

# RATIONAL APPROXIMATIONS OF IRRATIONAL NUMBERS

DIMITRIS KOUKOULOPOULOS

ABSTRACT. Given quantities  $\Delta_1, \Delta_2, \dots \geq 0$ , a fundamental problem in Diophantine approximation is to understand which irrational numbers  $x$  have infinitely many reduced rational approximations  $a/q$  such that  $|x - a/q| < \Delta_q$ . Depending on the choice of  $\Delta_q$  and of  $x$ , this question may be very hard. However, Duffin and Schaeffer conjectured in 1941 that if we assume a “metric” point of view, the question is governed by a simple zero–one law: writing  $\varphi$  for Euler’s totient function, we either have  $\sum_{q=1}^{\infty} \varphi(q)\Delta_q = \infty$  and then almost all irrational numbers (in the Lebesgue sense) are approximable, or  $\sum_{q=1}^{\infty} \varphi(q)\Delta_q < \infty$  and almost no irrationals are approximable. We present the history of the Duffin–Schaeffer conjecture and the main ideas behind the recent work of Koukoulopoulos–Maynard that settled it.

## 1. DIOPHANTINE APPROXIMATION

Let  $x$  be an irrational number. In many settings, practical and theoretical, it is important to find fractions  $a/q$  of small numerator and denominator that approximate it well. This fundamental question lies in the core of the field of *Diophantine approximation*.

### 1.1. First principles

The “high-school way” of approximating  $x$  is to use its decimal expansion. This approach produces fractions  $a/10^n$  such that  $|x - a/10^n| \approx 10^{-n}$  typically. However, the error can be made much smaller if we allow more general denominators [14, Theorem 2.1].

**Theorem 1.1.** *If  $x \in \mathbb{R} \setminus \mathbb{Q}$ , then  $|x - a/q| < q^{-2}$  for infinitely many pairs  $(a, q) \in \mathbb{Z} \times \mathbb{N}$ .*

Dirichlet (c. 1840) gave a short and clever proof of this theorem. However, his argument is non-constructive because it uses the pigeonhole principle. This gap is filled by the theory of continued fractions (which actually precedes Dirichlet’s proof).

Given any  $x \in \mathbb{R} \setminus \mathbb{Q}$ , we may write  $x = n_0 + r_0 \approx n_0$ , where  $n_0 = \lfloor x \rfloor$  is the integer part of  $x$  and  $r_0 = \{x\}$  is its fractional part. We then let  $n_1 = \lfloor 1/r_0 \rfloor$  and  $r_1 = \{1/r_0\}$ , so that  $x = n_0 + 1/(n_1 + r_1) \approx n_0 + 1/n_1$ . If we repeat this process  $j - 1$  more times, we find that

$$(1.1) \quad x \approx n_0 + \frac{1}{n_1 + \frac{1}{\dots + \frac{1}{n_j}}} \quad \text{with} \quad n_i = \left\lfloor \frac{1}{r_{i-1}} \right\rfloor, \quad r_i = \left\{ \frac{1}{r_{i-1}} \right\} \quad \text{for } i = 1, \dots, j.$$

If we write this fraction as  $a_j/q_j$  in reduced form, then a calculation reveals that

$$(1.2) \quad \begin{aligned} a_j &= n_j a_{j-1} + a_{j-2} & (j \geq 2), & \quad a_1 = n_0 n_1 + 1, & \quad a_0 = n_0; \\ q_j &= n_j q_{j-1} + q_{j-2} & (j \geq 2), & \quad q_1 = n_1, & \quad q_0 = 1. \end{aligned}$$

When  $j \rightarrow \infty$ , the right-hand side of (1.1), often denoted by  $[n_0; n_1, \dots, n_j]$ , converges to  $x$ . The resulting representation of  $x$  is called its *continued fraction expansion*. The quotients  $a_j/q_j$  are called the *convergents* of this expansion and they have remarkable properties [18]. We list some of them below, with the first one giving a constructive proof of Theorem 1.1.

**Theorem 1.2.** *Assume the above set-up and notations.*

- (a) *For each  $j \geq 0$ , we have  $1/(2q_j q_{j+1}) \leq |x - a_j/q_j| \leq 1/(q_j q_{j+1})$ .*
- (b) *For each  $j \geq 0$ , we have  $|x - a_j/q_j| = \min\{|x - a/q| : 1 \leq q \leq q_j\}$ .*
- (c) *If  $|x - a/q| < 1/(2q^2)$  with  $a$  and  $q$  coprime, then  $a/q = a_j/q_j$  for some  $j \geq 0$ .*

## 1.2. Improving Dirichlet's approximation theorem

It is natural to ask when a qualitative improvement of Theorem 1.1 exists. Inverting this question leads us to the following definition: we say that a real number  $x$  is *badly approximable* if there is  $c = c(x) > 0$  such that  $|x - a/q| \geq cq^{-2}$  for all  $(a, q) \in \mathbb{Z} \times \mathbb{N}$ .

We can characterize approximable numbers in terms of their continued fraction expansion. Indeed, Theorem 1.2(a) and relation (1.2) imply that  $1/4 \leq n_{j+1} q_j^2 |x - a_j/q_j| \leq 1$ . Hence, together with Theorem 1.2(c), this implies that  $x$  is badly approximable if, and only if, the sequence  $(n_j)_{j=0}^\infty$  is bounded. Famously, Lagrange proved that the quadratic irrational numbers are in one-to-one correspondence with the continued fractions that are eventually periodic [18, §10]. In particular, all such numbers are badly approximable.

A related concept to badly approximable numbers is the *irrationality measure*. For each  $x \in \mathbb{R}$ , we define it to be

$$\mu(x) := \sup\{\nu \geq 0 : 0 < |x - a/q| < q^{-\nu} \text{ for infinitely many pairs } (a, q) \in \mathbb{Z} \times \mathbb{N}\}.$$

Note that  $\mu(x) = 1$  if  $x \in \mathbb{Q}$ , whereas  $\mu(x) \geq 2$  if  $x \in \mathbb{R} \setminus \mathbb{Q}$  by Theorem 1.1. Moreover,  $\mu(x) = 2$  if  $x$  is badly approximable. In particular,  $\mu(x) = 2$  for all quadratic irrationals  $x$ . Remarkably, Roth [25] proved that  $\mu(x) = 2$  for all algebraic irrational numbers  $x$ .

Determining the irrationality measure of various famous transcendental constants is often very hard. We do know that  $\mu(e) = 2$ , where  $e$  denotes Euler's constant. However, determining  $\mu(\pi)$  is a famous open problem. Towards it, Zeilberger and Zudilin [29] proved that  $\mu(\pi) \leq 7.10320533 \dots$ . It is widely believed that  $\mu(\pi) = 2$ .

Instead of trying to reduce the error term in Dirichlet's approximation theorem, we often require a different type of improvement: restricting the denominators  $q$  to lie in some special set  $\mathcal{S}$ . The theory of continued fractions is of limited use for such problems, because the denominators it produces satisfy rigid recursive relations (cf. (1.2)).

For rational approximation with prime or square denominators, the best results at the moment are due to Matomäki [21] and Zaharescu [28], respectively.

**Theorem 1.3** (Matomäki (2009)). *Let  $x$  be an irrational number and let  $\varepsilon > 0$ . There are infinitely many integers  $a$  and prime numbers  $p$  such that  $|x - a/p| < p^{-4/3+\varepsilon}$ .*

**Theorem 1.4** (Zaharescu (1995)). *Let  $x$  be an irrational number and let  $\varepsilon > 0$ . There are infinitely many pairs  $(a, q) \in \mathbb{Z} \times \mathbb{N}$  such that  $|x - a/q^2| < q^{-8/3+\varepsilon}$ .*

Two important open problems are to show that Theorems 1.3 and 1.4 remain true even if we replace the constants  $4/3$  and  $8/3$  by 2 and 3, respectively.

## 2. METRIC DIOPHANTINE APPROXIMATION

Unable to answer simple questions about the rational approximations of specific numbers, a lot of research adopted a more statistical point of view. For example, given  $M > 2$ , what *proportion* of real numbers have irrationality measure  $\geq M$ ? This new perspective gives rise to the theory of *metric Diophantine approximation*, which has a much more analytic and probabilistic flavor than the classical theory of Diophantine approximation. As we will see, the ability to ignore small pathological sets of numbers leads to a much more robust theory that provides simple and satisfactory answers to very general questions.

In order to give precise meaning to the word “proportion”, we shall endow  $\mathbb{R}$  with a measure. Here, we will mainly use the Lebesgue measure (denoted by “meas”).

### 2.1. The theorems of Khinchin and Jarník-Besicovitch

The foundational result in the field of metric Diophantine approximation was proven by Khinchin in his seminal 1924 paper [17]. It is a rather general result: given a sequence  $\Delta_1, \Delta_2, \dots, \geq 0$  of “permissible margins of error”, we wish to determine for which real numbers  $x$  there are infinitely many pairs  $(a, q) \in \mathbb{Z} \times \mathbb{N}$  such that  $|x - a/q| < \Delta_q$ . Clearly, if  $x$  has this property, so does  $x + 1$ . Hence, we may focus on studying

$$(2.1) \quad \mathcal{A} := \{x \in [0, 1] : |x - a/q| < \Delta_q \text{ for infinitely many pairs } (a, q) \in \mathbb{Z} \times \mathbb{N}\}.$$

**Theorem 2.1** (Khinchin (1924)). *Let  $\Delta_1, \Delta_2, \dots \geq 0$  and let  $\mathcal{A}$  be defined as in (2.1).*

(a) *If  $\sum_{q=1}^{\infty} q\Delta_q < \infty$ , then  $\text{meas}(\mathcal{A}) = 0$ .*

(b) *If  $\sum_{q=1}^{\infty} q\Delta_q = \infty$  and the sequence  $(q^2\Delta_q)_{q=1}^{\infty}$  is decreasing, then  $\text{meas}(\mathcal{A}) = 1$ .*

**Corollary 2.2.** *For almost all  $x \in \mathbb{R}$ , we have  $|x - a/q| \leq 1/(q^2 \log q)$  for infinitely many  $(a, q) \in \mathbb{Z} \times \mathbb{N}$ . On the other hand, if  $c > 1$  is fixed, then for almost every  $x \in \mathbb{R}$ , the inequality  $|x - a/q| \leq 1/(q^2 \log^c q)$  admits only finitely many solutions  $(a, q) \in \mathbb{Z} \times \mathbb{N}$ .*

In particular, Corollary 2.2 implies that the set of badly approximable numbers has null Lebesgue measure. On the other hand, it also says that almost all real numbers have irrationality measure equal to 2. This last result is the main motivation behind the conjecture that  $\mu(\pi) = 2$ : we expect  $\pi$  to behave like a “typical” real number.

Naturally, the fact that  $\mathcal{W}_M := \{x \in \mathbb{R} : \mu(x) \geq M\}$  has null Lebesgue measure for  $M > 2$  raises the question of determining its Hausdorff dimension (denoted by  $\dim(\mathcal{W}_M)$ ). Jarník [16] and Besicovitch [5] answered this question independently of each other.

**Theorem 2.3** (Jarník (1928), Besicovitch (1934)). *We have  $\dim(\mathcal{W}_M) = 2/M$  for all  $M \geq 2$ .*

### 2.2. Generalizing Khinchin’s theorem

Following the publication of Khinchin’s theorem, research focused on weakening the assumption that  $q^2\Delta_q \searrow$  in part (b). Importantly, doing so would open the door to understanding rational approximations using only a restricted set of denominators. Indeed, if  $q^2\Delta_q \searrow$ , then either  $\Delta_q > 0$  for all  $q$ , or there is  $q_0$  such that  $\Delta_q = 0$  for all  $q \geq q_0$ . The second case is trivial, since it implies  $\mathcal{A} = \emptyset$ . So, if we wish to understand Diophantine approximation with a restricted set of denominators  $\mathcal{S}$  (which would require  $\Delta_q = 0$  for  $q \notin \mathcal{S}$ ), then we must prove a version of Theorem 2.1(b) without the assumption that  $q^2\Delta_q \searrow$ .

In order to understand better the forces at play here, it is useful to recast Khinchin's theorem in probabilistic terms. For each  $q$ , let us define the set

$$(2.2) \quad \begin{aligned} \mathcal{A}_q &:= \{x \in [0, 1] : \text{there is } a \in \mathbb{Z} \text{ such that } |x - \frac{a}{q}| < \Delta_q\} \\ &= [0, 1] \cap \bigcup_{0 \leq a \leq q} \left( \frac{a}{q} - \Delta_q, \frac{a}{q} + \Delta_q \right). \end{aligned}$$

Then  $\mathcal{A} = \{x \in [0, 1] : x \in \mathcal{A}_q \text{ infinitely often}\}$ , which we often write as  $\mathcal{A} = \limsup_{q \rightarrow \infty} \mathcal{A}_q$ . We may thus view  $\mathcal{A}$  as the event that for a number chosen uniformly at random from  $[0, 1]$ , an infinite number of the events  $\mathcal{A}_1, \mathcal{A}_2, \dots$  occur. A classical result from probability theory due to Borel and Cantelli [14, Lemmas 1.2 & 1.3] studies precisely this kind of questions.

**Theorem 2.4.** *Let  $(\Omega, \mathcal{F}, \mathbb{P})$  be a probability space, let  $E_1, E_2, \dots$  be events in that space, and let  $E = \limsup_{j \rightarrow \infty} E_j$  be the event that infinitely many of the  $E_j$ 's occur.*

(a) *(The first Borel–Cantelli lemma) If  $\sum_{j=1}^{\infty} \mathbb{P}(E_j) < \infty$ , then  $\mathbb{P}(E) = 0$ .*

(b) *(The second Borel–Cantelli lemma) If  $\sum_{j=1}^{\infty} \mathbb{P}(E_j) = \infty$  and the events  $E_1, E_2, \dots$  are mutually independent, then  $\mathbb{P}(E) = 1$ .*

**Remark.** Let  $N$  be the random variable that counts how many of the events  $E_1, E_2, \dots$  occur. We have  $\mathbb{E}[N] = \sum_{j=1}^{\infty} \mathbb{P}(E_j)$ . Hence, Theorem 2.4 says that, under certain assumptions,  $N = \infty$  almost surely if, and only if,  $\mathbb{E}[N] = \infty$ .

To use the above result in the set-up of Khinchin's theorem, we let  $\Omega = [0, 1]$  and equip it with the Lebesgue measure as its probability measure. The relevant events  $E_j$  are the sets  $\mathcal{A}_q$ . Notice that if  $\Delta_q > 1/(2q)$ , then  $\mathcal{A}_q = [0, 1]$ , in which case  $\mathcal{A}_q$  occurs immediately for all  $x \in [0, 1]$ . In order to avoid these trivial events, we will assume from now on that

$$(2.3) \quad \Delta_q \leq 1/(2q) \quad \text{for all } q \geq 1, \quad \text{whence} \quad \text{meas}(\mathcal{A}_q) = 2q\Delta_q.$$

In particular, we see that part (a) of Khinchin's theorem is a direct consequence of the first Borel–Cantelli lemma. On the other hand, the second Borel–Cantelli lemma relies crucially on the assumption that the events  $E_j$  are independent of each other, something that fails generically for the events  $\mathcal{A}_q$ . However, there are variations of the second Borel–Cantelli lemma, where the assumption of independence can be replaced by weaker quasi-independence conditions on the relevant events (cf. Section 3.1). From this perspective, part (b) of Khinchin's theorem can be seen as saying that the condition that the sequence  $(q^2\Delta_q)_{q=1}^{\infty}$  is decreasing guarantees enough approximate independence between the events  $\mathcal{A}_q$  so that the conclusion of the second Borel–Cantelli lemma remains valid.

In 1941, Duffin and Schaeffer published a seminal paper [8] that studied precisely what is the right way to generalize Khinchin's theorem so that the simple zero–one law of Borel–Cantelli holds. Their starting point was the simple observation that certain choices of the quantities  $\Delta_q$  create many dependencies between the sets  $\mathcal{A}_q$ , thus rendering many of the denominators  $q$  redundant. Indeed, note for example that if  $\Delta_3 = \Delta_{15}$ , then  $\mathcal{A}_3 \subseteq \mathcal{A}_{15}$  because each fraction with denominator 3 can also be written as a fraction with denominator 15. By exploiting this simple idea, Duffin and Schaeffer proved the following result:

**Proposition 2.5.** *There are  $\Delta_1, \Delta_2, \dots \geq 0$  such that  $\sum_{q=1}^{\infty} q\Delta_q = \infty$  and yet  $\text{meas}(\mathcal{A}) = 0$ .*

*Proof.* Let  $p_1 < p_2 < \dots$  be the primes in increasing order, let  $q_j = p_1 \cdots p_j$ , and let  $\mathcal{S}_j = \{dp_j : d|q_{j-1}\}$ . We then set  $\Delta_q = (q_j j \log^2 j)^{-1}$  if  $q \in \mathcal{S}_j$  for some  $j \geq 2$ ; otherwise, we set  $\Delta_q = 0$ . We claim that this choice satisfies the needed conditions.

Since  $\mathcal{A}_q \subseteq \mathcal{A}_{q_j}$  for all  $q \in \mathcal{S}_j$ , we have  $\mathcal{A} = \limsup_{j \rightarrow \infty} \mathcal{A}_{q_j}$ . In addition, since  $\sum_{j=1}^{\infty} q_j \Delta_{q_j} < \infty$ , we have  $\text{meas}(\limsup_{j \rightarrow \infty} \mathcal{A}_{q_j}) = 0$  by Theorem 2.1(a). Hence,  $\text{meas}(\mathcal{A}) = 0$ , as needed. On the other hand, we have that

$$\sum_{q \geq 1} q \Delta_q = \sum_{j \geq 2} \sum_{d|q_{j-1}} dp_j \cdot \frac{1}{q_j j \log^2 j} = \sum_{j \geq 2} \frac{1}{j \log^2 j} \prod_{i \leq j-1} \left(1 + \frac{1}{p_i}\right),$$

By the Prime Number Theorem [19, Theorem 8.1], the last product is  $\geq c \log j$  for some absolute constant  $c > 0$ . Consequently,  $\sum_{q=1}^{\infty} q \Delta_q = \infty$ , as claimed.  $\square$

In order to avoid the above kind of counterexamples to the generalized Khinchin theorem, Duffin and Schaeffer were naturally led to consider a modified set-up, where only reduced fractions are used as approximations. They thus defined

$$(2.4) \quad \mathcal{A}^* := \{x \in [0, 1] : |x - a/q| < \Delta_q \text{ for infinitely many reduced fractions } a/q\}.$$

We may write  $\mathcal{A}^*$  as the lim sup of the sets

$$(2.5) \quad \mathcal{A}_q^* := [0, 1] \cap \bigcup_{\substack{0 \leq a \leq q \\ \gcd(a, q) = 1}} \left(\frac{a}{q} - \Delta_q, \frac{a}{q} + \Delta_q\right).$$

Assuming that (2.3) holds, we readily find that

$$\text{meas}(\mathcal{A}_q^*) = 2\varphi(q)\Delta_q$$

where

$$\varphi(q) := \#\{1 \leq a \leq q : \gcd(a, q) = 1\}$$

is Euler's totient function. They then conjectured that the sets  $\mathcal{A}_q^*$  have enough mutual quasi-independence so that a simple zero-one law holds, as per the Borel–Cantelli lemmas.

**The Duffin–Schaeffer conjecture.** *Let  $\Delta_1, \Delta_2, \dots \geq 0$  and let  $\mathcal{A}^*$  be defined as in (2.4).*

(a) *If  $\sum_{q=1}^{\infty} \varphi(q)\Delta_q < \infty$ , then  $\text{meas}(\mathcal{A}^*) = 0$ .*

(b) *If  $\sum_{q=1}^{\infty} \varphi(q)\Delta_q = \infty$ , then  $\text{meas}(\mathcal{A}^*) = 1$ .*

Of course, part (a) follows from Theorem 2.4(a); the main difficulty is to prove (b).

The Duffin–Schaeffer conjecture is strikingly simple and general. Nonetheless, it does not answer our original question: what is the correct generalization of Khinchin's theorem, where we may use non-reduced fractions? This gap was filled by Catlin [7].

**Catlin's conjecture.** *Let  $\Delta_1, \Delta_2, \dots \geq 0$ , let  $\Delta'_q = \sup_{m \geq 1} \Delta_{qm}$ , and let  $\mathcal{A}$  be as in (2.1).*

(a) *If  $\sum_{q=1}^{\infty} \varphi(q)\Delta'_q < \infty$ , then  $\text{meas}(\mathcal{A}) = 0$ .*

(b) *If  $\sum_{q=1}^{\infty} \varphi(q)\Delta'_q = \infty$ , then  $\text{meas}(\mathcal{A}) = 1$ .*

As Catlin noticed, his conjecture is a direct corollary of the one by Duffin and Schaeffer. Indeed, let us consider the set

$$\mathcal{A}' = \{x \in [0, 1] : |x - a/q| < \Delta'_q \text{ for infinitely many reduced fractions } a/q\}.$$

This is the set  $\mathcal{A}^*$  with the quantities  $\Delta_q$  replaced by  $\Delta'_q$ , so we may apply the Duffin–Schaeffer conjecture to it. In addition, it is straightforward to check that

$$(2.6) \quad \mathcal{A} \setminus \mathbb{Q} = \mathcal{A}' \setminus \mathbb{Q}$$

when  $\Delta_q \rightarrow 0$ . This settles Catlin’s conjecture in this case. On the other hand, if  $\Delta_q \not\rightarrow 0$ , then  $\mathcal{A} = [0, 1]$  and  $\sum_{q=1}^{\infty} \varphi(q)\Delta'_q = \infty$ , so that Catlin’s conjecture is trivially true.

Just like in Theorem 2.3 of Jarník and Besicovitch, it would be important to also have information about the Hausdorff dimension of the sets  $\mathcal{A}$  and  $\mathcal{A}^*$  in the case when they have null Lebesgue measure. In light of relation (2.6), it suffices to answer this question for the latter set. Beresnevich and Velani [4] proved the remarkable result that the Duffin–Schaeffer conjecture implies a Hausdorff measure version of itself. This is a consequence of a much more general *Mass Transference Principle* that they established, and which allows transferring information concerning the Lebesgue measure of certain lim sup sets to the Hausdorff measure of rescaled versions of them. As a corollary, they proved:

**Theorem 2.6** (Beresnevich–Velani (2006)). *Assume that the Duffin–Schaeffer conjecture is true. Let  $\Delta_1, \Delta_2, \dots \geq 0$  be such that  $\sum_{q=1}^{\infty} \varphi(q)\Delta_q < \infty$ . Then the Hausdorff dimension of the set  $\mathcal{A}^*$  defined by (2.4) equals the infimum of the set of  $s > 0$  such that  $\sum_{q=1}^{\infty} \varphi(q)\Delta_q^s < \infty$ .*

### 2.3. Progress towards the Duffin–Schaeffer conjecture

Since its introduction in 1941, the Duffin–Schaeffer conjecture has been the subject of intensive research activity, with various special cases proven over the years. This process came to a conclusion recently with the proof of the full conjecture [20].

**Theorem 2.7** (Koukoulopoulos–Maynard (2020)). *The Duffin–Schaeffer conjecture is true.*

We will outline the main ideas of the proof of Theorem 2.7 in §3. But first we give an account of the work that preceded it.

**Notation.** Given two functions  $f, g : X \rightarrow \mathbb{R}$ , we write  $f(x) \ll g(x)$  (or  $f(x) = O(g(x))$ ) for all  $x \in X$  to mean that there is a constant  $C$  such that  $|f(x)| \leq Cg(x)$  for all  $x \in Y$ .

In the same paper where they introduced their conjecture, Duffin and Schaeffer proved the first general case of it:

**Theorem 2.8** (Duffin–Schaeffer (1941)). *The Duffin–Schaeffer conjecture is true for all sequences  $(\Delta_q)_{q=1}^{\infty}$  such that*

$$(2.7) \quad \limsup_{Q \rightarrow \infty} \frac{\sum_{q \leq Q} \varphi(q)\Delta_q}{\sum_{q \leq Q} q\Delta_q} > 0.$$

To appreciate this result, we must make a few comments about condition (2.7). Note that its left-hand side is the average value of  $\varphi(q)/q$  over  $q \in [1, Q]$ , where  $q$  is weighted by  $w_q := q\Delta_q$ . In particular, we may restrict our attention to  $q$  with  $\Delta_q > 0$ . Now, we know

$$\frac{\varphi(q)}{q} = \prod_{p|q} \left(1 - \frac{1}{p}\right).$$

In particular,  $\varphi(q)/q \leq 1$ , and the only way this ratio can become much smaller than 1 is if  $q$  is divisible by lots of small primes. To see this, let us begin by observing that  $q$  can have at most  $\log q / \log 2$  prime factors in total. Therefore,

$$(2.8) \quad \prod_{p|q, p > \log q} \left(1 - \frac{1}{p}\right) \geq \left(1 - \frac{1}{\log q}\right)^{\log q / \log 2} \geq \frac{1}{5}$$

for  $q$  large enough. In addition, we have

$$(2.9) \quad \prod_{\substack{(\log q)^{0.01} < p \leq \log q \\ p|q}} \left(1 - \frac{1}{p}\right) \geq \prod_{(\log q)^{0.01} < p \leq \log q} \left(1 - \frac{1}{p}\right) \geq \frac{1}{200}$$

for  $q$  large enough by Mertens' estimate [19, Theorem 3.4]. Already the above inequalities show that only the primes  $\leq (\log q)^{0.01}$  can affect the size of  $\varphi(q)/q$ . But more is true:  $\varphi(q)/q$  is small only if  $q$  is divided by *many* primes  $\leq (\log q)^{0.01}$ . Imagine for example that

$$(2.10) \quad \#\{p|q : e^{j-1} < p \leq e^j\} \leq e^j/j^2 + 1000$$

for  $j = 1, 2, \dots, 1 + \lfloor 0.01 \log \log q \rfloor$ . We would then have

$$\prod_{\substack{e^{j-1} < p \leq e^j \\ p|q}} \left(1 - \frac{1}{p}\right) \geq \left(1 - \frac{1}{e^j}\right)^{e^j/j^2 + 1000} = \exp\left(-1/j^2 + O(e^{-j})\right).$$

Multiplying this over all  $j$ , we deduce that  $\varphi(q)/q \geq c$  for some  $c > 0$  independent of  $q$ .

We have thus proven that for (2.7) to fail, the main contribution to the weighted sum  $\sum_{q \leq Q} w_q$  with  $w_q = q\Delta_q$  must come from integers for which (2.10) fails. As a matter of fact, (2.10) must fail for lots of  $j$ 's. This is an extremely rare event if we choose  $q$  *uniformly at random* from  $[1, Q]$  (or even if we choose it uniformly at random from various “nice” subsets of  $[1, Q]$ , such as the primes, or the values of a monic polynomial with integer coefficients). A simple way to see this is to calculate the average value of the function  $\#\{p|q : e^{j-1} < p \leq e^j\}$  with respect to the uniform counting measure on  $[1, Q]$ . We have

$$\frac{1}{Q} \sum_{q \leq Q} \#\{p|q : e^{j-1} < p \leq e^j\} = \sum_{e^{j-1} < p \leq e^j} \frac{\#\{q \leq Q : p|q\}}{Q} \leq \sum_{e^{j-1} < p \leq e^j} \frac{1}{p} \ll \frac{1}{j}$$

by Mertens' theorem [19, Theorem 3.4]. This is *much* smaller than  $e^j/j^2$ , so (2.10) should fail rarely as  $j \rightarrow \infty$ . (For instance, we may use Markov's inequality to see this claim.)

In conclusion, Theorem 2.8 settles the Duffin–Schaeffer conjecture when  $\Delta_q$  is mainly supported on “normal” integers, without too many small prime factors. In particular, it implies a significant improvement of Theorems 1.3 and 1.4 for almost all  $x \in \mathbb{R}$ .

**Corollary 2.9.** *For almost all  $x \in \mathbb{R}$ , there are infinitely many reduced fractions  $a/p$  and  $b/q^2$  such that  $p$  is prime,  $|x - a/p| < p^{-2}$  and  $|x - b/q^2| < q^{-3}$ .*

The next important step towards the Duffin–Schaeffer conjecture is a remarkable *zero–one law* due to Gallagher [12].

**Theorem 2.10** (Gallagher (1961)). *If  $\mathcal{A}^*$  is as in (2.4), then  $\text{meas}(\mathcal{A}^*) \in \{0, 1\}$ .*

Gallagher's theorem says *grosso modo* that either we chose the quantities  $\Delta_q$  to be “too small” and thus missed almost all real numbers, or we chose them “sufficiently large” so that almost all

numbers have the desired rational approximations. The Duffin–Schaeffer conjecture is then the simplest possible criterion to decide in which case we are.

The proof of Theorem 2.10 is a clever adaptation of an ergodic-theoretic argument due to Cassels [6] in the simpler setting of non-reduced rational approximations. We give Cassel’s proof and refer the interested readers to [12, 14] for the proof of Theorem 2.10.

**Theorem 2.11** (Cassels (1950)). *If  $\mathcal{A}$  is as in (2.1), then  $\text{meas}(\mathcal{A}) \in \{0, 1\}$ .*

*Proof.* We need the following fact [14, Lemma 2.1] that uses Lebesgue’s Density Theorem: Let  $I_1, I_2, \dots, J_1, J_2, \dots$  be intervals of lengths tending to 0, and let  $c > 0$ . For all  $k$ , suppose  $J_k \subseteq I_k$  and  $\text{meas}(J_k) \geq c \text{meas}(I_k)$ . Then  $\text{meas}(\limsup_{k \rightarrow \infty} I_k \setminus \limsup_{k \rightarrow \infty} J_k) = 0$ .

Now, for each  $r \geq 1$ , let  $\mathcal{A}^{(r)}$  be defined as in (2.1) but with  $\Delta_q/r$  in place of  $\Delta_q$ . Hence,  $\text{meas}(\mathcal{A} \setminus \mathcal{A}^{(r)}) = 0$  by the above fact. Therefore, if  $\mathcal{A}^{(\infty)} := \bigcap_{n=1}^{\infty} \mathcal{A}^{(n)}$ , then  $\text{meas}(\mathcal{A} \setminus \mathcal{A}^{(\infty)}) = 0$ . Now, consider the map  $\psi : [0, 1] \rightarrow [0, 1]$  defined by  $\psi(x) := \{2x\}$ , and note that  $\psi(\mathcal{A}^{(\infty)}) \subseteq \mathcal{A}^{(\infty)}$ . In particular,  $\frac{1}{N} \sum_{n=0}^{N-1} 1_{\mathcal{A}^{(\infty)}}(\psi^n(x)) = 1$  for all  $x \in \mathcal{A}^{(\infty)}$  and all  $N \in \mathbb{N}$ . Since  $\psi$  is ergodic with respect to the Lebesgue measure [26, p. 293 & 305–6], Birkhoff’s Ergodic Theorem [26, Ch. 6, Cor. 5.6] implies that  $\text{meas}(\mathcal{A}^{(\infty)}) \in \{0, 1\}$ .  $\square$

The first significant step towards establishing the Duffin–Schaeffer conjecture for irregular sequences  $\Delta_q$ , potentially supported on integers with lots of small prime factors, was carried out by Erdős [10] and Vaaler [27].

**Theorem 2.12** (Erdős (1970) – Vaaler (1978)). *The Duffin–Schaeffer conjecture is true for all sequences  $(\Delta_q)_{q=1}^{\infty}$  such that  $\Delta_q = O(1/q^2)$  for all  $q$ .*

This theorem is of course most interesting when  $\sum_{q=1}^{\infty} \varphi(q)\Delta_q = \infty$ . Since  $\Delta_q = O(1/q^2)$  and  $\varphi(q) \leq q$ , we find  $\sum_{q \in \mathcal{S}} 1/q = \infty$  with  $\mathcal{S} = \{q : \Delta_q > 0\}$ . In particular,  $\mathcal{S}$  must be somewhat dense in  $\mathbb{N}$ . Therefore, Theorem 2.12 has the advantage over Theorem 2.8 that  $\mathcal{S}$  can contain many irregular integers, and the disadvantage that it has to be quite dense.

The Duffin–Schaeffer conjecture has a natural analogue in  $\mathbb{R}^k$  with  $k \geq 2$ : given  $\Delta_1, \Delta_2, \dots \geq 0$ , let  $\mathcal{A}^*(k)$  be the set of  $\vec{x} = (x_1, \dots, x_k) \in \mathbb{R}^k$  for which there are infinitely many  $k$ -tuples  $(a_1/q, \dots, a_k/q)$  of reduced fractions with  $|x_j - a_j/q| < \Delta_q$  for all  $j$ . Then  $\mathcal{A}^*(k)$  should contain almost no or almost all  $\vec{x} \in \mathbb{R}^k$ , according to whether the series  $\sum_{q=1}^{\infty} (\varphi(q)\Delta_q)^k$  converges or diverges. This was proven by Pollington and Vaughan [22].

**Theorem 2.13** (Pollington–Vaughan (1990)). *The  $k$ -dimensional Duffin–Schaeffer conjecture is true for all  $k \geq 2$ .*

Following this result, a lot of research focused on proving the Duffin–Schaeffer conjecture when the series  $\sum_{q=1}^{\infty} \varphi(q)\Delta_q$  diverges fast enough (see, e.g., [14, Theorem 3.7(iii)], [15, 3]). Aistleitner, Lachmann, Munsch, Technau and Zafeiropoulos [2] proved the Duffin–Schaeffer conjecture when  $\sum_{q=1}^{\infty} \varphi(q)\Delta_q/(\log q)^\varepsilon = \infty$  for some  $\varepsilon > 0$ . A report by Aistleitner [1], announced at the same time as [20], explains how to replace  $(\log q)^\varepsilon$  by  $(\log \log q)^\varepsilon$ .

### 3. THE MAIN INGREDIENTS OF THE PROOF OF THE DUFFIN–SCHAEFFER CONJECTURE

#### 3.1. Borel–Cantelli without independence

Recall the definition of the sets  $\mathcal{A}_q^*$  in (2.5). Let us assume that  $\Delta_q \leq 1/(2q)$  for all  $q$  (cf. (2.3)) so that  $\text{meas}(\mathcal{A}_q^*) = 2\varphi(q)\Delta_q \in [0, 1]$ , and let us also suppose that  $\sum_{q=1}^{\infty} \varphi(q)\Delta_q = \infty$ . The first

technical difficulty we must deal with is how to prove an analogue of the second Borel–Cantelli lemma (cf. Theorem 2.4(b)) without assuming that the events  $\mathcal{A}_q^*$  are independent. We follow an idea due to Turan, which is already present in [8].

By Gallagher’s zero–one law, it is enough to show that  $\text{meas}(\mathcal{A}^*) > 0$ . Since  $\bigcup_{q \geq Q} \mathcal{A}_q^* \searrow \mathcal{A}^*$ , we may equivalently prove that there is some constant  $c > 0$  such that  $\text{meas}(\bigcup_{q \geq Q} \mathcal{A}_q^*) \geq c$  for all large  $Q$ . In order to limit the potential overlap among the sets  $\mathcal{A}_q^*$ , we only consider an appropriate subset of them. Since  $\text{meas}(\mathcal{A}_q^*) = 2\varphi(q)\Delta_q \in [0, 1]$  for all  $q$ , and since  $\sum_{q \geq Q} \varphi(q)\Delta_q = \infty$ , there must exist some  $R \geq Q$  such that

$$(3.1) \quad 1 \leq \sum_{q \in [Q, R]} \text{meas}(\mathcal{A}_q^*) \leq 2.$$

We will only use the events  $\mathcal{A}_q^*$  with  $q \in [Q, R]$ . We trivially have the union bound

$$\text{meas} \left( \bigcup_{q \in [Q, R]} \mathcal{A}_q^* \right) \leq \sum_{q \in [Q, R]} \text{meas}(\mathcal{A}_q^*) \leq 2.$$

If we can show that the sets  $\mathcal{A}_q^*$  with  $q \in [Q, R]$  do not overlap too much, so that

$$(3.2) \quad \text{meas} \left( \bigcup_{q \in [Q, R]} \mathcal{A}_q^* \right) \geq c \sum_{q \in [Q, R]} \text{meas}(\mathcal{A}_q^*) \geq c,$$

we will be able to deduce that  $\text{meas}(\bigcup_{q \in [Q, R]} \mathcal{A}_q^*) \geq c$  and *a fortiori* that  $\text{meas}(\bigcup_{q \geq Q} \mathcal{A}_q^*) \geq c$ . As the following lemma shows, (3.2) is true under (3.1) as long as we can control the correlations of the events  $\mathcal{A}_q^*$  on average.

**Lemma 3.1.** *Let  $E_1, \dots, E_k$  be events in the probability space  $(\Omega, \mathcal{F}, \mathbb{P})$ . We then have that*

$$\mathbb{P} \left( \bigcup_{j=1}^k E_j \right) \geq \frac{(\sum_{j=1}^k \mathbb{P}(E_j))^2}{\sum_{i,j=1}^k \mathbb{P}(E_i \cap E_j)}.$$

*Proof.* Let  $N = \sum_j 1_{E_j}$ . We then have  $\mathbb{E}[N] = \sum_j \mathbb{P}(E_j)$ . On the other hand, the Cauchy–Schwarz inequality implies that

$$\mathbb{E}[N]^2 = \mathbb{E}[1_{N>0} \cdot N]^2 \leq \mathbb{P}(\text{supp}(N)) \cdot \mathbb{E}[N^2].$$

Since  $\text{supp}(N) = \bigcup_j E_j$  and  $N^2 = \sum_{i,j} 1_{E_i \cap E_j}$ , the lemma follows.  $\square$

The following proposition summarizes the discussion of this section.

**Proposition 3.2.** *Let  $\Delta_1, \Delta_2, \dots \geq 0$ , and let  $\mathcal{A}_q^*$  be as in (2.5).*

(a) *If  $C > 0$  and  $R \geq Q \geq 1$  are such that*

$$(3.3) \quad 1 \leq \sum_{q \in [Q, R]} \text{meas}(\mathcal{A}_q^*) \leq 2 \quad \text{and} \quad \sum_{Q \leq q < r \leq R} \text{meas}(\mathcal{A}_q^* \cap \mathcal{A}_r^*) \leq C,$$

*then  $\text{meas}(\bigcup_{q \in [Q, R]} \mathcal{A}_q^*) \geq 1/(2 + 2C)$ .*

(b) *If there are infinitely many disjoint intervals  $[Q, R]$  satisfying (3.3) with the same constant  $C > 0$ , then  $\text{meas}(\limsup_{q \rightarrow \infty} \mathcal{A}_q^*) = 1$ .*

### 3.2. A bound on the pairwise correlations

As per Proposition 3.2, we need to control the correlations of the events  $\mathcal{A}_q^*$ . To this end, we have a lemma of Pollington–Vaughan [22] (see also [10, 27]).

**Lemma 3.3.** *Let  $q, r$  be two distinct integers  $\geq 2$ , let  $\Delta_q, \Delta_r \geq 0$ , let  $\mathcal{A}_q^*, \mathcal{A}_r^*$  be as in (2.5), and let  $M(q, r) = 2 \max\{\Delta_q, \Delta_r\} \text{lcm}[q, r]$ . If  $M(q, r) \leq 1$ , then  $\mathcal{A}_q^* \cap \mathcal{A}_r^* = \emptyset$ . Otherwise,*

$$\text{meas}(\mathcal{A}_q^* \cap \mathcal{A}_r^*) \ll \varphi(q)\Delta_q \cdot \varphi(r)\Delta_r \cdot \exp\left(\sum_{\substack{p|qr/\text{gcd}(q,r)^2 \\ p > M(q,r)}} \frac{1}{p}\right).$$

*Proof.* Let  $\Delta = \max\{\Delta_q, \Delta_r\}$ ,  $\delta = \min\{\Delta_q, \Delta_r\}$  and  $M = M(q, r)$ . The intervals  $I_a = (\frac{a}{q} - \Delta_q, \frac{a}{q} + \Delta_q)$  and  $J_b = (\frac{b}{r} - \Delta_r, \frac{b}{r} + \Delta_r)$  intersect only if  $2\Delta > |\frac{a}{q} - \frac{b}{r}|$ . Since the right-hand side is  $\geq 1/\text{lcm}[q, r]$  when  $\text{gcd}(a, q) = \text{gcd}(b, r) = 1$ , we infer that  $\mathcal{A}_q^* \cap \mathcal{A}_r^* = \emptyset$  if  $M \leq 1$ .

Now, assume that  $M > 1$ . Since  $\text{meas}(I_a \cap J_b) \leq 2\delta$  for all  $a, b$ , we have

$$\text{meas}(\mathcal{A}_q^* \cap \mathcal{A}_r^*) \leq 2\delta \cdot \#\left\{ \begin{array}{l} 1 \leq a \leq q, \quad \text{gcd}(a, q) = 1 \\ 1 \leq b \leq r, \quad \text{gcd}(b, r) = 1 \end{array} : \left| \frac{a}{q} - \frac{b}{r} \right| < 2\Delta \right\}.$$

Let  $a/q - b/r = m/\text{lcm}[q, r]$ . Then  $1 \leq |m| \leq M$  and  $\text{gcd}(m, q_1 r_1) = 1$ , where  $q_1 = q/d$  and  $r_1 = r/d$  with  $d = \text{gcd}(q, r)$ . For each such  $m$ , a straightforward application of the Chinese Remainder Theorem gives that the number of admissible pairs  $(a, b)$  is

$$\leq d \prod_{p|\text{gcd}(d, q_1 r_1 m)} \left(1 - \frac{1}{p}\right) \prod_{p|d, p \nmid q_1 r_1 m} \left(1 - \frac{2}{p}\right) \leq d \frac{\prod_{p|d} (1 - \frac{1}{p})^2}{\prod_{p|\text{gcd}(d, q_1 r_1)} (1 - \frac{1}{p})} \cdot \frac{|m|}{\varphi(|m|)},$$

where we used that  $1 - 2/p \leq (1 - 1/p)^2$ . We then sum this inequality over  $m$  and use Lemma 3.4 below to complete the proof. (For full details, see [22] or [14, Lemma 2.8].)  $\square$

**Lemma 3.4.** *Fix  $C \geq 1$ , and let  $(a_p)_{p \text{ prime}}$  be a sequence taking values in  $[0, C]$ . Then*

$$\sum_{n \leq x} \prod_{p|n} a_p \ll_C x \exp\left(\sum_{p \leq x} \frac{a_p - 1}{p}\right) \quad \text{for all } x \geq 1.$$

*Proof.* See Theorem 14.2 in [19].  $\square$

### 3.3. Generalizing the Erdős–Vaaler argument

The next step is to study averages of  $\exp(\sum_{p|qr/\text{gcd}(q,r)^2, p > M(q,r)} 1/p)$ . This gets a bit too technical in general, so we focus on the following special case:

**Theorem 3.5.** *Let  $Q \geq N \geq 2$ , and let  $\mathcal{S} \subseteq \{Q \leq q \leq 2Q : q \text{ square-free}\}$  be such that*

$$(3.4) \quad N/2 \leq \sum_{q \in \mathcal{S}} \frac{\varphi(q)}{q} \leq N.$$

*We then have*

$$(3.5) \quad \sum_{q, r \in \mathcal{S}} \frac{\varphi(q)\varphi(r)}{qr} \exp\left(\sum_{\substack{p|qr/\text{gcd}(q,r)^2 \\ p > Q/[N \text{gcd}(q,r)]}} \frac{1}{p}\right) \ll N^2.$$

*In particular, if  $\mathcal{A}_q^*$  is as in (2.5) with  $\Delta_q = 1/(qN)$ , then  $\text{meas}(\bigcup_{q \in \mathcal{S}} \mathcal{A}_q^*) \gg 1$ .*

**Remark.** To see the last assertion, recall the notation  $M(q, r) = 2 \max\{\Delta_q, \Delta_r\} \text{lcm}[q, r]$  from Lemma 3.3. By the assumptions of the theorem, we have  $M(q, r) \geq 2Q/[N \gcd(q, r)]$  for  $q, r \in \mathcal{S}$ . Hence, if (3.5) holds, then  $\sum_{q, r \in \mathcal{S}} \text{meas}(\mathcal{A}_q^* \cap \mathcal{A}_r^*) \ll 1$  by Lemma 3.3. We may then apply Proposition 3.2 to deduce that  $\text{meas}(\bigcup_{q \in \mathcal{S}} \mathcal{A}_q^*) \gg 1$ .

When  $N \gg Q$ , Theorem 3.5 follows from the work of Erdős and Vaaler (Theorem 2.12), but when  $N = o(Q)$  it was not known prior to [20] in this generality. The proof begins by adapting the Erdős–Vaaler argument to this more general set-up.

First, we must control the sum over primes in (3.5). Using (2.10) turns out to be too crude, so we modify our approach. Let  $t_j = \exp(2^j)$  and  $j_0$  be such that  $\sum_{t < p \leq t^2} 1/p \leq 1$  for  $t \geq t_{j_0}$  ( $j_0$  exists by Mertens' theorems [19, Theorem 3.4].) Moreover, let

$$\mathcal{L}(q, r) = \sum_{\substack{p|qr/\gcd(q,r)^2 \\ p > Q/[N \gcd(q,r)]}} \frac{1}{p}, \quad \lambda_t(q) = \sum_{\substack{p|q \\ p > t}} \frac{1}{p}, \quad L_t(q, r) = \sum_{\substack{p|qr/\gcd(q,r)^2 \\ p > t}} \frac{1}{p}.$$

If  $L_{t_{j_0}}(q, r) \leq 101$ , then obviously  $\mathcal{L}(q, r) \ll 1$ . Otherwise, there is an integer  $j \geq j_0$  such that  $L_{t_j}(q, r) > 101 \geq L_{t_{j+1}}(q, r)$ . Since  $j \geq j_0$ , we then also have  $L_{t_{j+1}}(q, r) > 100$ . Now, note that if  $Q/[N \gcd(q, r)] \geq t_{j+1}$ , then  $\mathcal{L}(q, r) \leq L_{t_{j+1}}(q, r) \leq 101$ .

To sum up,  $\mathcal{L}(q, r) \ll 1$ , unless  $(q, r) \in \mathcal{B}_{t_{j+1}}$  for some  $j \geq j_0$ , where

$$\mathcal{B}_t := \{(q, r) \in \mathcal{S} \times \mathcal{S} : \gcd(q, r) > Q/(Nt), L_t(q, r) > 100\}.$$

We study the contribution of such pairs to the left-hand side of (3.5): if  $(q, r) \in \mathcal{B}_{t_{j+1}}$ , then

$$\mathcal{L}(q, r) \leq 101 + \sum_{p \leq t_{j+1}} \frac{1}{p} \leq \log \log t_{j+1} + O(1) = j \log 2 + O(1)$$

by Mertens' estimate. In conclusion, Theorem 3.5 will follow if we can show that

$$(3.6) \quad \sum_{(q,r) \in \mathcal{B}_t} \frac{\varphi(q)\varphi(r)}{qr} \ll \frac{N^2}{t} \quad \text{for all } t \geq t_{j_0+1}.$$

Now, let us consider the special case when  $N \gg Q$ , which corresponds to the Erdős–Vaaler theorem. The inequality  $\gcd(q, r) > Q/(Nt)$  is then basically trivially, so we must prove (3.6) by exploiting the condition  $L_t(q, r) > 100$ . Indeed, writing  $d = \gcd(q, r)$ ,  $q = dq_1$  and  $r = dr_1$ , we find that  $\lambda_t(q_1) > 50$  or  $\lambda_t(r_1) > 50$ . By symmetry, we have

$$\#\mathcal{B}_t \leq 2 \sum_{d \leq 2Q} \#\{r_1 \leq 2Q/d\} \cdot \#\{q_1 \leq 2Q/d : \lambda_t(q_1) > 50\}.$$

The number of  $r_1$ 's is of course  $\leq 2Q/d$ . Moreover, using Chernoff's inequality and Lemma 3.4 with  $a_p = \exp(1_{p>t} \cdot t/p)$ , we find that

$$\#\{q_1 \leq 2Q/d : \lambda_t(q_1) > 50\} \leq \sum_{q_1 \leq 2Q/d} \exp(-50t + t\lambda_t(p)) \ll e^{-50t} Q/d.$$

Putting everything together, we conclude that

$$(3.7) \quad \#\mathcal{B}_t \ll e^{-t} Q^2 \quad \text{for all } t \geq 1.$$

In particular, (3.6) holds, thus proving Theorem 3.5 when  $N \gg Q$ .

On the other hand, if  $N = o(Q)$ , the condition that  $\gcd(q, r) > Q/(Nt)$  for all  $(q, r) \in \mathcal{B}_t$  is non-trivial and we must understand it and exploit it to prove Theorem 3.5. Indeed, if we treat the

weights  $\varphi(q)/q$  as roughly constant in (3.4), we see that  $\mathcal{S}$  contains about  $N$  integers from  $[Q, 2Q]$ , i.e., it is a rather sparse set. On the other hand, if  $t$  is not too large, then (3.7) gives no savings compared to the trivial upper bound  $\#\mathcal{B}_t \leq \#\mathcal{S}^2 \approx N^2$ .

Since the condition that  $L_t(q, r) > 100$  is insufficient, let us ignore it temporarily and focus on the condition that  $\gcd(q, r) > Q/(Nt)$  for all  $(q, r) \in \mathcal{B}_t$ . There is an obvious way in which this condition can be satisfied for many pairs  $(q, r) \in \mathcal{S} \times \mathcal{S}$ : if there is some *fixed* integer  $d > Q/(Nt)$  that divides a large proportion of integers in  $\mathcal{S}$ . Notice that the number of total multiples of  $d$  in  $[Q, 2Q]$  is about  $Q/d < t \cdot N$ , which is compatible with (3.4). We thus arrive at the following key question:

**Model Problem.** *Let  $D \geq 1$  and  $\delta \in (0, 1]$ , and let  $\mathcal{S} \subseteq [Q, 2Q] \cap \mathbb{Z}$  be a set of  $\gg \delta Q/D$  elements such that there are  $\geq \delta \#\mathcal{S}^2$  pairs  $(q, r) \in \mathcal{S} \times \mathcal{S}$  with  $\gcd(q, r) > D$ . Must there be an integer  $d > D$  that divides  $\gg \delta^{100} Q/D$  elements of  $\mathcal{S}$ ?*

It turns out that the answer to the Model Problem as stated is no. However, a technical variant of it is true, that takes into account the weights  $\varphi(q)/q$  in (3.4) and (3.6), and that is asymmetric in  $q$  and  $r$ . We shall explain this in the next section.

For now, let us assume that the Model Problem as stated has an affirmative answer, and let us see how this yields Theorem 3.5. Suppose (3.6) fails for some  $t$ . By the Model Problem, there must exist an integer  $d > Q/(Nt)$  dividing  $\gg t^{-100} \#\mathcal{S}$  members of  $\mathcal{S}$ . We might then also expect that  $\#\mathcal{B}_t \gg t^{-200} \#\{(dm, dn) \in \mathcal{B}_t : m, n \geq 1\}$ . But note that if  $(q, r) = (dm, dn) \in \mathcal{B}_t$ , then  $m, n \leq 2Q/d < 2tN$  and  $qr/\gcd(q, r)^2 = mn/\gcd(m, n)^2$ . In particular,  $L_t(m, n) > 100$ , so the argument leading to (3.7) implies that the number of  $(dm, dn) \in \mathcal{B}_t$  is  $\ll e^{-t} t^2 N^2$ . Hence,  $\mathcal{B}_t \ll e^{-t} t^{202} N^2 \ll N^2/t$ , as needed.

### 3.4. An iterative compression algorithm

To attack the Model Problem, we view it as a question in graph theory: consider the graph  $G$ , with vertex set  $\mathcal{S}$  and edge set  $\mathcal{B}_t$ . If the edge density of  $G$  is  $\geq 1/t$ , must there exist a dense subgraph  $G'$  all of whose vertices are divisible by an integer  $> Q/(Nt)$ ?

To locate this “structured” subgraph  $G'$ , we use an iterative “compression” argument, roughly inspired by the papers of Erdős-Ko-Rado [11] and Dyson [9]. With each iteration, we pass to a smaller set of vertices, where we have additional information about which primes divide them. Of course, we must ensure that we end up with a sizeable graph. We do this by judiciously choosing the new graph at each step so that it has at least as many edges as what the qualitative parameters of the old graph might naively suggest. This way the new graph will have improved “structure” and “quality”. When the algorithm terminates, we will end up with a fully structured subset of  $\mathcal{S}$ , where we know that all large GCDs are due to a large fixed common factor. This will then allow us to exploit the condition that  $L_t(q, r) > 100$  for all edges  $(q, r)$ . Importantly, our algorithm will also control the set  $\mathcal{B}_t$  in terms of the terminal edge set. Hence the savings from the condition  $L_t(q, r) > 100$  in the terminal graph will be transferred to  $\mathcal{B}_t$ , establishing (3.6).

One technical complication is that the iterative algorithm necessitates to view  $G$  as a bipartite graph. In addition, it is important to use the weights  $\varphi(q)/q$ . We thus set

$$\mu(\mathcal{V}) = \sum_{v \in \mathcal{V}} \frac{\varphi(v)}{v} \quad \text{for } \mathcal{V} \subset \mathbb{N}; \quad \mu(\mathcal{E}) = \sum_{(v,w) \in \mathcal{E}} \frac{\varphi(v)\varphi(w)}{vw} \quad \text{for } \mathcal{E} \subset \mathbb{N}^2.$$

Let us now explain the algorithm in more detail. We set  $\mathcal{V}_0 = \mathcal{W}_0 = \mathcal{S}$  and construct two decreasing sequences of sets  $\mathcal{V}_0 \supseteq \mathcal{V}_1 \supseteq \mathcal{V}_2 \supseteq \dots$  and  $\mathcal{W}_0 \supseteq \mathcal{W}_1 \supseteq \mathcal{W}_2 \supseteq \dots$ , as well as a sequence of distinct primes  $p_1, p_2, \dots$  such that either  $p_j$  divides all elements of  $\mathcal{V}_j$ , or it is coprime to all elements of  $\mathcal{V}_j$  (and similarly with  $\mathcal{W}_j$ ). Since  $\mathcal{S}$  consists solely of square-free integers, there are integers  $a_j, b_j$  dividing  $p_1 \cdots p_j$ , and such that  $\gcd(v, p_1 \cdots p_j) = a_j$  and  $\gcd(w, p_1 \cdots p_j) = b_j$  for all  $v \in \mathcal{V}_j$  and all  $w \in \mathcal{W}_j$ .

Assume we have constructed  $\mathcal{V}_i, \mathcal{W}_i, p_i$  as above for  $i = 1, \dots, j$ . Let  $\mathcal{E}_i = \mathcal{B}_t \cap (\mathcal{V}_i \times \mathcal{W}_i)$  be the edge sets. We then pick a new prime  $p_{j+1}$  that occurs as common factor of  $\gcd(v, w)$  for at least one edge  $(v, w) \in \mathcal{E}_j$ . (If there is no such prime, the algorithm terminates.) Then, we pick  $\mathcal{V}_{j+1}$  to be either  $\mathcal{V}_j^{(1)} := \{v \in \mathcal{V}_j : p_{j+1} | v\}$  or  $\mathcal{V}_j^{(0)} := \{v \in \mathcal{V}_j : p_{j+1} \nmid v\}$  (and similarly with  $\mathcal{W}_{j+1}$ ). Deciding how to make this choice is the most crucial part of the proof and we will analyze it in more detail below. At any rate, it is clear that after a finite number of steps, this process will terminate. We will thus arrive at sets of vertices  $\mathcal{V}_J$  and  $\mathcal{W}_J$  where  $a = a_J$  divides all elements of  $\mathcal{V}_J$ ,  $b = b_J$  divides all elements of  $\mathcal{W}_J$ , and  $\gcd(v, w) = \gcd(a, b)$  for all edges  $(v, w) \in \mathcal{E}_J \subseteq \mathcal{B}_t$ . In particular,  $\gcd(a, b) > Q/(Nt)$ , as long as  $\mathcal{E}_J \neq \emptyset$ . We have thus found our fixed large common divisor, so that we can use the Erdős–Vaaler argument as in §3.3 to control the size of  $\mathcal{E}_J$ . If we can ensure that  $\mathcal{E}_J$  is a large enough portion of  $\mathcal{E}_0 = \mathcal{B}_t$ , we will have completed the proof.

Let us now explain how to make the choice of which subgraph to focus on each time. Let  $G_j = (\mathcal{V}_j, \mathcal{W}_j, \mathcal{E}_j)$  be the bipartite graph at the  $j$ -iteration. Because we will use an unbounded number of iterations, it is important to ensure that  $G_{j+1}$  has more edges than “what the qualitative parameters of  $G_j$  would typically predict”. One way to assign meaning to this vague phrase is to use the edge density  $\#\mathcal{E}_j / (\#\mathcal{V}_j \#\mathcal{W}_j)$ . Actually, in our case, we should use the weighted density

$$\delta_j = \frac{\mu(\mathcal{E}_j)}{\mu(\mathcal{V}_j)\mu(\mathcal{W}_j)}.$$

Naively, we might guess that  $\mu(\mathcal{E}_{j+1}) \approx \delta_j \mu(\mathcal{V}_{j+1}) \mu(\mathcal{W}_{j+1})$ , meaning that  $\delta_{j+1} \approx \delta_j$ . So we might try to choose  $G_{j+1}$  so that  $\delta_{j+1} \geq \delta_j$ . This would be analogous to Roth’s “density increment” strategy [23, 24]. Unfortunately, such an argument loses all control over the size of  $\mathcal{E}_j$ , so we cannot use information on  $\mathcal{E}_J$  to control  $\mathcal{E}_0 = \mathcal{B}_t$  (which is our end goal).

In a completely different direction, we can use the special GCD structure of our graphs to come up with another “measure of quality” of our new graph compared to the old one. Recall the integers  $a_{j+1}$  and  $b_{j+1}$ . We then have

$$(3.8) \quad \#\mathcal{E}_j \leq \#\left\{m \leq \frac{2Q}{a_j}, n \leq \frac{2Q}{b_j} : \gcd(m, n) > \frac{Q/(Nt)}{\gcd(a_j, b_j)}\right\}.$$

If all pairs  $(m, n)$  on the right-hand side of (3.8) were due to a fixed divisor of size  $> [Q/(Nt)] / \gcd(a_j, b_j)$ , then we would conclude that

$$\#\mathcal{E}_j \ll t^2 N^2 \cdot \frac{\gcd(a_j, b_j)^2}{a_j b_j}.$$

Actually, Green and Walker [13] proved recently that this bound is true, even without the presence of a universal divisor. So it makes sense to consider the quantity  $\#\mathcal{E}_j \cdot a_j b_j / \gcd(a_j, b_j)^2$  as a qualitative measure of  $G_j$ . As a matter of fact, since we are weighing  $v$  with  $\varphi(v)/v$ , and we have  $\varphi(v)/v \leq \varphi(a_j)/a_j$  whenever  $a_j | v$ , we may even consider

$$\lambda_j := \frac{a_j b_j}{\gcd(a_j, b_j)^2} \cdot \frac{a_j b_j}{\varphi(a_j)\varphi(b_j)} \cdot \mu(\mathcal{E}_j).$$

Let us see a different argument for why this quantity might be a good choice, by studying the effect of each prime  $p \in \{p_1, \dots, p_j\}$  to the parameters  $Q/a_j$ ,  $Q/b_j$  and  $[Q/(Nt)]/\gcd(a_j, b_j)$  that control the size of  $m$ ,  $n$ , and  $\gcd(m, n)$ , respectively, in (3.8):

- *Case 1:*  $p|a_j$  and  $p|b_j$ . Then  $p$  reduces the upper bounds on the size of both  $m$  and  $n$  by a factor  $1/p$ . On the other hand, it also reduces the lower bound on their GCD (that affects both  $m$  and  $n$ ) by  $1/p$ . Hence, we are in a balanced situation.
- *Case 2:*  $p \nmid a_j$  and  $p \nmid b_j$ . In this case,  $p$  affects no parameters.
- *Case 3:*  $p|a_j$  and  $p \nmid b_j$ . Then  $p$  reduces the upper bound on  $m$  by a factor  $1/p$ , but it does not affect the bound on  $n$  nor on  $\gcd(m, n)$ . This is an advantageous situation, gaining us a factor of  $p$  compared to what we had. Accordingly,  $\lambda_j$  is multiplied by  $p$  in this case. This gain allows us to afford a big loss of vertices when falling in this “asymmetric” case (a proportion of  $1 - O(1/p)$ ).
- *Case 4:*  $p \nmid a_j$  and  $p|b_j$ . Then we gain a factor of  $p$  as in the previous case.

Iteratively increasing  $\lambda_j$  would be adequate for showing (3.6), by mimicking the Erdős–Vaaler argument from §3.3. Unfortunately it is not possible to guarantee that  $\lambda_j$  increases at each stage because it is not sensitive enough to the edge density, and so this proposal also fails. However, we will show that (a small variation of ) the hybrid quantity

$$(3.9) \quad q_j := \delta_j^9 \lambda_j,$$

can be made to increase at each step, while keeping track of the sizes of the vertex sets. We call  $q_j$  the *quality* of  $G_j$ .

Let us now discuss how we might carry out the “quality increment” strategy. Given  $\mathcal{V}_j$  and  $p_{j+1}$ , we wish to set  $\mathcal{V}_{j+1} = \mathcal{V}_j^{(k)}$  and  $\mathcal{W}_{j+1} = \mathcal{W}_j^{(\ell)}$  for some  $k, \ell \in \{0, 1\}$ . Let us call  $G_j^{(k, \ell)}$  each of the four potential choices for  $G_{j+1}$ . For their quality  $q_j^{(k, \ell)}$ , we have:

$$\begin{aligned} \frac{q_j^{(1,1)}}{q_j} &= \left(\frac{\delta_j^{(1,1)}}{\delta_j}\right)^{10} \alpha\beta \left(1 - \frac{1}{p}\right)^{-2}, & \frac{q_j^{(1,0)}}{q_j} &= \left(\frac{\delta_j^{(1,0)}}{\delta_j}\right)^{10} \alpha(1 - \beta)p \left(1 - \frac{1}{p}\right)^{-1}, \\ \frac{q_j^{(0,1)}}{q_j} &= \left(\frac{\delta_j^{(0,1)}}{\delta_j}\right)^{10} (1 - \alpha)\beta p \left(1 - \frac{1}{p}\right)^{-1}, & \frac{q_j^{(0,0)}}{q_j} &= \left(\frac{\delta_j^{(0,0)}}{\delta_j}\right)^{10} (1 - \alpha)(1 - \beta), \end{aligned}$$

where  $\delta_j^{(k, \ell)}$  is the edge density of  $G_j^{(k, \ell)}$ ,  $\alpha = \mu(\mathcal{V}_j^{(1)})/\mu(\mathcal{V}_j)$  is the proportion of vertices in  $\mathcal{V}_j$  that are divisible by  $p_{j+1}$ , and similarly  $\beta = \mu(\mathcal{W}_j^{(1)})/\mu(\mathcal{W}_j)$ . In addition, we have

$$\delta_j^{(1,1)}\alpha\beta + \delta_j^{(1,0)}\alpha(1 - \beta) + \delta_j^{(0,1)}(1 - \alpha)\beta + \delta_j^{(0,0)}(1 - \alpha)(1 - \beta) = \delta_j,$$

so that if one of the  $\delta_j^{(k, \ell)}$ 's is smaller than  $\delta$ , some other must be larger. Such an unbalanced situation is advantageous, so let us assume that  $\delta_j^{(k, \ell)} \sim \delta_j$  for all  $k, \ell$ .

Notice that we have an extra factor  $p$  in the asymmetric cases (0, 1) and (1, 0). We can then easily obtain a quality increment in one of these two cases, unless  $\alpha, \beta \ll 1/p$ , or if  $\alpha, \beta \geq 1 - O(1/p)$ . It turns out that the former case can be treated with a trick. So, the real difficulty is to obtain a quality increment when  $\alpha, \beta$  are both close to 1. As a matter of fact, the critical case is when  $\alpha, \beta \sim 1 - 1/p$ . Indeed, we then have  $q_j^{(k, \ell)} \sim 1$  in all four cases, so we maintain a constant quality no matter which subgraph we choose to focus on.

It is important to remark here that the factor  $(1 - 1/p)^{-2}$  in the case  $(k, \ell) = (1, 1)$  is essential (the factors  $(1 - 1/p)^{-1}$  in the asymmetric cases are less important as it turns out). Without this extra factor, we would not have been able to guarantee that the quality stays at least as big as  $q_j$ . Crucially, this factor originates from the weights  $\varphi(v)/v$  of the vertices that are naturally built in the Duffin–Schaeffer conjecture and that dampen down contributions from integers with too many prime divisors.

We conclude this discussion by going back to the Model Problem. We mentioned in §3.3 that this problem is false. The reason is a counterexample due to Sam Chow, a square-free version of which is given by  $\mathcal{S} = \{P/j : j|P, x/2 \leq j \leq x\}$  with  $P = \prod_{p \leq x} p$ . Indeed, all pairwise GCDs here are  $\geq P/x^2$ , but there is no fixed integer of size  $\gg P/x^2$  dividing a positive proportion of elements of this set. In addition, note that if  $p \leq x/\log x$ , then the proportion of  $\mathcal{S}$  divisible by  $p$  is  $\sim 1 - 1/p$ , just like in the critical case discussed above.

### 3.5. The quality increment argument

We now discuss the formal details of our iterative algorithm. We must first set up some notation. We say that  $G = (\mathcal{V}, \mathcal{W}, \mathcal{E}, \mathcal{P}, a, b)$  is a *square-free GCD graph* if:

- $\mathcal{V}$  and  $\mathcal{W}$  are non-empty, finite sets of square-free integers;
- $(\mathcal{V}, \mathcal{W}, \mathcal{E})$  is a bipartite graph, meaning that  $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{W}$ ;
- $\mathcal{P}$  is a finite set of primes, and  $a$  and  $b$  divide  $\prod_{p \in \mathcal{P}} p$ ;
- $a|v$  and  $b|w$  for all  $(v, w) \in \mathcal{V} \times \mathcal{W}$ ;
- if  $(v, w) \in \mathcal{E}$  and  $p \in \mathcal{P}$ , then  $p | \gcd(v, w)$  precisely when  $p | \gcd(a, b)$ .

We shall refer to  $(\mathcal{P}, a, b)$  as the *multiplicative data* of  $G$ . Furthermore, we defined the *edge density* of  $G$  by  $\delta(G) := \frac{\mu(\mathcal{E})}{\mu(\mathcal{V})\mu(\mathcal{W})}$ , and its *quality* by

$$q(G) := \delta(G)^9 \cdot \mu(\mathcal{E}) \cdot \frac{ab}{\gcd(a, b)^2} \cdot \frac{ab}{\varphi(ab)} \cdot \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^{3/2}}\right)^{-10}.$$

In addition, we define the set of “remaining large primes” of  $G$  by

$$\mathcal{R}(G) := \{p \notin \mathcal{P} : p > 5^{100}, p | \gcd(v, w) \text{ for some } (v, w) \in \mathcal{E}\}.$$

Finally, if  $G' = (\mathcal{V}', \mathcal{W}', \mathcal{E}', \mathcal{P}', a', b')$  is another square-free GCD graph, we call it a *subgraph* of  $G$  if  $\mathcal{V}' \subseteq \mathcal{V}$ ,  $\mathcal{W}' \subseteq \mathcal{W}$ ,  $\mathcal{E}' \subseteq \mathcal{E}$ ,  $\mathcal{P}' \supseteq \mathcal{P}$ ,  $\prod_{p|a', p \in \mathcal{P}} p = a$ ,  $\prod_{p|b', p \in \mathcal{P}} p = b$ .

**Lemma 3.6** (The quality increment argument). *Let  $G = (\mathcal{V}, \mathcal{W}, \mathcal{E}, \mathcal{P}, a, b)$  be a square-free GCD graph, let  $p \in \mathcal{R}(G)$ , and let  $\alpha = \frac{\mu(\{v \in \mathcal{V} : p|v\})}{\mu(\mathcal{V})}$  and  $\beta = \frac{\mu(\{w \in \mathcal{W} : p|w\})}{\mu(\mathcal{W})}$ .*

- (a) *If  $\min\{\alpha, \beta\} \leq 1 - 5^{12}/p$ , then there is a subgraph  $G'$  of  $G$  with multiplicative data  $(\mathcal{P} \cup \{p\}, ap^k, bp^\ell)$  for some  $k, \ell \in \{0, 1\}$  satisfying  $\delta(G')^m q(G') \geq 2^{k \neq \ell} \delta(G)^m q(G)$  for  $m \in \{0, 1\}$ .*
- (b) *If  $\min\{\alpha, \beta\} > 1 - 5^{12}/p$ , then there is a subgraph  $G'$  of  $G$  with set of primes  $\mathcal{P} \cup \{p\}$  and with quality  $q(G') \geq q(G)$ .*

*Proof.* Each  $k, \ell \in \{0, 1\}$  define a subgraph of  $G$  with multiplicative data  $(\mathcal{P} \cup \{p\}, ap^k, bp^\ell)$ . Indeed, we merely need to focus on the vertex subsets  $\mathcal{V}_k = \{v \in \mathcal{V} : p^k || v\}$  and  $\mathcal{W}_\ell = \{w \in \mathcal{W} : p^\ell || w\}$ . This new GCD graph is formally given by the sextuple  $G_{k, \ell} = (\mathcal{V}_k, \mathcal{W}_\ell, \mathcal{E}_{k, \ell}, \mathcal{P} \cup \{p\})$ .

$\{p\}, ap^k, bp^\ell)$ , where  $\mathcal{E}_{k,\ell} = \mathcal{E} \cap (\mathcal{V}_k \times \mathcal{W}_\ell)$ . Let  $\delta_{k,\ell} = \frac{\mu(\mathcal{E}_{k,\ell})}{\mu(\mathcal{E})}$ ,  $\alpha_k = \frac{\mu(\mathcal{V}_k)}{\mu(\mathcal{V})}$  and  $\beta_\ell = \frac{\mu(\mathcal{W}_\ell)}{\mu(\mathcal{W})}$ , so that  $\alpha_0 = 1 - \alpha$ ,  $\alpha_1 = \alpha$ ,  $\beta_0 = 1 - \beta$  and  $\beta_1 = \beta$ . We then have

$$(3.10) \quad \frac{\delta(G_{k,\ell})^m q(G_{k,\ell})}{\delta(G)^m q(G)} = \frac{\delta_{k,\ell}^{10+m} (\alpha_k \beta_\ell)^{-9-m} p^{1_{k \neq \ell}}}{(1 - 1/p)^{k+\ell} (1 - p^{-3/2})^{10}},$$

(a) We claim that there exist choices of  $k, \ell \in \{0, 1\}$  such that

$$(3.11) \quad \delta_{k,\ell} \geq \begin{cases} (\alpha_k \beta_k)^{9/10} & \text{if } k = \ell, \\ \frac{\alpha(1 - \beta) + (1 - \alpha)\beta}{5} & \text{if } k \neq \ell. \end{cases}$$

To prove this claim, it suffices to show that

$$(3.12) \quad (\alpha\beta)^{9/10} + ((1 - \alpha)(1 - \beta))^{9/10} + \frac{2}{5} \cdot [\alpha(1 - \beta) + (1 - \alpha)\beta] \leq 1.$$

Let  $u = \max\{\alpha\beta, (1 - \alpha)(1 - \beta)\}$ . Then

$$(\alpha\beta)^{9/10} + ((1 - \alpha)(1 - \beta))^{9/10} \leq u^{2/5} [(\alpha\beta)^{1/2} + ((1 - \alpha)(1 - \beta))^{1/2}] \leq u^{2/5}$$

by the Cauchy–Schwarz inequality. On the other hand, we have

$$\alpha(1 - \beta) + (1 - \alpha)\beta = 1 - \alpha\beta - (1 - \alpha)(1 - \beta) \leq 1 - u.$$

In conclusion, the left-hand side of (3.12) is  $\leq u^{2/5} + 2(1 - u)/5 \leq 1$ , as needed.

Now, if (3.11) is true with  $k = \ell$ , part (a) of the lemma follows immediately by (3.10) upon taking  $G' = G_{k,k}$ . Assume then that (3.11) fails when  $k = \ell$ . We separate two cases.

*Case 1:*  $\max\{\alpha, \beta\} > 5^{12}/p$ . We know that (3.11) holds for some choice of  $k \neq \ell$ . Suppose that  $k = 1$  and  $\ell = 0$  for the sake of concreteness; the other case is similar. Then, (3.10) implies

$$\frac{\delta(G_{1,0})^m q(G_{1,0})}{\delta(G)^m q(G)} \geq \left( \frac{\alpha(1 - \beta) + \beta(1 - \alpha)}{5} \right)^{10+m} \frac{p}{(\alpha(1 - \beta))^{9+m}} \geq \frac{\alpha(1 - \beta) + \beta(1 - \alpha)}{5^{11}} p$$

for  $m \leq 1$ . The proof is complete by taking  $G' = G_{1,0}$ , unless  $\alpha(1 - \beta) + \beta(1 - \alpha) < 2 \cdot 5^{11}/p$ . In this case, we claim that either  $\max\{\alpha, \beta\} < 5^{12}/p$  or  $\min\{\alpha, \beta\} > 1 - 5^{12}/p$  (both of which we have assumed are false). By symmetry, we may assume  $\alpha \leq 1/2$ . Then  $\beta/2 \leq \beta(1 - \alpha) < 2 \cdot 5^{11}/p$ , as needed. In particular,  $\beta \leq 1/2$  (because  $p > 5^{100}$ ), and thus  $\alpha/2 \leq \alpha(1 - \beta) < 2 \cdot 5^{11}/p$ . We have thus reached a contradiction. This proves the lemma in this case.

*Case 2:*  $\max\{\alpha, \beta\} \leq 5^{12}/p$ . We must then have  $\delta_{1,1} \leq (\alpha\beta)^{9/10} \leq 5^{22}p^{-9/5}$ . Let us now define the GCD subgraph  $G' = (\mathcal{V}, \mathcal{W}, \mathcal{E}', \mathcal{P} \cup \{p\}, a, b)$ , where  $\mathcal{E}' = \mathcal{E} \setminus (\mathcal{V}_1 \times \mathcal{W}_1)$ . Notice that we trivially have  $a|v$  and  $b|w$ . In addition, since we have removed all edges  $(v, w)$  where  $p$  divides both  $v$  and  $w$ , we must have that  $p \nmid \gcd(v, w)$  whenever  $(v, w) \in \mathcal{E}'$ . So, indeed, we see that  $G'$  is a GCD subgraph of  $G$ . Moreover,

$$\frac{\delta(G')^m q(G')}{\delta(G)^m q(G)} = \left( \frac{\mu(\mathcal{E}')}{\mu(\mathcal{E})} \right)^{10+m} (1 - p^{-3/2})^{-10} = (1 - \delta_{1,1})^{10+m} (1 - p^{-3/2})^{-10} \geq 1$$

for  $m \leq 1$ , because  $\delta_{1,1} \leq 5^{22}p^{-9/5}$  and  $p > 5^{100}$ . This proves the lemma in this case too.

(b) Let  $c = (1 - p^{-3/2})^{-1}$ . Using (3.10), we get a quality increment by letting  $G' = G_{k,\ell}$  if one of the following inequalities holds:

$$(3.13) \quad \begin{aligned} c\delta_{1,1} &\geq (\alpha\beta)^{9/10} (1 - 1/p)^{2/10}; & c\delta_{0,0} &\geq ((1 - \alpha)(1 - \beta))^{9/10}; \\ c\delta_{1,0} &\geq (\alpha(1 - \beta))^{9/10} p^{-1/10}; & c\delta_{0,1} &\geq ((1 - \alpha)\beta)^{9/10} p^{-1/10}. \end{aligned}$$

Let  $\alpha = 1 - A/p$  and  $\beta = 1 - B/p$  with  $A, B \in [0, 5^{12}]$ . It suffices to show that

$$(3.14) \quad c \geq \left(1 - \frac{A}{p}\right)^{\frac{9}{10}} \left(1 - \frac{B}{p}\right)^{\frac{9}{10}} \left(1 - \frac{1}{p}\right)^{\frac{2}{10}} + \frac{(AB)^{\frac{9}{10}}}{p^{9/5}} + \frac{\left(1 - \frac{A}{p}\right)^{\frac{9}{10}} B^{\frac{9}{10}} + A^{\frac{9}{10}} \left(1 - \frac{B}{p}\right)^{\frac{9}{10}}}{p}.$$

Indeed, the right-hand side of (3.14) is

$$\begin{aligned} &\leq \exp\left(-\frac{0.9A + 0.9B + 0.2}{p}\right) + \frac{5^{22}}{p^{9/5}} + \frac{A^{9/10} + B^{9/10}}{p} \\ &\leq 1 - \frac{0.9A + 0.9B + 0.2}{p} + \frac{(0.9A + 0.9B + 0.2)^2}{2p^2} + \frac{5^{22}}{p^{9/5}} + \frac{A^{9/10} + B^{9/10}}{p}, \end{aligned}$$

where we used the inequalities  $0 \leq 1 - x \leq e^{-x} \leq 1 - x + x^2/2$ , valid for all  $x \in [0, 1]$ . By the inequality of arithmetic and geometric means, we have  $0.9A + 0.1 \geq A^{9/10}$  and  $0.9B + 0.1 \geq B^{9/10}$ . Hence, the right-hand side of (3.14) is

$$\leq 1 + \frac{(0.9A + 0.9B + 0.2)^2}{2p^2} + \frac{5^{11}}{p^{9/5}} \leq 1 + \frac{5^{25}}{p^2} + \frac{5^{22}}{p^{9/5}} \leq 1 + \frac{1}{p^{3/2}} \leq c$$

for  $p > 5^{100}$ . This completes the proof of the part (b) of the lemma.  $\square$

### 3.6. Proof of Theorem 3.5

Let  $Q, N, S$  and  $\mathcal{B}_t$  with  $t \geq t_{j_0+1}$  be as in §3.3. We want to prove (3.6). We may assume that  $\mu(\mathcal{B}_t) \geq \mu(S)^2/t$ ; otherwise, (3.6) is trivially true.

Consider the GCD graph  $G_0 := (\mathcal{S}, \mathcal{S}, \mathcal{B}_t, \emptyset, \emptyset, \emptyset)$ , and note that  $\delta(G_0) \geq 1/t$ . We repeatedly apply part (a) of Lemma 3.6 to create a sequence of distinct primes  $p_1, p_2, \dots$  and of square-free GCD graphs  $G_j = (\mathcal{V}_j, \mathcal{W}_j, \mathcal{E}_j, \{p_1, \dots, p_j\}, a_j, b_j)$ ,  $j = 1, 2, \dots$ , with  $G_j$  a subgraph of  $G_{j-1}$ . Assuming we have applied Lemma 3.6 (a)  $j$  times, we may apply it once more if there is  $p \in \mathcal{R}(G_j)$  dividing a proportion  $\leq 1 - 5^{12}/p$  of  $\mathcal{V}_j$  and  $\mathcal{W}_j$ .

Naturally, the above process will terminate after a finite time, say after  $J_1$  steps and we will arrive at a GCD graph  $G_{J_1}$  such that if  $p \in \mathcal{R}(G_{J_1})$ , then  $p$  divides a proportion  $> 1 - 5^{12}/p$  of the vertex sets  $\mathcal{V}_{J_1}$  and  $\mathcal{W}_{J_1}$ . In addition, the sequence of GCD graphs produced is such that  $\delta(G_j)^m q(G_j) \geq 2^{1j \in \mathcal{D}} \delta(G_{j-1})^m q(G_{j-1})$  for  $m \in \{0, 1\}$ , where

$$\mathcal{D} = \{j \leq J_1 : p_j \text{ divides } a_{J_1} b_{J_1} / \gcd(a_{J_1}, b_{J_1})^2\}.$$

In particular,

$$(3.15) \quad \delta(G_{J_1})^m q(G_{J_1}) \geq 2^{\#\mathcal{D}} \delta(G_0)^m q(G_0) \quad \text{for } m \in \{0, 1\}.$$

To proceed, we must separate two cases.

*Case 1:*  $q(G_{J_1}) \geq t^{30} q(G_0)$ . We apply repeatedly Lemma 3.6 (either part (a) or (b), according to whether the condition  $\min\{\alpha, \beta\} \leq 1 - 5^{12}/p$  holds or fails) to create a sequence of primes  $p_{J_1+1}, p_{J_1+2}, \dots$  that are distinct from each other and from  $p_1, \dots, p_{J_1}$ , and of square-free GCD graphs  $G_j = (\mathcal{V}_j, \mathcal{W}_j, \mathcal{E}_j, \{p_1, \dots, p_j\}, a_j, b_j)$ ,  $j = J_1 + 1, J_1 + 2, \dots$ , with  $G_j$  a subgraph of  $G_{j-1}$ . As before, this process will terminate, say after  $J_2 - J_1$  steps, and we will arrive at a GCD graph  $G_{J_2}$  with  $\mathcal{R}(G_{J_2}) = \emptyset$ . By construction, we have

$$q(G_{J_2}) \geq q(G_{J_2-1}) \geq \dots \geq q(G_{J_1}) \geq t^{30} q(G_0).$$

In addition, we have

$$(3.16) \quad q(G_0) = \frac{\mu(\mathcal{B}_t)^{10}}{\mu(\mathcal{S})^{18}} \geq \frac{\mu(\mathcal{B}_t)^{10}}{N^{18}}$$

by (3.4). (In particular, note that  $q(G_0) > 0$ , so  $q(G_{J_2}) > 0$  and thus  $\mathcal{E}_{J_2} \neq \emptyset$ .) On the other hand, if we let  $a = a_{J_2}$  and  $b = b_{J_2}$ , then  $\gcd(v, w) \mid \gcd(a, b)P$  with  $P = \prod_{p \leq 5^{100}} p$  for all  $(v, w) \in \mathcal{E}_{J_2}$ . In particular,  $\gcd(a, b) > Q/(Pnt)$ . Moreover,

$$\mu(\mathcal{E}_{J_2}) \leq \sum_{m \leq 2Q/a} \sum_{n \leq 2Q/b} \frac{\varphi(am)}{am} \cdot \frac{\varphi(bn)}{bn} \leq \frac{\varphi(a)\varphi(b)}{ab} \cdot \frac{4Q^2}{ab}.$$

Since  $\delta(G_{J_2}) \leq 1$  and  $\prod_p (1 - 1/p^{3/2})^{-10} < \infty$ , we then have

$$(3.17) \quad q(G_{J_2}) \ll \mu(\mathcal{E}_{J_2}) \frac{ab}{\gcd(a, b)^2} \frac{ab}{\varphi(a)\varphi(b)} \ll t^2 N^2.$$

Recalling that  $q(G_{J_2}) \geq t^{30} q(G_0)$ , relations (3.16) and (3.17) complete the proof of (3.6), and thus of Theorem 3.5 in this case.

*Case 2:*  $q(G_{J_1}) < t^{30} q(G_0)$ . In this case, we do not have such a big quality gain, so we need to use that  $L_t(v, w) > 100$  for all  $(v, w) \in \mathcal{B}_t$ . But we must be very careful because this condition might be dominated by the prime divisors of the fixed integers  $a$  and  $b$  we are constructing. Before we proceed, note that (3.15) implies that

$$(3.18) \quad \delta(G_{J_1}) \geq \delta(G_0) \cdot \frac{q(G_0)}{q(G_{J_1})} \geq \frac{1}{t} \cdot \frac{1}{t^{30}} = \frac{1}{t^{31}}.$$

Let  $\mathcal{R} = \mathcal{R}(J_1)$  and let  $p \in \mathcal{R}$ . By the construction of  $G_{J_1}$ ,  $p$  divides a proportion  $> 1 - 5^{12}/p$  of the vertex sets  $\mathcal{V}_{J_1}$  and  $\mathcal{W}_{J_1}$ . Therefore,

$$\mu\left(\{(v, w) \in \mathcal{E}_{J_1} : p \mid vw / \gcd(v, w)^2\}\right) \leq \frac{2 \cdot 5^{12}}{p} \mu(\mathcal{V}_{J_1}) \mu(\mathcal{W}_{J_1}) \leq \frac{5^{13} t^{31}}{p} \mu(\mathcal{E}_{J_1}),$$

where we used (3.18). As a consequence, we find

$$\sum_{(v, w) \in \mathcal{E}_{J_1}} \frac{\varphi(v)\varphi(w)}{vw} \sum_{\substack{p > t^{32}, p \in \mathcal{R} \\ p \mid vw / \gcd(v, w)^2}} \frac{1}{p} \leq \sum_{p > t^{32}} \frac{5^{13} t^{31} \mu(\mathcal{E}_{J_1})}{p^2} \leq \frac{\mu(\mathcal{E}_{J_1})}{100}.$$

Hence, if we let

$$\mathcal{E}_{J_1}^{\text{good}} = \left\{ (v, w) \in \mathcal{E}_{J_1} : \sum_{\substack{p > t^{32}, p \in \mathcal{R} \\ p \mid vw / \gcd(v, w)^2}} \frac{1}{p} \leq 1 \right\},$$

Markov's inequality implies that  $\mu(\mathcal{E}_{J_1}^{\text{good}}) \geq 0.99 \mu(\mathcal{E}_{J_1})$ . We then define the GCD graph  $G'_0 = (\mathcal{V}_{J_1}, \mathcal{W}_{J_1}, \mathcal{E}_{J_1}^{\text{good}}, \mathcal{P}, a_{J_1}, b_{J_1})$ . Note that

$$g(G'_0) = \left( \frac{\mu(\mathcal{E}_{J_1}^{\text{good}})}{\mu(\mathcal{E}_{J_1})} \right)^{10} q(G_{J_1}) \geq \frac{q(G_{J_1})}{2} \geq \frac{q(G_0)}{2}.$$

Next, we apply repeatedly Lemma 3.6 to create a sequence of distinct primes  $p_{J_1+1}, p_{J_1+2}, \dots \in \mathcal{R}$  and of GCD graphs  $G'_j = (\mathcal{V}'_j, \mathcal{W}'_j, \mathcal{E}'_j, \{p_1, \dots, p_{J_1+j}\}, a'_j, b'_j)$ ,  $j = 1, \dots$ , with  $G'_j$  a subgraph

of  $G'_{j-1}$ . This process will terminate, say after  $K$  steps, and we will arrive at a GCD graph  $G'_K$  with  $\mathcal{R}(G'_K) = \emptyset$ . By construction, we have

$$(3.19) \quad q(G'_K) \geq q(G'_{K-1}) \geq \cdots \geq q(G'_0) \geq q(G_0)/2 > 0.$$

In particular,  $\mathcal{E}'_K \neq \emptyset$ . It remains to give an upper bound on  $q(G'_K)$ .

Let  $a' = a'_K$  and  $b = b'_K$ , and recall that  $P = \prod_{p \leq 5^{100}} p$ . Then  $\gcd(v, w) \mid \gcd(a', b')P$  for all  $(v, w) \in \mathcal{E}'_K$ . In particular,  $\gcd(a', b') > Q/(PNt)$ . Moreover, if  $(v, w) \in \mathcal{E}'_K$  and we let  $v = a'm$  and  $w = b'n$ , then

$$100 < L_t(v, w) \leq 5 + L_{t^{32}}(v, w) \leq 6 + \sum_{\substack{p > t^{32}, p \notin \mathcal{R} \\ p \mid vw / \gcd(v, w)^2}} \frac{1}{p} \leq 6 + \frac{\#\mathcal{D}}{t^{32}} + L_{t^{32}}(m, n),$$

where the first inequality is true because  $(v, w) \in \mathcal{B}_t$ , the second one because  $\sum_{y < p \leq y^2} 1/p \leq 1$  for  $y \geq t_{j_0}$ , the third one because  $(v, w) \in \mathcal{E}_{J_1}^{\text{good}}$ , and the fourth one because if  $p$  divides  $a'b'/\gcd(a', b')^2$  and  $p \notin \mathcal{R}$ , then  $p \in \mathcal{D}$ . Now, since  $2^{\#\mathcal{D}} \leq q(G_{J_1})/q(G_0) \leq t^{30}$ , we have that  $L_{t^{32}}(m, n) > 93$ . Therefore,

$$\mu(\mathcal{E}'_K) \leq \sum_{\substack{m \leq 2Q/a', n \leq 2Q/b' \\ L_{t^{32}}(m, n) > 93}} \frac{\varphi(a')\varphi(b')}{a'b'} \ll \frac{\varphi(a')\varphi(b')}{a'b'} \cdot \frac{4Q^2}{a'b'} e^{-t^{32}},$$

by arguing as in the proof of (3.7). We may then insert this inequality into the definition of  $q(G'_K)$  and conclude that  $q(G'_K) \ll e^{-t^{32}} t^2 N^2$ . Together with (3.19) and (3.16), this completes the proof of (3.6), and thus of Theorem 3.5 in this last case as well.

#### ACKNOWLEDGMENTS

The author is grateful to James Maynard for his comments on a preliminary version of the paper, and also to Andrew Granville for pointing out some inaccuracies in the published version.

#### FUNDING

The author is supported by the *Courtois Chair II in fundamental research* of the Université de Montréal, the *Natural Sciences and Engineering Research Council of Canada* (Discovery Grant 2018-05699), and the *Fonds de recherche du Québec - Nature et technologies* (projets de recherche en équipe 256442 and 300951).

#### REFERENCES

- [1] C. Aistleitner, *Decoupling theorems for the Duffin–Schaeffer problem*. Progress report (2019), 24 pages, arXiv:1907.04590.
- [2] C. Aistleitner, T. Lachmann, M. Munsch, N. Technau, A. Zafeiropoulos, *The Duffin–Schaeffer conjecture with extra divergence*. Adv. Math. 356 (2019), 106808, 11 pp.
- [3] V. Beresnevich, G. Harman, A. K. Haynes and S. Velani, *The Duffin–Schaeffer conjecture with extra divergence II*. Math. Z. 275 (2013), no. 1-2, 127–133.
- [4] V. Beresnevich, S. Velani, *A mass transference principle and the Duffin–Schaeffer conjecture for Hausdorff measures*. Ann. of Math. (2) 164 (2006), no. 3, 971–992.
- [5] A. S. Besicovitch, *Sets of Fractional Dimensions (IV): On Rational Approximation to Real Numbers*. J. London Math. Soc. 9 (1934), no. 2, 126–131.
- [6] J. W. S. Cassels, *Some metrical theorems in Diophantine approximation. I*. Proc. Cambridge Philos. Soc. 46 (1950), 209–218.

- [7] P. A. Catlin, *Two problems in metric Diophantine approximation. I*. J. Number Theory 8 (1976), no. 3, 282–288.
- [8] R. J. Duffin and A. C. Schaeffer, *Khinchin’s problem in metric Diophantine approximation*. Duke Math. J. 8 (1941), 243–255.
- [9] F. J. Dyson, *A theorem on the densities of sets of integers*. J. London Math. Soc. 20 (1945), 8–14.
- [10] P. Erdős, *On the distribution of the convergents of almost all real numbers*. J. Number Theory 2 (1970), 425–441.
- [11] P. Erdős, C. Ko, R. Rado, *Intersection theorems for systems of finite sets*. Quart. J. Math. Oxford Ser. (2) 12 (1961), 313–320.
- [12] P. Gallagher, *Approximation by reduced fractions*. J. Math. Soc. Japan 13 (1961), 342–345.
- [13] B. Green, A. Walker, *Extremal problems for GCDs*. Preprint (2020), arXiv:2012.02078.
- [14] G. Harman, *Metric number theory*. London Mathematical Society Monographs. New Series, 18. The Clarendon Press, Oxford University Press, New York, 1998.
- [15] A. K. Haynes, A. D. Pollington, S. L. Velani, *The Duffin–Schaeffer conjecture with extra divergence*. Math. Ann. 353 (2012), no. 2, 259–273.
- [16] V. Jarník, *Zur metrischen Theorie der diophantischen Approximationen*. Proc. Mat. Fyz., 36 (1928) 91–106.
- [17] A. Khintchine, *Einige Sätze über Kettenbrüche, mit Anwendungen auf die Theorie der Diophantischen Approximationen*. Math. Ann. 92 (1924), no. 1-2, 115–125.
- [18] A. Khinchin, *Continued fractions*. Dover Publications, Inc., Mineola, NY, 1997.
- [19] D. Koukoulopoulos, *The distribution of prime numbers*. Graduate Studies in Mathematics, 203. American Mathematical Society, Providence, RI, 2019.
- [20] D. Koukoulopoulos, J. Maynard, *Ann. of Math. (2)* 192 (2020), no. 1, 251–307.
- [21] K. Matomäki, *The distribution of  $\alpha p$  modulo one*. Math. Proc. Cambridge Philos. Soc. 147 (2009), no. 2, 267–283.
- [22] A. D. Pollington and R. C. Vaughan, *The  $k$ -dimensional Duffin and Schaeffer conjecture*. Mathematika 37 (1990), no. 2, 190–200.
- [23] K. F. Roth, *Sur quelques ensembles d’entiers*. C. R. Acad. Sci. Paris 234 (1952), 388–390.
- [24] K. F. Roth, *On certain sets of integers*. J. London Math. Soc. 28 (1953), 104–109.
- [25] K. F. Roth, *Rational approximations to algebraic numbers*. Mathematika 2 (1955), 1–20; corrigendum, 168.
- [26] E. M. Stein, R. Shakarchi, *Real analysis. Measure theory, integration, and Hilbert spaces*. Princeton Lectures in Analysis, 3. Princeton University Press, Princeton, NJ, 2005.
- [27] J. D. Vaaler, *On the metric theory of Diophantine approximation*. Pacific J. Math. 76 (1978), no. 2, 527–539.
- [28] A. Zaharescu, *Small values of  $n^2\alpha \bmod 1$* . Invent. Math. 121 (1995), no. 2, 379–388.
- [29] D. Zeilberger, W. Zudilin, *The irrationality measure of  $\pi$  is at most 7.103205334137...* Mosc. J. Comb. Number Theory 9 (2020), no. 4, 407–419.

DÉPARTEMENT DE MATHÉMATIQUES ET DE STATISTIQUE, UNIVERSITÉ DE MONTRÉAL, CP 6128 SUCC. CENTRE-VILLE, MONTRÉAL, QC H3C 3J7, CANADA

*Email address:* dimitris.koukoulopoulos@umontreal.ca