

# Norm-graphs: variations and applications

NOGA ALON <sup>1</sup>

*School of Mathematics, Institute for Advanced Study  
Olden Lane, Princeton, NJ 08540 and  
Department of Mathematics, Tel Aviv University  
Tel Aviv, Israel 69978  
e-mail: noga@math.tau.ac.il*

LAJOS RÓNYAI <sup>2</sup>

*Computer and Automation Institute, Hungarian Academy of Sciences  
1111 Budapest, Lágymányosi u. 11, Hungary  
e-mail: lajos@nyest.ilab.sztaki.hu*

TIBOR SZABÓ <sup>3</sup>

*School of Mathematics, Institute for Advanced Study  
Olden Lane, Princeton, NJ 08540 and  
University of Illinois at Urbana-Champaign  
1409 W Green St, Urbana, IL 61801  
e-mail: tszabo@math.uiuc.edu*

## Abstract

We describe several variants of the norm-graphs introduced by Kollár, Rónyai, and Szabó and study some of their extremal properties. Using these variants we construct, for infinitely many values of  $n$ , a graph on  $n$  vertices with more than  $\frac{1}{2}n^{5/3}$  edges, containing no copy of  $K_{3,3}$ , thus slightly improving an old construction of Brown. We also prove that the maximum number of vertices in a complete graph whose edges can be colored by  $k$  colors with no monochromatic copy of  $K_{3,3}$  is  $(1 + o(1))k^3$ . This answers a question of Chung and Graham. In addition we prove that for every fixed  $t$ , there is a family of subsets of an  $n$  element set whose so-called dual shatter function is  $O(n^t)$  and whose discrepancy is  $\Omega(n^{1/2-1/2t}\sqrt{\log n})$ . This settles a problem of Matoušek.

---

<sup>1</sup>Research supported in part by a State of New Jersey grant, by a USA Israeli BSF grant, and by the Hermann Minkowski Minerva Center for Geometry at Tel Aviv University.

<sup>2</sup>Research supported in part by OTKA Grants 016503, 016524, NWO-OTKA Grant 048.011.002, MKM Grant FKFP 0612/1997 and EC Grant ALTEC KIT.

<sup>3</sup>Research supported in part by the Alfred P. Sloan Foundation Grant 96-6-2 and the State of New Jersey.

# 1 Introduction

Let  $H$  be a fixed graph. The classical problem from which extremal graph theory has originated is to determine the maximum number of edges in a graph on  $n$  vertices which does not contain a copy of  $H$ . This maximum value is the *Turán number* of  $H$  and is customarily denoted by  $\text{ex}(n, H)$ .

Because of the Erdős-Simonovits-Stone Theorem — which supplies an asymptotic formula for  $\text{ex}(n, H)$  for every fixed graph  $H$  of chromatic number at least 3 — the determination of the Turán numbers is particularly interesting when  $H$  is bipartite. In most of these cases even the question of finding the correct order of magnitude (that is, determining the value of  $\text{ex}(n, H)$  up to a constant factor depending on  $H$ ) is open.

The problem of estimating the Turán numbers of complete bipartite graphs (which is sometimes called the “Zarankiewicz problem”) is of special interest, and received a considerable amount of attention during the years. (See, e.g., Chapter VI, Section 2 of Bollobás [1] and the more recent paper of Füredi [9] for some details and references.)

Let  $t, s$  be positive integers with  $t \leq s$ . We denote by  $K_{t,s}$  the complete bipartite graph with  $t + s$  vertices and  $ts$  edges. Kővári, T. Sós and Turán [11] proved that for every fixed  $t$  and  $s \geq t$ :

$$\text{ex}(n, K_{t,s}) \leq \frac{1}{2}(s-1)^{1/t}n^{2-\frac{1}{t}} + \frac{1}{2}(t-1)n, \quad (1)$$

The right hand side is conjectured to give the correct order of magnitude for every fixed  $t$  and  $s$ . However, the best known general lower bound, obtained by the probabilistic method, yields only

$$c'n^{2-\frac{s+t-2}{st-1}} \leq \text{ex}(n, K_{t,s}), \quad (2)$$

where  $c'$  is a positive absolute constant, (cf. e.g., [7], p.61, proof of inequality (12.19).)

Note that for all  $t, s$  such that  $2 \leq t \leq s$ , we have  $\frac{s+t-2}{st-1} > \frac{1}{t}$ , hence the lower bound (2) is always of a lower order of magnitude than the upper bound (1).

The upper bound (1) was proven to be asymptotically tight for all pairs  $(t, s)$  with  $s \geq t = 2$  (Erdős, Rényi and T. Sós [6], Brown [2] for  $s = t = 2$ , Füredi [9] for  $s \geq t = 2$ ).

For  $t = s = 3$  an asymptotic formula is known as well. Brown [2] gave a construction and Füredi [8] improved on (1), thus proving

$$\text{ex}(n, K_{3,3}) = \frac{1}{2}n^{5/3} + o(n^{5/3}). \quad (3)$$

Brown's construction clearly supplies the correct order of magnitude for  $t = 3$  and any fixed  $s \geq 3$ . More recently, in [12], the authors described a general construction which established the optimality of the upper bound (1) up to a constant factor (depending only on  $s$  and  $t$ ) for every  $t > 3$  and  $s > t!$ .

Here we first show that a simple variant of the construction of [12] implies that the upper bound (1) is in fact optimal up to a constant factor even for  $s > (t-1)!$ . We next describe several

applications of this variant and some related ones to various extremal problems. In particular, we describe explicit  $K_{3,3}$ -free graphs which are slightly denser than those in the construction of Brown. The properties of these graphs enable us to use them for determining the asymptotic behavior of the multicolor Ramsey number  $R_k(K_{3,3})$ , which is the maximum number of vertices in a complete graph whose edges can be colored by  $k$  colors without a monochromatic copy of  $K_{3,3}$ . It turns out that this number is  $(1 + o(1))k^3$ , thus settling a problem of Chung and Graham [3], [4], who showed (with Spencer) that this number is at least  $\Omega(k^3/\log^3 k)$  and at most  $(2 + o(1))k^3$ . The order of magnitude of several related Ramsey numbers can also be determined in a similar manner.

A slight variation of the construction, motivated by ideas of Füredi [9], supplies some additional information on the behavior of the Turán numbers  $\text{ex}(n, K_{t,s})$  for  $s$  which is much larger than  $t$ . This is related to an extension of a question of Erdős.

Finally, using a simple generalization of the original construction of [12] we obtain tight lower bounds for several asymmetric instances of the Zarankiewicz problem. This helps to settle a problem of Matoušek in Discrepancy Theory.

The rest of the paper is organized as follows. In the next section we describe a projective version of the norm-graphs that supplies explicit dense  $K_{3,3}$ -free graphs. The proofs here require only elementary algebra. In section 3 we apply these graphs to obtain an asymptotic formula for the Ramsey number  $R_k(K_{3,3})$ . In Section 4 we define the projective norm-graphs in full generality and observe that they can be used to settle an extension of a question of Erdős. In Section 5 we use a slight variation of the original norm-graphs to study some asymmetric cases of the Zarankiewicz problem, and briefly describe the relevance of this construction to discrepancy theory.

Throughout the paper it is convenient to choose some of the parameters to be primes (or prime powers). In order to extend the results to every value of the parameters we always make use of the fact that there is a prime number between  $n$  and  $n + o(n)$ . (In the proof of Theorem 9 we even need this statement for primes congruent to 1 modulo a fixed number  $r$ .) For a much more general result we refer the reader to the paper of Huxley and Iwaniec [10].

## 2 Projective $K_{3,3}$ -free norm-graphs

Let  $GF(q)^*$  denote the multiplicative subgroup of the  $q$  element field. The graph  $H = H(q, 3)$  is defined as follows. The vertex set  $V(H)$  is  $GF(q^2) \times GF(q)^*$ . Two distinct vertices  $(A, a)$  and  $(B, b) \in V(H)$  are connected if and only if  $N(A + B) = ab$ , where  $N(X) = X^{1+q}$  is the norm<sup>4</sup> of  $X \in GF(q^2)$  over  $GF(q)$ . Of course  $N(X) \in GF(q)$  and it is clear that  $|V(H)| = q^3 - q^2$ . If  $(A, a)$  and  $(B, b)$  are adjacent, then  $(A, a)$  and  $B \neq -A$  determine  $b$ . Thus  $H$  is regular of degree  $q^2 - 1$ .

---

<sup>4</sup>The *norm* of the field extension  $GF(q^l)$  over  $GF(q)$  is the map  $N_l$  defined on  $GF(q^l)$  by  $N_l(A) = A \cdot A^q \cdots A^{q^{l-1}}$ . We drop the subscript  $l$  throughout, as it will be apparent from the context. Clearly  $N$  is a multiplicative function: if  $A, B \in GF(q^l)$  then  $N(AB) = N(A)N(B)$ . From  $N(A)^q = N(A)$  we infer that  $N(A) \in GF(q)$  for every  $A \in GF(q^l)$ . Indeed, the roots of the polynomial  $x^q - x$  are precisely the elements of  $GF(q)$ , and it vanishes at  $N(A)$ .

We prove that  $H(q, 3)$  is  $K_{3,3}$ -free and hence provides an improvement (in the second term) over Brown's construction for a dense  $K_{3,3}$ -free graph. (The Brown-graph has  $\frac{1}{2}n^{5/3} - \frac{1}{2}n^{4/3}$  edges for infinitely many values of  $n$ .)

**Theorem 1** *The graph  $H = H_{q,3}$  contains no subgraph isomorphic to  $K_{3,3}$ . Thus there exists a constant  $C$  such that for every  $n = q^3 - q^2$  where  $q$  is a prime power*

$$\text{ex}(n, K_{3,3}) \geq \frac{1}{2}n^{\frac{5}{3}} + \frac{1}{3}n^{\frac{4}{3}} + C.$$

It is worthwhile to note that the the upper bound of Füredi [8] is  $\text{ex}(n, K_{3,3}) \leq \frac{1}{2}n^{\frac{5}{3}} + n^{\frac{4}{3}} + 3n$ .

*Proof:* The statement of Theorem 1 is a direct consequence of the following: if  $(D_1, d_1), (D_2, d_2), (D_3, d_3)$  are distinct elements of  $V(H)$ , then the system of equations

$$\begin{aligned} N(X + D_1) &= xd_1 \\ N(X + D_2) &= xd_2 \\ N(X + D_3) &= xd_3 \end{aligned} \tag{4}$$

has at most two solutions  $(X, x) \in GF(q^2) \times GF(q)^*$ .

Observe that if the system has at least one common solution  $(X, x)$ , then

- (i)  $X \neq -D_i$  for any  $i = 1, 2, 3$  and
- (ii)  $D_i \neq D_j$  if  $i \neq j$ .

The latter is true, because if  $D_i = D_j$ , then the presence of a common neighbor implies  $d_i = d_j$ .

Because of (i) we can divide the first two equations by the last one and get rid of  $x$ . The norm is a multiplicative function, so we obtain  $N((X + D_i)/(X + D_3)) = d_i/d_3$ ,  $i = 1, 2$ .

We can divide each equation by  $N(D_i - D_3)$ , since these are nonzero by (ii). Then we can substitute  $Y = 1/(X + D_3)$ ,  $A_i = 1/(D_i - D_3)$  and  $b_i = d_i/(d_3N(D_i - D_3))$  and obtain the following two equations:

$$\begin{aligned} N(Y + A_1) &= (Y + A_1)(Y^q + A_1^q) = b_1 \\ N(Y + A_2) &= (Y + A_2)(Y^q + A_2^q) = b_2 \end{aligned} \tag{5}$$

where we used the fact that  $(A + B)^q = A^q + B^q$  for all  $A, B$  in  $GF(q^2)$ .

We need the following simple Lemma.

**Lemma 2** *Let  $K$  be a field and  $a_{ij}, b_i \in K$  for  $1 \leq i, j \leq 2$  such that  $a_{1j} \neq a_{2j}$ . Then the system of equations*

$$\begin{aligned} (x_1 - a_{11})(x_2 - a_{12}) &= b_1, \\ (x_1 - a_{21})(x_2 - a_{22}) &= b_2 \end{aligned} \tag{6}$$

*has at most two solutions  $(x_1, x_2) \in K^2$ .*

*Proof:* Subtracting the first equation from the second we get

$$(a_{11} - a_{21})x_2 + (a_{12} - a_{22})x_1 + a_{21}a_{22} - a_{11}a_{12} = b_2 - b_1.$$

Here we can express  $x_1$  in terms of a linear function of  $x_2$ , since  $a_{12} \neq a_{22}$ . Substituting this back into one of the two equations of (6) we obtain a quadratic equation in  $x_2$  with a nonzero leading coefficient (since  $a_{11} \neq a_{21}$ ). This has at most two solution in  $x_2$  and each one determines  $x_1$  uniquely.

□

We can apply the Lemma with  $x_1 = Y, x_2 = Y^q, a_{11} = -A_1, a_{12} = -A_1^q, a_{21} = -A_2, a_{22} = -A_2^q$ . The conditions of the Lemma hold since  $-A_1^q = a_{12} = a_{22} = -A_2^q$  would mean  $A_1 = A_2$ , which is impossible by (ii). Hence the system of equations (5) has at most two solutions in  $Y$ . These solutions are in one-to-one correspondence with the solutions  $(X, x)$  of the equations (4), so Theorem 1 is proved.

□

### 3 Ramsey numbers

Let  $k \geq 2$  be an integer and let  $G$  be a graph. The  $k$ -color Ramsey number  $R_k(G)$  is the maximum integer  $m$  such that one can color the edges of the complete graph  $K_m$  using  $k$  colors with no monochromatic copy of  $G$ .

The multicolor Ramsey number of a bipartite graph is strongly related to its Turán number through the following simple inequality.

$$k \cdot \text{ex}(R_k(G), G) \geq \binom{R_k(G)}{2} \tag{7}$$

Using the above inequality, an upper bound on the Turán number can immediately be converted into an upper bound on the corresponding multicolor Ramsey number. On the other hand we obtain a lower bound for the Ramsey number from a lower bound on the Turán number if our construction of a  $G$ -free graph can appropriately be used to construct an (almost) complete tiling of the complete graph.

In Brown's graph the vertices are the points of the 3-dimensional affine space over finite fields of order  $q$  with, say,  $q \equiv -1 \pmod{4}$ . The neighborhood of a vertex is given by the points of a "Euclidean sphere" around it. Unfortunately the construction *only* works if the "squared radius" of the sphere is a fixed quadratic residue modulo  $q$ . This is the main reason why it is not at all obvious how to make a tiling of the complete graph with the Brown graph.

Chung, Graham and Spencer ([3]) proved that  $ck^3/\log^3 k \leq R_k(K_{3,3}) \leq (2 + o(1))k^3$ . Chung, Erdős and Graham [5, 3, 4] raised the problem of determining or estimating this quantity more accurately.

The graph  $H(q, 3)$  enables us to answer this question and obtain an asymptotic formula for the multicolor Ramsey number of  $K_{3,3}$ .

**Theorem 3**  $R_k(K_{3,3}) = (1 + o(1))k^3$

*Proof:* Knowing Füredi's upper bound (3) for the Turán number of  $K_{3,3}$ , inequality (7) provides  $R_k(G) \leq (1 + o(1))k^3$ .

For the other direction we can exploit the advantages of the graph  $H(q, 3)$  over the Brown graph. We define an almost complete  $q - 1$ -coloring of the edges of  $K_{q^3 - 2q^2 + q}$ , such that there is no monochromatic  $K_{3,3}$ . The edges that are missing form disjoint complete bipartite graphs of order  $2q - 2$  and thus can be colored recursively.

The vertices of the complete graph are labeled by the elements in  $GF(q^2)^* \times GF(q)^*$ . If  $A \neq -B$ , color the edge between  $(A, a)$  and  $(B, b)$  by  $N(A + B)/ab$ . This way no color class contains a  $K_{3,3}$ . The proof of Theorem 1 works for any fixed color, because of the generality of Lemma 2.

The uncolored edges form  $(q^2 - 1)/2$  pairwise disjoint complete bipartite graphs, each of which has  $2(q - 1)$  vertices. Using the same construction recursively, one can color the edges of each such bipartite graph using at most  $(1 + o(1))(2q)^{1/3}$  additional colors. Since the uncolored copies of the graphs  $K_{q-1, q-1}$  are pairwise disjoint we can use the same set of new colors for each of them. The total number of colors is thus  $q + o(q)$ , implying the lower bound, in view of the known results about the distribution of primes, mentioned in the introduction.  $\square$

## 4 The general projective norm-graphs

All proofs in the previous sections of this paper are elementary. In order to prove the properties of the improved norm-graphs for  $t > 3$  we need the following lemma of [12], which generalizes our simple Lemma 2 proved in section 2. The proof in [12] requires some tools from elementary Algebraic Geometry.

**Lemma 4 ([12])** *Let  $K$  be a field and  $a_{ij}, b_i \in K$  for  $1 \leq i, j \leq t$  such that  $a_{i_1 j} \neq a_{i_2 j}$  if  $i_1 \neq i_2$ . Then the system of equations*

$$\begin{aligned} (x_1 - a_{11})(x_2 - a_{12}) \cdots (x_t - a_{1t}) &= b_1, \\ (x_1 - a_{21})(x_2 - a_{22}) \cdots (x_t - a_{2t}) &= b_2, \\ &\vdots \\ (x_1 - a_{t1})(x_2 - a_{t2}) \cdots (x_t - a_{tt}) &= b_t \end{aligned} \tag{8}$$

*has at most  $t!$  solutions  $(x_1, x_2, \dots, x_t) \in K^t$ .*

Now we are ready to define the improved norm-graph  $H = H(q, t)$  for any  $t > 2$ . Let  $V(H) = GF(q^{t-1}) \times GF(q)^*$ . Two distinct  $(A, a)$  and  $(B, b) \in V(G)$  are adjacent if and only if  $N(A + B) = ab$ ,

where the norm is understood over  $GF(q)$ , that is,  $N(x) = x^{1+q+\dots+q^{t-2}}$ . Note that  $|V(H)| = q^t - q^{t-1}$ . If  $(A, a)$  and  $(B, b)$  are adjacent, then  $(A, a)$  and  $B \neq -A$  determine  $b$ . Thus  $H$  is regular of degree  $q^{t-1} - 1$ .

**Theorem 5** *The graph  $H = H(q, t)$  contains no subgraph isomorphic to  $K_{t, (t-1)!+1}$ .*

*Proof:* The proof is a straightforward generalization of the proof of Theorem 1 with the remark that we need to use Lemma 4 (for  $t - 1$  equations) instead of Lemma 2.

□

Therefore, the following slight improvement of the main result of [12] holds.

**Corollary 6** *For every fixed  $t \geq 2$  and  $s \geq (t - 1)! + 1$  we have*

$$\text{ex}(n, K_{t,s}) \geq \frac{1}{2}n^{2-\frac{1}{t}} - O(n^{2-\frac{1}{t}-c}),$$

where  $c > 0$  is an absolute constant.

The improvement is most visible for small values of  $t$ , for example:

**Corollary 7**

$$\text{ex}(n, K_{4,7}) = \Theta(n^{7/4}).$$

Chung, Erdős and Graham [5, 3, 4] raised the problem of determining or estimating the multicolor Ramsey numbers  $R_k(K_{t,s})$ . The following straightforward generalization of Theorem 3 determines the order of magnitude of these numbers for all  $s \geq (t - 1)! + 1$ .

**Theorem 8** *Let  $t \geq 2$  and  $s \geq (t - 1)! + 1$  be fixed integers. Then*

$$R_k(K_{t,s}) = \Theta(k^t).$$

In [9] Füredi mentions that the area lacked constructions so badly that Erdős even proposed the problem of showing that

$$\lim_{s \rightarrow \infty} (\liminf_{n \rightarrow \infty} \text{ex}(n, K_{2,s})n^{-3/2}) = \infty.$$

In [9] this conjecture is proved in a strong way: exact asymptotics is given for  $\text{ex}(n, K_{2,s})$ .

Using Füredi's method together with our projective norm-graphs we prove the validity of Erdős's conjecture for any fixed  $t$  in place of 2:

$$\lim_{s \rightarrow \infty} (\liminf_{n \rightarrow \infty} \text{ex}(n, K_{t,s})n^{-(2-1/t)}) = \infty.$$

We are not able to give an asymptotics of  $\text{ex}(n, K_{t,s})$  like Füredi did for  $t = 2$ , but for any  $t \geq 3$  and  $s \geq (t - 1)! + 1$  our answer is tight up to a constant factor depending only on  $t$ . In particular the

known upper bound of  $\text{ex}(n, K_{3,s})$  comes within a factor of  $2^{\frac{1}{3}} + o(1)$  of the lower bound for every  $s \geq 3, s = 2r^2 + 1$ .

Let  $r$  be a positive integer which divides  $q - 1$ . Let  $Q_r$  denote the subgroup of  $GF(q)^*$  of order  $r$ . The vertex set of the graph  $H_r(q, t) = H_r$  is defined to be  $GF(q^{t-1}) \times (GF(q)^*/Q_r)$ . Two vertices  $(A, aQ_r)$  and  $(B, bQ_r)$  are adjacent in  $H_r$  iff  $N(A + B) \in abQ_r$ .

$H_r$  has  $(q^t - q^{t-1})/r$  vertices and each vertex has degree  $q^{t-1} - 1$ . It is also easy to see that  $H_r$  does not contain a  $K_{t, (t-1)!r^{t-1}+1}$ . Indeed, similarly to the proof of Theorem 5, the problem can be reduced to bounding the number of solutions of the following system of equations:

$$\begin{aligned} N(Y + A_1) &= (Y + A_1)(Y^q + A_1^q) \cdots (Y^{q^{t-2}} + A_1^{q^{t-2}}) &\in b_1 Q_r \\ N(Y + A_2) &= (Y + A_2)(Y^q + A_2^q) \cdots (Y^{q^{t-2}} + A_2^{q^{t-2}}) &\in b_2 Q_r \\ \vdots & &\vdots \\ N(Y + A_{t-1}) &= (Y + A_{t-1})(Y^q + A_{t-1}^q) \cdots (Y^{q^{t-2}} + A_{t-1}^{q^{t-2}}) &\in b_{t-1} Q_r \end{aligned} \tag{9}$$

Because of the generality of Lemma 4, for any choice of elements from  $b_1 Q_r, b_2 Q_r, \dots, b_{t-1} Q_r$  there are at most  $(t-1)!$  solutions. Since we have  $r^{t-1}$  choices on the right hand side of (9), the number of solutions is not more than  $(t-1)!r^{t-1}$ .

Hence, we proved the following.

**Theorem 9** *Let  $t \geq 2$  be fixed. There is a constant  $c_t$  such that for any  $s \geq (t-1)! + 1$  we have*

$$\text{ex}(n, K_{t,s}) \geq (1 + o(1)) \frac{c_t}{2} (s-1)^{\frac{1}{t}} n^{2-\frac{1}{t}}.$$

*In particular for  $t = 3$  and  $s = 2r^2 + 1$  we can take  $c_3 = 2^{-1/3}$*

## 5 An asymmetric construction for the Zarankiewicz problem

Let  $m \geq t \geq 1$  and  $n \geq s \geq 1$  be integers. The problem of Zarankiewicz asks about the maximum possible number of 1 entries in an  $n \times m$  matrix  $M$  with 0-1 entries such that  $M$  does not contain an  $s \times t$  submatrix consisting entirely of 1 entries. This maximum is usually denoted by  $z(n, m, s, t)$ . The problem of determining  $z(n, n, s, t)$  is related to that of finding the Turán number  $\text{ex}(n, K_{t,s})$  through the inequality  $z(n, n, s, t) \geq 2\text{ex}(n, K_{t,s})$ .

The upper bound of Kővári, T. Sós and Turán for the Turán number of  $K_{t,s}$  generalizes to the Zarankiewicz problem giving  $z(n, m, s, t) \leq (s-1)^{1/t} mn^{1-1/t} + (t-1)n$ , (as well as the symmetric bound obtained by exchanging  $n$  and  $m$  and  $s$  and  $t$ ).

The following theorem shows the real strength of Lemma 4. We are able to choose not only  $n$ , but roughly  $n^{1+1/t}$  subsets of size  $n^{1-1/t}$  each, out of an  $n$ -element set, without  $t$  of them having an intersection of size more than  $t!$ . This gives a tight lower bound in Zarankiewicz' problem for certain choices of  $n$  and  $m$ .

**Theorem 10** *Let  $t \geq 2$  and  $s > t!$  be fixed. If  $n^{1/t} \leq m \leq n^{1+1/t}$ , then*

$$z(n, m, s, t) = \Theta(mn^{1-\frac{1}{t}}).$$

*Proof:* Clearly, it suffices to prove the lower bound for  $n$  of the form  $q^t$ , where  $q$  is a prime power, and for  $m = (1 + o(1))n^{1+1/t}$ . Let us label the rows of the matrix with the elements of  $GF(q^t)$  and the columns with the elements of  $GF(q^t) \times GF(q)^*$ . Let the entry at  $(A, (B, b))$  be 1 iff  $N(A+B) = b$ . In this construction every row contains  $q^t - 1$  1 entries and every column contains  $q^{t-1} + q^{t-2} + \dots + q + 1$  1 entries. The matrix does not contain a  $(t! + 1) \times t$  submatrix all of whose entries are 1. To see this let us choose  $t$  distinct columns  $(D_1, d_1), \dots, (D_t, d_t)$ . If they have a row where each of their entries is a 1, then all the  $D_i$ s must be different, since  $N(X + D_i)$  determines  $d_i$ . We have to bound the number of solutions  $X$  of the equation system  $N(X + D_i) = d_i, i = 1, \dots, t$ . Since the  $D_i$ s are distinct we are able to use Lemma 4 and obtain that the number of solutions is at most  $t!$ .

□

The construction in the proof of Theorem 10 is exactly the missing ingredient needed to answer Matoušek's question in [13] about tight lower bounds for the maximum possible discrepancy of set systems with dual shatter functions of given order of magnitude. The *discrepancy*  $Disc(\mathcal{F})$  of a family  $\mathcal{F}$  of  $m$  subsets of an  $n$  element set  $X$  is the minimum, over all functions  $f : X \mapsto \{-1, 1\}$ , of the maximum, over all members  $F \in \mathcal{F}$ , of the quantity  $|\sum_{x \in F} f(x)|$ . The *dual shatter function*  $h$  of  $\mathcal{F}$  is the function  $h : \{1, 2, \dots, m\} \mapsto \{1, 2, \dots, n\}$  defined by letting  $h(g)$  denote the maximum, over all possible choices of  $g$  members of  $\mathcal{F}$ , of the number of atoms in the Venn diagram of these members.

In [14] it is proved that if the dual shatter function satisfies  $h(g) \leq O(g^t)$ , then for the discrepancy

$$Disc(\mathcal{F}) \leq O(n^{\frac{1}{2} - \frac{1}{2t}} \sqrt{\log n}). \quad (10)$$

This supplies nontrivial estimates in various geometric situations, where in most of these it is widely believed that the  $\sqrt{\log n}$  factor can be omitted.

In [13] it is shown, however, that for  $t = 2, 3$  the estimate (10) is tight (in some general, non-geometric examples). Suppose there is a family  $\mathcal{F} = \mathcal{F}_t$  of subsets of an  $n$  element set  $X$  such that the intersection of no  $t$  members of  $\mathcal{F}_t$  exceeds  $c(t)$ , each set  $F \in \mathcal{F}$  has at least  $c_1 n^{1-1/t}$  elements and  $|\mathcal{F}| > n^{1+\epsilon}$  for some absolute  $\epsilon > 0$ . The author in [13] shows that if  $\mathcal{G}$  is a (random) family of subsets of  $X$  obtained by picking one random subset of each member of  $\mathcal{F}$ , all choices being independent and uniform, then the dual shatter function of the resulting family  $\mathcal{G}$  is  $O(g^t)$  and, with high probability, its discrepancy is  $\Omega(n^{\frac{1}{2} - \frac{1}{2t}} \sqrt{\log n})$ . Using a clever semi-probabilistic construction Matoušek describes an appropriate family  $\mathcal{F}_t$  for  $t = 2$  and 3.

The construction of Theorem 10 provides us with a family  $\mathcal{F}_t$  of  $\Theta(n^{1+1/t})$  subsets of an  $n$  element set  $X$ , where each subset is of size  $\Theta(n^{1-1/t})$  and no  $t$  subsets have intersection of cardinality exceeding  $t!$ . Hence the estimate (10) is tight for all values of  $t$ .

## References

- [1] B. Bollobás, *Extremal Graph Theory*, Academic Press, 1978.
- [2] W. G. Brown, On graphs that do not contain a Thomsen graph, *Canad. Math. Bull.*, 9, (1966) 281-289.
- [3] F. R. K. Chung and R. L. Graham, On multicolor Ramsey numbers for bipartite graphs, *J. of Comb. Theory Series B*, 18 (1975), 164-169.
- [4] F. R. K. Chung and R. L. Graham, *Erdős on Graphs; his legacy of unsolved problems*, A K Peters, Ltd., 1998.
- [5] P. Erdős, Some new problems and results in graph theory and other branches of combinatorial mathematics, in *Combinatorics and Graph Theory (Calcutta, 1980)*, *Lecture Notes in Math.*, Vol. 885, 9-17. Berlin-New York: Springer-Verlag, 1981.
- [6] P. Erdős, A. Rényi and V. T. Sós, On a problem of graph theory, *Studia Sci. Math. Hungar.* 1, (1966), 215-235.
- [7] P. Erdős and J. Spencer, *Probabilistic Methods in Combinatorics*, Academic Press, London - New York, Akadémiai Kiadó, Budapest, 1974.
- [8] Z. Füredi, An upper bound on Zarankiewicz' problem, *Combin. Probab. Comput.* 5 (1996), no. 1, 29-33.
- [9] Z. Füredi, New asymptotics for bipartite Turán numbers, *J. Combin. Theory Ser. A* 75 (1996), no. 1, 141-144.
- [10] M. N. Huxley and H. Iwaniec, Bombieri's Theorem in short intervals, *Mathematika* 22 (1975), 188-194.
- [11] T. Kővári, V. T. Sós and P. Turán, On a problem of K. Zarankiewicz, *Colloquium Math.*, 3, (1954), 50-57.
- [12] J. Kollár, L. Rónyai and T. Szabó, Norm-graphs and bipartite Turán numbers, *Combinatorica* 16 (1996), no. 3, 399-406.
- [13] J. Matoušek, On discrepancy bounds via dual shatter function, *Mathematika* 44 (1997), no.1, 42-49.
- [14] J. Matoušek, E. Welzl and L. Wernisch, Discrepancy and  $\epsilon$  approximation for bounded VC dimension, *Combinatorica* 13 (1993), 455-466.