On the degree of regularity of a certain quadratic Diophantine equation

S.D. Adhikari [a], L. Boza [b], S. Eliahou [c,d], M.P. Revuelta [b], M.I. Sanz [b]

[a] Harish-Chandra Research Institute, HBNI, Chhatnag Road, Jhunsi, Allahabad-211 019, India
[b] Departamento de Matemática Aplicada I, Universidad de Sevilla, Avenida de la Reina Mercedes 4, C.P. 41012 Sevilla, Spain
[c] Univ. Littoral Côte d'Opale, EA 2597 - LMPA - Laboratoire de Mathématiques Pures et Appliquées Joseph Liouville, F-62228 Calais, France
[d] CNRS, FR 2956, France

ABSTRACT

We show that, for every positive integer r, there exists an integer $b = b(r)$ such that the 4-variable quadratic Diophantine equation $(x_1 - y_1)(x_2 - y_2) = b$ is r-regular. Our proof uses Szemerédi's theorem on arithmetic progressions.

1. Introduction

Denote $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. Given a polynomial $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, let $D(f)$ denote the corresponding Diophantine equation

$$f(x_1, x_2, \ldots, x_n) = 0.$$

This equation is said to be *r-regular*, for some integer $r \geq 1$, if for every r-coloring of $\mathbb{N}_+$, there is a monochromatic solution to it. It is said to be *regular* if it is r-regular for all $r \geq 1$. The *degree of regularity* of $D(f)$, denoted $\mathrm{dor}(D(f))$, is defined to be infinite if $D(f)$ is regular, or else, it is the largest r such that $D(f)$ is r-regular. Determining the degree of regularity of a given Diophantine equation is difficult in general, even if it is linear.

In this paper, we shall consider the 4-variable Diophantine quadratic equation

$$(x_1 - y_1)(x_2 - y_2) = b, \tag{1}$$

E-mail addresses: adhikari@hri.res.in (S.D. Adhikari), boza@us.es (L. Boza), eliahou@lmpa.univ-littoral.fr (S. Eliahou), pastora@us.es (M.P. Revuelta), isanz@us.es (M.I. Sanz).

denoted $Q(b)$, where b is a given positive integer. This equation is not regular. Indeed, it is not b-regular, and actually not even s-regular where $s = \lfloor\sqrt{b}\rfloor + 1$, as witnessed by the s-coloring given by the class mod s; for if x_1, y_1, x_2, y_2 are all congruent mod s, then $(x_1 - y_1)(x_2 - y_2)$ is divisible by s^2, and hence cannot equal b since $s^2 > b$. That is, we have $\text{dor}(Q(b)) \leq \lfloor\sqrt{b}\rfloor$. Our purpose in this paper is to show that, nevertheless, the numbers $\text{dor}(Q(b))$ are unbounded as b varies. Here is our main result.

Theorem 1.1. *Given a positive integer r, there is a positive integer $b = b(r)$ such that the equation $(x_1 - y_1)(x_2 - y_2) = b$ is r-regular.*

A more specific version is stated and proved in Section 3.

Our motivation to study this particular quadratic equation comes from previous work on the linear version

$$(x_1 - y_1) + (x_2 - y_2) = b,$$

and more generally on the $2k$-variable linear Diophantine equation

$$(x_1 - y_1) + \cdots + (x_k - y_k) = b, \tag{2}$$

the object of the following conjecture by Fox and Kleitman [6].

Conjecture 1.2. *Let $L_k(b)$ denote Eq. (2). Then*

$$\max_{b\in\mathbb{N}_+} dor(L_k(b)) = 2k - 1.$$

If true, that estimate would be best possible, since it is shown in [6] that $\text{dor}(L_k(b)) \leq 2k - 1$ for all $k, b \geq 1$. See [1,2] for solutions of the Fox–Kleitman conjecture for $k = 2$ and 3, respectively, and [12] for a very recent full proof.

Note that the solved case $k = 2$ of the conjecture and Theorem 1.1 imply a sharp contrast between the additive and the multiplicative versions of the equation, namely $\max_b \text{dor}(L_2(b)) = 3$ versus $\max_b \text{dor}(Q(b)) = \infty$.

1.1. Contents

Here is a brief description of the contents of the paper. In Section 2, we recall some classical problems on partition regularity. In Section 3, after recalling Szemerédi's theorem on arithmetic progressions, we prove our main result on the unboundedness of $\text{dor}(Q(b))$ as b varies. In Section 4, after setting up specific tools for the task at hand, we provide estimates for one of the numbers $M(k, \delta)$ involved in Szemerédi's theorem. In Section 5, we determine all $b \geq 1$ for which $Q(b)$ is 2-regular, as well as the smallest $b \geq 1$ for which $Q(b)$ is 3-regular. The last section is devoted to a few remarks and open questions.

2. Background

We first recall some background results and problems on partition regularity. The following abridged version of a theorem of Rado [9–11] characterizes the regular linear homogeneous equations on $\mathbb{Z}$.

Theorem 2.1 (*Radó's Theorem, Abridged Version*)**.** *For $n \geq 2$ and $c_1, \ldots, c_n \in \mathbb{Z} \setminus \{0\}$, the Diophantine equation*

$$c_1x_1 + \cdots + c_nx_n = 0 \tag{3}$$

is regular if and only $\sum_{i\in I} c_i = 0$ for some non-empty subset $I \subseteq \{1, \ldots, n\}$.

One of the main open problems in the linear case is Rado's *boundedness conjecture*. A simplified version of it states that if Eq. (3) is r-regular for some integer $r = r(n)$ only depending on n, then it is regular. See for instance [6], where the conjecture is settled for $n = 3$ with the value $r(3) = 24$. See also [3,4,7] for related papers.

Other open problems in the linear case concern the m-color Rado number of a given equation. Recall that for a Diophantine equation D, the m-color Rado number $R_m(D)$ of D is defined as the smallest positive integer N such that for every m-coloring of $[1, N]$, there is a monochromatic solution in $[1, N]$ to D. If no such N exists, then $R_m(D) = \infty$ by definition.

Still less is known in the nonlinear case. For instance, it is an open question whether the quadratic Diophantine equation

$$x^2 + y^2 = z^2 \tag{4}$$

is regular. According to a recent preprint using massive computer computations with a SAT solver, Eq. (4) turns out to be 2-regular [5]. More precisely, for every 2-coloring of the integer interval $[1, 7825]$, there is a monochromatic solution in that interval to Eq. (4), and 7825 is minimal in that respect. However, it is not known whether that equation is 3-regular, and it remains an open problem to determine its precise degree of regularity. Note that some other homogeneous quadratic equations in three variables have recently been shown to be regular [8].

3. Main result

In this section, we show that the numbers $\mathrm{dor}(Q(b))$ are unbounded as b varies.

3.1. Some tools

To start with, for the statement and proof of our main result, we need the deep theorem of Szemerédi about the existence of long arithmetic progressions in sufficiently dense subsets of sufficiently large integer intervals [13, p. 244, Corollary].

Theorem 3.1 (*Szemerédi*). *Given a desired length $k \in \mathbb{N}_+$ and a specified density $0 < \delta \leq 1$, there exists a positive integer $N = N(k, \delta)$ such that every subset $A \subseteq [1, N]$ of density $|A|/N \geq \delta$ contains an arithmetic progression of length k.*

For definiteness and in the sequel, we shall denote by $M(k, \delta)$ the *smallest* positive integer N with the above property.

We also need an elementary folklore lemma about the preservation of density under partitions of finite sets.

Lemma 3.2. *Let $A \subseteq E$ be nonempty finite sets. Denote $\delta = |A|/|E|$ the density of A in E. Let $E = E_1 \sqcup \cdots \sqcup E_r$ be a partition of E into r nonempty parts. Then there exists an index $i \leq r$ such that $|A \cap E_i|/|E_i| \geq \delta$.*

Proof. Assume for a contradiction that $|A \cap E_i|/|E_i| < \delta$ for all $i \leq r$. Then $|A \cap E_i| < \delta|E_i|$ for all $i \leq r$ and, summing over i, we get

$$\sum_i |A \cap E_i| < \delta \sum_i |E_i|.$$

Since $\sum_i |A \cap E_i| = |A|$ and $\sum_i |E_i| = |E|$, the above inequality leads to $|A| < \delta|E| = |A|$, a contradiction. □

3.2. Unboundedness of dor($Q(b)$)

Let $r \in \mathbb{N}_+$ be given. For the statement below, we invoke Szemerédi's theorem with the desired length $k = r! + 1$ and density $\delta = 1/r$. Let $N = M(r! + 1, 1/r)$. Then N has the property that *every* *subset $B \subseteq [1, N]$ of density $|B|/N \geq 1/r$ contains an arithmetic progression of length $r! + 1$.* Clearly, the same property holds for any integer interval $[a, a + N - 1]$ of length N.

Recall that $Q(b)$ denotes the Diophantine equation $(x_1 - y_1)(x_2 - y_2) = b$.

Theorem 3.3. *Let $r \in \mathbb{N}_+$, and let $N = M(r!+1, 1/r)$ be as defined above. Then the Diophantine equation $Q(N!r!)$ is r-regular.*

Proof. Let Δ be an arbitrary r-coloring of the integer interval $E = [1, (r + 1)N!]$. Then there exists a color class $S \subseteq E$ of density $|S|/|E| \geq 1/r$.

Let us partition E into subintervals of length N, as is possible since N divides $|E|$. By Lemma 3.2, there exists one such subinterval $A \subseteq E$ of size $|A| = N$ such that $|S \cap A|/|A| \geq 1/r$. By the defining property of N, the subset $S \cap A$ contains an arithmetic progression of length $r! + 1$, with common difference d for some $d \geq 1$. Thus, there exists $s \in S \cap A$ such that

$$\{s, s + d, \ldots, s + r!d\} \subseteq S \cap A. \quad (5)$$

Not much is known about d besides the inequality $r!d \leq N$. As customary in additive combinatorics, let us denote $S - S = \{s_1 - s_2 \mid s_1, s_2 \in S\}$.

Fact 1. *We have $[1, r!]d \subseteq S - S$.*

Indeed, for all $1 \leq j \leq r!$, we have $jd = (s + jd) - s$, and so $jd \in S - S$ by (5).

Set $m = N!/d$. Partition E into its classes mod m, and then partition each class mod m into subsets of cardinality $r+1$ of the form $C = \{a, a+m, \ldots, a+rm\} \subset E$. This is possible since m divides $|E|$ and $r+1$ divides $|E|/m$. By Lemma 3.2 again, for at least one such subset C, we must have $|S\cap C|/|C| \geq 1/r$. But since $|C| = r + 1$, this implies $|S \cap C| \geq 2$. Thus, there exist two distinct indices $0 \leq i < j \leq r$ such that $a + im, a + jm \in S \cap C$.

Fact 2. *We have $um \in S - S$ for some $u \in [1, r]$.*

Indeed, simply take $um = (a + jm) - (a + im)$ for the two elements in $S \cap C$ found above. Note that $1 \leq u = j - i \leq r$, as desired.

We now combine the above facts. Since $m = N!/d$, by Fact 2 we have

$$uN!/d \in S - S$$

for some $u \in [1, r]$. Now since u divides $r!$, we have $r!/u \in [1, r!]$, and hence $(r!/u)d \in [1, r!]d$. Therefore

$$(r!/u)d \in S - S$$

by Fact 1. Multiplying these two elements of $S - S$ together, it follows that

$$N!r! \in (S - S)(S - S).$$

That is, there exist $x_1, y_1, x_2, y_2 \in S$ such that $(x_1 - y_1)(x_1 - y_1) = N!r!$, thus yielding a monochromatic solution of equation $Q(N!r!)$. Therefore this equation is r-regular, as claimed. □

3.3. More properties of dor$(Q(b))$

The problem of determining $\mathrm{dor}(Q(b))$ as a function of $b \in \mathbb{N}_+$ is probably very difficult. In Section 5.1, we show that $\mathrm{dor}(Q(b)) \geq 2$ if and only if $b \in 4\mathbb{N}_+$, thereby improving the case $r = 2$ of Theorem 3.3. The case $r = 3$ of that result is improved in Section 5.2, where we show that $\mathrm{dor}(Q(36)) = 3$. We conclude this section with some general properties of $\mathrm{dor}(Q(b))$.

Proposition 3.4. *Let $b, m \in \mathbb{N}_+$. If $b \not\equiv 0 \bmod m^2$, then $\mathrm{dor}(Q(b)) \leq m - 1$.*

Proof. Consider the m-coloring of $\mathbb{N}_+$ given by the class mod m. That is, color classes correspond to congruence classes mod m. If m^2 does not divide b, then equation $(x_1 - y_1)(x_2 - y_2) = b$ has no monochromatic solution under this coloring, for if x_1, y_1, x_2, y_2 are of the same color, i.e., are congruent mod m, then m^2 divides $(x_1 - y_1)(x_2 - y_2)$. □

For instance, if b is not divisible by $36 = 6^2$, then equation $Q(b)$ is not 3-regular, as follows by successively taking $m = 2$ and $m = 3$ in the above result.

Proposition 3.5. *Let $b, t \in \mathbb{N}_+$. Then*

$$dor(Q(b)) \leq dor(Q(t^2 b)).$$

Proof. Set $r = \text{dor}(Q(b))$. Let $c : \mathbb{N}_+ \to [1, r]$ be an r-coloring. Define a new r-coloring $c' : \mathbb{N}_+ \to [1, r]$ by setting $c'(n) = c(tn)$ for all $n \geq 1$. Since $Q(b)$ is r-regular by hypothesis, there is a solution (x_1, y_1, x_2, y_2) of equation $Q(b)$ which is monochromatic under c'. Hence (tx_1, ty_1, tx_2, ty_2) is monochromatic under c. Moreover, since $(x_1 - y_1)(x_2 - y_2) = b$ by hypothesis, it follows that

$$(tx_1 - ty_1)(tx_2 - ty_2) = t^2 b.$$

Therefore (tx_1, ty_1, tx_2, ty_2) is a solution of equation $Q(t^2 b)$, and it is monochromatic under c as already seen. We conclude that $Q(t^2 b)$ is r-regular. □

4. On $M(3, 1/2)$

Theorem 3.3 involves the numbers $M(r!+1, 1/r)$ arising from Szemerédi's theorem. In this section, after setting up some useful tools, we determine this number for $r = 2$, namely $M(3, 1/2)$.

4.1. Detecting arithmetic progressions

Let $(G, +)$ be an abelian group. Here we set up some notation and terminology to help determine the presence or absence of arithmetic progressions of a given length in sequences in G. This will then be used in $G = \mathbb{Z}$ to show $M(3, 1/2) = 17$.

Let $A = (a_1, \dots, a_n)$ be a sequence in G of length $|A| = n$. A *block* in A is any subsequence of consecutive elements, i.e., of the form

$$A[i, j] = (a_i, a_{i+1}, \dots, a_j)$$

for some indices $1 \leq i, j \leq n$, allowing the empty subsequence if $j < i$. We denote by $\sigma(A) = \sum_i a_i$ the sum of the elements of A.

Definition 4.1. Let A be a finite sequence in G. A *block decomposition* of A is a sequence $(A_1, \dots, A_m)$ of consecutive blocks A_t of A, $1 \leq t \leq m$, whose concatenation is A. A *contraction* of A is a sequence in G of the form $(\sigma(A_1), \dots, \sigma(A_m))$ where $(A_1, \dots, A_m)$ is a block decomposition of A. A *minor* of A is a contraction of a block B of A or, equivalently, a block in a contraction of A.

For instance, if $A = (1, 5, 1, 8, 2, 3, 1)$ in $G = \mathbb{Z}$, then $((1, 5, 1), (8, 2), (3, 1))$ is a block decomposition of A and $(7, 10, 4)$ is the corresponding contraction of A. Some minors of A are $(6, 1, 8)$, $(7, 10)$, $(9, 5, 1)$, $(10, 3)$ and $(10, 4)$. Note that $(6, 1, 8)$ is a contraction of the block $(1, 5, 1, 8)$ in A, and a block in the contraction $(6, 1, 8, 6)$ of A.

Definition 4.2. Let $X = (x_0, x_1, \dots, x_n)$ be a sequence in G with $n \geq 1$. The *discrete derivative* of X is its sequence of successive jumps, i.e.,

$$\Delta(X) = (x_1 - x_0, \dots, x_n - x_{n-1}).$$

For instance, X is an arithmetic progression of length $n + 1$ in G if and only if $\Delta(X)$ is a constant sequence of length n.

Let us now observe that for a sequence X, block sums in $\Delta(X)$ correspond to differences of two terms in X.

Lemma 4.3. *Let $X = (x_0, x_1, \ldots, x_n)$ be a sequence in G. Let $A = \Delta(X) = (a_1, \ldots, a_n)$ where $a_i = x_i - x_{i-1}$ for $i \geq 1$. Let $B = A[i, j]$ for some $1 \leq i \leq j \leq n$. Then $\sigma(B) = x_j - x_{i-1}$.*

Proof. We have $\sigma(A[i, j]) = \sum_{i \leq t \leq j} (x_t - x_{t-1}) = x_j - x_{i-1}$. □

Here is a correspondence between subsequences of X and minors of $\Delta(X)$.

Lemma 4.4. *Let X be a finite sequence in G. If Y is a subsequence of X, then $\Delta(Y)$ is a minor of $\Delta(X)$. Conversely, if C is a minor of $\Delta(X)$, then $C = \Delta(Y)$ for some subsequence Y of X.*

Proof. Let $X = (x_0, x_1, \ldots, x_n)$ and $A = \Delta(X) = (a_1, \ldots, a_n)$ where $a_i = x_i - x_{i-1}$ for $i \geq 1$. Let $Y = (x_{i_0}, x_{i_1}, \ldots, x_{i_m})$ be a subsequence of X, with $0 \leq i_0 < i_1 < \cdots < i_m \leq n$. Then $\Delta(Y) = (x_{i_1} - x_{i_0}, \ldots, x_{i_m} - x_{i_{m-1}})$. Let $B_t = A[i_{t-1} + 1, i_t]$ for $1 \leq t \leq m$. By Lemma 4.3, we have

$$\Delta(Y) = (\sigma(B_1), \ldots, \sigma(B_m)).$$

Let $B = A[i_0 + 1, i_m]$. Then $(B_1, \ldots, B_m)$ is a block decomposition of B. Therefore $\Delta(Y)$ is a contraction of block B and hence a minor of A.

Conversely, let C be a minor of A. Hence there is a block B in A such that $C = (\sigma(B_1), \ldots, \sigma(B_m))$ for some block decomposition $(B_1, \ldots, B_m)$ of B. For each $1 \leq t \leq m$, we have $B_t = A[j_t, i_t]$ for some $1 \leq j_t \leq i_t \leq n$. Since the B_t's are consecutive blocks in B, and hence in A, we have $j_t = i_{t-1} + 1$ for $t \geq 2$. Thus, denoting $i_0 = j_1 - 1$, we have $B_t = A[i_{t-1} + 1, i_t]$ for all $1 \leq t \leq m$, and $\sigma(B_t) = x_{i_t} - x_{i_{t-1}}$ by Lemma 4.3. Therefore $C = \Delta(Y)$ where $Y = (x_{i_0}, x_{i_1}, \ldots, x_{i_m})$. □

This correspondence yields the following convenient tool to determine the presence or absence of arithmetic progressions of a given length in sequences in G.

Proposition 4.5. *Let X be a finite sequence in G. Then X contains an arithmetic progression of length $k \geq 3$ if and only if $\Delta(X)$ has a constant minor of length $k - 1$.*

Proof. If X contains an arithmetic sequence Y of length k, then $\Delta(Y)$ is a constant sequence of length $k-1$, and it is a minor of $\Delta(X)$ by the preceding lemma. Conversely, let C be a constant minor of length $k - 1$ of $\Delta(X)$. Then by the above lemma, there exists a subsequence Y of X such that $C = \Delta(Y)$, and Y is an arithmetic progression of length k since $\Delta(Y)$ is constant of length $k - 1$. □

For instance, let $X = (1, 2, 4, 5, 10, 11, 13, 14)$ in $G = \mathbb{Z}$. Let $A = \Delta(X)$. Then $A = (1, 2, 1, 5, 1, 2, 1)$ and A contains no constant minor of length 2 as easily checked by inspection. Therefore X contains no arithmetic progression of length 3.

4.2. Determining $M(3, 1/2)$

As an application in $G = \mathbb{Z}$, we obtain here the exact value of $M(r! + 1, 1/r)$ for $r = 2$. Even though the result is easy to obtain by computer, the present method will hopefully, in future works, yield exact values or good bounds in harder cases.

Proposition 4.6. *Every subset $X \subset [1, 17]$ of cardinality $|X| = 9$ contains an arithmetic progression of length 3.*

Proof. We first claim that the only sequences B in $\mathbb{N}_+$ such that $|B| = 4$, $\sigma(B) \leq 8$ and admitting no constant minor of length 2 satisfy $\sigma(B) = 8$. More precisely, the only such sequences are, up to reversal, $(1, 2, 4, 1)$ and $(2, 1, 4, 1)$. This is easy. Indeed, let (C_1, C_2) be a block decomposition of B with $|C_i| = 2$ for $i = 1, 2$. Since $\sigma(C_1) + \sigma(C_2) = \sigma(B) \leq 8$, and no C_i can be constant, then each C_i coïncides, up to reversal, with one of the sequences

$$(1, 2),\ (1, 3),\ (1, 4),\ (2, 3).$$

Moreover $\sigma(C_1) \neq \sigma(C_2)$, for otherwise $(\sigma(C_1), \sigma(C_2))$ would be a constant minor of length 2 of B. Up to reversal of B, we may assume $\sigma(C_1) < \sigma(C_2)$. Hence $C_1 = (1, 2)$ up to reversal, and $\sigma(C_2) = 4$ or 5. By considering all possible combinations, it is easily seen that $C_2 = (4, 1)$ is the only valid possibility. This proves the claim.

Assume, for a contradiction, that there exists $X \subset [1, 17]$ of cardinality $|X| = 9$ containing no arithmetic progression of length 3. Let $A = \Delta(X)$, when X is viewed as an increasing sequence. Then $|A| = 8$, $\sigma(A) = \max(X) - \min(X) \leq 16$ and A admits no constant minor of length 2. Let (B_1, B_2) be a block decomposition of A with $|B_1| = |B_2| = 4$. Then neither B_1 nor B_2 admits a constant minor of length 2. Moreover, since $\sigma(B_1) + \sigma(B_2) = \sigma(A) \leq 16$, we may assume $\sigma(B_1) \leq 8$ up to reversal of A. Hence $\sigma(B_1) = 8$ by the above claim. Therefore $\sigma(B_2) \leq 8$ as well, whence $\sigma(B_1) = 8$ by the above claim again. But then, $(\sigma(B_1), \sigma(B_2)) = (8, 8)$ is a constant minor of length 2 of A, a contradiction. □

Corollary 4.7. *We have* $M(3, 1/2) = 17$.

Proof. The proposition yields $M(3, 1/2) \leq 17$. In order to establish the equality, we must exhibit, for all $1 \leq m \leq 16$, a subset $X_m \subseteq [1, m]$ of density at least $1/2$ and containing no 3-term arithmetic progression. Let $X = \{1, 2, 4, 5, 10, 11, 13, 14\}$. Then the set X_m defined as follows will do:

$$X_m = \begin{cases} X \cap [1, m] & \text{if } m \neq 9 \\ \{1, 2, 4, 8, 9\} & \text{if } m = 9. \end{cases} \qquad \square$$

4.3. *Comparison with* $W(k, r)$

It would be desirable to determine $M(k, 1/r)$ for more instances of the pair (k, r), as nothing precise seems to be known about these numbers. We have started to make the first few steps towards that objective in a paper under preparation. Of course, these numbers are bounded below by the corresponding van der Waerden numbers. Given integers $k, r \geq 1$, recall that the van der Waerden number $W(k, r)$ denotes the least integer M such that, for every r-coloring of $[1, M]$, there is a monochromatic arithmetic progression of length k in $[1, M]$. Clearly, we have

$$M(k, 1/r) \geq W(k, r). \tag{6}$$

Indeed, let $N = M(k, 1/r)$, and consider any r-coloring of $[1, N]$. Then some color class $X \subseteq [1, N]$ is of density $|X|/N \geq 1/r$, and hence X contains an arithmetic progression of length k, of course monochromatic by construction.

The only exactly known van der Waerden numbers at the time of writing are given in the following table. See e.g. [14], a web page which also displays lower bounds on $W(k, r)$ for many more pairs (k, r).

$W(3, 2) = 9$	$W(3, 3) = 27$	$W(3, 4) = 76$
$W(4, 2) = 35$	$W(4, 3) = 293$	
$W(5, 2) = 178$		
$W(6, 2) = 1132$		

5. When *r* is small

In this section, we obtain sharper statements than Theorem 3.3 for $r = 2$ and 3. We also discuss some corresponding Rado numbers.

5.1. *The case* $r = 2$

For $r = 2$, and with the notation of Section 3, our main result states that with $N = M(3, 1/2)$, equation $(x_1 - y_1)(x_2 - y_2) = 2N!$ is 2-regular.

We have seen above that $M(3, 1/2) = 17$. Thus, Theorem 3.3 states that equation $Q(2 \cdot 17!)$ is 2-regular. However, we now show that the same already holds for equation $Q(4)$, and more generally for equation $Q(b)$ whenever $b \in 4\mathbb{N}_+$.

Proposition 5.1. *The equation* $(x_1 - y_1)(x_2 - y_2) = b$ *is 2-regular if and only if* b *is a multiple of* 4.

Proof. Proposition 3.4 implies that if $b \not\equiv 0 \bmod 4$, then $Q(b)$ is not 2-regular.

Assume now $b \equiv 0 \bmod 4$. First some notation. Let $X \subseteq \mathbb{N}_+$ be any nonempty subset. We denote $D(X) = (X - X) \cap \mathbb{N}$, the set of distances in X, and

$$D_2(X) = \{d_1 d_2 \mid d_1, d_2 \in D(X)\},$$

the set of products of two distances in X. Thus, *equation* $Q(b)$ *has a solution in* X *if and only if* $b \in D_2(X)$. Finally, we denote $\overline{X} = \mathbb{N}_+ \setminus X$.

Claim 1. *If* $m \in \mathbb{N} \setminus D(X)$, *then* $m + X \subseteq \overline{X}$.

Indeed, for any $x \in X$, we have $m = (m + x) - x$, and since m is not a distance in X, it follows that $m + x$ cannot belong to X.

Claim 2. *If* $D(X) \neq \mathbb{N}$, *then* $D(X) \subseteq D(\overline{X})$.

Indeed, let $d \in D(X)$. Then $d = x - y$ for some $x, y \in X$ with $x \geq y$. Let now $m \in \mathbb{N} \setminus D(X)$. Then $d = (m + x) - (m + y)$, and $m + x, m + y \in \overline{X}$ by Claim 1. Hence $d \in D(\overline{X})$.

Claim 3. *Let* $t \in \mathbb{N}$ *satisfy* $t + X \subseteq X$. *Then* $t\mathbb{N} \subseteq D(X)$.

Indeed, the hypothesis implies $nt + X \subseteq X$ for all $n \in \mathbb{N}$. Hence, for $x \in X$, we have $nt + x \in X$ and so $nt = (nt + x) - x \in D(X)$.

Let now $\mathbb{N}_+ = A_0 \sqcup A_1$ be a partition of $\mathbb{N}_+$ into two nonempty parts. Thus $A_{1-i} = \overline{A_i}$ for $i = 0, 1$. We must show that $Q(b)$ has a solution in either A_0 or A_1 or, equivalently, that $b \in D_2(A_0) \cup D_2(A_1)$.

Clearly, if $D(A_i) = \mathbb{N}$ for $i = 0$ or 1, we are done since then $b \in D_2(A_i)$. Assume now

$$D(A_0),\ D(A_1) \neq \mathbb{N}.$$

Claim 4. *Let* $m \in \mathbb{N} \setminus D(A_0)$. *Then* $2m\mathbb{N}_+ \subseteq D(A_0)$.

Indeed, Claim 1 implies

$$m + A_0 \subseteq \overline{A_0} = A_1. \tag{7}$$

Moreover, Claim 2 implies both $D(A_0) \subseteq D(A_1)$ and $D(A_1) \subseteq D(A_0)$. Therefore

$$D(A_0) = D(A_1).$$

Hence $m \in \mathbb{N} \setminus D(A_1)$, and Claim 1 implies

$$m + A_1 \subseteq A_0. \tag{8}$$

It follows from (7) and (8) that $2m + A_0 \subseteq A_0$, and then Claim 3 implies

$$2m\mathbb{N}_+ \subseteq D(A_0).$$

This settles Claim 4. We now examine four possible cases.

Case 1. *Assume* $1 \notin D(A_0)$. Then Claim 4 implies $2\mathbb{N}_+ \subseteq D(A_0)$. Hence $2, b/2 \in D(A_0)$, implying $b = 2 \cdot b/2 \in D_2(A_0)$.

Case 2. *Assume* $1 \in D(A_0)$ *and* $2 \notin D(A_0)$. Then Claim 4 implies $4\mathbb{N}_+ \subseteq D(A_0)$. Hence $b \in D(A_0)$, and since $1 \in D(A_0)$ it follows that $b \in D_2(A_0)$.

Case 3. *Assume* $1 \in D(A_0)$ *and* $b/2 \notin D(A_0)$. Then Claim 4 implies $b \in D(A_0)$. But since $1 \in D(A_0)$, it follows that $b \in D_2(A_0)$.

Case 4. *Assume* $1, 2, b/2 \in D(A_0)$. Then $b = 2 \cdot b/2 \in D_2(A_0)$.

All four cases lead to the conclusion $b \in D_2(A_0)$. Therefore $Q(b)$ is 2-regular. $\square$

Remark 5.2. As easily seen, the 2-color Rado number for equation $Q(4)$ is equal to 5. That is, for any 2-coloring of $[1, 5]$, there is a monochromatic solution to that equation, and 5 is minimal for that property.

5.2. The case $r = 3$

We now show that equation $(x_1 - y_1)(x_2 - y_2) = 36$ is 3-regular. By Proposition 3.4, the right-hand side $b = 36$ is minimal for that property.

Again, this is a much sharper statement than that provided by Theorem 3.3 for $r = 3$. Indeed, the number $N = M(6! + 1, 1/3)$ is huge already, since $N \geq W(721, 3)$ by (6), and even more so is the constant term $b = 6N!$ involved in our main result.

As in [1], for a finite sequence A in $\mathbb{N}_+$, we denote by $\mathrm{bs}(A)$ the set of all *signed block sums* in A, i.e.,

$$\mathrm{bs}(A) = \{\pm\sigma(B) \mid B \text{ is a block in } A\}.$$

We shall also need the following ad-hoc definition, specifically tailored to deal with equation $Q(36)$. Of course, it may be easily adapted to deal with equation $Q(b)$ for any $b \geq 1$.

Definition 5.3. A sequence $A = (a_1, \ldots, a_n)$ of positive integers is said to be *admissible* if $\mathrm{bs}(A)$ contains no solution of the equation $uv = 36$, i.e., contains none of the following subsets:

$$\{6\}, \{4, 9\}, \{3, 12\}, \{2, 18\}, \{1, 36\}. \tag{9}$$

Moreover, if A is admissible and $\sigma(A) \leq t$ for some integer t, then A is said to be t-admissible. Finally, if A is not admissible then A is said to be *forbidden*.

For instance, the sequence $A = (1, 1, 9, 1)$ is 12-admissible. Indeed, we have $\mathrm{bs}(A) \cap \mathbb{N} = \{0, 1, 2, 9, 10, 11, 12\}$, a set containing no subset $\{u, v\}$ from list (9).

Remark 5.4. Every block in a t-admissible sequence is itself t-admissible. A sequence A is admissible if and only if its reverse sequence A' is admissible.

In the sequel, as in [1], we say that a set $X \subseteq \mathbb{N}_+$ is *regular with respect to a Diophantine equation D* if X contains a solution of D.[1]

Lemma 5.5. *Let X be a finite subset of $\mathbb{N}_+$. Let $A = \Delta(X)$ be the discrete derivative of X. Then X is regular with respect to equation $Q(36)$ if and only if A is forbidden.*

Proof. We have $X - X = \mathrm{bs}(A)$ as follows from Lemma 4.3. Hence X is regular if and only if $36 = uv$ for some $u, v \in X - X$, if and only if A is forbidden. □

Proposition 5.6. *Every 18-admissible sequence A of length 6 satisfies $\sigma(A) = 18$ and contains 1. More precisely, the list of all such sequences, up to reversal, is:*

$$(1, 3, 1, 3, 7, 3),\ (1, 3, 4, 3, 4, 3),\ (1, 3, 7, 3, 1, 3),$$
$$(3, 1, 3, 1, 3, 7),\ (3, 1, 3, 4, 3, 4),\ (3, 4, 3, 1, 3, 4).$$

Proof. The proof is completely elementary but too long to be included here. It exploits the fact that if $(a_1, \ldots, a_r, c)$ is t-admissible then $(a_1, \ldots, a_r)$ is $(t - 1)$-admissible, and in fact $(t - c)$-admissible. Thus, one may start with the set of all 13-admissible sequences of length 1, look for their respective extensions of length 2 which are 14-admissible, and so on up to length 6. This process takes a few hours by hand, or a few microseconds on a suitably programmed home computer.

As an illustrative example, consider the 8-admissible sequence $A = (1, 3, 1, 3)$ of length 4. It is admissible since the set $\mathrm{bs}(A) \cap \mathbb{N}_+ = \{1, 3, 4, 5, 7, 8\}$ contains none of the forbidden subsets in list (9).

---

[1] That is, if there is some solution $(x_1, \ldots, x_n)$ of D with $x_i \in X$ for all i.

We now seek all extensions $C = (1, 3, 1, 3, c)$ of A which are 17-admissible, hence with $1 \leq c \leq 9$. Now $c \neq 1$, for otherwise $\mathrm{bs}(C)$ would contain the prohibited subset $\{4, 9\}$, with $4 = \sigma((1, 3))$ and $9 = \sigma(C)$. Similarly, we have $c \neq 2$, for otherwise $\mathrm{bs}(C)$ would contain the prohibited subset $\{6\}$, where $6 = \sigma((1, 3, 2))$. In the same way, one may exclude all values of c in the interval $[1, 9]$ except $c = 7$, and easily conclude that $(1, 3, 1, 3, 7)$ is the only 17-admissible extension of length 5 of A. □

Corollary 5.7. *Equation $Q(36)$ is 3-regular. More precisely, every subset $X \subseteq [1, 37]$ of density $|X|/37 \geq 1/3$ is regular with respect to $Q(36)$.*

Proof. We first claim that there are no 36-admissible sequences B of length 12. Indeed, let B be a sequence in $\mathbb{N}_+$ of length 12 such that $\sigma(B) \leq 36$, and assume for a contradiction that B is admissible. Then $B = A_1A_2$, the juxtaposition of two admissible sequences of length 6. As $\sigma(B) \leq 36$, we have $\sigma(A_i) \leq 18$ for $i = 1$ or 2. We may assume $\sigma(A_1) \leq 18$ up to reversal of B. Now Proposition 5.6 implies $\sigma(A_1) = 18$, and therefore $\sigma(A_2) = 18$ as well since $\sigma(A_2) = \sigma(B) - \sigma(A_1) \leq 36 - 18 = 18$. Thus $\sigma(B) = 36$, whence $36 \in \mathrm{bs}(B)$. Now B contains 1, since A_1 does by Proposition 5.6 again. Therefore $\mathrm{bs}(B)$ contains $\{1, 36\}$ and hence is not admissible, a contradiction.

Let now $X \subseteq [1, 37]$ be of density at least 1/3, i.e., satisfying $|X| \geq 13$. We must show that X contains a solution of $Q(36)$. Removing elements if necessary, we may assume $|X| = 13$. Let $B = \Delta(X)$, the discrete derivative of X when X is viewed as an increasing sequence. Then B is of length 12, and B satisfies $\sigma(B) = \max X - \min X \leq 36$. Then B is not admissible by the above claim. Hence B is regular with respect to $Q(36)$ by Lemma 5.5. □

Corollary 5.8. *We have $\mathrm{dor}(Q(36)) = 3$. Moreover, for all $t \in \mathbb{N}_+$, equation $Q(36t^2)$ is 3-regular.*

Proof. We have $\mathrm{dor}(Q(36)) \geq 3$ by the above corollary, and $\mathrm{dor}(Q(36)) \leq 3$ by Proposition 3.4. The second assertion follows from the 3-regularity of $Q(36)$ and Proposition 3.5. □

Corollary 5.9. *The 3-color Rado number for equation $Q(36)$ is equal to 37.*

Proof. Let R denote the 3-color Rado number for $Q(36)$. We have $R \leq 37$, since Corollary 5.7 implies that for every 3-coloring of $[1, 37]$, there will be a monochromatic solution of $Q(36)$. To see that $R \geq 37$, it suffices to exhibit a 3-coloring of $[1, 36]$ admitting no monochromatic solution to $Q(36)$. Here is such a coloring, the three color classes being as follows:

$$X_1 = \{1, 2, 5, 6, 9, 16, 19, 20, 23, 24, 27, 34\},$$
$$X_2 = \{3, 10, 13, 14, 17, 18, 21, 28, 31, 32, 35, 36\},$$
$$X_3 = \{4, 7, 8, 11, 12, 15, 22, 25, 26, 29, 30, 33\}. \quad \square$$

6. Concluding remarks

Several problems related to the contents of this paper remain widely open and would deserve further investigation. Here is a short selection.

1. What is the degree of regularity of equation $Q(b)$ as a function of b? We showed here that, as b varies, the numbers $\mathrm{dor}(Q(b))$ are both finite and unbounded.
2. Given $r \geq 1$, can one determine all $b \in \mathbb{N}_+$ such that $\mathrm{dor}(Q(b)) = r$? For $r = 2$, our answer is all $b \equiv 0 \bmod 4$. For $r \geq 3$, can one similarly expect the answer to be given by suitable congruence classes? For instance, for $r = 3$, is the answer given by $b \equiv 0$ or $\pm 36 \bmod 180$? We do not know, but some preliminary indices point to an answer of this type.
3. Given $r \geq 1$, what is the smallest $b = b(r)$ such that $Q(b)$ is r-regular? Theorem 3.3 provides the upper bound $b(r) \leq M(r! + 1, 1/r)!r!$ but, as observed in cases $r = 2$ and 3, this is very far from being optimal. We have seen that $b(2) = 4$ and $b(3) = 36$. What is $b(4)$, for instance? More generally, what is the expected growth of $b(r)$ as a function of r?
4. Given $r, b \geq 1$, what is the r-color Rado number of equation $Q(b)$? In this paper, we provided the answer for the pairs $(r, b) = (2, 4)$ and $(3, 36)$.

References

[1] S.D. Adhikari, L. Boza, S. Eliahou, M.P. Revuelta, M.I. Sanz, Equation-regular sets and the Fox-Kleitman conjecture, Discrete Math. 341 (2018) 287–298.

[2] S.D. Adhikari, S. Eliahou, On a conjecture of Fox and Kleitman on the degree of regularity of a certain linear equation, in: Combinatorial and Additive Number Theory II: CANT, New York, NY, USA, 2015 and 2016 Springer, New York, in: Springer Proceedings in Mathematics & Statistics Series, vol. 220, 2017. http://dx.doi.org/10.1007/978-3-319-68032-3.

[3] A. Bialostocki, G. Bialostocki, D. Schaal, A zero-sum theorem, J. Combin. Theory Ser. A 101 (2003) 147–152.

[4] A. Bialostocki, H. Lefmann, T. Meerdink, On the degree of regularity of some equations, Discrete Math. 4 (1996) 49–60.

[5] J. Cooper, R. Overstreet, Coloring so that no Pythagorean Triple is Monochromatic. Preprint 2015, available at http://people.math.sc.edu/cooper/satpyth.pdf.

[6] J. Fox, D.J. Kleitman, On Rado's Boundedness Conjecture, J. Combin. Theory Ser. A 113 (2006) 84–100.

[7] J. Fox, R. Radoičić, On the degree of regularity of generalized van der Waerden triples, Integers 5 (2005) A32, 6 pp.

[8] N. Frantzikinakis, B. Host, Higher Order Fourier Analysis of Multiplicative Functions and Applications, 2016. arXiv:1403.0945v2 [Math.NT].

[9] R. Rado, Some recent results in combinatorial analysis, Congrès International des Mathématiciens, Oslo, 1936.

[10] R. Rado, Studien zur Kombinatorik, Math. Z. 36 (1933) 424–480.

[11] R. Rado, Verallgemeinerung eines Satzes von van der Waerden mit Anwendungen auf ein problem der Zahlentheorie, Sonderausgabe aus den Sitzungsbericten der Preuss, Akad. Wiss. Phys. -Math. Klasse 17 (1933) 1–10.

[12] T. Schoen, K. Taczala, The degree of regularity of the equation $\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} y_i + b$, Moscow J. Combin. Number Theory 7 (2017) 74–93 [162–181].

[13] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, Acta Arith. 27 (1975) 199–245.

[14] Van der Waerden numbers, http://www.vdwnumbers.org.