Contemporary Mathematics
Volume **00**, XXXX

A new entropy inequality for the Erdős distance problem

Nets Hawk Katz and Gábor Tardos

Abstract. This note combines the techniques of two earlier papers [**T**] and [**K**] for an improved lower bound on the long standing (see e.g. [**E**],[**M**],[**SzT**], and [**CSzT**]) Erdős problem on distinct distances in the plane: Given n distinct points in the plane what is the minimum number of *distinct* distances they determine. We improve the $\Omega(n^{19/22-\epsilon})$ bound for this problem stated in [**K**] to

$$\Omega\left(n^{\frac{48-14e}{55-16e}-\epsilon}\right),$$

where e is the base of the natural logarithm and $\epsilon > 0$ is arbitrary.

The proof of this lower bound (just as the proofs of the last three such bounds) is based on the connection between this problem and the following problem on distinct sums: Given an n by s real matrix with all sn entries distinct, what is the minimum number of *distinct* pairwise sums formed by adding two distinct entries of a common row of the matrix. The connection between the two problems was discovered by J. Solymosi and Cs. Tóth [**ST**]; the distinct sum problem was explicitly formulated in [**T**] where some bounds were established. The paper [**K**] proves stronger bounds for the distinct sum problem in the special case $s = 5$. This note combines the techniques of that paper with those of [**T**] to obtain similar bounds for higher values of s.

Lower bounds on the distinct sum problem were also applied in [**STT**] and [**PT**]. Plugging in our bounds, one can automatically improve the results of these papers on the number of occurrences of the k most frequent distances among n points and the number of isosceles triangles determined by n points in the plane.

§1. Introduction, definitions

The results of this note follow by simply combining the techniques of two earlier papers of the authors [**K**] and [**T**]. We will use the notation of [**T**] and many of the lemmas there, so the reader is advised to read that paper first. Nonetheless we recall the definitions from that paper.

For an n by s matrix $A = (a_{ij})$ we define $S(A) = \{a_{ij} + a_{ik} \mid 1 \leq i \leq n, 1 \leq j < k \leq s\}$ the set of pairwise sums of entries from the same row. Let $f_s(n)$ be the

1991 *Mathematics Subject Classification.* 05D99.

Key words and phrases. entropy, Erdős distance problem, restricted sumsets.

The first author was in part supported by the NSF grant 0100601. The second author was partially supported by the grant OTKA T037486.

minimum size $|S(A)|$ for a real n by s matrix with all its sn entries being pairwise distinct.

Both $f_3(n)$ and $f_4(n)$ are $\Theta(n^{1/3})$. The order of magnitude of $f_s(n)$ for higher values of s is not known. I. Ruzsa [**R**] gave the best known construction, which establishes

$$f_{2k}(n) = O\left(n^{\frac{1}{2}-\frac{1}{4k-2}}\right),$$

for any fixed k. The first lower bound was proved in [T]:

$$f_{2k-1}(n) \geq n^{\frac{1}{c_k}},$$

with the values c_k defined below. The paper [K] improves the lower bound for $f_5(n)$ establishing

$$f_5(n) = \Omega\left(n^{\frac{7}{19}-\epsilon}\right),$$

for any $\epsilon > 0$. As $1/c_k < 1/e < 7/19$ for any k this also improves the lower bound for all the functions $f_s(n)$ for $s > 5$ as $f_s(n)$ is clearly increasing in s. Nevertheless we present here the formula defining c_k as these values will play a role in the bounds presented in this note.

For $2 \leq k \leq 14$ we let

$$c_k = \sum_{i=0}^{k} \frac{1}{i!} + \frac{1}{(k-1)k!}.$$

For $k \geq 14$ we let

$$c_k = \sum_{i=0}^{k} \frac{1}{i!} + \frac{k^3 - 7k^2 + 20k - 40}{(k^4 - 8k^3 + 26k^2 - 46k + 40)k!}.$$

Either definition gives the same value for c_{14} and we clearly have that the values c_k tend to e, the base of the natural logarithm, as k goes to infinity.

The proof of the lower bound in [**T**] is based on an involved calculation of entropies of different functions. For a discreet random variable R, its *entropy* is given by

$$H(R) = -\sum_x P[R = x] \log P[R = x],$$

where the summation extends for all values x taken by R with positive probability. Here and later in this note H denotes the binary entropy and log stands for the binary logarithm. The entropy of a random variable is the amount of information obtained by resolving its value. The idea which this note will refine is that because of various arithmetic identities between entries of a matrix and their sums, the amount of information obtained from resolving an entry can be controlled using the amount of information obtained in resolving a sum.

Consider an n by s real matrix A with all its entries distinct. The basic probability space considered is that of a uniformly distributed random row $R = (R_1, \ldots, R_s)$ of A. Clearly

$$H(R) = \log n.$$

Let $I = \{1, 2, \ldots, s\}$ be the set of column indexes. In [T] we considered subsets U and V of I (not both the empty set) and defined $p_{UV}(R)$ to be the sequence of numbers consisting of the differences $R_i - R_j$ for $i, j \in U$ and for $i, j \in V$ and the sums $R_i + R_j$ for $i \in U$ and $j \in V$. We defined

$$H(U, V) = H(p_{UV}(R)),$$

and formed the normalized averages

$$H_{i,j} = 1 - \frac{1}{\log n \binom{n}{i}\binom{n-i}{j}} \sum_{U,V} H(U, V),$$

for $i, j \geq 0$ with $1 \leq i + j \leq s$ where the summation extends for all disjoint pairs of subsets U and V of I with $|U| = i$, $|V| = j$.

The paper [**T**] is based on establishing numerous linear inequalities connecting the values $H(U, V)$ (Lemma 3 of [**T**]) and using them to bound $|S(A)|$. We are going to simply quote these inequalities. The novelty in the paper [**K**] is basically proving yet another similar inequality. This is not explicit in the paper, so we have to prove the new inequality. We do this in the next section. In the third section we combine all these inequalities to give our new lower bounds for $|S(A)|$. In the final section we discuss the implications of our result (including the improved bound on the Erdős problem on distinct distances in the plane) and the possible directions for further improvements.

§2 The new inequality

Let i, j and k be three distinct indices from I. Let $U = \{i, j, k\}$.

Lemma 1.

$$2H(\{i\}, \{j\}) + 2H(\{j\}, \{k\}) + H(\{i\}, \{k\}) \geq H(\{i, k\}, \{j\}) - 2H(U, \emptyset) + 3 \log n.$$

Proof. The important new idea in [**K**](which appeared in a slightly different context in [**KT**]) is to consider (instead of a single random row) random *pairs* of rows of the matrix A and a specially defined function ν on them. Consider the following distribution $[R, S]$ on pairs of rows of A: select R uniformly randomly from the n rows of A and then select S uniformly randomly among those rows of A satisfying

$$p_{U\emptyset}(R) = p_{U\emptyset}(S).$$

Throughout this section, we use square brackets instead of parentheses for tuples of random variables so as not to conflict with the notation of the previous section. Notice that S is also distributed uniformly among the n rows and we have

$$H(R) = H(S) = \log n, \tag{1}$$

$$H([R, S]) = 2 \log n - H(U, \emptyset). \tag{2}$$

The equivalence of the three definitions of the following function comes from $p_{U\emptyset}(R) = p_{U\emptyset}(S)$:

$$\nu(R, S) = (R_i + R_k) + 2S_j = (R_i + R_j) + (S_j + S_k) = (R_j + R_k) + (S_i + S_j).$$

First we use *subadditivity* of the entropy which states that for random variables X and Y we have $H(X) + H(Y) \geq H([X, Y])$. We also use *monotonicity* stating that if the value of X determines the value of Y then $H(X) \geq H(Y)$. These are obvious from an information theoretic point of view.

Clearly, $\nu(R,S)$ and R_i+R_k together determine S_j, and since all the entries of A are distinct, S_j determines the entire row S. Furthermore, S determines the pattern $p_{U\emptyset}(R)$ and thus, together with R_i+R_k they determine the values R_i and R_k and by that the entire row R. By the subadditivity and the monotonicity of the entropy we thus have

$$H(\nu(R,S))+H(R_i+R_k)\geq H([R,S]). \tag{3}$$

Next we use the *submodularity* of the entropy function: if either one of the random variables X and Y determines the value of the variable Z, then $H(X)+H(Y)\geq H([X,Y])+H(Z)$. This inequality implies the other information inequalities we used. It is usually referred to as the non-negativity of the conditional mutual information. For this, and all other simple properties of the entropy we use in this note see e.g. Lemma 3.2 on page 49 of [**CsK**].

As either one of the pairs $[R_i+R_j,S_j+S_k]$ or $[R_j+R_k,S_i+S_j]$ determines the value of the function ν (as their sum) we have

$$\begin{aligned}&H([R_i+R_j,S_j+S_k])+H([R_j+R_k,S_i+S_j])\\&\geq H([R_i+R_j,S_j+S_k,R_j+R_k,S_i+S_j])+H(\nu(R,S)).\end{aligned} \tag{4}$$

By the subadditivity we have

$$H(R_i+R_j)+H(S_j+S_k)\geq H([R_i+R_j,S_j+S_k]), \tag{5}$$

$$H(R_j+R_k)+H(S_i+S_j)\geq H([R_j+R_k,S_i+S_j]). \tag{6}$$

The row R determines the pattern $p_{U\emptyset}(S)$ and, together with S_i+S_j they determine S_i and S_j and thus the entire row S. We apply submodularity to $X=R, Y=[R_i+R_j,S_j+S_k,R_j+R_k,S_i+S_j]$, and $Z=[R_i+R_j,R_j+R_k]$, observing by monotonicity that $H[R,R_i+R_j,S_j+S_k,R_j+R_k,S_i+S_j]\geq H[R,S]$ to obtain

$$H([R_i+R_j,S_j+S_k,R_j+R_k,S_i+S_j])+H(R)\geq H([R,S])+H([R_i+R_j,R_j+R_k]). \tag{7}$$

Simply add the Inequalities (3-7) to get

$$\begin{aligned}&H(R_i+R_k)+H(R_i+R_j)+H(R_j+R_k)+H(S_i+S_j)+H(S_j+S_k)\\&\geq 2H([R,S])-H(R)+H([R_i+R_j,R_j+R_k]).\end{aligned} \tag{8}$$

Here $H(R_i+R_k)=H(\{i\},\{k\})$ as R is uniformly distributed among the rows of A. Similar arguments about the other four terms simplify the left hand side of (8) to $H(\{i\},\{k\})+2H(\{i\},\{j\})+2H(\{j\},\{k\})$. The first two terms of the right hand side of (8) is given by Equations (1) and (2). Finally for the last term of (8) we have $H([R_i+R_j,R_j+R_k])=H(\{i,k\},\{j\})$ as R is a uniformly distributed random row and (R_i+R_j,R_j+R_k) and the pattern $p_{\{i,k\}\{j\}}(R)$ mutually determine each other, so they have the same entropy. Applying all these simplifications to Inequality (8) the statement of the lemma follows. □

§3 Combining the old and new inequalities

We start with the standard averaging argument that shifts focus from the variables $H(U,V)$ to the variables $H_{i,j}$.

LEMMA 2. $5H_{1,1}-H_{2,1}+2H_{3,0}\leq 3$.

Proof. Consider the inequality claimed by Lemma 1 for all possible triples (i,j,k). Simply sum all these inequalities and then a rearrangement gives the statement of this lemma. □

Our lower bound method works for odd values of $s \geq 5$. We assume $s = 2k-1$ for some $k \geq 3$.

We collect all the inequalities we need for our bound. All of them come from [**T**] except the statement of Lemma 2 which basically comes from [**K**]. We will freely use the trivial fact of $H_{i,j} = H_{j,i}$ (see e.g. Lemma 4/a of [**T**]) and use the following equivalent form of Lemma 2:

$$5H_{1,1} - H_{1,2} + 2H_{0,3} \leq 3. \tag{9}$$

By Lemma 4/e (convexity) of [**T**] we have

$$2H_{1,1} \leq H_{0,1} + H_{1,2}, \tag{10}$$

$$H_{1,2} - H_{2,3} \leq 2(H_{0,2} - H_{1,2}). \tag{11}$$

By Lemmas 4/c and 4/f of [**T**] we have

$$H_{1,1} + H_{0,2} \leq 1. \tag{12}$$

Finally we also need an inequality of the following form:

$$H_{2,3} \leq \alpha_3 H_{0,3}, \tag{13}$$

where the constant α_3 is to be determined later. Such an inequality is proved in the proof of Theorems 8 and 10 of [**T**]. We sketch the argument here. For the reader's convenience we restate Lemmas 5, 6, and 9 of [**T**] as parts a, b, and c of the following lemma.

Lemma 3.

a.) We have $H_{k-2,k-1} \leq \frac{3}{k-1} H_{0,k-1}$

b.) Suppose we have $H_{j-1,j} \leq \alpha H_{0,j}$ *for some* $3 \leq j < k$ *and* $\alpha > 0$. *If* $(j-3)\alpha \leq 2$ *then we also have* $H_{j-2,j-1} \leq \beta H_{0,j-1}$ *for* $\beta = \frac{2+\alpha}{j+\alpha} > 0$ *and* $(j-4)\beta \leq 2$ *is also satisfied.*

c.) If $k \geq 14$ *we have* $H_{k-3,k-2} \leq \frac{2k+3}{k^2-k+4} H_{0,k-2}$.

We use Lemma 3/b recursively to find an inequality of the form (13). The base case for $k \leq 14$ is $\alpha_{k-1} = 3/(k+1)$ provided by Lemma 3/a, while for $k \geq 14$ Lemma 3/c provides the base case: $\alpha_{k-2} = (2k+3)/(k^2-k+4)$. We proceed by reverse induction obtaining inequalities with progressively lower subscripts until $\alpha_2 = (2+\alpha_3)/(3+\alpha_3) = c_k - 2$ is found. This is done in detail in [**T**] Theorems 8 and 10. Here c_k is the value defined in Section 1. Thus we have that Inequality (13) holds with

$$\alpha_3 = \frac{1}{3-c_k} - 3. \tag{14}$$

For $k = 3$ the above argument is not valid (the base case of the reverse induction is $\alpha_2 = 3/4$ so we cannot argue about α_3). But for $k = 3$ Equation (14) gives $\alpha_3 = 1$ and thus Inequality (13) follows simply from the monotonicity condition Lemma 4/b of [**T**].

Let us combine the Inequalities (9-13) with the positive coefficients α_3, $6-\alpha_3$, 2, 4, and 2, respectively. We get

$$(16+3\alpha_3)H_{1,1} \le 10+2\alpha_3. \tag{15}$$

Using Lemma 4/d of [**T**], Inequality (15) and Equation (14) we get

$$\frac{\log|S(A)|}{\log n} \ge 1-H_{1,1} \ge \frac{6+\alpha_3}{16+3\alpha_3} = \frac{10-3c_k}{24-7c_k}.$$

We have just proved the following

THEOREM 4. *For any $k \ge 3$ we have*

$$f_{2k+1}(n) \ge n^{\frac{10-3c_k}{24-7c_k}}.$$

4. Corollaries and concluding remarks

First we use that c_k tends to e, the base of the natural logarithm to state

COROLLARY 5. *For any $\epsilon > 0$ there exists an $s > 0$ such that for all $n > 0$ we have*

$$f_s(n) \ge n^{\frac{10-3e}{24-7e}-\epsilon}.$$

Using the connection between the distinct sum problem studied in this note and the distinct distance problem of Erdős found in [**ST**] and stated explicitly in Corollary 14 of [**T**] we have

COROLLARY 6. *For any constant $\epsilon > 0$ the following is true. Any collection P of n distinct points in the plane has an element from which the number of distinct distances to the other points is*

$$\Omega\left(n^{\frac{48-14e}{55-16e}-\epsilon}\right).$$

The main results of the papers [**STT**] and [**PT**] automatically improve when plugging in the new bound for $f_s(n)$ stated in Corollary 5. We state the improved bounds here for completeness. Both of these results follow from bounds on the number of incidences between a set of points and another set of systems of concentric circles. The bounds on the number of these incidences also improves but we refrain from stating the complicated upper bound here.

COROLLARY 7. *For any constant $\epsilon > 0$ the following is true. Any collection of n distinct points in the plane the number of occurences of the "most popular" k distances is*

$$O\left(n^{\frac{5}{3}} \cdot \left(\frac{k}{n^{\frac{1}{3}}}\right)^{\frac{55-16e}{89-26e}+\epsilon}\right).$$

COROLLARY 8. *For any constant $\epsilon > 0$ the following is true. Any collection of n distinct points in the plane determine*

$$O\left(n^{\frac{117-34e}{55-16e}+\epsilon}\right)$$

isosceles triangles.

The special cases of Theorem 4 for the first few values of k are as follows:

$$f_5(n) \ge n^{\frac{7}{19}},$$

$$f_7(n) \geq n^{\frac{33}{89}},$$
$$f_9(n) \geq n^{\frac{59}{159}}.$$

All these are slight improvements of the $\Omega(n^{7/19-\epsilon})$ bound of [**K**].

The numeric values of the exponents in the Corollaries 5 and 6 are

$$\frac{10-3e}{24-7e} = 0.371107\ldots,$$
$$\frac{48-14e}{55-16e} = 0.864137\ldots.$$

These represent slight improvement over the corresponding exponents

$$\frac{7}{19} = 0.368421\ldots,$$
$$\frac{19}{22} = 0.863636\ldots$$

of [**K**].

Note that the lower bounds of [**T**] on $|S(A)|$ work for all matrices A with the property that no two rows share *more than a single common entry.* Our results here use however that *all entries of A are distinct.*

The improvements of [**K**] and this note over the results in [**T**] were possible because a new probability distribution (on pairs of rows) was considered. We expect that our results could be further improved by considering another distribution or simply the entropies of another functions of these distributions. Whenever one discovers a linear constraint on the entropies which contradicts the optimal solution under the present constraints, it is a straightforward (but sometimes technical) task to solve the new linear program and find an improved bound this way. In this note, we have followed precisely this approach based on the new inequality implicit in [**K**].

References

[CSzT] F. Chung, E. Szemerédi, W. Trotter, *The number of different distances determined by a set of n points in the Euclidean plane*, Discrete and Computational Geometry **7** (1992), 1–11.

[CsK] I. Csiszár, J. Körner, *Information Theory: Coding theorems for discrete memoryless systems*, Academic Press, New York, 1981.

[E] P. Erdős, *On sets of distances of n points*, American Mathematical Monthly **53** (1946), 248–250.

[K] N. Katz, *An improvement of a lemma of Tardos*, submitted to *Combinatorica.*

[KT] N. Katz, T. Tao, *New Bounds for Kakeya Problems*, Journal D'Analyse Mathématique **87** (2002), 231–263.

[M] L. Moser, *On the different distances determined by n points*, American Mathematical Monthly **59** (1952), 85–91.

[PT] J. Pach, G. Tardos, *Isosceles triangles determined by a planar point set*, Graphs and Combinatorics **18** (2002), 769–779.

[R] I. Ruzsa, *A Problem on restricted sumsets*, to appear in this volume.

[ST] J. Solymosi, Cs. Tóth, *Distinct Distances in the Plane*, Discrete and Computational Geometry **25** (2001), 629–634.

[STT] J. Solymosi, G. Tardos, Cs. Tóth, *The k most frequent distances in the plane*, to appear, Discrete and Computational Geometry.

[SzT] E. Szemerédi, W. Trotter, *Extremal problems in discrete geometry*, Combinatorica **3** (1983), 381–392.

[T] G. Tardos, *On distinct sums and distinct distances*, to appear, Advances in Mathematics.

Department of Mathematics, Washington University, St. Louis
E-mail address: nets@math.wustl.edu

Rényi Institute, Budapest, Hungary
E-mail address: tardos@renyi.hu