A note on distinct distances in rectangular lattices

Javier Cilleruelo†  Micha Sharir‡  Adam Sheffer§

July 18, 2014

Abstract

In his famous 1946 paper, Erdős [4] proved that the points of a $\sqrt{n} \times \sqrt{n}$ portion of the integer lattice determine $\Theta(n/\sqrt{\log n})$ distinct distances, and a variant of his technique derives the same bound for $\sqrt{n} \times \sqrt{n}$ portions of several other types of lattices (e.g., see [11]). In this note we consider distinct distances in rectangular lattices of the form $\{(i, j) \in \mathbb{Z}^2 | 0 \leq i \leq n^{1-\alpha}, \ 0 \leq j \leq n^\alpha\}$, for some $0 < \alpha < 1/2$, and show that the number of distinct distances in such a lattice is $\Theta(n)$. In a sense, our proof “bypasses” a deep conjecture in number theory, posed by Cilleruelo and Granville [3]. A positive resolution of this conjecture would also have implied our bound.

Keywords. Discrete geometry, distinct distances, lattice.

Given a set $P$ of $n$ points in $\mathbb{R}^2$, let $D(P)$ denote the number of distinct distances that are determined by pairs of points from $P$. Let $D(n) = \min_{|P|=n} D(P)$; that is, $D(n)$ is the minimum number of distinct distances that any set of $n$ points in $\mathbb{R}^2$ must always determine. In his celebrated 1946 paper [4], Erdős derived the bound $D(n) = O(n/\sqrt{\log n})$ by considering a $\sqrt{n} \times \sqrt{n}$ integer lattice. Recently, after 65 years and a series of progressively larger lower bounds1, Guth and Katz [8] provided an almost matching lower bound $D(n) = \Omega(n/\log n)$.

While the problem of finding the asymptotic value of $D(n)$ is almost completely solved, hardly anything is known about which point sets determine a small number of distinct distances. Consider a set $P$ of $n$ points in the plane, such that $D(P) = O(n/\sqrt{\log n})$. Erdős conjectured [6] that any such set “has lattice structure.” A variant of a proof of Szemerédi implies that there exists a line that contains $\Omega(\sqrt{\log n})$ points of $P$ (Szemerédi’s proof was communicated by Erdős in [5] and can be found in [9, Theorem 13.7]). A recent result of Pach and de Zeeuw [10] implies that any constant-degree curve that contains no lines and

---

1Work by Javier Cilleruelo has been supported by grants MTM 2011-22851 of MICINN and ICMAT Severo Ochoa project SEV-2011-0087. Work by Adam Sheffer and Micha Sharir has been supported by Grants 338/09 and 892/13 from the Israel Science Fund, by the Israeli Centers of Research Excellence (ICORE) program (Center No. 4/11), and by the Hermann Minkowski-MINERVA Center for Geometry at Tel Aviv University.

†Instituto de Ciencias Matematicas (CSIC-UAM-UC3M-UCM), and Departamento de Matematicas, Universidad Autónoma de Madrid, 28049 Madrid, Spain. francescoguava.cilleruelo@uam.es

‡School of Computer Science, Tel Aviv University, Tel Aviv 69978, Israel. michas@tau.ac.il

§Corresponding author. School of Computer Science, Tel Aviv University, Tel Aviv 69978, Israel. shef-fera@tau.ac.il

circles cannot be incident to more than \( O(n^{3/4}) \) points of \( P \). Another recent result, by Sheffer, Zahl, and de Zeeuw [12] implies that no line can contain \( \Omega(n^{7/8}) \) points of \( P \), and no circle can contain \( \Omega(n^{5/6}) \) such points.

In this note we make some progress towards the understanding of the structure of such sets, by showing that rectangular lattices cannot have a sublinear number of distinct distances. Specifically, we consider the number of distinct distances that are determined by an \( n^{1-\alpha} \times n^{\alpha} \) integer lattice, for some \( 0 < \alpha \leq 1/2 \). We denote this number by \( D_\alpha(n) \).

The case \( \alpha = 1/2 \) is the case of the square \( \sqrt{n} \times \sqrt{n} \) lattice, which determines \( D_{1/2}(n) = \Theta(n/\sqrt{\log n}) \) distinct distances, as already mentioned above. Surprisingly, we show here a different estimate for \( \alpha < 1/2 \).

**Theorem 1.** For \( \alpha < 1/2 \), the number of distinct distances that are determined by an \( n^{1-\alpha} \times n^{\alpha} \) integer lattice is

\[
D_\alpha(n) = n + o(n).
\]

**Proof.** We consider the rectangular lattice

\[
R_\alpha(n) = \{(i, j) \in \mathbb{Z}^2 \mid 0 \leq i \leq n^{1-\alpha}, 0 \leq j \leq n^\alpha\}.
\]

Notice that every distance between a pair of points of \( R_\alpha(n) \) is also spanned by \((0, 0)\) and another point of \( R_\alpha(n) \). This immediately implies \( D_\alpha(n) \leq n + O(n^{1-\alpha}) \). In the rest of the proof we derive a lower bound for \( D_\alpha(n) \). For this purpose, we consider the sublattice

\[
R'_\alpha(n) = \{(i, j) \in \mathbb{Z}^2 \mid 2n^\alpha \leq i \leq n^{1-\alpha}, 0 \leq j \leq n^\alpha\};
\]

since \( \alpha < 1/2 \), \( R'_\alpha(n) \neq \emptyset \) for \( n \geq n_0(\alpha) \), a suitable constant depending on \( \alpha \). We also consider the functions

\[
r(m) = \left| \{(i, j) \in R'_\alpha(n) \mid i^2 + j^2 = m\} \right|,
\]

\[
d(m) = \left| \{(i, j) \in R'_\alpha(n) \mid i^2 - j^2 = m\} \right|.
\]

Observe that the smallest (resp., largest) value of \( m \) for which \( d(m) \neq 0 \) is \( 3n^{2\alpha} \) (resp., \( n^{1-2\alpha} \)).

We have the identities

\[
\sum_m r(m) = \sum_m d(m), \quad \text{(1)}
\]

\[
\sum_m r^2(m) = \sum_m d^2(m). \quad \text{(2)}
\]

The identity (1) is trivial. To see (2) we observe that the sum \( \sum_m r^2(m) \) counts the number of ordered quadruples \((i, j, i', j')\), for \((i, j, i', j') \in R'_\alpha(n)\), such that \( i^2 + j^2 = i'^2 + j'^2 \). But this quantity also counts the number of those ordered quadruples \((i, j, i', j')\), for \((i, j, i', j') \in R'_\alpha(n)\), such that \( i^2 - j^2 = i'^2 - j'^2 \), which is the value of the sum \( \sum_m d^2(m) \). Putting (1) and (2) together we have

\[
\sum_m \binom{r(m)}{2} = \sum_m \binom{d(m)}{2}. \quad \text{(3)}
\]
Writing $M_k$ for the set of those $m$ with $r(m) = k$, we have $\sum_k k|M_k| = |R'_\alpha(n)|$. On the other hand,

\[
D_\alpha(n) \geq \sum_{k \geq 1} |M_k| = \sum_{k \geq 1} k|M_k| - \sum_{k \geq 1} (k-1)|M_k| = |R'_\alpha(n)| - \sum_{k \geq 2} (k-1)|M_k|.
\]

Thus $D_\alpha(n) \geq n - O(n^{2\alpha} + n^{1-\alpha}) - \sum_{k \geq 2} (k-1)|M_k|$. Using the inequality $k - 1 \leq \binom{k}{2}$ and (3), we have

\[
\sum_{k \geq 2} (k-1)|M_k| \leq \sum_{k \geq 2} \binom{k}{2} |M_k| = \sum_{m} \binom{r(m)}{2} = \sum_{m} \binom{d(m)}{2}.
\]

Theorem 1 is therefore a trivial consequence of the following proposition.

**Proposition 2.**

\[
\sum_{m} \binom{d(m)}{2} = O\left(n^{2\alpha} \log^2 n\right).
\]

**Proof.** We need the following easy lemma.

**Lemma 3.** If a positive integer $m$ can be written as the product of two integers in two different ways, say $m = m_1m_2 = m_3m_4$, then there exists a quadruple of positive integers $(s_1, s_2, s_3, s_4)$ satisfying

\[
m_1 = s_1s_2, \quad m_2 = s_3s_4, \quad m_3 = s_1s_3, \quad m_4 = s_2s_4.
\]

**Proof.** Since $m_1$ divides $m_3m_4$, we have $m_1 = s_1s_2$ for some $s_1 \mid m_3$ and some $s_2 \mid m_4$. Putting $s_3 = m_3/s_1$ and $s_4 = m_4/s_2$, we have $m_2 = s_3s_4$, $m_3 = s_1s_3$, and $m_4 = s_2s_4$.

We write

\[
\sum_{m} \binom{d(m)}{2} = \sum_{1 \leq l \leq n^{1-2\alpha}} \sum_{m \in I_l} \binom{d(m)}{2},
\]

where $I_l = [l^2n^{2\alpha}, (l+1)^2n^{2\alpha})$. We observe that the union of the intervals, namely $[n^{2\alpha}, (1 + n^{1-2\alpha})^2n^{2\alpha})$, covers all the possible $m$ with $d(m) \neq 0$.

Now we estimate $\sum_{m \in I_l} \binom{d(m)}{2}$ for a fixed $l$, by viewing the binomials as counting unordered pairs of distinct pairs whose difference of squares is $m$. Let $a^2 - b^2 = c^2 - d^2$ ($a > c$ and $b > d$) be such a pair of distinct representations of some $m$, which is counted in the above sum $\sum_{m \in I_l} \binom{d(m)}{2}$. Since $m \in I_l$ we have

\[
l^2n^{2\alpha} \leq a^2 - b^2 < (l+1)^2n^{2\alpha}.
\]

Thus,

\[
l^2n^{2\alpha} \leq a^2 < (l+1)^2n^{2\alpha} + b^2 \leq ((l+1)^2 + 1)n^{2\alpha} < (l+2)^2n^{2\alpha}.
\]
The same inequality holds for c, so we have

\[ \ln^\alpha a, c < (l + 2)n^\alpha. \]  \hspace{1cm} (4)

Applying Lemma 3 to \((a - c)(a + c) = (b - d)(b + d)\) (clearly, the two products are distinct), we obtain a quadruple of integers \((s_1, s_2, s_3, s_4)\) satisfying

\[
\begin{align*}
    s_1s_2 &= a - c, & s_3s_4 &= a + c, \\
    s_1s_3 &= b - d, & s_2s_4 &= b + d.
\end{align*}
\]

Using (4) and \(0 \leq b, d \leq n^\alpha\) we have the following inequalities:

\[
\begin{align*}
    1 &\leq s_1, s_2, s_3, s_4 \leq 2n^\alpha, \\
    2\ln^\alpha &\leq s_3s_4 < (2l + 4)n^\alpha. \hspace{1cm} (5)
\end{align*}
\]

It is clear from the above inequalities that \(s_i \leq 2n^\alpha\), for \(i = 1, \ldots, 4\). From \(s_2s_4 \leq 2n^\alpha\), \(s_1s_3 \leq 2n^\alpha\), and \(2\ln^\alpha \leq s_3s_4\), we also deduce that

\[
1 \leq s_2 \leq \frac{s_3}{l} \quad \text{and} \quad 1 \leq s_1 \leq \frac{s_4}{l}. \hspace{1cm} (6)
\]

Choose \(s_3\) between 1 and \(2n^\alpha\). Then choose \(s_4\), according to (5), in the range \(\left[\frac{2\ln^\alpha}{s_3}, \frac{(2l + 4)n^\alpha}{s_3}\right]\).

Then choose \(s_1\) and \(s_2\), according to (6), in \(\frac{s_3}{l} \leq \frac{s_4}{l} \leq \frac{(2l + 4)n^\alpha}{l^2}\) ways. The overall number of quadruples \((s_1, s_2, s_3, s_4)\) under consideration is thus at most

\[
\sum_{1 \leq s_3 \leq 2n^\alpha} \frac{4n^\alpha}{s_3} \cdot \frac{(2l + 4)n^\alpha}{l^2} = O\left(\frac{n^{2\alpha + \log n}}{l}\right).
\]

Finally we have

\[
\sum_m \left(\frac{d(m)}{2}\right) \leq \sum_{1 \leq l \leq n^{1-2\alpha}} \sum_{m \in I_l} \left(\frac{d(m)}{2}\right) = O\left(\sum_{l \leq n^{1-2\alpha}} \frac{n^{2\alpha + \log n}}{l}\right) = O\left(n^{2\alpha + \log^2 n}\right). \]

**Discussion.** Theorem 1 is closely related to a special case of a fairly deep conjecture in number theory, stated as Conjecture 13 in Cilleruelo and Granville [3]. This special case, given in [3, Eq. (5.1)], asserts that, for any integer \(N\), and any fixed \(\beta < 1/2\),

\[
\left| \{(a, b) \in \mathbb{Z}^2 \mid a^2 + b^2 = N, \ |b| < N^{\beta}\} \right| \leq C_\beta,
\]

where \(C_\beta\) is a constant that depends on \(\beta\) (but not on \(N\)). A simple geometric argument shows that this is true for \(\beta \leq 1/4\) but it is unknown for any \(1/4 < \beta < 1/2\). If that latter conjecture were true, a somewhat weaker version of Theorem 1 would follow. Indeed, let \(N\) be an integer that can be written as \(i^2 + j^2\), for \(\frac{1}{2}n^{1-\alpha} \leq i \leq n^{1-\alpha}\) and \(j \leq n^\alpha\). Then \(N = \Theta(n^{2(1-\alpha)})\), and \(j = O(N^{\beta})\), for \(\beta = \alpha/(2(1-\alpha)) < 1/2\).

Conjecture 13 of [3] would then imply that the number of pairs \((i, j)\) as above is at most the constant \(C_\beta\). In other words, each of the \(\Theta(n)\) distances in the portion of \(R_\alpha(n)\) with
\[ i \geq \frac{1}{2} n^{1-\alpha}, \] interpreted as a distance from the origin \((0,0)\), can be attained at most \(C_\beta\) times. Hence \(D_\alpha(n) = \Theta(n)\), as asserted in Theorem 1.

The general form of conjecture 13 [3] asserts that the number of integer lattice points on an arc of length \(N^{\beta}\) on the circle \(a^2 + b^2 = N\) is bounded by some constant \(C_\beta\), for any \(\beta < 1/2\). Cilleruelo and Córdoba [2] have proved this for \(\beta < 1/4\). See also Bourgain and Rudnick [1] for some consequences of this conjecture.

A heuristic argument that supports the above conjecture is the following: It is well known that the quantity \(r(N)\), that counts the number of lattice points on the circle \(x^2 + y^2 = N\), satisfies \(r(N) \ll N^\varepsilon\) for any \(\varepsilon > 0\). If the lattice points were distributed at random along the circle, an easy calculation would show that the probability that an arc of length \(N^{\beta}\) contains \(k\) lattice points is bounded by \((r(N)^k)N^{(k-1)(\beta-1/2)}\). Now, for any \(\beta < 1/2\), there exists \(k\) such that the infinite sum \(\sum_N \left(\frac{r(N)^k}{N^{(k-1)(\beta-1/2)}}\right)\) converges, and the Borel–Cantelli Lemma would then imply that, with probability 1, only a finite number of circles can contain \(k\) lattice points on arcs of length \(N^{\beta}\).

**Acknowledgements.** The authors would like to thank Zeev Rudnick for useful discussions on some of the number-theoretic issues.

**References**


