.** *For all  $N \in \mathbb{N}$  there is a set  $A \subset \mathbb{F}_2^\infty$  of size  $N$  that is not  $N^{1/(2-c)-o(1)}$ -stable where  $c = \log_8(1 + \frac{5-2\sqrt{2}}{3+2\sqrt{2}}) = 0.152\dots$*

*Proof.* Write  $G := \mathbb{F}_2^\infty$ ; let  $l \in \mathbb{N}$  be a parameter to be optimised later; let  $R := \binom{2l}{l}$ ; and let  $S_1, \dots, S_R$  be an enumeration of the subsets of  $[2l]$  of size  $l$  such that  $S_r \cup S_{R+1-r} = [2l]$  for all  $r \in \{1, \dots, R\}$ . (For example, proceed iteratively: first select  $S_1$  arbitrarily, then put  $S_R := [2l] \setminus S_1$ ; select  $S_2$  from what remains and put  $S_{R-1} := [2l] \setminus S_2$ ; etc.) Write

$$V_S := \{x \in G : x_i = 0 \text{ whenever } i \notin S\} \quad \text{for } S \subset [2l].$$

Let  $u_1, \dots, u_R, w_1, \dots, w_R \subset G$  be such that

$$(2.3) \quad u_i + w_j + V_{[2l]} \text{ are pairwise disjoint for } 1 \leq i, j \leq R$$

(for example by selecting greedily). For each  $1 \leq i \leq R$ , let  $v_1^{(i)}, \dots, v_{2^l}^{(i)}$  be an enumeration of  $V_{S_i}$ . Finally, let

$$\Delta_{i,j} := \begin{cases} V_{S_i} + V_{S_{R+1-j}} & \text{if } i < j, \\ \{v_m^{(i)} + v_n^{(R+1-i)} : 1 \leq m \leq n \leq 2^l\} & \text{if } i = j, \end{cases}$$

and

$$A := \bigcup_{1 \leq i \leq j \leq R} (u_i + w_j + \Delta_{i,j}).$$

Now

$$\begin{aligned}
|A| &\leq 2^{2l} \sum_{1 \leq i, j \leq R} 2^{-|S_i \cap S_j|} = 2^{2l} \sum_{S, T \subset [2l], |S|=|T|=l} 2^{-|S \cap T|} \\
&= 2^{2l} \sum_{s=0}^l \binom{2l}{s} \binom{2l-s}{l-s} \binom{l}{l-s} 2^{-s} = \binom{2l}{l} 2^{2l} \sum_{s=0}^l \binom{l}{s}^2 2^{-s} \\
&\leq 2^{4l} \left( \sum_{s=0}^l \binom{l}{s} \sqrt{2}^{-s} \right)^2 = 2^{4l} \left( 1 + \frac{1}{\sqrt{2}} \right)^{2l}.
\end{aligned}$$

Now let

$$\begin{aligned}
s &= (s_1, \dots, s_{R2^l}) \\
&:= (u_1 + v_1^{(1)}, \dots, u_1 + v_{2^l}^{(1)}, u_2 + v_1^{(2)}, \dots, u_R + v_1^{(R)}, \dots, u_R + v_{2^l}^{(R)}), \\
t &= (t_1, \dots, t_{R2^l}) \\
&:= (w_1 + v_1^{(R)}, \dots, w_1 + v_{2^l}^{(R)}, w_2 + v_1^{(R-1)}, \dots, w_R + v_1^{(1)}, \dots, w_R + v_{2^l}^{(1)}).
\end{aligned}$$

Suppose that  $1 \leq i, j \leq R2^l$ , and let  $1 \leq b, b' \leq R$  and  $1 \leq a, a' \leq 2^l$  be the unique integers such that

$$i = a + 2^l(b-1) \quad \text{and} \quad j = a' + 2^l(b'-1),$$

so that

$$(2.4) \quad s_i + t_j = u_b + w_{b'} + v_a^{(b)} + v_{a'}^{(R+1-b')}.$$

If  $i \leq j$  then either

- $b < b'$ , in which case  $s_i + t_j \in u_b + w_{b'} + V_{S_b} + V_{S_{R+1-b'}} \subset A_0 \subset A$ ; or
- $b = b'$ , in which case  $a \leq a'$  and  $s_i + t_j \in u_b + w_b + \Delta_{b,b} \subset A$ .

In the other direction, suppose  $s_i + t_j \in A$ . Then by definition of  $A$  there are some  $1 \leq i' \leq j' \leq R$  such that  $s_i + t_j \in u_{i'} + w_{j'} + \Delta_{i',j'}$ . By (2.4) we have  $s_i + t_j \in u_b + w_{b'} + V_{[2l]}$  and so by (2.3) we see that  $i' = b$  and  $j' = b'$ . Either

- $b \neq b'$ , in which case the fact that  $b = i' \leq j' = b'$  implies that  $b < b'$  and hence  $i < j$ ; or
- $b = b'$ , in which case  $i' = j' = b$  and there are elements  $1 \leq m' \leq n' \leq 2^l$  such that  $s_i + t_j = u_b + w_b + v_{m'}^{(b)} + v_{n'}^{(R+1-b)}$ , which substituted into (2.4) gives  $v_a^{(b)} + v_{a'}^{(R+1-b)} = v_{m'}^{(b)} + v_{n'}^{(R+1-b)}$ ; since  $S_b \cap S_{R+1-b} = \emptyset$ , it follows that  $a = m'$  and  $a' = n'$ , so that  $i \leq j$  since  $m' \leq n'$ .

It follows that  $A$  has the  $R2^l$ -order property, and taking  $l$  suitably in terms of  $N$  gives the result. ■

**Acknowledgements.** My thanks to Julia Wolf for useful conversations on this topic, and to an anonymous referee for carefully reading the paper and in particular highlighting an error in the proof of Lemma 2.1.

## References

- [BC<sup>+</sup>17] J. Blasiak, T. Church, H. Cohn, J. A. Grochow, E. Naslund, W. F. Sawin and C. Umans, *On cap sets and the group-theoretic approach to matrix multiplication*, Discrete Anal. 2017, art. 3, 27 pp.
- [CZ01] E. Casanovas and M. Ziegler, *Stable theories with a new predicate*, J. Symbolic Logic 66 (2001), 1127–1140.
- [Con18] G. Conant, *Multiplicative structure in stable expansions of the group of integers*, Illinois J. Math. 62 (2018), 341–364.
- [Con19] G. Conant, *Stability and sparsity in sets of natural numbers*, Israel J. Math. 230 (2019), 471–508.
- [CLP17] E. Croot, V. F. Lev and P. P. Pach, *Progression-free sets in  $\mathbb{Z}_4^n$  are exponentially small*, Ann. of Math. (2), 185 (2017), 331–337.
- [DE19] Z. Dvir and B. L. Edelman, *Matrix rigidity and the Croot–Lev–Pach lemma*, Theory Comput. 15 (2019), art. 8, 7 pp.
- [EG17] J. S. Ellenberg and D. Gijswijt, *On large subsets of  $\mathbb{F}_q^n$  with no three-term arithmetic progression*, Ann. of Math. (2), 185 (2017), 339–343.
- [Gre05] B. J. Green, *Finite field models in additive combinatorics*, in: Surveys in Combinatorics 2005, London Math. Soc. Lecture Note Ser. 327, Cambridge Univ. Press, Cambridge, 2005, 1–27.
- [GR07] B. Green and I. Z. Ruzsa, *Freiman’s theorem in an arbitrary abelian group*, J. London Math. Soc. (2) 75 (2007), 163–175.
- [Mac71] A. Macintyre, *On  $\omega_1$ -categorical theories of abelian groups*, Fund. Math. 70 (1971), 253–270.
- [MS77] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes. I*, North-Holland Math. Library 16, North-Holland, Amsterdam, 1977.
- [PS18] D. Palacín and R. Sklinos, *On superstable expansions of free abelian groups*, Notre Dame J. Formal Logic 59 (2018), 157–169.
- [Pet12] G. Petridis, *New proofs of Plünnecke-type estimates for product sets in groups*, Combinatorica 32 (2012), 721–733.
- [PV91] P. Pudlák and Z. Vavřín, *Computation of rigidity of order  $n^2/r$  for one simple matrix*, Comment. Math. Univ. Carolin. 32 (1991), 213–218.
- [She71] S. Shelah, *Stability, the f.c.p., and superstability; model theoretic properties of formulas in first order theory*, Ann. Math. Logic 3 (1971), 271–362.
- [Sis18] O. Sisask, *Convolutions of sets with bounded VC-dimension are uniformly continuous*, arXiv:1802.02836 (2018).
- [TV06] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Stud. Adv. Math. 105, Cambridge Univ. Press, Cambridge, 2006.
- [TW18] C. Terry and J. Wolf, *Quantitative structure of stable sets in finite abelian groups*, arXiv:1805.06847 (2018).
- [TW19] C. Terry and J. Wolf, *Stable arithmetic regularity in the finite field model*, Bull. London Math. Soc. 51 (2019), 70–88.
- [Val77] L. G. Valiant, *Graph-theoretic arguments in low-level complexity*, in: Lecture Notes in Computer Sci. 53, Springer, Berlin, 1977, 162–176.

- [Wol15] J. Wolf, *Finite field models in arithmetic combinatorics—ten years on*, Finite Fields Appl. 32 (2015), 233–274.

Tom Sanders  
Mathematical Institute  
University of Oxford  
Radcliffe Observatory Quarter  
Woodstock Road  
Oxford OX2 6GG, United Kingdom  
E-mail: tom.sanders@maths.ox.ac.uk