ACTA ARITHMETICA
189.4 (2019)

On theorems of Wirsing and Sanders

by

Zhenchao Ge and Thái Hoàng Lê (University, MS)

1. Introduction. For two sets X, Y we denote by $X + Y$ the sumset $\{x + y : x \in X,\, y \in Y\}$ and by kX the k-fold sumset $X + \cdots + X$ (k times). A set $H \subset \mathbb{Z}$ is called an *essential component* if $\sigma(A + H) > \sigma(A)$ for any $A \subset \mathbb{Z}$ with $0 < \sigma(A) < 1$, where $\sigma(A)$ is the Schnirelmann density of A. In [8], Wirsing constructed essential components in $\mathbb{Z}$ with small counting functions. He also proved the following finite version of his main result.

Theorem 1.1 ([8, Theorem 4]). *Let $n \geq 1$ and $A \subset \mathbb{Z}$ be any subset of $[1, 2^n]$. Let $H = \{\pm 2^k : k \geq 0\} \cup \{0\}$ and $B = (A + H) \cap [1, 2^n]$. Then*

$$|B| \geq |A| + \sqrt{\frac{2}{n}}\,|A|\left(1 - \frac{|A|}{2^n}\right).$$

Wirsing's argument is elementary, very simple and surprisingly effective. In this note, we will adapt it to prove an analogous result for vector spaces over a finite field. The adaptation is straightforward for $\mathbb{F}_2^n$, but less so for $\mathbb{F}_p^n$ if $p \geq 3$.

Theorem 1.2. *Let p be a prime and $e_1, \ldots, e_n$ be a basis of $\mathbb{F}_p^n$. Put $H = \{e_1, \ldots, e_n\} \cup \{0\}$. Then for any $A \subset \mathbb{F}_p^n$, we have*

$$|A + H| \geq |A| + \frac{c(p)}{\sqrt{n}}|A|\left(1 - \frac{|A|}{p^n}\right)$$

for some constant $c(p) > 0$. We can take $c(2) = \sqrt{2}$ and $c(p) = \Omega(p^{-3/2})$.

As an application, we will quickly deduce the following generalization of a theorem of Sanders [7, Theorem 1.2]. By the *density* of a subset $A \subset X$ in X, we mean $|A|/|X|$.

2010 *Mathematics Subject Classification*: Primary 11B30; Secondary 11B05.
Key words and phrases: difference sets, sumsets, isoperimetric inequalities, finite fields.
Received 25 January 2018; revised 26 August 2018.
Published online 3 June 2019.

DOI: 10.4064/aa180125-20-9

THEOREM 1.3. *Let p be a prime. Then there is a constant $c'(p) > 0$ such that the following holds. If $A \subset \mathbb{F}_p^n$ has density $\alpha > 1/2 - \frac{c'(p)}{\sqrt{n}}$, then $A - A$ contains a subspace of codimension* 1.

Sanders' theorem is a special case of Theorem 1.3 when $p = 2$. In Section 2 we will prove a general result for Cartesian products (Theorem 2.1). The main Theorems 1.2 and 1.3 are proved in Sections 3 and 4, respectively.

2. Wirsing's argument for Cartesian products. Let $(q_k)_{k=1}^{\infty}$ be a sequence of positive integers. Write $I_k = \{0, 1, \ldots, q_k - 1\}$. Define

$$Q_n = \prod_{k=1}^{n} I_k.$$

The *Hamming distance* between two elements $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ of Q_n is

$$d(\mathbf{x}, \mathbf{y}) := |\{1 \le i \le n : x_i \ne y_i\}|. \tag{2.1}$$

For a set $A \subset Q_n$ and $r \ge 0$, we define the neighborhood of A with radius r as

$$B(A, r) = B_n(A, r) = \{\mathbf{x} \in Q_n : \text{there exists } \mathbf{y} \in A \text{ such that } d(\mathbf{x}, \mathbf{y}) \le r\}.$$

We will prove the following:

THEOREM 2.1. *For any set $A \subset Q_n$, we have*

$$|B_n(A, 1)| \ge |A| + \sqrt{\frac{2}{\sum_{i=1}^{n}(q_i - 1)}}\,|A|\Big(1 - \frac{|A|}{|Q_n|}\Big). \tag{2.2}$$

REMARK 2.2. After writing this paper, we learned that in the special case $Q_n = \{0, 1\}^n$, Theorem 2.1 appeared as [2, Theorem 3] with a very similar argument.

We will need the following estimate in the proof of Theorem 2.1.

LEMMA 2.3. *For any non-negative real numbers $x_1, \ldots, x_m$, we have*

$$\sum_{1 \le i \le j \le m} (x_i + x_{i+1} + \cdots + x_j)^2 \le m\Big(\sum_{i=1}^{m}(x_1 + \cdots + x_i)\Big)^2. \tag{2.3}$$

Proof. This follows simply from comparing coefficients. For $1 \le k \le m$, the coefficient of x_k^2 in LHS is $k(m + 1 - k)$, while its coefficient in RHS is $m(m + 1 - k)^2$. For $1 \le k < l \le m$, the coefficient of $x_k x_l$ in LHS is $2k(m + 1 - l)$, while its coefficient in RHS is $2m(m + 1 - l)(m + 1 - k)$. ∎

Proof of Theorem 2.1. Let ζ_n be a sequence of positive reals to be determined later. Ultimately, we will make the choice $\zeta_n = \sqrt{2/\sum_{i=1}^{n}(q_i - 1)}$, but for now we will write them as generic numbers. The conditions imposed on the ζ_n's will come from the proof.

We will prove by induction on n that for any $A \subset Q_n$, we have

$$|B_n(A,1)| \geq |A| + \zeta_n |A| \left(1 - \frac{|A|}{|Q_n|}\right). \tag{2.4}$$

When $n = 1$ and $A \subset Q_1$, we have $B_1(A,1) = Q_1$. We easily see that (2.4) is true whenever

$$\zeta_1 \leq \frac{q_1}{q_1 - 1}. \tag{2.5}$$

For the inductive step, suppose (2.4) is true for all subsets of Q_{n-1} with a constant ζ_{n-1} in place of ζ_n. For $X \subset Q_{n-1}$ and $Y \subset I_n$, we write

$$X \oplus Y = \{(\mathbf{x}, y) \in Q_n : \mathbf{x} \in X,\ y \in Y\}.$$

Let $A \subset Q_n$. For any $i \in I_n$, we define

$$A_i = \{\mathbf{a} \in Q_{n-1} : (\mathbf{a}, i) \in A\}.$$

Then clearly we have the partition

$$A = \bigsqcup_{i=0}^{q_n - 1} A_i \oplus \{i\}, \tag{2.6}$$

and consequently

$$|A| = \sum_{i=0}^{q_n-1} |A_i|. \tag{2.7}$$

Our first observation is that for any $i \in I_n$, we have $A_i \oplus I_n \subset B_n(A,1)$. This leads to the bound

$$|B_n(A,1)| \geq q_n |A_i| \tag{2.8}$$

for any $i \in I_n$. Next, we observe that for $i \in I_n$, we have $B_{n-1}(A_i,1) \oplus \{i\} \subset B_n(A,1)$. Clearly the sets $B_{n-1}(A_i,1) \oplus \{i\}$ are disjoint. Thus we have yet another bound

$$|B_n(A,1)| \geq \sum_{i=0}^{q_n-1} |B_{n-1}(A_i,1)|. \tag{2.9}$$

Without loss of generality we may assume $|A_0| \geq |A_1| \geq \cdots \geq |A_{q_n-1}|$. From (2.8) and (2.7), we deduce

$$|B_n(A,1)| \geq |A| + \sum_{k=0}^{q_n-1} (|A_0| - |A_k|).$$

We distinguish two cases.

Case 1:

$$\sum_{k=0}^{q_n-1}(|A_0|-|A_k|)\geq \zeta_n|A|\left(1-\frac{|A|}{|Q_n|}\right).$$

In this case (2.4) follows immediately.

Case 2:

$$\sum_{k=0}^{q_n-1}(|A_0|-|A_k|)\leq \zeta_n|A|\left(1-\frac{|A|}{|Q_n|}\right). \tag{2.10}$$

Using (2.9) and the induction hypothesis for each $A_k\subset Q_{n-1}$, we have

$$\begin{aligned}|B_n(A,1)| &\geq \sum_{k=0}^{q_n-1}\left\{|A_k|+\zeta_{n-1}|A_k|\left(1-\frac{|A_k|}{|Q_{n-1}|}\right)\right\} \\ &= |A|+\zeta_{n-1}|A|-\frac{\zeta_{n-1}}{|Q_{n-1}|}\sum_{k=0}^{q_n-1}|A_k|^2.\end{aligned} \tag{2.11}$$

Moreover,

$$\sum_{k=0}^{q_n-1}|A_k|^2=\frac{1}{q_n}\Big(|A|^2+\sum_{0\leq i<j\leq q_n-1}(|A_i|-|A_j|)^2\Big). \tag{2.12}$$

For $i=1,\dots,q_n-1$, put $x_i=|A_{i-1}|-|A_i|\geq 0$. Then (2.10) reads

$$\sum_{i=1}^{q_n-1}(x_1+\cdots+x_i)\leq \zeta_n|A|\left(1-\frac{|A|}{|Q_n|}\right).$$

On the other hand,

$$\sum_{0\leq i<j\leq q_n-1}(|A_i|-|A_j|)^2=\sum_{1\leq i\leq j\leq q_n-1}(x_i+x_{i+1}+\cdots+x_j)^2.$$

Thus Lemma 2.3 implies that

$$\sum_{k=0}^{q_n-1}|A_k|^2\leq \frac{1}{q_n}\left(|A|^2+(q_n-1)\zeta_n^2|A|^2\left(1-\frac{|A|}{|Q_n|}\right)^2\right). \tag{2.13}$$

Putting this into (2.11) yields

(2.14)

$$\begin{aligned}|B_n(A,1)| &\geq |A|+\zeta_{n-1}|A|-\frac{\zeta_{n-1}}{|Q_n|}\left(|A|^2+(q_n-1)\zeta_n^2|A|^2\left(1-\frac{|A|}{|Q_n|}\right)^2\right) \\ &= |A|+\zeta_{n-1}|A|\left(1-\frac{|A|}{|Q_n|}\right)-\frac{\zeta_{n-1}}{|Q_n|}\cdot(q_n-1)\zeta_n^2|A|^2\left(1-\frac{|A|}{|Q_n|}\right)^2 \\ &\geq |A|+\zeta_{n-1}\left(1-(q_n-1)\frac{\zeta_n^2}{4}\right)|A|\left(1-\frac{|A|}{|Q_n|}\right).\end{aligned}$$

Here (2.14) follows from the fact that

$$\frac{|A|}{|Q_n|}\left(1-\frac{|A|}{|Q_n|}\right)\le\frac{1}{4}.$$

Thus (2.4) follows if we have

$$\zeta_{n-1}\left(1-(q_n-1)\frac{\zeta_n^2}{4}\right)\ge\zeta_n. \tag{2.15}$$

We now choose $\zeta_n=\sqrt{2/\sum_{i=1}^n(q_i-1)}$. Then

$$\zeta_1=\sqrt{\frac{2}{q_1-1}}\le\frac{q_1}{q_1-1}$$

and (2.5) is satisfied. The condition (2.15) is also satisfied, since

$$\zeta_n^2=\zeta_{n-1}^2\left(1-(q_n-1)\frac{\zeta_n^2}{2}\right)\le\zeta_{n-1}^2\left(1-(q_n-1)\frac{\zeta_n^2}{4}\right)^2. \ \blacksquare$$

It is possible to iterate (2.2) to give a non-trivial bound for $B(A,r)$ for arbitrary r, and this is what Wirsing did in [8, Section 4.3].

3. Proof of Theorem 1.2. We identify $\mathbb{F}_p^n$ with $Q_n=\{0,1,\ldots,p-1\}^n$ via the map

$$(x_1,\ldots,x_n)\mapsto\sum_{i=1}^n x_ie_i.$$

Let $E=\{e_1,\ldots,e_n\}$. Then $B(A,1)=A\cup(A+E)\cup\cdots(A+(p-1)\cdot E))\subset A+(p-1)H$, where $k\cdot E:=\{ke_i:i=1,\ldots,n\}$. Theorem 2.1 implies that

$$|A+(p-1)H|\ge|A|+\sqrt{\frac{2}{(p-1)n}}\,|A|\left(1-\frac{|A|}{p^n}\right).$$

We will use Plünnecke's inequality [5] in the following form [6, Theorem 1.2.1]: if

$$\mu_k:=\inf\left\{\frac{|X+kH|}{|X|}:X\subset A,\ X\ne\emptyset\right\},$$

then the sequence $\{\mu_k^{1/k}\}_{k=1}^\infty$ is decreasing.

For any $X\subset A$, $X\ne\emptyset$, we have

$$\frac{|X+(p-1)H|}{|X|}\ge1+\sqrt{\frac{2}{(p-1)n}}\left(1-\frac{|X|}{p^n}\right)\ge1+\sqrt{\frac{2}{(p-1)n}}\left(1-\frac{|A|}{p^n}\right).$$

Therefore,

$$\mu_{p-1}^{1/(p-1)}\ge\left(1+\sqrt{\frac{2}{(p-1)n}}\left(1-\frac{|A|}{p^n}\right)\right)^{1/(p-1)}\ge1+\frac{c(p)}{\sqrt{n}}\left(1-\frac{|A|}{p^n}\right)$$

for some $c(p) = \Omega(p^{-3/2})$. Since

$$\frac{|A+H|}{|A|} \geq \mu_1 \geq \mu_{p-1}^{1/(p-1)},$$

Theorem 1.2 follows. If $p = 2$, then the use of Plünnecke's inequality is unecessary and we can take $c(2) = \sqrt{2}$.

4. Proof of Theorem 1.3. Let $A \subset \mathbb{F}_p^n$ be a subset of density $\alpha > 1/2 - c'(p)/\sqrt{n}$. By choosing $c'(p)$ sufficiently small we can certainly assume that $\alpha \geq 1/4$. Following Sanders, we will first show:

Claim 1. *$A - A \supset (x + U)^c$ for some $x \in \mathbb{F}_p^n$ and a subspace U of codimension 1 of $\mathbb{F}_p^n$.*

To put it in a different way, $S := (A - A)^c$ is contained in an affine subspace of codimension 1. Suppose for a contradiction that this is not true. Let s be any element of S. Then $S - s$ contains n linearly independent vectors, say $e_1, \ldots, e_n$. Put $H = \{0, e_1, \ldots, e_n\}$. Then $s + H \subset S$. By definition of S, we have $(S + A) \cap A = \emptyset$. Hence,

$$\frac{|H+A|}{p^n} = \frac{|s+H+A|}{p^n} \leq \frac{|S+A|}{p^n} \leq 1 - \alpha. \tag{4.1}$$

Sanders deduced a contradiction from this by repeated applications of Plünnecke's inequality and McDiarmid's inequality. Thanks to Theorem 1.2, we have a contradiction immediately. Indeed, since

$$\frac{|H+A|}{p^n} \geq \alpha + \frac{c(p)}{\sqrt{n}}\alpha(1-\alpha) \geq \alpha + \frac{3}{16}\frac{c(p)}{\sqrt{n}},$$

we have a contradiction if we choose $c'(p) \leq \frac{3}{32}c(p)$. Claim 1 follows.

For the rest of the proof we argue similarly to Sanders.

Claim 2. *If $V \neq \{0\}$ is any subspace of $\mathbb{F}_p^n$, then $A - A \supset V \setminus (U + x)$ for some subspace U of codimension 1 of V and $x \in V$.*

We observe that, by averaging over $t \in \mathbb{F}_p^n$, there is a translate $t + A$ such that the density of $(t + A) \cap V$ in V is at least α. Since $A - A \supset (t + A) \cap V - (t + A) \cap V$, Claim 2 follows from Claim 1.

Claim 3. *$A - A \supset (x + U)^c$ for some subspace $U \lneq \mathbb{F}_p^n$ and $x \notin U$.*

To see that this implies Theorem 1.3, let W be any subspace of codimension 1 of $\mathbb{F}_p^n$ such that $U \subset W$ and $x \notin W$ (the existence of W may be seen from taking a basis of $\mathbb{F}_p^n$ containing x and a basis of U). Then $A - A \supset (x + U)^c \supset (x + W)^c \supset W$.

We now prove Claim 3. Let U be the smallest subspace of $\mathbb{F}_p^n$ such that $A - A \supset (x + U)^c$ for some x. Such a U exists by Claim 1. We now show that $x \notin U$. Suppose for a contradiction that $x \in U$, i.e. $U^c \subset A - A$. Since

$\{0\} \subset A - A$, we have $\dim U \geq 1$. By Claim 2, there are a subspace U' of codimension 1 of U and $y \in U$ such that $A - A \supset U \setminus (U' + y)$. Therefore,

$$A - A \supset U^c \cup (U \setminus (U' + y)) = (U' + y)^c$$

contradicting the minimality of U.

5. Further discussions. It is instructive to compare Theorem 2.1 with other estimates for $B(A, 1)$. The case $Q_n = \{0, 1\}^n$ (i.e., the hypercube) has been extensively studied in the context of vertex isoperimetric inequalities for graphs. Harper's theorem [3] says that among all sets $A \subset \{0, 1\}^n$ of size k, $|B(A, 1)|$ is minimized when A is the first k elements in the simplicial ordering. For $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n) \in \{0, 1, \ldots\}^n$, we set $\mathbf{x} < \mathbf{y}$ in the simplicial ordering if either $\sum_{i=1}^n x_i < \sum_{i=1}^n y_i$, or $\sum_{i=1}^n x_i = \sum_{i=1}^n y_i$ and for some j we have $x_j > y_j$ and $x_i = y_i$ for all $i < j$. In particular, if $|A| = \sum_{i=0}^r \binom{n}{i}$, then $|B(A, 1)|$ is minimized when A is a Hamming ball with radius r. Our bound (2.2) is weaker than Harper's when the density of A is small, but is comparable when the density of A is bounded away from 0 and 1 (see (5.4) below).

Bollobás and Leader [1, Theorem 8] generalized Harper's theorem to $Q_n = \prod_{k=1}^n I_k$, though their notion of Hamming distance is quite different from ours. Just as Harper's theorem, their result is optimal, but it does not seem straightforward to extract from their result an explicit bound like (2.2).

McDiarmid's inequality [4, Corollary 7.6] states that if $A \subset Q_n = \prod_{k=1}^n I_k$, then

$$\frac{|B(A, r)|}{|Q_n|} \geq 1 - \frac{|Q_n|}{|A|} \exp\left(-\frac{r^2}{2n}\right). \tag{5.1}$$

The bound (5.1) is useful when r is large (for an application, see [9]), but sometimes it is worse than trivial (e.g. when the density of A in Q_n is close to 0 or 1). On the other hand, the bound given by (2.2) is always non-trivial.

Plünnecke's inequality implies that for any sets A, B in a commutative group, we have

$$|kB| \leq \left(\frac{|A + B|}{|A|}\right)^k |A|.$$

This gives the following bound.

Proposition 5.1. *If $A \subset Q_n = \prod_{k=1}^n I_k$, then*

$$|B(A, 1)| \geq |A| + \frac{1}{n}|A|\left(1 - \frac{|A|}{|Q_n|}\right). \tag{5.2}$$

Proof. We identify each I_k with a commutative group G_k on q_k elements and Q_n with the group $\bigoplus_{k=1}^n G_k$. Then $B(A, 1) = A + B$, where

$$B = \bigcup_{k=1}^{n} \{\mathbf{x} = (0, \ldots, 0, x_k, 0, \ldots, 0) \in Q_n : x_k \in G_k\}.$$

Clearly $nB = Q_n$, hence

$$|Q_n| \leq \left(\frac{|B(A,1)|}{|A|}\right)^n |A|,$$

which implies

$$|B(A,1)| \geq |A| \left(\frac{|A|}{|Q_n|}\right)^{-1/n} \geq |A| + \frac{1}{n}|A|\left(1 - \frac{|A|}{|Q_n|}\right)$$

as desired. ■

In the special case where $q_1 = \cdots = q_n = q$, Theorem 2.1 becomes

Corollary 5.2. *Let $q \geq 2$ and $Q_n = \{0, 1, \ldots, q-1\}^n$. Then for any $A \subset Q_n$, we have*

$$|B(A,1)| \geq |A| + \sqrt{\frac{2}{(q-1)n}}\,|A|\left(1 - \frac{|A|}{|Q_n|}\right). \tag{5.3}$$

The factor $\sqrt{n}$ in (5.3) is best possible in terms of order of magnitude. To see this, we take $q = 2$ and

$$A = \left\{(x_1, \ldots, x_n) \in \{0,1\}^n : \sum_{i=1}^{n} x_i \leq \frac{n}{2}\right\}.$$

Then

$$B(A,1) = \left\{(x_1, \ldots, x_n) \in \{0,1\}^n : \sum_{i=1}^{n} x_i \leq \frac{n}{2} + 1\right\}$$

and

$$\frac{1}{2} \leq \frac{|A|}{|Q_n|} \leq \frac{|B(A,1)|}{|Q_n|} \leq \frac{1}{2} + O\left(\frac{1}{\sqrt{n}}\right), \tag{5.4}$$

where the last inequality follows from the central limit theorem (or from the fact that the largest binomial coefficient $\binom{n}{r}$ is $O(2^n/\sqrt{n})$).

On the other hand, there are many reasons to believe that the factor $\sqrt{q-1}$ in (5.3) should not be there. Indeed, in the spirit of the previous example, we take

$$A = \left\{(x_1, \ldots, x_n) \in \{0, 1, \ldots, q-1\}^n : \sum_{i=1}^{n} x_i \leq \frac{(q-1)n}{2}\right\}.$$

Then it is easy to see that

$$B(A,1) \supset \left\{(x_1, \ldots, x_n) \in \{0, 1, \ldots, q-1\}^n : \sum_{i=1}^{n} x_i \leq \frac{(q-1)(n+1)}{2}\right\}.$$

For this particular A, the central limit theorem implies

$$|B(A,1)| \geq |A| + \frac{1}{O(\sqrt{n})}|A|\left(1 - \frac{|A|}{|Q_n|}\right),$$

where $O(\sqrt{n})$ is independent of q. Furthermore, neither of the bounds (5.1) and (5.2) depends on the q_i's. Thus it is natural to ask:

QUESTION 5.3. *Is there a function $f : [0,1] \to \mathbb{R}$ such that $f > 0$ on $(0,1)$ and*

$$\frac{|B(A,1)|}{|Q_n|} \geq \alpha + \frac{1}{\sqrt{n}} f(\alpha)$$

for all $Q_n = \prod_{k=1}^{n} I_k$ and $A \subset Q_n$ of density α?

If the answer to Question 5.3 is affirmative, then the constant $c(p)$ in Theorem 1.2 can be taken to be $\Omega(p^{-1})$ and it is easy to see that this is best possible.

Acknowledgements. We would like to thank the referee for a careful reading of our paper and for numerous suggestions which improved the presentation of the paper, and Terence Tao for helpful discussions. We are grateful to both the referee and Tao for pointing out the connection with the vertex isoperimetric problem and for providing relevant references.

The second author was supported by National Science Foundation Grant DMS-1702296 and a Ralph E. Powe Junior Faculty Enhancement Award from Oak Ridge Associated Universities.

References

[1] B. Bollobás and I. Leader, *Compressions and isoperimetric inequalities*, J. Combin. Theory Ser. A 56 (1991), 47–62.

[2] D. Christofides, D. Ellis and P. Keevash, *An approximate isoperimetric inequality for r-sets*, Electron. J. Combin. 20 (2013), no. 4, art. 15, 12 pp.

[3] L. H. Harper, *Optimal numberings and isoperimetric problems on graphs*, J. Combin. Theory 1 (1966), 385–393.

[4] C. McDiarmid, *On the method of bounded differences*, in: Surveys in Combinatorics, 1989, (Norwich, 1989), London Math. Soc. Lecture Note Ser. 141, Cambridge Univ. Press, Cambridge, 1989, 148–188.

[5] H. Plünnecke, *Eigenschaften und Abschätzungen von Wirkungsfunktionen*, BMwF-GMD-22, Gesellschaft für Mathematik und Datenverarbeitung, Bonn, 1969.

[6] I. Z. Ruzsa, *Sumsets and structure*, in: Combinatorial Number Theory and Additive Group Theory, Adv. Courses Math. CRM Barcelona, Birkhäuser, Basel, 2009, 87–210.

[7] T. Sanders, *Green's sumset problem at density one half*, Acta Arith. 146 (2011), 91–101.

[8] E. Wirsing, *Thin essential components*, in: Topics in Number Theory (Debrecen, 1974), Colloq. Math. Soc. János Bolyai 13, North-Holland, Amsterdam, 1976, 429–442.

[9] J. Wolf, *The structure of popular difference sets*, Israel J. Math. 179 (2010), 253–278.

Zhenchao Ge, Thái Hoàng Lê
Department of Mathematics
The University of Mississippi
University, MS 38677, U.S.A.
E-mail: zge@go.olemiss.edu
leth@olemiss.edu