Mathematika 65 (2019) 929–949 © 2019 University College London
doi:10.1112/S002557931900024X

THERE IS NO KHINTCHINE THRESHOLD FOR METRIC PAIR CORRELATIONS

CHRISTOPH AISTLEITNER, THOMAS LACHMANN AND NICLAS TECHNAU

Abstract. We consider sequences of the form $(a_n\alpha)_n$ mod 1, where $\alpha \in [0,1]$ and where $(a_n)_n$ is a strictly increasing sequence of positive integers. If the asymptotic distribution of the pair correlations of this sequence follows the Poissonian model for almost all α in the sense of Lebesgue measure, we say that $(a_n)_n$ has the metric pair correlation property. Recent research has revealed a connection between the metric theory of pair correlations of such sequences, and the additive energy of truncations of $(a_n)_n$. Bloom, Chow, Gafni and Walker speculated that there might be a convergence/divergence criterion which fully characterizes the metric pair correlation property in terms of the additive energy, similar to Khintchine's criterion in the metric theory of Diophantine approximation. In the present paper we give a negative answer to such speculations, by showing that such a criterion does not exist. To this end, we construct a sequence $(a_n)_n$ having large additive energy which, however, maintains the metric pair correlation property.

§1. *Introduction.* Let $x_1, \dots, x_N$ be numbers in the unit interval. The distribution of the pair correlations of these numbers is described by the function

$$R(s,N) = \frac{1}{N}\{1 \leqslant i \neq j \leqslant N : \|x_i - x_j\| \leqslant s/N\}, \quad s \geqslant 0, \tag{1}$$

where $\|\cdot\|$ denotes the distance to the nearest integer. If for an infinite sequence $(x_n)_n$ we have

$$R(s,N) \to 2s \tag{2}$$

for all $s \geqslant 0$, then we say that the distribution of pair correlations is (asymptotically) *Poissonian*. Note that a sequence of independent, identically distributed (i.i.d.) random points, picked from a uniform distribution on [0, 1], almost surely has Poissonian pair correlations. The term "Poissonian" comes from a similarity with the distribution of the spacings between points in a Poisson process, which, however, only becomes really meaningful when also considering higher correlations (triple, quadruple, etc.) or so-called level spacings (which are in general much more difficult to handle than pair correlations).

The interest in such problems goes back to a paper by Berry and Tabor [**3**], where they gave a conjectural framework for the distribution of energy spectra of integrable quantum systems (see [**11**] for a survey). Their model led to strong

Received 15 February 2018, published online 23 July 2019.
MSC (2010): 11B30, 11K60 (primary), 05A18, 11B25, 11K06 (secondary).

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

mathematical interest in distributional properties of spacing of sequences such as $(n\alpha)_n$ mod 1 (corresponding to the "harmonic oscillator") and $(n^2\alpha)_n$ mod 1 (corresponding to the "boxed oscillator"). The case of $(n\alpha)_n$ is easier to analyse; one can use considerations based on continued fractions to show that the pair correlations of this sequence cannot be Poissonian for any α, since for some N the initial segment $(\alpha, 2\alpha, \dots, N\alpha)$ mod 1 is too regularly spaced. The case of $(n^2\alpha)_n$ is much harder and is far from being well understood. It is conjectured that the pair correlations for this sequence should be Poissonian, unless α is very well approximable by rationals; however, there exist only some partial results in this direction (see, for example, [**9**, **13**, **15**]). From the metric perspective, the situation is easier: it is known that the pair correlations of $(n^2\alpha)_n$ mod 1 are Poissonian for almost all α, in the sense of Lebesgue measure. The same is true if $(n^2)_n$ is replaced by $(n^d)_n$ for some integer $d \geqslant 3$, or by an exponentially growing sequence $(a_n)_n$ of integers; see [**12**, **14**]. We denote this property by saying that these sequences have the *metric pair correlation property*. In a recent paper [**2**], a connection was established between the question whether a sequence has the metric pair correlation property, and the asymptotic order of its so-called additive energy. Let $(a_n)_n$ be a sequence of distinct positive integers, let A_N denote its initial segment $a_1, \dots, a_N$, and denote by $E(A_N)$ the additive energy of A_N, which is defined as

$$E(A_N) = \#\{n_1, n_2, n_3, n_4 \leqslant N : \ a_{n_1} + a_{n_2} = a_{n_3} + a_{n_4}\}. \tag{3}$$

Trivially, the additive energy is always between N^2 and N^3. Throughout this paper we will use the formulation "the order of the additive energy of a sequence", when more precisely speaking we mean the order (as a function of N) of the additive energy of the N first elements of the sequence.

The main results of [**2**] say that a sequence has the metric pair correlation property if its additive energy is of order at most $N^{3-\varepsilon}$ for some $\varepsilon > 0$, while it does not have the metric pair correlation property if the additive energy exceeds cN^3 for infinitely many N for some constant $c > 0$. This fits together very well with the examples from above, since sequences of the form $(n^d)_n$ for $d \geqslant 2$ and lacunary sequences are known to have very small additive energy, while the additive energy of the sequence $a_n = n$, $n \geqslant 1$, is of the maximal possible order.

So the general philosophy is that a sequence has the metric pair correlation property as soon as its additive energy is slightly below the maximal possible order. However, a precise threshold is not known. Some results in this direction are as follows.

- The primes do not have the metric pair correlation property, as shown by Walker [**16**]. The additive energy of the sequence of primes is roughly of order $N^3/(\log N)$.
- There exists a sequence having additive energy of order $N^3/(\log N \log\log N)$ which does not have the metric pair correlation property [**10**].
- For every $\varepsilon > 0$ there exists a sequence having additive energy of order $N^3/(\log N(\log\log N)^{1+\varepsilon})$ which has the metric pair correlation property (unpublished, but not difficult to construct using methods from [**4**, **10**]).

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

These results indicate that there is a sort of transitional behaviour when the additive energy lies around the "critical" order of roughly $N^3/(\log N \log\log N)$. The methods used in [4, 10] indicate a close connection between this sort of question and problems from metric Diophantine approximation, where the classical theorem of Khintchine gives a zero–one law in terms of the convergence/divergence of the series of measures of the target intervals (see, for example, [8]). It is tempting to speculate that a similar convergence/divergence criterion might also exist for the metric theory of pair correlations, where the crucial quantity is the additive energy of $(a_n)_n$. This idea was discussed in a recent paper of Bloom *et al* [4], where they noted that there "appears to be reasonable evidence to speculate a sharp Khintchine-type threshold, that is, to speculate that the metric Poissonian property should be completely determined by whether or not a certain sum of additive energies is convergent or divergent". They raise the following problem, which they call the "fundamental question":

> Is it true that if $E(A_N) \sim N^3\psi(N)$, for some weakly decreasing function $\psi : \mathbb{Z}_{\geqslant 1} \to [0, 1]$, then $(a_n)_n$ is metric Poissonian if and only if
>
> $$\sum_{N\geqslant 1} \psi(N)/N \tag{4}$$
>
> converges?

In the present paper, we show that the answer to the question above is negative, and that the metric pair correlation property cannot be fully characterized in terms of the additive energy alone. For this purpose, we construct a sequence $(a_n)_n$ whose additive energy is of order roughly $N^3/(\log N)^{3/4}$, and which *does* have the metric pair correlation property. More precisely, we prove the following theorem.

THEOREM 1. *For every $\varepsilon > 0$ there exists a strictly increasing sequence $(a_n)_n$ of positive integers which has the metric pair correlation property, and whose additive energy satisfies*

$$E(A_N) \gg \frac{N^3}{(\log N)^{3/4+\varepsilon}}. \tag{5}$$

Note that the additive energy of the sequence from the conclusion of Theorem 1 is significantly larger than the putative threshold, which is around $N^3/(\log N)$. Furthermore, as the examples above showed, the additive energy of a sequence which does *not* have the metric pair correlation property can be of asymptotic order N^3, but it can also be of asymptotic order roughly $N^3/(\log N)$. Thus the metric theory of pair correlations cannot simply be reduced to a convergence/divergence criterion in terms of the additive energy alone. Instead, the picture is more complicated and can be described as follows.

- If the additive energy is below a certain threshold, then the sequence does have the metric pair correlation property.

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

- If the additive energy is above a certain threshold (for infinitely many N), then the sequence cannot have the metric pair correlation property. (This threshold is different from the one in the point above.)
- Between these upper and lower thresholds there is a transition zone, where knowing the additive energy alone is not sufficient to determine the metric pair correlation behaviour of the sequence. Thus, in this range the metric pair correlation property is determined by some additional arithmetic properties of the sequence.

We note that while our result says that the metric pair correlation property cannot be characterized in terms of the additive energy alone, it leaves the problem of finding some other way of characterizing the metric pair correlation property in terms of some arithmetic properties of $(a_n)_n$. It is likely that there is a zero–one law in the metric theory of pair correlations, but actually even this is not known. Also, our result still leaves questions concerning the quantitative connection between additive energy and the metric theory of pair correlations. For example, is it possible that a sequence having additive energy of order $N^3/(\log\log N)$ also has the metric pair correlation property? In the other direction, is it possible that the additive energy is of order $N^3/(\log N)^2$ and the sequence does not have the metric pair correlation property?[1] Closing the gaps in our knowledge in this field would be very desirable, as phenomena from both additive combinatorics and Diophantine approximation seem to be at work here.

§2. *Preliminaries.*

2.1. *Construction of the sequence.* We will construct our sequence $(a_n)_n$ as the concatenation of successive "blocks". All these blocks are either finite arithmetic or finite geometric progressions. The geometric blocks will contain the majority of the numbers which constitute the final sequence, but they will not be responsible for making the additive energy of the final sequence large, since geometric progressions always have small additive energy. The contribution of the geometric blocks to the distribution of pair correlations will be "random", in accordance with the well-known heuristic that lacunary systems exhibit properties which are also shown by independent random systems (see, for example, [**14**] for this phenomenon in connection with pair correlations, and [**1**] for the wider context). In our context "random" behaviour means Poissonian behaviour of the pair correlations, so the geometric blocks are responsible for the final sequence being metric Poissonian. The arithmetic blocks contain only a minority of all the elements of the final sequence, while being responsible for making the additive energy large. The main task will be to show that while these arithmetic blocks boost the additive energy, their contribution to the distribution of pair correlations is asymptotically negligible. To control the contribution of arithmetic blocks we will use tools from metric Diophantine approximation.

[1] While the present paper was being refereed, a paper by Bloom and Walker addressing this question appeared on the arXiv. They proved that there exists an (unspecified) constant $C > 1$ such that a sequence has the metric pair correlations property whenever its additive energy is of asymptotic order at most $N^3/(\log N)^C$; see [**5**].

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

The key point of the construction lies in the fact that the arithmetic blocks which are used in the construction have different prime numbers as their step sizes[2]. The fact that the step sizes of the arithmetic blocks are prime numbers will play a key role in two parts of the proof. On the one hand, using the theory of continued fractions at some point we will be led to counting the number of solutions of a certain equation; the assumption that the step size is a (large) prime will imply that we only have to count solutions which are a multiple of that prime, thus effectively reducing the number of solutions. This will allow us to control the contribution which comes from elements contained within one and the same arithmetic block. On the other hand, to control the contribution of the interaction of elements from two different arithmetic blocks, we will use a variance estimate which boils down to counting the maximal number of solutions of a simple Diophantine equation. Again, the fact that the moduli are (different) primes will reduce the maximal number of solutions of the equation. We will add some further comments on the heuristic reasoning behind the proof after first formulating precisely the way in which our sequence is constructed.

Notation. We fix some $\varepsilon > 0$. Throughout the rest of this paper we assume without loss of generality that ε is "small", say $\varepsilon < 1/100$. We will use Landau notation $o, \mathcal{O}$, and Vinogradov symbols $\ll, \gg$, with their usual meaning in analytic number theory (i.e. $f \ll g$ meaning that $|f|$ is bounded by a constant times $|g|$, for all possible arguments). The symbol $f \asymp g$ means that $f \ll g$ as well as $f \gg g$. If the implied constant depends on some parameter, we will indicate the dependence by a corresponding subscript. However, we will not indicate any dependence on ε, since throughout the proof ε is assumed to be fixed. We write λ for the Lebesgue measure on $\mathbb{R}$. Finally, we write $\lfloor \cdot \rfloor$ for the integer part of a real number.

In Lemma 1 below we construct the moduli of the arithmetic blocks.

LEMMA 1. *There exist an index $j_0 \geqslant 1$ and a sequence $(m_j)_{j \geqslant j_0}$ of primes such that*

$$m_j \asymp j^{1/4}, \tag{6}$$

and such that $m_j \neq m_i$ whenever $j - 3 \log j < i < j$, for all $i, j \geqslant j_0$.

Before proving the lemma, we briefly explain its meaning. The numbers m_j will be the moduli of the arithmetic progressions in our construction. The first condition in the lemma says that these moduli are of asymptotic order roughly $j^{1/4}$. The second condition guarantees that the step size of the jth arithmetic progression is different from the step size of the ith arithmetic progression, whenever i is "close" to j. So arithmetic blocks whose indices are close by can never have the same step size, which will guarantee that there is no undesired interaction between such blocks (this will play a crucial role in the proof of Lemma 7 below). On the other hand, if i and j are not close to each other, then

[2] We will need to use a "recycling process" for the prime moduli, since there are not enough different primes of the appropriate size available to have a different step size for each arithmetic block.

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

the corresponding arithmetic blocks are allowed to have the same step size—this is the "recycling process", which was mentioned in the preceding footnote, and which is necessary since the step sizes of the blocks grow more slowly than the indices of the blocks themselves. However, this will not cause any problems since the block sizes increase very quickly and any interaction between a block and some other block of much smaller cardinality will always be negligible.

Proof of Lemma 1. To define the value of m_j for all indices j in the range $16^d \leqslant j < 16^{d+1}$, $d \geqslant 0$, we note that the number of primes in the range

$$(2^d, 2^{d+1}) \tag{7}$$

is certainly at least d^2 for all sufficiently large d, by the prime number theorem. So assume that d is "large", and let $p_{d,1} < \cdots < p_{d,d^2}$ denote the first d^2 primes in the interval (7). We set

$$m_j := p_{d,r(j)}, \quad 16^d \leqslant j < 16^{d+1}, \tag{8}$$

where $r(j)$ is the unique remainder when reducing j mod d^2. Then (6) holds since $2^d = (16^d)^{1/4} \asymp j^{1/4}$. Furthermore, it can easily be seen that the second assertion of the lemma holds as well for sufficiently large d, since (8) guarantees that m_j cannot equal m_i whenever $|i - j|$ is small. Observe here that d^2 is of order roughly $(\log j)^2$, and thus much larger than $3 \log j$ for all sufficiently large j and d. □

Let j_0 be as in Lemma 1. For $j \geqslant j_0$ we recursively define sets $P_G(j)$ and $P_A(j)$ by setting

$$P_G(j) := \{2^{(\max P_A(j-1))} + 3^{j^h} : h = 0, \ldots, 2^j - 1\}, \tag{9}$$

$$P_A(j) := \{2^{(\max P_G(j))} + m_j h : h = 0, \ldots, \lfloor 2^j / j^{1/4+\varepsilon/3} \rfloor\}. \tag{10}$$

To make the construction well defined we need to specify the initial value $\max P_A(j_0 - 1)$, which is necessary for (9) in the case $j = j_0$; it does not matter what we choose, but let us agree that this quantity should be read as 1, and that accordingly $P_G(j_0) := \{2 + 3^{j_0^h} : h = 0, \ldots, 2^{j_0} - 1\}$.

The set $P_G(j)$ is a (shifted) geometric progression for each j, while the set $P_A(j)$ is a (shifted) arithmetic progression for each j. The sets $P_G(j)$ and $P_A(j)$ are arranged in increasing order; more precisely, we have

$$P_G(j) < P_A(j) < P_G(j+1) \tag{11}$$

for all $j \geqslant j_0$, where the symbol "$<$" means that every element of the set on the right-hand side exceeds every element of the set on the left-hand side.

The exponential factors $2^{(\cdots)}$ which appear in the definitions of all the sets P_G and P_A are quite arbitrary; what matters is only that the smallest element of $P_A(j)$ is much larger than the largest elements of $P_G(j)$, and so on. Thus the respective sets in our construction are not only ordered as shown by (11),

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

but there actually are huge gaps separating one item in this chain of inequalities from the next.

Finally, we specify the sequence $(a_n)_n$ by defining $a_n = a_n(\varepsilon)$ as the nth (smallest) element of

$$\bigcup_{j \geqslant j_0} (P_G(j) \cup P_A(j)),$$

for all $n \geqslant 1$. So $(a_n)_n$ contains all the numbers which are contained in $P_G(j)$ or $P_A(j)$ for some j, sorted in increasing order. We claim that the additive energy of this sequence is as large as specified in (5), and that the pair correlations of $(a_n\alpha)_n$ mod 1 are Poissonian for almost all α.

2.2. *The heuristic behind the construction.* Before turning to the proof of Theorem 1, we want to explain the heuristic behind the construction of the sequence $(a_n)_n$. In particular, we want to show why our construction allows is to go beyond the alleged "Khintchine threshold". Note that the distribution of the pair correlations of $(a_n\alpha)_n$ mod 1 depends not so much on the sequence $(a_n)_n$ itself as on the set of differences $\{a_n - a_m\}_{m,n}$ (as does the additive energy). Thus it is this difference set that has to be controlled.

Obviously the difference set of a finite arithmetic progression has a very special structure; it is essentially an arithmetic progression itself, and the cardinality of the difference set of an arithmetic progression is small while the additive energy is large. More precisely, the positive part of the difference set of an arithmetic progression with step size d and length M is itself an arithmetic progression with step size d and length $M - 1$, and each of the elements of the difference sets has at least one and at most $M - 1$ representations as a difference of elements of the original set. In our construction we combine arithmetic progressions with different prime moduli m_j. The number of such arithmetic progressions and their respective length is so large that they boost the additive energy of the total sequence; in contrast, we have to show that their contribution to the distribution of pair correlations is asymptotically negligible. In our setting, at the jth building block we have constructed roughly $N \approx 2^j$ elements of our sequence $(a_n)_n$. Each arithmetic progression at this level consists of roughly $\approx N/(\log N)^{1/4+\varepsilon/3}$ elements. One can easily check that this leads to the required lower bound for the additive energy. The size of the prime moduli m_j is roughly $(\log N)^{1/4}$.

To make sure that the contribution which one of these arithmetic progressions makes to the pair correlations is asymptotically negligible, we have to show (roughly speaking) that

$$\frac{N}{(\log N)^{1/4+\varepsilon/3}} \cdot \#\left\{q \leqslant N/(\log N)^{1/4+\varepsilon/3} : \|m_j q\alpha\| \leqslant \frac{1}{N}\right\} = o(N) \qquad (12)$$

for "typical" α in the sense of Lebesgue measure (where for simplicity we took $1/N$ rather than s/N for the length of the test interval). Here the factor $N/(\log N)^{1/4+\varepsilon/3}$ on the very left arises as the maximal number of representations which the number $m_j q$ has as a difference of two elements

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

of the arithmetic progression with step size m_j, and the upper bound $q \leqslant N/(\log N)^{1/4+\varepsilon/3}$ which restricts the maximal size of q comes from the length of the arithmetic blocks. The estimate (12) is true as long as the cardinality of the set on the left is asymptotically negligible in comparison to $(\log N)^{1/4+\varepsilon/3}$.

Essentially, the cardinality of this set only exceeds $(\log N)^{1/4+\varepsilon/3}$ when there is a

$$q \in \{1, \dots, N/(\log N)^{1/2+2\varepsilon/3}\}$$

such that $\|m_j q\alpha\|$ is less than $1/(N(\log N)^{1/4+\varepsilon/3})$, so that for the next $(\log N)^{1/4+\varepsilon/3}$ multiples of q we also have $\|m_j q\alpha\| \leqslant 1/N$, and so that all these multiples are still smaller than $N/(\log N)^{1/4+\varepsilon}$. Accordingly, one has to check if for typical α one should expect that there is a q such that

$$\|m_j q\alpha\| \leqslant \frac{1}{N(\log N)^{1/4+\varepsilon/3}}, \quad 1 \leqslant q \leqslant N/(\log N)^{1/2+2\varepsilon/3}.$$

Writing $N/(\log N)^{1/2+2\varepsilon/3} =: Q$, the inequality above essentially becomes

$$\|m_j q\alpha\| \leqslant \frac{1}{Q(\log Q)^{3/4+\varepsilon}}, \quad 1 \leqslant q \leqslant Q. \tag{13}$$

By Khintchine's convergence/divergence criterion this inequality looks like it should have infinitely many solutions for "typical" alpha, since the expression on the right-hand side is not summable as a function of Q. However, one major aspect is missing. The right-hand side of (13) is so small that the solutions of this inequality can be explicitly characterized by continued fraction theory; all solutions necessarily come from best approximations to α. We will show that (for typical alpha) we may assume that the denominators of best approximations to alpha are not divisible by the prime m_j; thus the number $m_j q$ cannot be a best approximation denominator itself. Rather, it must be the multiple of m_j and of a best approximation denominator, and accordingly for q itself to satisfy (13) we must have

$$\|q\alpha\| = \frac{\|m_j q\alpha\|}{m_j} \leqslant \frac{1}{m_j Q(\log Q)^{3/4+\varepsilon}} \approx \frac{1}{Q(\log Q)^{1+\varepsilon}}, \quad 1 \leqslant q \leqslant Q. \tag{14}$$

The right-hand side of (14) is summable as a function of Q, and thus by Khintchine's criterion we should only expect finitely many solutions for typical alpha. It turns out that this heuristic reasoning can be turned into an actual proof.

We emphasize again that the fact that m_j always is a prime played a crucial role in this reasoning, together with the fact that we may assume that the denominators of best approximations are not divisible by m_j (we will prove this fact in Lemma 2 below). Another crucial aspect is to show that two different arithmetic blocks do not "interact" in an undesired way; that is, we have to show that the difference sets of these respective progressions do not overlap too much. For this it will again be important that all the moduli are (different) primes, since then a fixed integer can only show up in the difference set of two arithmetic

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

progressions if it is a product of the two primes which constitute the respective step sizes. This will be proved in the form of a variance bound in Lemma 7.

Finally, let us explain why it is not possible to obtain even larger additive energy with such a construction. Obviously, the additive energy is increased when the length of the arithmetic blocks is increased, so we might try to do that. Furthermore, as (14) shows, increasing the size of the prime moduli m_j would also improve the argument, so we might try to do that as well. So let us assume that the length of the arithmetic blocks is changed from roughly $N/(\log N)^{1/4+\varepsilon/3}$ to $N/(\log N)^{\beta}$ for some β, and that the size of the prime moduli m_j is changed from roughly $(\log N)^{1/4}$ to $(\log N)^{\gamma}$ for some γ. If we do so, then instead of (12) we will have to show that

$$\frac{N}{(\log N)^{\beta}} \#\left\{ q \leqslant N/(\log N)^{\beta} : \|m_j q\alpha\| \leqslant \frac{1}{N} \right\} = o(N) \tag{15}$$

for "typical" alpha, with m_j of size roughly $m_j \approx (\log N)^{\gamma}$. Now recall that Legendre's theorem from continued fraction theory allows us to characterize the solutions (a, b) to $|b\alpha - a| < 1/(2b)$. We want to use this for $b = m_j q$, and thus in our application b might be as large as $N(\log N)^{\gamma-\beta}$. The term $1/N$ in (15) is preassigned, since it comes from the definition of pair correlations. So in order to apply Legendre's theorem we have to make sure that $N(\log N)^{\gamma-\beta} \ll N$, which implies $\gamma \leqslant \beta$. This restricts the size of the prime moduli (in terms of the length of the arithmetic progressions). When we carry out the heuristic reasoning above with general parameters (β, γ) instead of $(1/4 + \varepsilon/3, 1/4)$, then instead of (14) we will arrive at

$$\|q\alpha\| \leqslant \frac{1}{Q(\log Q)^{3\beta+\gamma}}, \quad 1 \leqslant q \leqslant Q. \tag{16}$$

The right-hand side is summable if $3\beta + \gamma > 1$. Since the additive energy is maximized by taking β as small as possible, and since we already know that we need to take $\gamma \leqslant \beta$, the minimal permissible value for β is restricted by the requirement $\beta > 1/4$. This is the choice of parameters which is made in our construction. One can also show that our choice of parameters is optimal with respect to the conditions imposed by the variance bound in Lemma 7, which also requires that $3\beta + \gamma > 1$. Thus some significant new ideas would be necessary to further increase the additive energy while preserving the metric pair correlation property.

2.3. *A useful partition, and organization of the paper.* The following partitioning underpins the rest of this paper. Here we need some notation from additive combinatorics. We write $X - Y$ for the difference set

$$X - Y := \{x - y : x \in X,\ y \in Y\}$$

of two sets $X, Y \subseteq \mathbb{Z}$. By $\#X$ we denote the cardinality of X. Furthermore, we write r_{X-Y} for the number of ways in which $d \in \mathbb{Z}$ can be represented as a

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

difference of elements of $X, Y \subseteq \mathbb{Z}$, that is,

$$\mathrm{r}_{X-Y}(d) := \#\{(x, y) \in X \times Y : d = x - y\}. \tag{17}$$

If no confusion can arise, we will simply write $\mathrm{r}(d)$ for $\mathrm{r}_{X-Y}(d)$. Recall that trivially

$$\mathrm{r}_{X-Y}(d) \leqslant \min\{\#X, \#Y\}.$$

Moreover, let $X^+ := X \cap \mathbb{Z}_{\geqslant 1}$ denote the set of positive elements of a set $X \subseteq \mathbb{Z}$. Since $A_N - A_N$ is symmetric around the origin, we can confine attention to its positive part.

Assume that $d \geqslant 0$ is the difference of two elements of A_N, that is, $d = x - y$. We will classify these differences, according to the origin of x and y. More precisely, we will distinguish between the following cases.

- Case (GG): x and y both come from geometric blocks, that is, $x, y \in \bigcup_j P_G(j)$.
- Case (AG): x comes from an arithmetic block, and y comes from a geometric block, that is, $x \in \bigcup_j P_A(j)$ and $y \in \bigcup_j P_G(j)$. Or, reciprocally, x comes from a geometric block and y comes from an arithmetic block.
- Case (AA_{diff}): x and y come from *different* arithmetic blocks, that is, $x \in P_A(j_1)$ for some j_1 and $y \in P_A(j_2)$ for some j_2, such that $j_1 \neq j_2$.
- Case (AA_{same}): x and y come from *the same* arithmetic block, that is, $x, y \in P_A(j)$ for some j.

We write $\mathcal{D}_N(GG)$ for the set of those d in the difference set $(A_N - A_N)^+$ which can be represented as Case (GG). In a similar way, we define $\mathcal{D}_N(AG)$, $\mathcal{D}_N(AA_{\mathrm{diff}})$, and $\mathcal{D}_N(AA_{\mathrm{same}})$.

The function R which was defined in (1) can be decomposed in a similar way in the form

$$R = R(GG) + R(AG) + R(AA_{\mathrm{diff}}) + R(AA_{\mathrm{diff}}). \tag{18}$$

For this decomposition, we set

$$\begin{aligned} R(GG) := R(GG, \alpha, s, N) &:= \frac{2}{N} \sum_{d \in \mathcal{D}_N(GG)} r(d) I_{s,N}(d\alpha), \\ I_{s,N}(x) &:= \begin{cases} 1 & \|x\| \leqslant s/N, \\ 0 & \text{otherwise}, \end{cases} \end{aligned} \tag{19}$$

where $r(d)$ counts only the number of Case (GG) representations which $d \geqslant 1$ has in the form $d = x - y$ such that $x, y \in A_N$. Note that the factor 2 in (19), which is not present in (1), comes from the fact that we restricted ourselves to the positive part of the difference set $A_N - A_N$. Similarly, we define $R(AG)$, $R(AA_{\mathrm{diff}})$ and $R(AA_{\mathrm{same}})$, where the function $r(d)$ is instead restricted to representations of d as Case (AG), Case (AA_{diff}) and Case (AA_{same}), respectively.

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

By using the same methods as in [2], one can easily conclude that

$$R(GG, \alpha, s, N) \to 2s \tag{20}$$

as $N \to \infty$, for almost all $\alpha \in [0, 1]$ and each $s > 0$. This follows from the fact that geometric progressions have small additive energy, and the fact that the cardinality of the geometric blocks is dominant over the total cardinality of the arithmetic blocks which implies that $1/N$ really is the correct normalization factor such that $R(GG)$ converges as desired for $N \to \infty$.

Thus it remains to show that all the remaining terms $R(AG)$, $R(AA_{\text{diff}})$ and $R(AA_{\text{same}})$ vanish in the limit $N \to \infty$, for almost all α.

The outline of the next sections is as follows. First, in §3, we analyse the contribution of $R(AA_{\text{same}})$. Here Diophantine approximation determines the counting[3]. Then, in §4, we prove variance estimates to control $R(AG)$ and $R(AA_{\text{diff}})$. Once these steps are completed, in §5 we use the Borel–Cantelli lemma with a sandwiching argument to finish the proof of Theorem 1.

§3. *Analysing the contribution of the small differences.* Before proceeding further, we need to recall some notions and results about continued fractions. For a (possibly finite) sequence $(\alpha_i)_i$ of strictly positive integers, we denote by

$$\alpha := [\alpha_1, \alpha_2, \ldots] = \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \cfrac{1}{\ddots}}}$$

the associated (possibly finite) continued fraction in the unit interval $[0, 1]$. Moreover, let p_n/q_n denote the nth convergent to α. Then the following are well-known facts; cf. for instance, [6, Ch. 1].

(1) Legendre's theorem. If a/b is a fraction with

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2},$$

then a/b is a convergent to α.

(2) We have

$$\left|\alpha - \frac{p_n}{q_n}\right| \asymp \frac{1}{\alpha_n q_n^2}, \tag{21}$$

where the implied constants are independent of α.

(3) Borel–Bernstein theorem. Let $B := (b_n)_n$ be a sequence of (strictly) positive real numbers, and consider the series

$$\sum_{n \geqslant 1} \frac{1}{b_n}. \tag{22}$$

[3] The mechanism furnishing these estimates is of a somewhat combinatorial nature, and related to so-called *Bohr sets*. The combinatorial nature of these sets also plays a key role in a recent paper of Chow; cf. [7].

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

If $V_B \subset [0,1]$ denotes the set of numbers $\alpha = [\alpha_1, \alpha_2, \ldots]$ satisfying $\alpha_n \leqslant b_n$ for all sufficiently large $n \geqslant 1$, then

$$\lambda(V_B) = \begin{cases} 1 & \text{if (22) converges,} \\ 0 & \text{if (22) diverges.} \end{cases}$$

LEMMA 2. *Let $(m_j)_{j\geqslant 1}$ be the sequence of primes from Lemma 1, which was used in (10) for the construction of our sequence. Then for almost all $\alpha \in [0,1]$ there exist only finitely many pairs of indices (j,n) such that the prime m_j divides q_n, and such that additionally $q_n/m_j \in [2^j/j^2, 2^j]$, where q_n is the denominator of a convergent to α.*

Proof. Assume that the denominator q_n of a convergent is divisible by a prime m_j, that is, there is a k such that $q_n = km_j$. When q_n is a convergent to α we have that $\|q_n\alpha\| \leqslant 1/q_n$, and thus $\|km_j\alpha\| \leqslant 1/(km_j)$. Thus to prove the lemma we have to show that almost all $\alpha \in [0,1]$ are contained in at most finitely many sets of the form

$$S_{j,k} := \left\{ x \in [0,1] : \|km_j x\| \leqslant \frac{1}{km_j} \right\}, \quad j = 1, 2, \ldots, 2^j/j^2 \leqslant k \leqslant 2^j.$$

We have

$$\lambda(S_{j,k}) = \frac{2}{km_j}.$$

Furthermore, we have

$$\sum_{j=1}^{\infty} \sum_{2^j/j^2 \leqslant k \leqslant 2^j} \frac{2}{km_j} \ll \sum_{j=1}^{\infty} \frac{\log j}{m_j}.$$

Recall that to construct our sequence $(m_j)_{j\geqslant 1}$ in Lemma 1 we selected d^2 primes from the range $(2^d, 2^{d+1})$, for each (sufficiently large) d. Thus

$$\sum_{j=1}^{\infty} \frac{\log j}{m_j} \ll \sum_{d} \frac{(\log\log d) d^2}{2^d} < \infty.$$

Thus, by the Borel–Cantelli lemma, almost all α are contained in only finitely many sets $S_{j,k}$. □

LEMMA 3. *Let*

$$M_j := \{ q \leqslant 2^j/j^{1/4+\varepsilon/3} : \|m_j q\alpha\| \leqslant s/2^j \}.$$

Then for almost all $\alpha \in [0,1]$ we have

$$\#M_j \ll_s j^{1/4}.$$

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

Proof. In this proof we suppress the potential dependence of the symbols "$\ll$" and "$\gg$" on s.

Let B denote the sequence $(n^{1+\varepsilon/3})_n$, and suppose that $\alpha \in V_B$ is an irrational number (recall that the set V_B was defined in the statement of the Borel–Bernstein theorem, before the statement of Lemma 2). By the Borel–Bernstein theorem, V_B has full Lebesgue measure. In the sequel we will assume that $\alpha \in [0,1]$ is a fixed number which is contained in V_B, and for which the conclusion of Lemma 2 holds. Note that the set of such α has full Lebesgue measure.

Let us note the following. Let q_m be the denominator of a convergent to α. Assume that

$$\|q_m\alpha\| \leqslant \frac{s}{2^j}. \tag{23}$$

Then, as noted above, we have

$$\|q_m\alpha\| \asymp \frac{1}{\alpha_m q_m}.$$

Since q_m grows at least exponentially in m, and since $\alpha \in V_B$ implies that $\alpha_m \ll m^{1+\varepsilon/3} \ll (\log q_m)^{1+\varepsilon/3}$, we thus see that (23) is only possible if

$$\frac{1}{(\log q_m)^{1+\varepsilon/3} q_m} \ll \frac{1}{2^j},$$

which in turn is only possible if

$$q_m \gg \frac{2^j}{j^{1+\varepsilon/3}}.$$

Now we argue in two steps.

(i) We first claim the following. If j is large enough, and if M_j is non-empty, then there exists a unique value of n such that q_n is the denominator of a convergent to α, such that $q_n \geqslant 2^j/j^2$, and such that

$$M_j \subseteq q_n\mathbb{Z}. \tag{24}$$

Indeed, if some q is contained in M_j, then for this q we have $\|m_j q\alpha\| \leqslant s/2^j < 1/(2m_j q)$, if j is sufficiently large. This is a consequence of our construction, where we have $m_j \asymp j^{1/4}$ and $q \leqslant 2^j/j^{1/4+\varepsilon/3}$. Let $p \in \mathbb{Z}$ be such that $\|m_j q\alpha\| = |m_j q\alpha - p|$. Then Legendre's theorem implies that there is some $n \geqslant 1$ with

$$\frac{p}{m_j q} = \frac{p_n}{q_n}. \tag{25}$$

As a consequence, since p_n and q_n are coprime, there is some integer $g \geqslant 1$ such that $m_j q = gq_n$ and $p = gp_n$. Then we have $\|m_j q\alpha\| = |gq_n\alpha - gp_n| = g|q_n\alpha - p_n|$, and from the reasoning following equation (23) we can deduce that $q_n \gg 2^j/j^{1+\varepsilon/3}$. Thus, provided that j is sufficiently large, q_n/m_j lies in the

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

range $[2^j/j^2, 2^j]$, and then, by Lemma 2, we can assume that q_n is not divisible by m_j.

Since we have now figured out that we may assume that m_j does not divide q_n, we conclude that p and q can actually both be written in the form $p = hm_j p_n$ and $q = hm_j q_n$ for some integer $h \geqslant 1$. Observe that (21) implies

$$\frac{m_j h}{\alpha_n q_n} \asymp \|m_j q\alpha\| \leqslant \frac{s}{2^j}, \tag{26}$$

and thus

$$\alpha_n q_n \gg m_j h 2^j \gg j^{1/4} 2^j.$$

Thus the well-known recursion $q_{n+1} = \alpha_n q_n + q_{n-1}$ yields $q_{n+1} \geqslant \alpha_n q_n \gg j^{1/4}2^j$ for sufficiently large j. However, M_j by definition is a subset of $\{1, \dots, 2^j/j^{1/4+\varepsilon/3}\}$. This shows that q_{n+1} is already too large to be contained in M_j, and consequently M_j consists only of integer multiples of q_n.

(ii) We now give an upper bound for the largest possible value of $h \geqslant 1$ such that $hm_j q_n \in M_j$. From (26) and the definition of M_j we deduce that

$$h \leqslant \frac{2^j}{q_n j^{1/4+\varepsilon/3}} \quad \text{as well as } h \ll \frac{\alpha_n q_n}{m_j 2^j}.$$

As noted above, we have $2^j/j^{1+\varepsilon/3} \ll q_n \ll 2^j/j^{1/4+\varepsilon/3}$. Thus

$$h \ll \max_{2^j/j^{1+\varepsilon/3} \ll x \leqslant 2^j/j^{1/4+\varepsilon/3}} \min\left\{\frac{2^j}{x j^{1/4+\varepsilon/3}}, \frac{\alpha_n x}{m_j 2^j}\right\},$$

where the $x \in \mathbb{R}$ maximizing the right-hand side, under the given constraints, is determined via

$$\frac{2^j}{x j^{1/4+\varepsilon/3}} = \frac{\alpha_n x}{m_j 2^j} \quad \Leftrightarrow \quad x^2 = \frac{m_j 2^{2j}}{j^{1/4+\varepsilon/3}\alpha_n}.$$

Thus, using $\alpha_n \ll (\log q_n)^{1+\varepsilon/3} \ll j^{1+\varepsilon/3}$, we finally obtain

$$h^2 \ll \frac{\alpha_n}{j^{1/4+\varepsilon/3} m_j} \ll j^{1/2}.$$

Thus $\#M_j \ll j^{1/4}$, which proves the lemma. □

§4. *Analysing the contribution of the large differences.* The Fourier series expansion of the indicator functions $I_{s,N}(\alpha)$ is given by

$$I_{s,N}(\alpha) \sim \sum_{n\in\mathbb{Z}} c_n e(n\alpha) \quad \text{where } c_n := \begin{cases} \sin(2\pi ns/N)/(\pi n) & \text{if } n \neq 0, \\ 2s/N & \text{if } n = 0, \end{cases} \tag{27}$$

where we write $e(\alpha)$ for $\exp(2\pi i\alpha)$. The next lemma is of a technical nature, and is used in a decoupling argument for the variance bounds, which are derived in §4.1.

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

LEMMA 4. *Define for integers $u, v > 0$ the quantity*

$$C(u, v) := \sum_{\substack{n_1, n_2 \in \mathbb{Z}\setminus\{0\}, \\ n_1 u = n_2 v}} c_{n_1} c_{n_2}. \tag{28}$$

Then

$$C(u, v) \ll \frac{\gcd(u, v)}{\max\{u, v\}}. \tag{29}$$

Moreover, for $u \neq 0$, we have

$$C(u, u) \ll_s N^{-1}. \tag{30}$$

Proof. Note that $n_1 u = n_2 v$ holds if and only if there is an integer $h \neq 0$ satisfying $n_1 = hu/\gcd(u, v)$ and $n_2 = hv/\gcd(u, v)$. Moreover, we observe that $|c_n| \leqslant \min\{2s/N, 1/|n|\}$ for $n \neq 0$. Combining these estimates with the Cauchy–Schwarz inequality yields

$$\begin{aligned} |C(u, v)|^2 &\leqslant \sum_{h \in \mathbb{Z}\setminus\{0\}} c^2_{h(u/\gcd(u,v))} \sum_{h \in \mathbb{Z}\setminus\{0\}} c^2_{h(v/\gcd(u,v))} \\ &\leqslant \sum_{h \in \mathbb{Z}\setminus\{0\}} \frac{(\gcd(u, v))^2}{(uh)^2} \sum_{h \in \mathbb{Z}\setminus\{0\}} \frac{(\gcd(u, v))^2}{(vh)^2}, \end{aligned}$$

which implies (29).

Furthermore,

$$C(u, u) \ll \sum_{n \leqslant N/2s} \frac{4s^2}{N^2} + \sum_{n > N/2s} \frac{1}{n^2},$$

which implies (30). □

From orthogonality relations, combined with (27), we obtain

$$\begin{aligned} N^2 \operatorname{Var}(R(AG, \cdot, s, N)) &= \int_0^1 \left(\sum_{d \in \mathcal{D}_N(AG)} r(d) \sum_{n \in \mathbb{Z}\setminus\{0\}} c_n e(dn\alpha) \right)^2 d\alpha \\ &= \sum_{u, v \in \mathcal{D}_N(AG)} r(u) r(v) C(u, v), \end{aligned} \tag{31}$$

where $r(\cdot)$ is the representation function which counts representations as Case (AG). A perfect analogue holds when (AG) is replaced by (AA_{diff}) everywhere in the formula (including in the definition of the representation function r).

The main term on the right-hand side, as we shall see, is the sum over the diagonal $(r(u))^2 C(u, u)$. To prove this, the next lemma shows that the contribution from the off-diagonal terms is small. More precisely, $C(u, v)$ is extremely small for two elements $u \neq v$ of $\mathcal{D}_N(AG)$ or $\mathcal{D}_N(AA_{\text{diff}})$.

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

LEMMA 5. *We have*

$$\sum_{\substack{u,v\in\mathcal{D}_N(AG),\\ u\neq v}} r(u)r(v)C(u,v) \ll 1, \tag{32}$$

where the representation function r counts representations from Case (AG). The same estimate holds if (AG) is replaced by (AA_{diff}).

Proof. This is not a critical part in the whole argument, and it is sufficient to use very rough estimates. We only give a brief outline of the proof. Let u and v be elements of the difference set $\mathcal{D}_N(AG)$ such that $0 < u < v$. Recall that different building blocks of our sequence are separated by huge constants. For u and v this leaves only two possibilities.

- The first is that u is of much smaller order than v, say $u \ll v^{1/2}$. By (29) we have $C(u,v) \ll \gcd(u,v)/\max\{u,v\}$. Since $\gcd(u,v) \leqslant u$, we have $C(u,v) \ll u/v \ll v^{-1/2}$.
- The second possibility is that u and v are of very similar size, and that consequently $v-u$ is very small in comparison with v. In this case we may assume, for example, that $v-u \ll v^{1/2}$. Again using $C(u,v) \ll \gcd(u,v)/\max\{u,v\}$, and now observing that $\gcd(u,v) \leqslant v-u \ll v^{1/2}$, we obtain $C(u,v) \ll v^{-1/2}$.

So in both cases $C(u,v)$ is small in comparison with v. By construction the difference set $\mathcal{D}_N(AG)$ is an extremely sparse set, due to the very fast growth of our sequence. Thus after summing over u and v we can obtain (32). A similar argument works when instead of $\mathcal{D}_N(AG)$ we consider $\mathcal{D}_N(AA_{\text{diff}})$. □

4.1. *Variance bounds.* We now have the tools at hand to derive the variance bounds for the auxiliary functions $R(AG,\cdot,s,N)$ and $R(AA_{\text{diff}},\cdot,s,N)$ which were defined in (19).

LEMMA 6. *For every fixed $s > 0$, we have*

$$\operatorname{Var}(R(AG,\cdot,s,N)) \ll_s N^{-1/2}. \tag{33}$$

Proof. Again this is not a crucial lemma, and it is sufficient to use very rough estimates. Note that trivially $\#\mathcal{D}_N(AG) \leqslant N^2$. Let $u \in \mathcal{D}_N(AG)$. Then, using again the fact that our sequence increases very quickly, we can easily show that the number of Case (AG) representations $r(u)$ which u has as the difference of two elements from A_N is very small. To give a quantitative statement, we could easily show that $r(u) \ll N^{1/4}$, uniformly in u (this is just a very rough estimate). Hence (30) implies

$$\sum_{u\in\mathcal{D}_N(AG)} r(u)^2|C(u,u)| \ll_s (\#\mathcal{D}_N(AG))N^{1/2}N^{-1} \ll_s N^{3/2}.$$

Together with (31) and (32), this implies (33). □

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

The contribution coming from numbers which arise as the difference between two numbers from different arithmetic blocks is a bit more difficult to control. To see this, note that when there are two arithmetic progressions with different step sizes m_{j_1} and m_{j_2}, there are certain numbers which have many representations as a number from the first arithmetic progression, minus a number from the second arithmetic progression. To control the contribution from such numbers, we will make crucial use of the fact that in our construction the step sizes m_{j_1} and m_{j_2} are prime numbers.

LEMMA 7. *For every fixed $s > 0$, we have*

$$\mathrm{Var}(R(AA_{\mathrm{diff}}, \cdot, s, N)) \ll_s \frac{1}{(\log N)^{1+\varepsilon/2}}. \tag{34}$$

Proof. Let N be given. There is some J such that $a_N \in P_A(J) \cup P_G(J)$, and by construction for this value of J we have $J \asymp \log N$. By (31) and Lemma 5 we have

$$\begin{aligned}\mathrm{Var}(R(AA_{\mathrm{diff}}, \cdot, s, N)) &\leqslant \frac{1}{N^2} \sum_{u,v \in \mathcal{D}_N(AA_{\mathrm{diff}})} r(u)r(v)|C(u,v)| \\ &\ll \frac{1}{N^2}\Bigg(1 + \sum_{1 \leqslant j_1 < j_2 \leqslant J} \sum_{u \in P_A(j_2) - P_A(j_1)} r(u)^2 |C(u,u)|\Bigg),\end{aligned}$$

where $r(u)$ counts the number of representation of u as the difference between an element of $P_A(j_2)$ and an element of $P_A(j_1)$. Here we used the fact that due to the huge constants which separate different blocks in our construction, for given u there is only one pair (j_1, j_2) such that $u \in P_A(j_2) - P_A(j_1)$, except perhaps for finitely many (small) values of u.

Let $j_1 < j_2$ be fixed. First assume that $j_1 < J - 2\log J$. We note that the cardinality of the set $P_A(j_2) - P_A(j_1)$ is bounded by

$$\begin{aligned}\#\{P_A(j_2) - P_A(j_1)\} &\ll \max\{P_A(j_2) - P_A(j_1)\} - \min\{P_A(j_2) - P_A(j_1)\} \\ &\ll m_{j_2} \frac{N}{(\log N)^{1/4+\varepsilon/3}} \\ &\ll \frac{N}{(\log N)^{\varepsilon/3}}.\end{aligned} \tag{35}$$

Then by the trivial estimate $r(u) \ll \#P_A(j_1) \ll N/(\log N)^{2\log 2 + 1/4}$, and since $2\log 2 + 1/4 > 16/10$, we have

$$\begin{aligned}\frac{1}{N^2} \sum_{\substack{j_1, j_2, \\ j_1 < J - 2\log J}} \sum_{u \in P_A(j_2) - P_A(j_1)} r(u)^2 |C(u,u)| &\ll_s \frac{J^2}{N^2} \frac{N^3}{(\log N)^{16/5}} \frac{1}{N} \\ &\ll \frac{1}{(\log N)^{6/5}}.\end{aligned} \tag{36}$$

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

It remains to control the contribution from the range $J - 2\log J \leqslant j_1 < j_2 \leqslant J$. Here it plays a crucial role that, for j_1, j_2 in this range, by construction there are two *different* primes m_{j_1} and m_{j_2} which form the step sizes of the arithmetic progression $P_A(j_1)$ and $P_A(j_2)$, respectively (cf. Lemma 1). Therefore, in such a situation $r(u)$ is bounded by the number of solutions $(x, y) \in \mathbb{Z}^2$ to the linear Diophantine equation

$$\tilde{u} = m_{j_2}x - m_{j_1}y \quad \text{where } \tilde{u} := u - \min\{P_A(j_2)\} + \min\{P_A(j_1)\},$$

and (x, y) satisfies the additional restriction that $1 \leqslant x, y \leqslant N/(\log N)^{1/4+\varepsilon/3}$. Since m_{j_1} and m_{j_2} are prime numbers, the set of integer solutions to this equation admits the form

$$(x_0 + hm_{j_1}, y_0 - hm_{j_2}),$$

where $h \in \mathbb{Z}$ and (x_0, y_0) is some solution to the above equation. Moreover, the size of j_1 and j_2, together with (6), ensures that $m_{j_1} \asymp m_{j_2} \asymp (\log N)^{1/4}$. Hence,

$$r(u) \ll \frac{N}{(\log N)^{1/2+\varepsilon/3}}. \tag{37}$$

Thus using (30), (35) and (37), and noting that $\log J \ll \log\log N \ll (\log N)^{\varepsilon/2}$, we obtain that

$$\begin{aligned}\frac{1}{N^2} &\sum_{\substack{j_1, j_2,\\ J-2\log J \leqslant j_1 < j_2 \leqslant J}} \sum_{u \in P_A(j_2) - P_A(j_1)} r(u)^2 |C(u,u)| \\ &\ll_s \frac{1}{N^2} \sum_{\substack{j_1, j_2,\\ J-2\log J \leqslant j_1 < j_2 \leqslant J}} \frac{N^3}{(\log N)^{1+\varepsilon}} \frac{1}{N} \\ &\ll \frac{1}{(\log N)^{1+\varepsilon/2}}.\end{aligned}$$

Combining this with (36) yields (34). □

§5. *Proof of Theorem 1.* Let N be given. There is a number J such that $a_N \in P_A(J) \cup P_G(J)$, and for this value of J we have $J \asymp \log N$ and $2^J \asymp N$. Then

$$E(A_N) \geqslant E(P_A(J-1)) \gg \frac{N^3}{(\log N)^{3/4+\varepsilon}},$$

where we used that the additive energy of an arithmetic progression is proportional to the third power of its cardinality, and that by construction $\#P_A(J-1) \gg 2^J/J^{1/4+\varepsilon/3} \gg N/(\log N)^{1/4+\varepsilon/3}$. Thus the additive energy of the sequence constructed in our example is indeed as large as claimed in the statement of the theorem.

It remains to show that $(a_n)_n$ has the metric pair correlation property. Recall that the contribution coming from the geometric blocks gives the desired

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

convergence $R(GG, \alpha, s, N) \to 2s$ for almost all α, for every fixed $s > 0$, cf. (20). It is a standard procedure to use the variance estimates and the results from the previous section to conclude that the contribution of the parts $R(AG)$ and $R(AA_{\text{diff}})$ tends to zero in the limit; thus we will only give a brief outline. Fix a rational $s > 0$. Define the sequence

$$N_m = \lfloor \exp(m^{1/(1+\varepsilon/2)}) \rfloor$$

and note that $N_{m+1}/N_m \to 1$. If N is such that $N_m \leqslant N < N_{m+1}$, then

$$N R(AG, \alpha, s, N) \leqslant N_{m+1} R(AG, \alpha, N_{m+1}/N_m s, N_{m+1}).$$

Denote by $E_{AG,s}(N_m)$ the "exceptional" set

$$\{\alpha \in [0, 1] : |R(AG, \alpha, N_m/N_{m+1}s, N) - \mu_{AG,s}(N_m)| \geqslant 1/\log\log N_m\},$$

where $\mu_{AG,s}(N_m)$ is the expected value of $R(AG, \alpha, N_m/N_{m+1}s, N)$. Observe that $\mu_{AG,s}(N_m) \to 0$ as $m \to \infty$, since the indices of those elements of $(a_n)_n$ which come from an arithmetic block are contained in a set of zero density within the total index set. Combining Chebyshev's inequality with the variance estimates from Lemmas 6 and 7, and applying the Borel–Cantelli lemma, we obtain

$$R(AG, \alpha, s, N) \underset{N\to\infty}{\longrightarrow} 0, \tag{38}$$

for all rational s and for Lebesgue almost all $\alpha \in [0, 1]$. Exactly the same argument works if (AG) is replaced by (AA_{diff}).

Finally we have to show that $R(AA_{\text{same}}) \to 0$ for almost all α. Let $s > 0$ be fixed, and assume that s is rational. By the Borel–Bernstein theorem, almost no $\alpha \in [0, 1]$ has infinitely many $d \geqslant N/(\log N)^{3/2}$ such that $I_{s,N}(d\alpha) = 1$. Hence it is sufficient to estimate the contribution of those differences d which are contained in $(P_A(j) - P_A(j))^+$ for a value of j which is close to J. More precisely, we can restrict j to the range $J - 2\log J \leqslant j \leqslant J$. By Lemma 3, for almost all $\alpha \in [0, 1]$ we have

$$\begin{aligned} &R(AA_{\text{same}}, \alpha, s, N) \\ &\quad \ll \frac{1}{N} \sum_{J-2\log J \leqslant j \leqslant J} \frac{2^j}{j^{1/4+\varepsilon/3}} \cdot \#\left\{ d \in (P_A(j) - P_A(j))^+ : \|d\alpha\| \leqslant \frac{s}{N} \right\} \\ &\quad \ll_s \frac{1}{N} \sum_{J-2\log J \leqslant j \leqslant J} \frac{2^j}{j^{\varepsilon/3}} \\ &\quad \ll (\log N)^{-\varepsilon/6}, \end{aligned} \tag{39}$$

where we estimated $\log J \ll \log\log N \ll (\log N)^{\varepsilon/6}$.

Thus we have $R(GG) \to 2s$, $R(AG) \to 0$, $R(AA_{\text{diff}}) \to 0$ and $R(AA_{\text{same}}) \to 0$, for all rational $s > 0$, for almost all α. However, if this convergence holds for all rational $s > 0$ and almost all α, then by monotonicity it must also hold for all real $s > 0$ and almost all α. In view of the decomposition (18), this concludes the proof of the theorem.

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

Acknowledgements. The authors would like to thank the anonymous referee for many valuable suggestions which significantly improved the presentation of this paper. C. A. is supported by the Austrian Science Fund (FWF), projects Y-901 and F 5512-N26. T. L. is also supported by FWF project Y-901. N. T. was supported by FWF project W1230, and by EPSRC Programme Grant EP/J018260/1. A non-trivial proportion of the present work was carried out while N. T. visited the number theory group of the University of York. He wishes to thank this group for its warm hospitality and the pleasant memories.

References

1. C. Aistleitner, Metric number theory, lacunary series and systems of dilated functions. In *Uniform Distribution and Quasi-Monte Carlo Methods* (*Radon Series on Computational and Applied Mathematics* **15**), De Gruyter (Berlin, 2014), 1–16.
2. C. Aistleitner, G. Larcher and M. Lewko, Additive energy and the Hausdorff dimension of the exceptional set in metric pair correlation problems. With an appendix by Jean Bourgain. *Israel J. Math.* **222**(1) (2017), 463–485.
3. M. Berry and M. Tabor, Level clustering in the regular spectrum. *Proc. R. Soc. Lond. Ser. A: Math. Phys. Eng. Sci.* **356**(1686) (1977), 375–394.
4. T. F. Bloom, S. Chow, A. Gafni and A. Walker, Additive energy and the metric Poissonian property. *Mathematika* **64**(3) (2018), 679–700.
5. T. F. Bloom and A. Walker, GCD sums and sum-product estimates. *Preprint*, 2018, arXiv:1806.07849.
6. Y. Bugeaud, *Approximation by Algebraic Numbers* (*Cambridge Tracts in Mathematics* **160**), Cambridge University Press (Cambridge, 2004).
7. S. Chow, Bohr sets and multiplicative Diophantine approximation. *Duke Math. J.* **167**(9) (2018), 1623–1642.
8. G. Harman, *Metric Number Theory* (*London Mathematical Society Monographs. New Series* **18**), Clarendon Press (Oxford, 1998).
9. D. R. Heath-Brown, Pair correlation for fractional parts of αn^2. *Math. Proc. Cambridge Philos. Soc.* **148**(3) (2010), 385–407.
10. T. Lachmann and N. Technau, On exceptional sets in the metric Poissonian pair correlations problem. *Monatsh. Math.* **189** (2019), 137–156.
11. J. Marklof, The Berry–Tabor conjecture. In *European Congress of Mathematics,* Vol. II *(Barcelona, 2000)* (*Progress in Mathematics* **202**), Birkhäuser (Basel, 2001), 421–427.
12. Z. Rudnick and P. Sarnak, The pair correlation function of fractional parts of polynomials. *Comm. Math. Phys.* **194**(1) (1998), 61–70.
13. Z. Rudnick, P. Sarnak and A. Zaharescu, The distribution of spacings between the fractional parts of $n^2\alpha$. *Invent. Math.* **145**(1) (2001), 37–57.
14. Z. Rudnick and A. Zaharescu, The distribution of spacings between fractional parts of lacunary sequences. *Forum Math.* **14**(5) (2002), 691–712.
15. J. L. Truelsen, Divisor problems and the pair correlation for the fractional parts of $n^2\alpha$. *Int. Math. Res. Not. IMRN* **2010**(16) (2010), 3144–3183.
16. A. Walker, The primes are not metric Poissonian. *Mathematika* **64**(1) (2018), 230–236.

Christoph Aistleitner,
Institute for Analysis and Number Theory,
University of Technology Graz,
Steyrergasse 30,
8010 Graz,
Austria
E-mail: aistleitner@math.tugraz.at

Thomas Lachmann,
Institute for Analysis and Number Theory,
University of Technology Graz,
Steyrergasse 30,
8010 Graz,
Austria
E-mail: lachmann@math.tugraz.at

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press

Niclas Technau,
Raymond and Beverly Sackler School of
Mathematical Sciences,
Tel Aviv University,
69978 Tel Aviv,
Israel
E-mail: technau@math.tugraz.at

https://doi.org/10.1112/S002557931900024X Published online by Cambridge University Press