ON SUBSETS OF $\mathbb{F}_q^n$ CONTAINING NO k-TERM PROGRESSIONS

Y. LIN AND J. WOLF

ABSTRACT. In this short note we prove that for any fixed integer k and any prime power $q \geq k$, there exists a subset of $\mathbb{F}_q^{2k}$ of size $q^{2(k-1)}+q^{k-1}-1$ which contains no k points on a line, and hence no k-term arithmetic progressions. As a corollary we obtain an asymptotic lower bound as $n \to \infty$ for $r_k(\mathbb{F}_q^n)$ when $q \geq k$, which can be interpreted as the finite field analogue of Behrend's construction for longer progressions.

1. INTRODUCTION

A central result in arithmetic combinatorics is Szemerédi's theorem, which states that for every positive integer k, every sufficiently dense subset of $\{1, 2, \ldots, N\}$ contains a k-term arithmetic progression. Denoting by $r_k(N)$ the maximum size of a subset of $\{1, 2, \ldots, N\}$ that contains no k-term arithmetic progression, Szemerédi [1] showed that $r_k(N) = o(N)$. The special case $k = 3$ is Roth's theorem [2], with a current best bound of $r_3(N) = O(N(\log N)^{-2/3+\epsilon})$ due to Bourgain [3]. When $k > 4$, the best known bounds are due to Gowers [4] and of the form $O(N(\log\log N)^{-c})$, where the constant c goes to zero in a way that is doubly exponential in k.

On the other hand, the best known example of a large subset of $\{1, 2, \ldots, N\}$ that contains no 3-term arithmetic progression was constructed by Behrend [5] in 1946. His example shows that $r_3(N) = \Omega(N \exp(-c(\log N)^{1/2}))$ for some constant c, and has not been meaningfully improved in over 60 years, but see [6, 7]. Behrend's construction was extended to cover the case of longer progressions by Rankin [8]. His argument was recently rediscovered by Łaba and Lacey [9] and yields bounds of the form $r_{2^k+1}(N) = \Omega(N \exp(-c(\log N)^{1/k+1}))$ (see also [10]).

As well as in the integers, Szemerédi-type problems have been extensively studied in the so-called "finite field" setting, and an excellent survey can be found in [11]. Let $\mathbb{F}_q^n$ be the n-dimensional vector space over a fixed finite field with q elements. In this context, it is natural to define $r_k(\mathbb{F}_q^n)$ to be the maximum size of a subset of $\mathbb{F}_q^n$ that contains no k-term arithmetic progressions. It turns out that it is often advantageous to first tackle a Szemerédi-type problem in the finite field setting, where one has plenty of exact algebraic

substructure available. Many times this simplifies the technical aspects of a problem, and more often than not the main ideas of a proof transfer naturally to the integer case.

Roth's original argument [2] was elegantly adapted to the $\mathbb{F}_3^n$ setting by Meshulam [12] to give an upper bound of the form $r_3(\mathbb{F}_3^n) = O(N(\log N)^{-1})$, where we have used $N = 3^n$ to denote the size of the ambient group $\mathbb{F}_3^n$. For longer progressions, Green and Tao [13] have shown that $r_4(\mathbb{F}_5^n) = O(N(\log N)^{-c})$, where $N = 5^n$.

As far as the lower bound is concerned, Edel [14] showed that $r_3(\mathbb{F}_3^n) = \Omega(N^{0.7249})$. It is an important and wide open problem to determine whether or not $r_3(\mathbb{F}_3^n) = (3 - o(1))^n$.

In this paper we complete the picture by constructing large subsets of $\mathbb{F}_q^n$ that contain no k-term arithmetic progressions for $q \geq k > 3$. More specifically, we prove the following theorem.

Theorem 1. *Let k be a positive integer. Let $\mathbb{F}_q$ be the finite field of q elements such that $q \geq k$. Then there is a subset of $\mathbb{F}_q^{2k}$ of size $q^{2(k-1)} + q^{k-1} - 1$ that contains no k points on a line, and hence no k-term arithmetic progression.*

Note that if A and B are subsets of $\mathbb{F}_q^m$ and $\mathbb{F}_q^n$, respectively, that contain no k-term arithmetic progression, then their Cartesian product $A \times B := \{(a, b) : a \in A, b \in B\}$ is a subset of $\mathbb{F}_q^{m+n}$ that contains no k-term arithmetic progression. Thus, by taking the product of the set constructed in Theorem 1 with itself many times, we obtain the following corollary.

Corollary 2. *Let k be a positive integer. Let $\mathbb{F}_q$ be the finite field of q elements such that $q \geq k$. For any n divisible by $2k$, we have*

$$r_k(\mathbb{F}_q^n) = \Omega((q^{2(k-1)} + q^{k-1} - 1)^{n/2k}).$$

For fixed q and k, this result improves upon the more trivial lower bound of $\Omega(N^{1-1/k})$, where $N = q^n$ (see Corollary 4). It is in some sense analogous to the aforementioned extension of Behrend's construction to k-term arithmetic progressions in [8, 9, 10]. As far as we are aware, Corollary 2 is the first general result in this direction.

2. Subsets of $\mathbb{F}_q^n$ containing no 3-term arithmetic progressions

As was already mentioned in the introduction, the best known bounds when $q = k = 3$ are due to Edel [14]. In this very short section we summarize what is known for general finite fields $\mathbb{F}_q$ and 3-term arithmetic progressions.

Bierbrauer [15] showed that for any finite field $\mathbb{F}_q$ with at least 3 elements, there exists a subset of $\mathbb{F}_q^3$ with q^2 elements that does not contain 3 points on a line. By taking a

Cartesian product of this set with itself sufficiently many times, it is clear that for any prime power $q \geq 3$ and any n divisible by 3, we have

$$r_3(\mathbb{F}_q^n) = \Omega((q^2)^{n/3}). \tag{1}$$

It turns out that by an ingenious product construction this lower bound can be improved. Indeed, it is shown in [15] that there exists a subset of $\mathbb{F}_q^6$ of size $q^4 + q^2 - 1$ that does not contain 3 points on a line, and hence that for any prime power $q \geq 3$ and any n divisible by 6, we have

$$r_3(\mathbb{F}_q^n) = \Omega((q^4 + q^2 - 1)^{n/6}). \tag{2}$$

We have stated the results in this section without proof, and shall now turn to generalizing them to longer progressions.

3. Subsets of $\mathbb{F}_q^n$ containing no k-term arithmetic progressions

From now on we pursue the general problem of determining the maximum size of a subset of $\mathbb{F}_q^n$ not containing any k-term arithmetic progressions for $k \geq 3$. By a brute force argument, it is not hard to show that we have

$$r_4(\mathbb{F}_5^2) = 11,$$

which implies that $r_4(\mathbb{F}_5^n) = \Omega(N^{\log 11/(2\log 5)}) = \Omega(N^{0.7449})$. For longer progressions, examples even in small dimension are hard to come by. As a special case ($k = 4$) of Proposition 3 below we first prove that there exists a subset of $\mathbb{F}_5^4$ of size 125 which does not contain any 4-term arithmetic progressions. In other words $r_4(\mathbb{F}_5^n) = \Omega(N^{\log 125/(4\log 5)}) = \Omega(N^{0.75})$.

Proposition 3. *Let k be positive integer. Let $\mathbb{F}_q$ be the finite field of q elements such that $q \geq k$. Then there is a subset of $\mathbb{F}_q^k$ of size q^{k-1} containing no k points on a line, hence no k-term arithmetic progressions.*

This theorem immediately implies the following corollary by taking Cartesian products as usual.

Corollary 4. *Let k be a positive integer and $\mathbb{F}_q$ be the finite field with q elements. Whenever $q \geq k$ and n is divisible by k, we have*

$$r_k(\mathbb{F}_q^n) = \Omega((q^{k-1})^{n/k}) = \Omega(N^{1-1/k}).$$

Proof of Proposition 3. The proof is essentially a generalization of the argument in [15] used to prove (1) above. Let $g \in \mathbb{F}_q[x_2, x_3, \ldots, x_k]$ be a homogeneous polynomial of degree

$k-1$ such that the only solution to $g(x_2, x_3, \ldots, x_k) = 0$ is $(0, 0, \ldots, 0)$. The reader in doubt about the existence of such a polynomial may refer to page 6 of [16], for example. Consider $f(x_1, x_2, \ldots, x_k) = x_1 + g(x_2, x_3, \ldots, x_k)$ and let $S = \{(x_1, x_2, \ldots, x_k) : f(x_1, x_2, \ldots, x_k) = 0\}$. Then $|S| = q^{k-1}$ because x_1 is uniquely determined by $x_2, x_3, \ldots, x_k$ via the relation $x_1 = -g(x_2, x_3, \ldots, x_k)$.

Suppose that S does contain k points on a line, then there exist vectors $(u_1, u_2, \ldots, u_k)$, $(v_1, v_2, \ldots, v_k) \neq (0, 0, \ldots, 0)$ such that $(u_1, u_2, \ldots, u_k) + \lambda(v_1, v_2, \ldots, v_k) \in S$ for k different values of $\lambda \in \mathbb{F}_q$. Since $f(u_1 + \lambda v_1, u_2 + \lambda v_2, \ldots, u_k + \lambda v_k)$ is a polynomial in λ of degree at most $k-1$, it follows that this polynomial is identically zero. By considering the coefficient of λ^k it follows that $g(v_2, \ldots, v_k) = 0$ and by choice of g we get $(v_2, \ldots, v_k) = (0, 0, \ldots, 0)$. Now the coefficient of λ^1 is v_1, hence $v_1 = 0$, a contradiction.

□

It turns out that we can do even better, and that Bierbrauer's product construction [15] which leads to (2) for 3-term arithmetic progressions can also be adapted to longer progressions. The remainder of this section is devoted to proving the following result.

Theorem 5. *Let $k \geq 4$ be a positive integer. Let $\mathbb{F}_q^k$ be a finite field with q elements such that $q \geq k$. Then there exists a subset of $\mathbb{F}_q^{2k}$ of size $q^{2(k-1)} + q^{k-1} - 1$ that contains no k points on a line.*

The main construction is described in Proposition 7 below. We say that k points $p_1, p_2, \ldots, p_k$ in $\mathbb{F}_q^n$ are *projectively collinear* if there exist non-zero vectors u and $v \in \mathbb{F}_q^n$ and scalars α_i and $\beta_i \in \mathbb{F}_q$, not both zero, such that $p_i = \alpha_i u + \beta_i v$ for all $1 \leq i \leq k$. The following statement is easy to check.

Lemma 6. *Let $p_1, p_2, \ldots, p_k$ be elements of $\mathbb{F}_q^n$. Then $p_1, p_2, \ldots, p_k$ are collinear if and only if the points $(1, p_1), (1, p_2), \ldots, (1, p_k) \in \mathbb{F}_q^{n+1}$ projectively collinear.*

Proposition 7. *Let S be as in the proof of Proposition 3. Let $e_1 = (1, 0, 0, \ldots, 0) \in \mathbb{F}_q^k$. Let $T = T_1 \cup T_2 \cup T_3$, where $T_1 = \{(x, y, 1) : x \in S, y \in S\}$, $T_2 = \{(x, e_1, 0) : x \in S\}$ and $T_3 = \{(e_1, y, 0) : y \in S\}$ are subsets of $\mathbb{F}_q^{2k+1}$. Then no k points of $T \subseteq \mathbb{F}_q^{2k+1}$ are projectively collinear.*

Proof. Suppose to the contrary that there exist k points $p_1, p_2, \ldots, p_k \in T$ that are projectively collinear. This means that there exist non-zero vectors $u, v \in \mathbb{F}_q^{2k+1}$ and $(\alpha_i, \beta_i) \in \mathbb{F}_q^2$ with $(\alpha_i, \beta_i) \neq (0, 0)$ such that $p_i = \alpha_i u + \beta_i v$ for all $1 \leq i \leq k$. Write $u = (u_1, u_2, \ldots, u_{2k+1})$ and $v = (v_1, v_2, \ldots, v_{2k+1})$. We distinguish two main cases.

Case 1. u_{2k+1} and v_{2k+1} are not both zero. Without loss of generality, we can suppose that $u_{2k+1} = 0$, $v_{2k+1} \neq 0$ (otherwise, subtract $\frac{u_{2k+1}}{v_{2k+1}} v$ from u).

We first establish that there exists at most one index i such that $p_i \in T_2$. Suppose that $p_i \in T_2$ and consider the last co-ordinate. Since $u_{2k+1} = 0, v_{2k+1} \neq 0$, it follows that $\beta_i = 0$. Moreover, $(u_{k+1}, u_{k+2}, \ldots, u_{2k}) = ae_1$ for some non-zero $a \in \mathbb{F}_q$ and $a\alpha_i = 1$. Hence $\alpha_i = 1/a$ and $p_i = \frac{1}{a}u = \frac{1}{u_{k+1}}u$ is uniquely determined, so there exists at most one index i such that $p_i \in T_2$.

For a similar reason, there exists at most one index j such that $p_j \in T_3$.

Case 1.A. Not all of the points p_i belong to T_1. Without loss of generality, suppose $p_k \in T_2$. By the above discussion, $(u_{k+1}, \ldots, u_{2k}) = ae_1$ for some non-zero $a \in \mathbb{F}_q$. By considering the last co-ordinate of any $p_i \in T_1$ we get $\beta_i = \frac{1}{v_{2k+1}}$. Write $p_i = (p_{i1}, p_{i2}, \ldots, p_{i,2k+1})$. Hence $(p_{i,k+1}, p_{i,k+2}, \ldots, p_{i,2k}) = \frac{1}{v_{2k+1}}(v_{k+1}, v_{k+2}, \ldots, v_{2k}) + \alpha_i a e_1$. Since $f(p_{i,k+1}, p_{i,k+2}, \ldots, p_{i,2k}) = 0$ and $(p_{i,k+2}, p_{i,k+3}, \ldots, p_{i,2k}) = (\frac{v_{k+2}}{v_{2k+1}}, \frac{v_{k+3}}{v_{2k+1}}, \ldots, \frac{v_{2k}}{v_{2k+1}})$ only depends on v, it follows that $p_{i,k+1} = -g(p_{i,k+2}, p_{i,k+3}, \ldots, p_{i,2k})$ only depends on v. Since $p_{i,k+1} = \frac{v_{k+1}}{v_{2k+1}} + a\alpha_i = \frac{v_{k+1}}{v_{2k+1}} + u_{k+1}\alpha_i$, it follows that α_i only depends on u, v. So we concluded that if not all of the p_is belong to T_1, then at most one of them belong to T_1.

Since there are also at most one i such that $p_i \in T_2$ or T_3, it follows that there are at most three i such that $p_i \in T_1 \cup T_2 \cup T_3$. But $p_1, p_2, \ldots, p_k \in T_1 \cup T_2 \cup T_3$ and $k \geq 4$, a contradiction.

Case 1.B. All the points p_i are in T_1. Since any point in T_1 has last co-ordinate 1, if k of them are projectively collinear then k elements in $S \times S \subset \mathbb{F}_q^{2k}$ are collinear by Lemma 6. This is impossible because $S \subset \mathbb{F}_q^k$ does not have k points on a line.

Case 2. $(u_{2k+1}, v_{2k+1}) = (0, 0)$. In this case, all the p_is lie in $T_2 \cup T_3$.

Case 2.A. There exist no indices $i \neq j$ such that $p_i \in T_2$ and $p_j \in T_3$. By symmetry of the argument, we may assume that all the points p_i lie in T_2. Since any point in T_2 has $(k+1)^{th}$ co-ordinate equal to 1, if k of them are projectively collinear then k elements in $S \subset \mathbb{F}_q^k$ are collinear by Lemma 6, which is impossible.

Case 2.B. There exist points $p_i \in T_2$ and $p_j \in T_3$. We shall show that no other point p_l, $l \neq j$, belongs to T_3. Since any $p_j \in T_3$ has first co-ordinate 1, it follows that at least one of u_1 and v_1 is non-zero. Without loss of generality, we can suppose that $u_1 = 0$, $v_1 \neq 0$ (otherwise, subtract $\frac{u_1}{v_1} v$ from u).

Let us first suppose that $(u_1, u_2, \ldots, u_k) \neq (0, 0, \ldots, 0)$ so that for some $2 \leq l \leq k$, $u_l \neq 0$. For any index j such that $p_j \in T_3$, consider the first co-ordinate. Since $u_1 = 0, v_1 \neq 0$, it follows that $\beta_j = 1/v_1$. Considering the l^{th} co-ordinate, which is zero for all elements in

T_3, we get that $\alpha_j u_l + \beta_j v_l = 0$. Together with $\beta_j = 1/v_1$, we have that $\alpha_j = -v_l/v_1 u_l$. Hence both α_j and β_j are uniquely determined by u and v.

In the case when $(u_1, u_2, \ldots, u_k) = (0, 0, \ldots, 0)$, we need a slightly more elaborate argument. Considering the first k co-ordinates of any $p_j \in T_3$, we see that there exists $a \in \mathbb{F}, a \neq 0$ such that $(v_1, v_2, \ldots, v_k) = ae_1$, and $\beta_j = 1/a$. Since both u and v have the l^{th} co-ordinates equal to zero for all $2 \leq l \leq k$, so does any $p_i \in T_2$. Combining this with the fact that the first k co-ordinates of any element of T_2 must be a zero of f, it follows that the first k co-ordinates of p_i are all zero and hence $\beta_i = 0$ for any $p_i \in T_2$. Now by considering the $(k+1)^{th}$ to $(2k)^{th}$ co-ordinate of p_i, one sees that $(u_{k+1}, u_{k+2}, \ldots, u_{2k}) = be_1$ for some $b \in \mathbb{F}_q, b \neq 0$. Next we observe that the $(k+1)^{th}$ to $(2k)^{th}$ co-ordinate of p_j are $(b\alpha_j + v_{k+1}/a, v_{k+2}/a, v_{k+3}/a, \ldots, v_{2k}/a)$. Since this point is a zero of f, we see that $b\alpha_j + v_{k+1}/a = -g(v_{k+2}/a, v_{k+3}/a, \ldots, v_{2k}/a)$, hence $\alpha_j = (-g(v_{k+2}/a, v_{k+3}/a, \ldots, v_{2k}/a) - v_{k+1}/a)/b$. Thus, both α_j, β_j are uniquely determined by u and v.

In either case, we see that for any $p_j \in T_3$, α_j and β_j are uniquely determined by u and v. It follows that there exists at most one index j such that $p_j \in T_3$.

A similar argument shows that there exists at most one index i such that $p_i \in T_2$. Hence there are at most two p_is that belong to $T_2 \cup T_3$. But $p_1, p_2, \ldots, p_k \in T_2 \cup T_3$ and $k \geq 4$, a final contradiction which completes the proof. □

Proof of Theorem 5. Let T be as in Proposition 7. It is clear that $|T| = q^{2k-2} + 2q^{k-1}$. We consider points in T with first co-ordinate equal to 0. Suppose $x = (x_1, x_2, 1) \in T_1$ has first co-ordinate equal to 0, then x_1 is an element in S with first co-ordinate equal to 0. Because the only solution to $g(x_2, x_3, \ldots, x_k) = 0$ is $(0, 0, \ldots, 0)$, we find that $x_1 = (0, 0, \ldots, 0)$. Since x_2 can be any element of S, we see that there are q^{k-1} points in T_1 with first co-ordinate equal to 0. By a similar argument we see that there is exactly one point in T_2 with first co-ordinate equal to 0. There are no such points in T_3 since any vector in T_3 has first co-ordinate equal to 1. Hence there are $(q^{2k-2} + 2q^{k-1}) - (q^{k-1} + 1) = q^{2k-2} + q^{k-1} - 1$ points in T with non-zero first co-ordinate. Define

$$T^* = \{(a_1, a_2, \ldots, a_{2k+1})/a_1 : (a_1, a_2, \ldots, a_{2k+1}) \in T, a_1 \neq 0\}.$$

Then the size of T^* is $q^{2k-2} + q^{k-1} - 1$. Because no k distinct points of $T \subset \mathbb{F}_q^{2k+1}$ are projectively collinear, the same holds for $T^* \subset \mathbb{F}_q^{2k+1}$. Since all elements of T^* have first co-ordinate equal to 1, the set $H = \{h \in \mathbb{F}_q^{2k} : (1, h) \in T^*\}$ is a subset of $\mathbb{F}_q^{2k}$ of size $q^{2k-2} + q^{k-1} - 1$. Furthermore, H contains no k collinear points by Lemma 6 above. □

As an immediate corollary we have the following result.

Corollary 8. *Let k be a positive integer and $\mathbb{F}_q$ be the finite field with q elements. Whenever $q \geq k$ and n is divisible by $2k$, we have*

$$r_k(\mathbb{F}_q^n) = \Omega((q^{2(k-1)} + q^{k-1} - 1)^{n/2k}).$$

For fixed q and k, this beats the bound obtained in Corollary 4 asymptotically. In particular, we find that $r_4(\mathbb{F}_5^n) = \Omega(N^{\log 15749/(8 \log 5)}) = \Omega(N^{0.7506})$, a very slight improvement over the bound resulting from Corollary 4.

4. Concluding remarks and open questions

As far as the upper bounds for $r_k(\mathbb{F}_q^n)$ are concerned, the case $k = 4$ is very different from the case $k = 3$. In particular, it is not possible to adapt Meshulam's Fourier analytic argument [12] to give an upper bound for the 4-term progression case. So-called "higher-order Fourier analysis" is required to deal with the case of longer progressions, which originated in the work of Gowers [4]. It is worth noticing that such an increase in conceptual difficulty does not occur in our construction of the corresponding lower bound.

We have seen time and again that by taking Cartesian products of a progression-free subset $A \subseteq \mathbb{F}_q^m$ with itself, we obtain a subset of $\mathbb{F}_q^n$ that contains no k points in arithmetic progression. However, Theorem 5 above as well as the argument in [14] show that taking Cartesian products produces by no means the best construction. It therefore seems reasonable to ask if the product construction by Edel [14] can be adapted to longer progressions.

In Section 2 we saw that there exists a subset of $\mathbb{F}_q^3$ of size q^2 that contains no 3 points on a line. It can in fact be shown that q^2 is best possible, see [17, 18]. In Section 3 we showed that there exists a subset of $\mathbb{F}_q^k$ of size q^{k-1} that contains no k points on a line, as long as $q \geq k$. It would be interesting to know whether the set obtained in Proposition 3 was best possible in this sense.

We can also explore the problem in a more general setting by replacing the field $\mathbb{F}_q$ with a ring such as $\mathbb{Z}/4\mathbb{Z}$. An upper bound for $r_3((\mathbb{Z}/4\mathbb{Z})^n)$ was very recently obtained by Sanders [19], and is of interest since it beats the $O(N(\log N)^{-1})$ bound which in the case of a field is considered to be the limit of the Fourier analytic method. A computer search in [19] revealed that $r_3((\mathbb{Z}/4\mathbb{Z})^3) = 16$, which gives rise to a lower bound on $r_3((\mathbb{Z}/4\mathbb{Z})^n)$ in the usual way. Can Proposition 3 and Theorem 5 be adapted to $\mathbb{Z}/4\mathbb{Z}$?

It is worth noticing that the progression-free sets constructed in this paper (as well as those in [5], [8], [9], [14]) obey the stronger property that they contain no k points on a line. It

would be of great interest to make use of this additional piece of information in order to improve the bounds in Theorem 8.

Acknowledgements. Both authors gratefully acknowledge the generous support of the MIT Department of Mathematics during the summer of 2008, and the first author in addition that of the Lord Foundation.

References

[1] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 299–345.

[2] K.F. Roth, *On certain sets of integers,* J. London Math. Soc. **28** (1953), 104–109.

[3] J. Bourgain, *Roth's theorem on progressions revisited*, J. d'Analyse Math. **104** (2008), 155–192.

[4] W.T. Gowers, *A new proof of Szemeredi's Theorem for arithmetic progressions of length four*, GAFA **8** (1998), 529–551.

[5] F.A. Behrend, *On sets of integers which contain no three elements in arithmetic progression*, Proc. Nat. Acad. Sci **32** (1946), 331–332.

[6] M. Elkin *An improved construction of progression-free sets*, preprint, available at http://arxiv.org/pdf/0801.4310, 2008.

[7] B.J. Green and J. Wolf, *A note on Elkin's improvement of Behrend's construction*, to appear in *Additive Number Theory: Festschrift In Honor Of The Sixtieth Birthday Of Melvyn B. Nathanson*, Springer, currently available at http://arxiv.org/pdf/0810.0732, 2008.

[8] R.A. Rankin, *Sets of integers containing not more than a given number of terms in arithmetical progression*, Proc. Roy. Soc. Edinburgh Sect. A **65** (1962), 332–344.

[9] I. Łaba and M. Lacey, *On sets of integers not containing long arithmetic progressions*, preprint, available at http://arxiv.org/pdf/math/0108155, 2001.

[10] K. O'Bryant *Sets of integers that do not contain long arithmetic progressions*, preprint, available at http://arxiv.org/pdf/0811.3057, 2008.

[11] B.J. Green, *Finite field models in arithmetic combinatorics*, Surveys in Combinatorics, London Math. Soc. Lecture Notes 327 (2005), 1–27.

[12] R. Meshulam, *On subsets of finite abelian groups with no* 3*-term arithmetic progressions*, J. Combin. Theory Ser. A **71** (1995), 168–172.

[13] B.J. Green and T. Tao, *New bounds for Szemerédi's Theorem, I: progressions of length 4 in finite field geometries*, Proc. Lond. Math. Soc. (3) 98 (2009), no. 2, 365–392.

[14] Y. Edel, *Extensions of generalized product caps*, Des. Codes Cryptogr. **31** (2004), 5–14.

[15] J. Bierbrauer, *Large caps*, J. Geom. **76** (2003), 16–51.

[16] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, 1966, out of print.

[17] R.C. Bose, *Mathematical theory of the symmetrical factorial design*, Sankhȳa **8** (1947), 107–166.

[18] B. Qvist, *Some remarks concerning curves of the second degree in a finite plane*, Ann. Acad. Sci. Fenn. Ser. A **134** (1952).

[19] T. Sanders, *Roth's Theorem in* $(\mathbb{Z}/4\mathbb{Z})^n$, submitted, available at http://arxiv.org/pdf/0807.5101, 2008.

Stanford University, Department of Mathematics, Stanford, CA 94305, U.S.A
E-mail address: ylin2@math.stanford.edu

Rutgers, The State University of New Jersey, Department of Mathematics, Piscataway, NJ 08854, U.S.A.
E-mail address: julia.wolf@cantab.net