

AN OVERLAPPING THEOREM WITH APPLICATIONS

JAVIER CILLERUELO AND GÉRALD TENENBAUM

ABSTRACT. We establish a general and optimal lower bound for the complete sum of the probabilities of k -intersections of n events. We then describe various applications to additive and multiplicative number theory, graph theory, coding theory, study of lattice points on circles, and divisors of polynomials

1. INTRODUCTION

Let μ be a positive measure on a set Ω , $\{E_j\}_{j=1}^k$ a family of measurable subsets, and set

$$\tau_m := \sum_{1 \leq j_1 < \dots < j_m \leq k} \mu(E_{j_1} \cap \dots \cap E_{j_m}) \quad (m \geq 1).$$

We address here the problem of obtaining lower bounds for τ_m in terms of τ_1 . For $m \geq 2$, the quantity τ_m may be thought of as the global amount of m -overlapping in the family $\{E_j\}_{j=1}^k$.

Many problems in Combinatorial Number Theory may be tackled by using estimates for τ_m . According to the specific situation under consideration, appropriate choices of the set Ω , the family of subsets $\{E_j\}_{j=1}^k$ and the measure μ may be performed.

The integer parameter $m \geq 1$ being fixed, our results will be conveniently described in terms of the continuous, piecewise linear, interpolation of the binomial coefficients $\binom{n}{m}$ ($n \in \mathbb{N}$). Thus, we define

$$Q_m(x) := \binom{\lfloor x \rfloor}{m} + \binom{\lfloor x \rfloor}{m-1} \langle x \rangle = \binom{\lfloor x \rfloor}{m} \langle x \rangle + \binom{\lfloor x \rfloor + 1}{m} (1 - \langle x \rangle) \quad (x \in \mathbb{R}^+)$$

where $\lfloor x \rfloor$ and $\langle x \rangle$ denote respectively the integer part and the fractional part of x . We have

$$Q_m(x) \geq \binom{x}{m} \quad (x \in \mathbb{R}^+),$$

for the right-hand side is a convex function of x , with equality when x is an integer. We also note that $Q_1(x) = x$, and that, for all m , the function Q_m is continuous, convex and satisfies $Q_m(x) = 0$ whenever $x \leq m - 1$.

We state our main result in a probabilistic setting.

Date: March 8, 2008.

1991 Mathematics Subject Classification. 60C05.

Key words and phrases. Probability of intersections, divisors, lattice points, Sidon sets, graph theory, divisors of polynomials, coding theory.

The authors take pleasure in thanking Bernardo López for helpful suggestions on the presentation of sections 1 and 2.

Theorem 1.1 (Overlapping Theorem). *Let $(\Omega, \mathcal{A}, \mathbb{P})$ be a probability space and let $\{E_j\}_{j=1}^k$ denote a family of events. Write*

$$\sigma_m := \sum_{1 \leq j_1 < \dots < j_m \leq k} \mathbb{P}(E_{j_1} \cap \dots \cap E_{j_m}) \quad (m \geq 1).$$

Then we have

$$(1.1) \quad \sigma_m \geq Q_m(\sigma_1).$$

The case $m = 2$ is essentially due to Gillis [6]. The general bound has been outlined by Klazar in [7]. By a different method, we prove the above result in the next section, together with the fact that inequality (1.1) is optimal in its generality.

In section 3, we describe various applications. The results obtained are not all new: our main purpose is to point out that they all allow a unified approach.

2. THE OVERLAPPING THEOREM

We first prove Theorem 1.1. Put $f(\omega) := \sum_{1 \leq j \leq k} \mathbf{1}_{E_j}(\omega)$. Then

$$(1+t)^{f(\omega)} = \prod_{1 \leq j \leq k} (1 + \mathbf{1}_{E_j}(\omega)t) \quad (\omega \in \Omega).$$

Equating coefficients of t^m on both sides, we obtain

$$Q_m(f(\omega)) = \binom{f(\omega)}{m} = \sum_{1 \leq j_1 < \dots < j_m \leq k} \mathbf{1}_{E_{j_1}} \mathbf{1}_{E_{j_2}} \dots \mathbf{1}_{E_{j_m}} \quad (\omega \in \Omega).$$

Integrating with respect to $d\mathbb{P}(\omega)$, we obtain $\sigma_m = \mathbb{E}(Q_m(f))$.

Since Q_m is convex, we may apply Jensen's inequality (see, e.g., [11], Theorem 3.3) to get

$$Q_m(\sigma_1) = Q_m(\mathbb{E}(f)) \leq \mathbb{E}(Q_m(f)) = \sigma_m$$

□

It is not difficult to see that Theorem 1.1 cannot be improved. Let $I = \mathbb{R}/\mathbb{Z}$ be equipped with the Haar measure. For given $0 < \sigma < k \in \mathbb{N}$ and all integers j , $1 \leq j \leq k$, we define

$$E_j := \{x \in I : 0 \leq x + j/k < \sigma/k \pmod{1}\},$$

so that each E_j has measure σ/k . Put $\nu = \lfloor \sigma \rfloor$. Then each $x \in I$ belongs to exactly ν or $\nu + 1$ sets E_j , the latter case being excluded if $\sigma \in \mathbb{N}$. Thus

$$f(x) = \sum_{1 \leq j \leq k} \mathbf{1}_{E_j}(x) \in \{\nu, \nu + 1\} \quad (x \in I).$$

Writing $A_\kappa := f^{-1}(\{\kappa\})$, we infer that

$$\mathbb{E}(f) = \sigma = \nu \mathbb{P}(A_\nu) + (\nu + 1) \mathbb{P}(A_{\nu+1}) = \nu + \mathbb{P}(A_{\nu+1}).$$

This implies in turn, with $w := \mathbb{P}(A_{\nu+1}) = \sigma - \nu$,

$$\mathbb{E}(Q_m(f)) = \binom{\nu+1}{m} w + \binom{\nu}{m} (1-w) = Q_m(\sigma).$$

Actually, equality holds if and only if $f = \sum \mathbf{1}_{E_j}$ takes no more than two consecutive integer values and $\mathbb{E}(f) = \sigma$.

For most the applications, the next corollary, which is also optimal, is sufficient.

Corollary 2.1. *Let $(\Omega, \mathcal{A}, \mathbb{P})$ be a probability space and let $\{E_j\}_{j=1}^k$ denote a family of events. Then, for each $m \geq 1$, we have*

$$\binom{k}{m} \max_{1 \leq j_1 < \dots < j_m \leq k} \mathbb{P}(E_{j_1} \cap \dots \cap E_{j_m}) \geq Q_m(\sigma_1).$$

Proof. This is obvious since σ_m is a sum with $\binom{k}{m}$ summands. \square

We now proceed with our optimality assertion.

Theorem 2.2. *Let $0 < \sigma \leq k \in \mathbb{N}$. There exist a probability space and a sequence of events $\{E_j\}_{j=1}^k$ such that every intersection*

$$E_{j_1} \cap \dots \cap E_{j_m}, \quad 1 \leq j_1 < \dots < j_m \leq k$$

has probability $Q_m(\sigma)/\binom{k}{m}$.

Proof. Let $k \in \mathbb{N}$, $A := [1, k] \cap \mathbb{N}$, $\Omega := \mathcal{P}(A)$, and define

$$E_j := \{J \subset A : j \in J\} \in \Omega \quad (1 \leq j \leq k).$$

Let $\nu := \lfloor \sigma \rfloor$, $w := \sigma - \nu$, and let Ω_ν denote the subset of Ω comprising all sets E with ν elements. Then, obviously,

$$f(E) = \sum_{1 \leq j \leq k} \mathbf{1}_{E_j}(E) = \nu, \quad \sum_{j_1 < \dots < j_m} \mathbf{1}_{E_{j_1}}(E) \dots \mathbf{1}_{E_{j_m}}(E) = \binom{\nu}{m} \quad (E \in \Omega_\nu).$$

Hence, selecting \mathbb{P} as the uniform measure μ_ν supported on Ω_ν ,

$$\sigma_m = \mathbb{E} \left(\binom{f}{m} \right) = \binom{\nu}{m}.$$

Furthermore, by symmetry, all $E_{j_1} \cap \dots \cap E_{j_m}$ have the same probability. By linear combination, the above is also true for $\mathbb{P} = w\mu_{\nu+1} + (1-w)\mu_\nu$. Therefore we get for this choice

$$\sigma_m = w \binom{\nu+1}{m} + (1-w) \binom{\nu}{m} = Q_m(\sigma).$$

\square

3. APPLICATIONS

3.1. Primes. Our first application is an unusual proof of a well-known estimate for the sum of the reciprocals of primes.

Theorem 3.1. *For $n \geq 3$, we have*

$$\sum_{p \leq n} \frac{1}{p} \leq \frac{\log \log(2n+1)}{\log 2} + 1.$$

Proof. Let X denote the random variable defined by

$$\mathbb{P}(X = r) = \begin{cases} 1/n & \text{for } 1 \leq r \leq n \\ 0 & \text{otherwise,} \end{cases}$$

and, for each prime $p \leq n$, select $E_p := \{\omega : X(\omega) \equiv 0 \pmod{p}\}$. We have,

$$\sigma_m = \sum_{p_{i_1} < \dots < p_{i_m} \leq n} \mathbb{P}(E_{p_{i_1}} \dots E_{p_{i_m}}) = \frac{1}{n} \sum_{p_{i_1} < \dots < p_{i_m} \leq n} \left\lfloor \frac{n}{p_{i_1} \dots p_{i_m}} \right\rfloor \leq \sum_{\substack{1 \leq r \leq n \\ \nu(r)=m}} \frac{1}{r}.$$

where $\nu(r)$ denotes the number of prime factors of r . This also holds for $m = 0$ if we set $\sigma_0 = 1$. Therefore

$$2^{\sigma_1} = \sum_{m \geq 0} \binom{\sigma_1}{m} \leq \sum_{m \geq 0} \sigma_m \leq \sum_{1 \leq r \leq n} \frac{1}{r} \leq \log(2n + 1).$$

the stated bound follows, since we have from above

$$\sigma_1 = \frac{1}{n} \sum_{p \leq n} \left\lfloor \frac{n}{p} \right\rfloor \geq \sum_{p \leq n} \frac{1}{p} - 1.$$

□

3.2. Graphs. The study of extremal problems in graph theory was initiated by Erdős and Turán. The theorem below was originally proved by Kővari, Sós and Turán [8]. The complete bipartite graph $K_{r,s}$ is a graph with two sets of vertices, one with r members and one with s , such that each vertex in one set is adjacent to every vertex in the other set and to no vertex in its own set.

Theorem 3.2. *Let r, s be positive integers and G be a graph with n vertices containing no subgraph $K_{r,s}$. Then G contains at most*

$$\frac{1}{2}(r-1)^{1/s}n^{2-1/s} + \frac{1}{2}(s-1)n$$

edges.

Proof. Let V be the set of vertices of G , so that $|V| = n$, and E be the set of edges. Define a random variable $X : \Omega = V \rightarrow V$ with law $\mathbb{P}(X = v) = 1/n$ and, for each $v \in V$, let $E_v := \{\omega : \{X(\omega), v\} \in E\}$, $\deg(v) := |E_v|$. Then $\mathbb{P}(E_v) = \deg(v)/n$ and

$$\sigma_1 = \frac{1}{n} \sum_{v \in E} \deg(v) = \frac{2|E|}{n}.$$

Since G contains no subgraph of type $K_{r,s}$, we have $\mathbb{P}(E_{v_1} \cdots E_{v_s}) \leq (r-1)/n$ whenever the E_{v_j} are pairwise distinct. Therefore,

$$\sigma_s \leq \frac{r-1}{n} \binom{n}{s}.$$

Now we apply the overlapping theorem to obtain

$$(3.1) \quad \frac{r-1}{n} \frac{n^s}{s!} \geq \frac{r-1}{n} \binom{n}{s} \geq \sigma_s \geq \binom{\sigma_1}{s} = \binom{2|E|/n}{s} \geq \frac{(2|E|/n - (s-1))^s}{s!}.$$

This yields the required inequality. □

Remark. It is known that the constant $(r-1)^{1/2}/2$ is sharp for $s = 2$.

3.3. Sidon sets. A set of integers A is called a Sidon set if all sums

$$a + a' \quad (a \leq a', a \in A, a' \in A)$$

are distinct. A major problem in this theory consists in estimating the size $F(N)$ of the largest Sidon set contained in $\{1, \dots, N\}$. Erdős [5] proved the upper bound

$$F(N) \leq N^{1/2} + O(N^{1/4})$$

and Lindström [10] gave a more precise estimate (stated and proved below) which has not been improved in 37 years. Ruzsa [12] gave a new proof of it, using an easy but interesting lemma, which we prove via the overlapping theorem.

Lemma 3.3. *Let A and B be two finite sets of integers. If A is a Sidon set then*

$$|A + B| \geq \frac{|A|^2|B|}{|A| + |B| - 1}.$$

Proof. Let X denote the integer random variable with law given by

$$\mathbb{P}(X = m) = \begin{cases} 1/|A + B| & \text{if } m \in A + B \\ 0 & \text{otherwise.} \end{cases}$$

For each $b \in B$ we set $E_b = \{X \in A + b\}$. Then $\mathbb{P}(E_b) = |A|/|A + B|$ and

$$\sigma_1 = \frac{|A||B|}{|A + B|}.$$

On the other hand, if $b \neq b'$, $\mathbb{P}(E_b E_{b'}) \leq 1/|A + B|$, for A is a Sidon set, whence $\sigma_2 \leq \binom{|B|}{2}/|A + B|$. Finally,

$$\binom{|B|}{2} \frac{1}{|A + B|} \geq \sigma_2 \geq Q_2(\sigma_1) \geq \frac{\sigma_1(\sigma_1 - 1)}{2} = \frac{|A||B|}{2|A + B|} \left(\frac{|A||B|}{|A + B|} - 1 \right),$$

and the stated inequality follows. \square

Theorem 3.4 (Lindström). *If $A \subset [1, N]$ is a Sidon set, then $|A| \leq N^{1/2} + N^{1/4} + 1$.*

Proof. Write $|A| = m$, take $B = \{1, \dots, n\}$ with $n = \lfloor (mN)^{1/2} \rfloor + 1$ and apply above lemma. We get

$$N + (Nm)^{1/2} \geq N + n - 1 \geq |A + B| \geq \frac{m^2 n}{m + n - 1} \geq \frac{m^2 (mN)^{1/2}}{m + (mN)^{1/2}},$$

from which we derive that $m \leq \left(\sqrt{N^{1/2} + \frac{1}{4}} + \frac{1}{2} \right)^2 < N^{1/2} + N^{1/4} + 1$. \square

3.4. Coding theory. Write $Z_q := [1, q] \cap \mathbb{N}$. The Hamming distance $d(w, w')$ of two words $w, w' \in Z_q^n$ of length n , is the number of locations at which the letters from w and w' are different. A classical problem in coding theory is to estimate the cardinality $A_q(n, d)$ of the largest code in Z_q^n with given minimal Hamming distance d . Applying the overlapping theorem, we establish an upper bound for this problem, known as Plotkin bound.

Theorem 3.5 (Plotkin bound). *Assume $qd > n(q - 1)$. Then*

$$A_q(n, d) \leq \frac{qd}{qd - n(q - 1)}.$$

Proof. Let $\Omega := \{(k, h) : 1 \leq k \leq n, 0 \leq h \leq q-1\}$ and define a random variable X such that

$$\mathbb{P}(X = (k, h)) = \frac{1}{nq}.$$

Assume $C := \{w_i : 1 \leq i \leq A_q(n, d)\}$ is a code such that $\min_{i \neq j} d(w_i, w_j) = d$. Writing k_i for the k th letter, or k -component, of w_i we consider the events

$$E_i := \bigcup_{1 \leq k \leq n} \{X = (k, k_i)\} \quad (1 \leq i \leq A_q(d, n)).$$

Then $\mathbb{P}(E_i) = 1/q$ and $\sigma_1 = A_q(n, d)/q$. Also

$$E_i E_j = \bigcup_{1 \leq k \leq n} \{X = (k, k_i) = (k, k_j)\},$$

so

$$P(E_i E_j) = \frac{n - d(w_i, w_j)}{qn} \leq \frac{n - d}{qn}.$$

Therefore,

$$\binom{A_q(n, d)}{2} \frac{n - d}{qn} \geq \sigma_2 \geq Q_2(\sigma_1) \geq \binom{A_q(n, d)/q}{2},$$

and the required bound follows. \square

3.5. Divisors. Given integers a_1, \dots, a_k , we denote by (a_1, \dots, a_k) their greatest common divisor.

Theorem 3.6. *Let $\alpha \in]0, 1[$, $n \in \mathbb{N}^*$ and $\{d_j\}_{j=1}^k$ a set of divisors of n such that $\min_{1 \leq j \leq k} d_j \geq n^\alpha$. Then, for all $m \geq 1$, we have*

$$\max_{1 \leq j_1 < \dots < j_m \leq k} (d_{j_1}, \dots, d_{j_m}) > n^{\alpha m}$$

where $\alpha_m := Q_m(k\alpha) / \binom{k}{m}$.

Proof. Let X denote the random variable defined by

$$(3.2) \quad \mathbb{P}(X = p^\nu) = \frac{\log p}{\log n} (p^\nu | n)$$

Let $E_j = \{\omega : X | d_j\}$. Then $\mathbb{P}(E_j) = (\log d_j) / \log n$ and

$$\mathbb{P}(E_{j_1} \cdots E_{j_m}) = \frac{\log(d_{j_1}, \dots, d_{j_m})}{\log n}.$$

We observe that $\sigma_1 = \sum_{j=1}^k \mathbb{P}(E_j) \geq k\alpha$. We may hence apply Corollary 2.1 to infer that there exist d_{j_1}, \dots, d_{j_m} such that

$$\frac{\log(d_{j_1}, \dots, d_{j_m})}{\log n} = \mathbb{P}(E_{j_1} \cdots E_{j_m}) \geq Q_m(\sigma_1) \binom{k}{m}^{-1} \geq Q_m(k\alpha) \binom{k}{m}^{-1}.$$

\square

For all values of k, m and α , the exponent α_m is optimal.

Theorem 3.7. *For any positive integer k , and for any α , $0 \leq \alpha \leq 1$, there exists infinitely many integers n with k divisors $n^\alpha < d_1 < \dots < d_k \leq n$ and such that, for each m , $2 \leq m \leq k$ and for any $d_{i_1} < \dots < d_{i_m}$ we have $(d_{i_1}, \dots, d_{i_m}) \leq n^{\alpha_m + o(1)}$, where $\alpha_m := Q_m(k\alpha) / \binom{k}{m}$.*

Proof. The result is obtained in a straightforward manner by adapting the construction of Theorem 2.3. We omit the details. \square

The case $m = 2$ was studied in [3], where the following result was stated.

Corollary 3.8. *For $\alpha > 0$, $k \in \mathbb{N}^*$, $\alpha_2 = Q_2(k\alpha)/\binom{k}{2}$, the interval $]n^\alpha, n^\alpha + n^{\alpha_2}]$, contains at most, $k - 1$ divisors of n .*

Proof. Apply Theorem 3.6 for $m = 2$, noticing that if d_i, d_j belong to an interval I , then $(d_i, d_j) \leq |I|$. \square

Remark. It is an interesting and difficult problem to decide whether the exponent α_2 in the corollary is sharp.

It is a natural problem to consider the divisors of an integer lying in an arithmetic progression. We give an easy proof of the following theorem of Lenstra [9]

Corollary 3.9 (Lenstra). *Let $\alpha > 1/4$, $n, q \in \mathbb{N}^*$, $q > n^\alpha$. Then, the number of divisors d of n such that $d \equiv a \pmod{q}$ is bounded by a function of α alone.*

Proof. Write $q = n^{(1/4)+2\varepsilon}$. We prove that the number of divisors in the form $d_i = a + m_i q$ lying in the interval $I_r = [n^{r\varepsilon}, n^{(r+1)\varepsilon}]$ is bounded by $1 + 1/\varepsilon$ for each integer r with $0 \leq r \leq 1/\varepsilon$. This indeed implies that the total number of divisors in the arithmetic progression $a \pmod{q}$ is bounded by $(1 + 1/\varepsilon)^2$.

Let k be the number of divisors in I_r . Then, there exist i, j such that

$$n^{(r+1)\varepsilon} \geq d_i - d_j = q(m_i - m_j) \geq q(m_i, m_j) \geq q(d_i, d_j) \geq n^{(1/4)+2\varepsilon} n^{Q_2(kr\varepsilon)/\binom{k}{2}}.$$

Thus, $r\varepsilon + \varepsilon \geq \frac{1}{4} + 2\varepsilon + \{kr\varepsilon(kr\varepsilon - 1)\}/\{k(k-1)\}$, which may be rewritten as

$$\frac{1}{k-1} \geq \frac{(1/4) + \varepsilon}{r\varepsilon(1-r\varepsilon)} - 1.$$

Since $r\varepsilon(1-r\varepsilon) \leq 1/4$, we obtain $k \leq 1 + 1/\varepsilon$, as required. \square

The following result was suggested by R. de la Bretèche and was used in [1].

Corollary 3.10. *Let $\varepsilon \in]0, 1]$ and $\alpha \in [0, 1]$. For all $n \in \mathbb{N}^*$ and all a, q such that $(a, q) = 1$, $q > n^{\alpha-\alpha^2+2\varepsilon}$, we have*

$$|\{d \mid n : d \equiv a \pmod{q}, n^\alpha < d \leq n^{\alpha+\varepsilon}\}| \leq (\alpha - \alpha^2 + \varepsilon)/\varepsilon.$$

Proof. Let $d_j = a + m_j q$ ($1 \leq j \leq k$) be divisors of n in $]n^\alpha, n^{\alpha+\varepsilon}[$. From Theorem 3.6 with $m = 2$, we see that

$$\max_{1 \leq i < j \leq k} (d_i, d_j) > n^{\alpha^2}.$$

However, we have $(d_i, d_j) = (m_i q + a, (m_i - m_j)q) \leq |m_i - m_j| \leq n^{\alpha+\varepsilon}/q \leq n^{\alpha^2-\varepsilon}$ for all i, j with $i \neq j$. This is sufficient. \square

Changing the probability measure in Theorem 1.1, we get interesting variants of the above results. An example, given here without proof, is the following, where $\nu(d)$ denotes the number of distinct prime factors of d .

Theorem 3.11. *Let $0 < \alpha < 1$ and $n \geq 1$. Assume $\{d_j\}_{j=1}^k$ is a set of distinct divisors of n with $\nu(d_j) > \alpha\nu(n)$ for all j . Then*

$$\max_{1 \leq i < j \leq k} \nu((d_i, d_j)) > \alpha_2 \nu(n).$$

3.6. Lattice points on circles. It is known that the number of lattice points on the circle $x^2 + y^2 = n$ is not bounded uniformly in n . Schinzel proved that, on the circle $x^2 + y^2 = R^2$, an arc of length $R^{1/3}$ contains at most two lattice points. In [2], Córdoba and the first author proved a more general result for which we now provide a simpler proof using Theorem 1.1.

Theorem 3.12. *Let $x^2 + y^2 = R^2$ be a circle, $k \in \mathbb{N}^*$, and $\gamma_k := 1/(4[k/2] + 2)$. Then, an arc of length $R^{1/2 - \gamma_k}$ contains at most k lattice points.*

Proof. Let $x^2 + y^2 = R^2 = n = \prod_{1 \leq s \leq t} |\pi_s|^{2m_s}$ be a circle, where the $\pi_s \in \mathbb{Z}[i]$ are Gaussian primes, and $m_s \in \mathbb{N}^*$ ($1 \leq s \leq t$). Assume that there are $k + 1$ lattice points ν_1, \dots, ν_{k+1} of $\mathbb{Z}[i]$ on an arc of length R^γ . Let X denote the random variable defined by

$$\mathbb{P}(X = \overline{\pi_s^a}) = \mathbb{P}(X = \pi_s^b) = \frac{\log |\pi_s|}{\log n} \quad (1 \leq s \leq t, 1 \leq a, b \leq m_s).$$

For each $j \in [1, k + 1]$ put $E_j := \{X : X | \nu_j\}$. Then

$$\mathbb{P}(E_j) = \frac{\log |\nu_j|}{\log n} = \frac{1}{2}$$

and

$$\mathbb{P}(E_i E_j) = \frac{\log |(\nu_i, \nu_j)|}{\log n} \leq \frac{\log |\nu_i - \nu_j|}{\log n} < \frac{\log R^\gamma}{\log n} = \frac{\gamma}{2}.$$

Thus, $\sigma_2 < \frac{1}{2} \binom{k+1}{2} \gamma$ and $\sigma_1 = (k + 1)/2$. Therefore

$$\binom{k+1}{2} \frac{\gamma}{2} > \sigma_2 \geq Q_2(\sigma_1) \geq Q_2\left(\frac{k+1}{2}\right),$$

and so $\gamma > 2Q_2\left(\frac{k+1}{2}\right) / \binom{k+1}{2} = \frac{1}{2} - 1/(4[k/2] + 2)$. \square

We do not know whether the number of lattice points on arcs of length $R^{1/2}$ can be bounded independently of R . The above theorem yields that the number of lattice points on such arcs is $\ll \log R$.

3.7. Polynomials. The overlapping theorem may be used to provide an alternative proof of the following result, due to Jiménez and the first author [4].

Theorem 3.13. *Let $\gamma > 0$, $M(x) \in \mathbb{Z}[x]$ and $F_1(x), \dots, F_k(x)$ be k divisors of $M(x)$ in $\mathbb{Z}[x]$ such that $\min_{1 \leq j \leq k} \deg F_j \geq \gamma \deg M$. Then there exist $i, j \in [1, k]$, $i \neq j$, such that*

$$\deg(F_i - F_j) \geq (\deg M) Q_2(k\gamma) \binom{k}{2}^{-1} \geq \deg M \left\{ \gamma^2 - \frac{\gamma(1-\gamma)}{k-1} \right\}.$$

Proof. Write $M = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ a decomposition of $M(x)$ as a product of irreducible factors in $\mathbb{Z}[x]$. Let X denote the random variable defined by

$$\mathbb{P}(X = p_s^\alpha) = \frac{\deg p_s}{\deg M} \quad (1 \leq s \leq t, 1 \leq \alpha \leq \alpha_s).$$

Let $E_j = \{\omega : X | F_j(x)\}$. Then $\mathbb{P}(E_j) = (\deg F_j) / \deg M \geq \gamma$. By Corollary 2.1, there exist distinct indices i, j such that

$$\mathbb{P}(E_i E_j) \geq Q_2(\sigma_1) \binom{k}{2}^{-1} \geq Q_2(k\gamma) \binom{k}{2}^{-1} \geq \gamma^2 - \frac{\gamma(1-\gamma)}{k-1}.$$

We complete the proof by observing that

$$\mathbb{P}(E_i E_j) = \frac{\deg(F_j, F_i)}{\deg M} \leq \frac{\deg(F_i - F_j)}{\deg M}.$$

□

REFERENCES

- [1] R. de la Bretèche, Nombre de valeurs polynomiales qui divisent un entier, *Math. Proc. Cambridge Philos. Soc.* **131** (2001), no. 2, 193–209.
- [2] J. Cilleruelo, A. Córdoba, Trigonometric polynomials and lattice points, *Proc. Amer. Math. Soc.* **115** (1992), no. 4, 899–905.
- [3] J. Cilleruelo, J. Jiménez-Urroz, The hyperbola $xy = N$, *J. Théor. Nombres Bordeaux* **12** (2000), no. 1, 87–92.
- [4] J. Cilleruelo, J. Jiménez-Urroz, Divisors in a Dedekind domain, *Acta Arith* **85** (1998), no. 3, 229–233.
- [5] P. Erdős, P. Turán, On a problem of Sidon in additive number theory, and on some related problems, *J. London Math. Soc.* **16** (1941) 212–215.
- [6] J. Gillis, Note on a property of measurable sets, *Journal London Math. Soc.* **11** (1936), 139–141.
- [7] M. Klazar, Comments on a result of Trotter and Winkler in combinatorial probability, *Paul Erdős and his mathematics* (Budapest, 1999), 127–129, Jnos Bolyai Math. Soc., Budapest, 1999.
- [8] T. Kővari, V. T. Sós, P. Turán, On a problem of K. Zarankiewicz, *Colloquium Math* **3** (1954) 50–57.
- [9] H.W. Lenstra, Divisors in residue classes, *Mathematics of computation* **42** (1984), no. 165, 331–340.
- [10] B. Lindström, On a combinatorial problem in number theory, *Canad. Math. Bull.* **8** (1965) 477–490.
- [11] W. Rudin, *Real and complex analysis*, Third edition, McGraw-Hill, 1987.
- [12] I. Z. Ruzsa, Solving a linear equation in a set of integers, I, *Acta Arith*, **65** (1993), no. 3, 259–282.

JAVIER CILLERUELO, DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD AUTÓNOMA DE MADRID, MADRID 28049, ESPAÑA.

E-mail address: franciscojavier.cilleruelo@uam.es

GÉRALD TENENBAUM, INSTITUT ÉLIE CARTAN, UNIVERSITÉ HENRI POINCARÉ, B.P. 239, 54506 VANDŒUVRE-LÈS-NANCY, FRANCE.

E-mail address: gerald.tenenbaum@iecn.u-nancy.fr