GCD SUMS AND SUM-PRODUCT ESTIMATES

THOMAS F. BLOOM AND ALED WALKER

ABSTRACT. In this note we prove a new estimate on so-called GCD sums (also called Gál sums), which, for certain coefficients, improves significantly over the general bound due to de la Bretèche and Tenenbaum. We use our estimate to prove new results on the equidistribution of sequences modulo 1, improving over a result of Aistleitner, Larcher, and Lewko on how the metric poissonian property relates to the notion of additive energy. In particular, we show that arbitrary subsets of the squares are metric poissonian.

1. INTRODUCTION

For any two natural numbers n and m, let (n,m) denote their greatest common divisor. Let A be a finite set of natural numbers, and let $f : A \longrightarrow \mathbb{C}$ be any function. For $\alpha \in (0,1]$, the so-called GCD sum

$$\sum_{a,b \in A} \frac{(a,b)^{2\alpha}}{(ab)^{\alpha}} f(a)\overline{f(b)} \tag{1}$$

has received particular interest ([10, 9, 2, 5, 6, 11, 8]), owing to its connections to the resonance method for finding large values of $\zeta(\alpha + it)$ (for instance in [1, 8]) and to equidistribution problems (for instance in [4]).

As mentioned by the authors of [2] and [8], the value $\alpha = 1/2$ represents a critical case, and we shall pay especial attention to this value in our arguments. The best bound in this instance was established by Bondarenko and Seip.

Theorem 1 ([5]). *Let $A \subset \mathbb{N}$ with $|A| = N$, and let $f : A \longrightarrow \mathbb{C}$ be any function. Then*

$$\Big| \sum_{a,b \in A} \frac{(a,b)}{\sqrt{ab}} f(a)\overline{f(b)} \Big| \leq \exp\left(C\sqrt{\frac{\log N \log\log\log N}{\log\log N}} \right) \|f\|_2^2,$$

for some absolute constant $C > 0$, provided that N is large enough for the logarithms to be defined.

Here, and throughout the paper,

$$\|f\|_1 := \sum_{a \in A} |f(a)|, \qquad \|f\|_2^2 := \sum_{a \in A} |f(a)|^2.$$

The authors de la Bretèche and Tenenbaum have recently shown [8] that Theorem 1 is true with the value $C = 2\sqrt{2} + o(1)$, and that $2\sqrt{2}$ is the best possible constant. The purpose of this note is to use results from arithmetic combinatorics, of a 'sum-product' flavour, to improve this bound in the special case in which the coefficient function f enjoys some additional structure. We will then given an application of this result to metric number theory.

We prove the following general result for α in the range $1/2 \leqslant \alpha \leqslant 1$.

Theorem 2. *Let $f : \mathbb{N} \longrightarrow \mathbb{C}$ be any function with finite support. Let K be some parameter greater than 3 such that*

$$\sum_{ab=cd} f(a)f(b)\overline{f(c)f(d)} \leqslant K\|f\|_2^4. \tag{2}$$

Then

$$\sum_{a,b} f(a)\overline{f(b)}\frac{(a,b)^2}{ab} \ll (\log\log K)^{O(1)}\|f\|_2^2.$$

Furthermore, for α in the range $1/2 < \alpha < 1$,

$$\sum_{a,b} f(a)\overline{f(b)}\frac{(a,b)^{2\alpha}}{(ab)^\alpha} \ll \exp(O_\alpha((\log K)^{1-\alpha}(\log\log K)^{-\alpha}))\|f\|_2^2.$$

Finally, at the critical value $\alpha = 1/2$, if $\|f\|_1 \geqslant 3$ and $K \geqslant \log\|f\|_1$ then

$$\sum_{a,b} f(a)\overline{f(b)}\frac{(a,b)}{\sqrt{ab}} \ll (\log\|f\|_1 + O(1))^{-1}\exp(O((\log K \log\log\|f\|_1)^{1/2}))\|f\|_2^2.$$

One can fruitfully apply these bounds when f has some additive structure, for example when $f(n) = r(n)$, where

$$r(n) = r_A(n) = |\{(a,b) \in A^2 : a - b = n\}|$$

for some finite set $A \subset \mathbb{N}$. A suitable upper bound on the multiplicative energy of $r(n)$ is provided by the sum-product techniques of arithmetic combinatorics.

Theorem 3. *If $A \subset \mathbb{N}$ is a finite set and $r = r_A$ is the representation function defined above then*

$$\sum_{kl=mn} r(k)r(l)r(m)r(n) \ll |A|^6 \log|A|.$$

This theorem is due to Roche-Newton and Rudnev (it is essentially Proposition 4 of [13]) but in section 3 we give a much simpler proof due to Murphy, Roche-Newton, and Shkredov [12].

As an immediate corollary, we obtain the following bound.

Theorem 4. *If $A \subset \mathbb{N}$ is a finite set with $|A| = N$, and $r = r_A$ is the representation function defined above, then, provided N is large enough,*

$$\sum_{\substack{n_i,n_j \in A-A \\ n_i,n_j > 0}} \frac{(n_i,n_j)}{\sqrt{n_in_j}}r(n_i)r(n_j) \ll (\log N)^{O(1)}\exp(O((\log\tfrac{N^3}{E(A)}\log\log N)^{1/2}))E(A),$$

where

$$E(A) := \sum_{n \in \mathbb{Z}} r(n)^2$$

is the additive energy of A.

Proof. We apply the third case of Theorem 2 to the function $f(n) := r(n)1_{\mathbb{N}}(n)$, and with $K := C(\log N)(\frac{N^3}{E(A)})^2$ for some large constant C. Theorem 3 then implies that condition (2) is satisfied. Furthermore $\|f\|_1 = \frac{N(N-1)}{2}$, and so $K \geqslant \log\|f\|_1$. The result then follows. $\qquad\square$

Theorem 4 improves over the general bound in Theorem 1 in the cases where $E(A) \geqslant N^{3-o(1)}$. We will use this to improve upon a result of Aistleitner-Larcher-Lewko concerning the metric poissonian property, a notion from metric number theory that we will now briefly introduce. For more on this property, see [4, 7, 16].

Definition 5. *If $\mathcal{A}$ is an increasing sequence of natural numbers, for $\alpha \in [0,1]$ and $s > 0$ define*

$$F(\alpha, s, N, \mathcal{A}) := \frac{1}{N} \sum_{\substack{x_i, x_j \in A_N \ x_i \neq x_j \\ \|\alpha(x_i - x_j)\| \leqslant s/N}} 1,$$

where A_N is the truncation of $\mathcal{A}$ to the first N elements. We say that $\mathcal{A}$ is metric poissonian *if for almost all $\alpha \in [0,1]$, for all $s > 0$*

$$F(\alpha, s, N, \mathcal{A}) \to 2s$$

as $N \to \infty$.

The metric poissonian property is a strong notion of equidistribution for dilates of sequences, motivated by certain concerns in quantum physics (see [14]).

We prove the following theorem, continuing the line of work [4, 16, 7, 3] that investigates the relationship between the metric poissonian property and the notion of additive energy.

Theorem 6. *There exists an absolute positive constant C such that the following is true. Let $\mathcal{A}$ be a sequence of natural numbers, with truncations A_N, and suppose that*

$$E(A_N) \ll N^3/(\log N)^C.$$

Then $\mathcal{A}$ is metric poissonian.

This improves over the result of Theorem 1 of [4], in which the same conclusion was shown to hold under the stronger hypotheses $E(A_N) \ll N^{3-\delta}$ (for some positive δ).

We make no attempt to optimise the value of C in Theorem 6. We have previously speculated that any value of C greater than 1 should suffice (Fundamental question, [7]), and this could still be true (it is not precluded by the counterexample constructed in [3]). Unfortunately it does not seem as if the method presented in this paper will be able to prove this result, at least not without substantial modification.

In [7] we showed, under some additional and rather stringent density assumptions, that any $C > 2$ suffices: in Theorem 6 we recover a bound of the same shape without any density assumptions. This enables us to prove the following corollary, answering a question from [4].

Corollary 7. *Let $\mathcal{A}$ be an arbitrary infinite subset of the squares. Then $\mathcal{A}$ is metric poissonian.*

Proof. This follows directly from Theorem 6 and the result of Sanders (Theorem 11.7 of [15]) that if A_N is a set of N squares then $E(A_N) \ll N^3 \exp(-c_1 \log^{c_2} N)$ for some absolute positive constants c_1 and c_2. $\square$

Notation: We use the standard Bachmann-Landau asymptotic notation, as well as the Vinogradov symbol $\ll$. Unlike some authors, we use $f \ll g$ to mean that there exists some constant C for which $|f(n)| \leqslant C|g(n)|$ for *all* natural numbers n, and not just for n sufficiently large. The symbol $f \asymp g$ means that both $f \ll g$ and $g \ll f$ hold.

2. Proofs

The proof of Theorem 2 will involve the following random model for the zeta function. Let $\{X(p) : p \text{ prime}\}$ be a collection of independent random variables, each uniformly distributed on S^1. For every $n \in \mathbb{N}$ define $X(n) := \prod_{p^a \| n} X(p)^a$. Then define

$$\zeta_X(\alpha) := \sum_{n \in \mathbb{N}} \frac{X(n)}{n^\alpha}.$$

For fixed $\alpha > 1/2$, this series converges with probability 1. We will use the following moment estimates from [11].

Lemma 8. *When $\zeta_X(\alpha)$ is defined as above, and l is a real number, we have*

$$\log \mathbb{E}\,|\zeta_X(\alpha)|^{2l} \ll \begin{cases} l \log \log l & \alpha = 1 \\ C_\alpha l^{1/\alpha}(\log l)^{-1} & 1/2 < \alpha < 1 \\ l^2 \log(\alpha - 1/2) & 1/2 < \alpha \end{cases} \tag{3}$$

for some positive constant C_α. The first two cases hold provided $l \geqslant 3$, and the final case holds provided $l \geqslant 1$.

Proof. This is Lemma 6 of [11]. The range of uniformity in l is not specified there, but it is quickly seen from their argument that the above ranges of l are acceptable. $\square$

Proof of Theorem 2. We use the ideas of Lewko and Radziwill from [11]. Let

$$D(X) := \sum_{n \in \mathbb{N}} f(n)X(n).$$

Then on the one hand

$$\mathbb{E}(|\zeta_X(\alpha)D(X)|^2) = \sum_{n_1,n_2,m_1,m_2} (n_1 n_2)^{-\alpha} f(m_1)\overline{f(m_2)} 1_{n_1 m_1 = n_2 m_2}$$

$$= \sum_n \left| \sum_{m|n} f(m)(m/n)^\alpha \right|^2$$

$$= \zeta(2\alpha) \sum_{a,b} f(a)\overline{f(b)} \frac{(a,b)^{2\alpha}}{(ab)^\alpha}.$$

On the other hand, by splitting the expectation according to whether $|\zeta_X(\alpha)| < V$, and using the identity $\mathbb{E}(|D(X)|^2) = \|f\|_2^2$, for all positive l and V we have

$$\mathbb{E}(|\zeta_X(\alpha)D(X)|^2) \leqslant V^2 \|f\|_2^2 + V^{-2l}\mathbb{E}(|\zeta_X(\alpha)|^{2l+2}|D(X)|^2). \tag{4}$$

Now our approach differs from [11]. Instead of removing $D(X)$ from the second summand using an L^∞ bound, we use the Cauchy-Schwarz inequality. This shows that (4) is at most

$$V^2 \|f\|_2^2 + V^{-2l}\mathbb{E}(|D(X)|^4)^{\frac{1}{2}}\mathbb{E}(|\zeta_X(\alpha)|^{4l+4})^{\frac{1}{2}}. \tag{5}$$

Expanding out the expectation we see that

$$\mathbb{E}(|D(X)|^4) = \sum_{ab=cd} f(a)f(b)\overline{f(c)f(d)} \leq K\|f\|_2^4.$$

Suppose first that $\alpha = 1$. Then, by Lemma 8, the bound in (5) is

$$\ll \|f\|_2^2(V^2 + V^{-2l}K^{\frac{1}{2}}\exp(O(l \log \log l))).$$

Choosing $V = (\log l)^C$, with C large enough, and $l = \log K + 3$, this is

$$\ll (\log \log K)^{O(1)}\|f\|_2^2$$

as claimed. (Note that, since $K \geqslant 3$ by assumption, $\log l \ll \log \log K$).

When $1/2 < \alpha < 1$, (5) enjoys the bound

$$\|f\|_2^2(V^2 + V^{-2l}K^{\frac{1}{2}}\exp(O_\alpha(l^{1/\alpha}(\log l)^{-1}))).$$

Picking $V = \exp(C_\alpha l^{-1+1/\alpha}(\log l)^{-1})$, with C_α large enough, and $l = (\log K)^\alpha(\log \log K)^\alpha + 3$ yields the result.

It remains to tackle the case $\alpha = 1/2$, which we do by interpolating from $\alpha > 1/2$. More precisely, let $\alpha = 1/2 + 1/\log\|f\|_1$. By Hölder's inequality

$$\sum_{a,b} \frac{(a,b)}{\sqrt{ab}} f(a)\overline{f(b)} \ll \left(\sum_{a,b} \frac{(a,b)^{2\alpha}}{(ab)^\alpha} f(a)\overline{f(b)} \right)^{1/2\alpha}.$$

Using the estimate $\zeta(s) = (s-1)^{-1} + O(1)$ and (5) gives

$$\sum_{a,b} \frac{(a,b)^{2\alpha}}{(ab)^\alpha} f(a)f(b) \ll (\log\|f\|_1 + O(1))^{-1}\|f\|_2^2 (V^2 + V^{-2l}K^{1/2}\exp(O(l^2\log\log\|f\|_1))).$$

We now choose $V = \exp(Cl(\log\log\|f\|_1))$, with C large enough, and $l = (\log K)^{1/2}(\log\log\|f\|_1)^{-1/2}$. Note that the assumption $K \geqslant \log\|f\|_1$ implies that $l \geqslant 1$, and so our application of Lemma 8 was valid. The result then follows. $\square$

Proof of Theorem 6. Fixing two positive values s and ε, it will be enough to show that for almost all α there exists a natural number $N(\alpha, s, \varepsilon)$ such that

$$|F(\alpha, s, N, \mathcal{A}) - 2s| < \varepsilon \tag{6}$$

for every $N > N(s, \alpha, \varepsilon)$. (The theorem then follows by considering all rational values of s and ε: this argument is also used to conclude section 6 of [7]).

We have the following lemma of Aistleitner-Larcher-Lewko, which is essentially Lemma 3 of [4].

Lemma 9. *If $s \asymp 1$ then*

$$\mathrm{Var}(F, N) := \int_0^1 |F(\alpha, s, N, \mathcal{A}) - 2s|^2 \, d\alpha \ll \frac{\log N}{N^3} \sum_{\substack{n_i, n_j \in A_N - A_N \\ n_i, n_j > 0}} \frac{(n_i, n_j)}{\sqrt{n_i n_j}} r(n_i) r(n_j).$$

Applying Theorem 4, this implies that

$$\mathrm{Var}(F, N) \ll (\log N)^{O(1)} \exp(O(\log \tfrac{N^3}{E(A)} \log\log N)^{1/2}) \frac{E(A)}{N^3}.$$

Therefore, assuming $\frac{E(A)}{N^3} \leq (\log N)^{-C}$ for some sufficiently large absolute constant $C > 0$,

$$\mathrm{Var}(F, N) \ll (\log N)^{-3/2}.$$

We may now conclude in a similar fashion as in [4] and [7]. Indeed, let $\eta > 0$ be a small positive quantity to be chosen later, and for $j \in \mathbb{N}$ let $N_j := \lfloor e^{\eta j} \rfloor$. With this choice, $\sum_j \mathrm{Var}(F, N_j) < \infty$. By Chebyschev's inequality and the Borel-Cantelli Lemma, this implies that for almost all α there exists a value $j(\alpha, s, \varepsilon)$ such that for all $j \geqslant j(\alpha, s, \varepsilon)$ one has

$$|F(\alpha, s\tfrac{N_j}{N_{j+1}}, N_j, \mathcal{A}) - 2s| < \varepsilon/2, \qquad |F(\alpha, s\tfrac{N_{j+1}}{N_j}, N_j, \mathcal{A}) - 2s| < \varepsilon/2. \tag{7}$$

Let N be large, and choose j such that $N_j < N \leqslant N_{j+1}$. Then

$$N_j F(\alpha, s\tfrac{N_j}{N_{j+1}}, N_j, \mathcal{A}) \leqslant NF(\alpha, s, N, \mathcal{A}) \leqslant N_{j+1} F(\alpha, s\tfrac{N_{j+1}}{N_j}, N_j, \mathcal{A}).$$

Using this sandwiching, and the fact that $N_{j+1}/N_j = 1 + O(\eta)$, one may establish from (7) that, if N is large enough so that $j \geqslant j(\alpha, s, \varepsilon)$,

$$|F(\alpha, s, N, \mathcal{A}) - 2s| \leqslant \varepsilon/2 + O_s(\eta).$$

If η is small enough, (6) follows. $\square$

3. Sum-product estimates

This section is devoted to presenting a proof of Theorem 3. The first proof used the deep methods of Guth and Katz, but subsequently Murphy, Roche-Newton, and Shkredov gave a simpler proof using only the Szemerédi-Trotter theorem (see Theorem 2.1 of [12]). Since the proof is short and elementary, but rather difficult to extract from [12], we include a proof here.

We will require the following simple consequence of the Szemerédi-Trotter theorem (Corollary 2.2 of [12]).

Theorem 10. *Let $t \geqslant 2$ be a parameter. If L is a finite set of lines in $\mathbb{R}^2$ such that at most $O(|L|^{1/2})$ such lines intersect at any point then the number of points on more than t lines is $O(|L|^2/t^3)$.*

We use this to prove the following result.

Lemma 11. *For any finite sets $A, Z \subset \mathbb{R}$*
$$\sum_{n,m} r(n)r(m)1_{n/m\in Z} \ll |A|^3|Z|^{1/2}.$$

Proof. Let $r(y,z)$ count the number of $a, b \in A$ such that $a + bz = y$. Then
$$\sum_{n,m} r(n)r(m)1_{n/m\in Z} = \sum_{z\in Z}\sum_{y} r(y,z)^2.$$

By Theorem 10 the number of (y,z) such that $r(y,z) \geq t$ is $O(|A|^4/t^3)$. With u some parameter to be chosen later, splitting the sum by whether $r(y,z) \geq u$ and dividing the large values dyadically, we have
$$\sum_{z\in Z}\sum_{y} r(y,z)^2 \ll u|Z||A|^2 + \sum_{2^i\geq u}\frac{|A|^4}{2^i}$$
$$\ll u|Z||A|^2 + u^{-1}|A|^4.$$

The lemma follows by choosing $u \asymp |A||Z|^{-1/2}$. $\qquad\square$

Proof of Theorem 3. This follows from Lemma 11 following another dyadic decomposition. Indeed, since one has the trivial bound $r(k) \leqslant |A|$ for all k,
$$\sum_{km=ln} r(k)r(l)r(m)r(n) = \sum_{z}\Big|\sum_{n/m=z} r(n)r(m)\Big|^2$$
$$= \sum_{i=1}^{\lceil 2\log|A|\rceil}\sum_{z\in Z_i}\Big|\sum_{n/m=z} r(n)r(m)\Big|^2, \qquad (8)$$

where
$$Z_i := \Big\{z : e^{i-1} \leqslant \Big|\sum_{n/m=z} r(n)r(m)\Big| < e^i\Big\}.$$

So (8) is at most
$$\sum_{i=1}^{\lceil 2\log|A|\rceil} |Z_i|e^{2i}.$$

But applying Lemma 11 to Z_i yields $|Z_i| \ll |A|^6 e^{-2i}$. So
$$\sum_{km=ln} r(k)r(l)r(m)r(n) \ll |A|^6\log|A|,$$

as desired. $\qquad\square$

4. FINAL REMARKS

Considering the improvements of Bondarenko and Seip on GCD sums with $\alpha = 1/2$, we do not think that Theorem 4 has the quantitatively optimal form. However, to offer a substantial improvement we suspect that one would have to combine the incidence geometry argument of this paper with the compression arguments used in [5] and [8], or find some other means to take simultaneous advantage of both the additive and multiplicative structures of the sums involved. We have not been able to see a way of doing this, and indeed in our argument above we separate the additive and multiplicative structures early on, through applying Cauchy-Schwarz to (4).

Though in Theorem 6 we have refined the state of knowledge about the relationship between the metric poissonian property and additive energy, it is still unclear what the truth should be. We know from [3] that there is no sharp threshold phenomenon, but we still believe that Theorem 6 is true for any C greater than 1, which, up to $(\log N)^{o(1)}$ factors, would be an optimal result.

REFERENCES

[1] Christoph Aistleitner. Lower bounds for the maximum of the Riemann zeta function along vertical lines. *Math. Ann.*, 365(1-2):473–496, 2016.

[2] Christoph Aistleitner, István Berkes, and Kristian Seip. GCD sums from Poisson integrals and systems of dilated functions. *J. Eur. Math. Soc. (JEMS)*, 17(6):1517–1546, 2015.

[3] Christoph Aistleitner, Thomas Lachmann, and Niclas Technau. There is no khintchine threshold for metric pair correlations. arXiv:1802.02659.

[4] Christoph Aistleitner, Gerhard Larcher, and Mark Lewko. Additive energy and the Hausdorff dimension of the exceptional set in metric pair correlation problems. *Israel J. Math.*, 222(1):463–485, 2017. With an appendix by Jean Bourgain.

[5] Andriy Bondarenko and Kristian Seip. GCD sums and complete sets of square-free numbers. *Bull. Lond. Math. Soc.*, 47(1):29–41, 2015.

[6] Andriy Bondarenko and Kristian Seip. Large greatest common divisor sums and extreme values of the Riemann zeta function. *Duke Math. J.*, 166(9):1685–1701, 2017.

[7] Sam Chow, Thomas F. Bloom, Ayla Gafni, and Aled Walker. Additive energy and the metric poissonian property. arXiv:1709.02634, to appear in Mathematika.

[8] Régis de la Bretèche and Gerald Tenenbaum. Sommes de Gál et applications. arXiv:1804.01629.

[9] Tony Dyer and Glyn Harman. Sums involving common divisors. *J. London Math. Soc. (2)*, 34(1):1–11, 1986.

[10] I. S. Gál. A theorem concerning Diophantine approximations. *Nieuw Arch. Wiskunde (2)*, 23:13–38, 1949.

[11] Mark Lewko and Maksym Radziwiłł. Refinements of Gál's theorem and applications. *Adv. Math.*, 305:280–297, 2017.

[12] Brendan Murphy, Oliver Roche-Newton, and Ilya Shkredov. Variations on the sum-product problem. *SIAM J. Discrete Math.*, 29(1):514–540, 2015.

[13] Oliver Roche-Newton and Misha Rudnev. On the Minkowski distances and products of sum sets. *Israel J. Math.*, 209(2):507–526, 2015.

[14] Zeév Rudnick and Peter Sarnak. The pair correlation function of fractional parts of polynomials. *Comm. Math. Phys.*, 194(1):61–70, 1998.

[15] Tom Sanders. On the Bogolyubov-Ruzsa lemma. *Anal. PDE*, 5(3):627–655, 2012.

[16] Aled Walker. The primes are not metric Poissonian. *Mathematika*, 64(1):230–236, 2018.

HEILBRONN INSTITUTE FOR MATHEMATICAL RESEARCH, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRISTOL, UNIVERSITY WALK, BRISTOL BS8 1TW, UNITED KINGDOM
E-mail address: matfb@bristol.ac.uk

ANDREW WILES BUILDING, UNIVERSITY OF OXFORD, RADCLIFFE OBSERVATORY QUARTER, WOODSTOCK RD, OXFORD OX2 6GG, UNITED KINGDOM
E-mail address: walker@maths.ox.ac.uk