COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA 16 (3) (1996) 399–406

NORM-GRAPHS AND BIPARTITE TURÁN NUMBERS

JÁNOS KOLLÁR[1], LAJOS RÓNYAI[2] and TIBOR SZABÓ

Received August 2, 1995

For every $t>1$ and positive n we construct explicit examples of graphs G with $|V(G)|=n$, $|E(G)| \geq c_t \cdot n^{2-\frac{1}{t}}$ which do not contain a complete bipartite graph $K_{t,t!+1}$. This establishes the exact order of magnitude of the Turán numbers $\mathrm{ex}(n, K_{t,s})$ for any fixed t and all $s \geq t!+1$, improving over the previous probabilistic lower bounds for such pairs (t,s). The construction relies on elementary facts from commutative algebra.

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 $\mathrm{ex}(n,H)$.

The determination of Turán numbers is particularly interesting when H is bipartite, as in most cases even the order of magnitude is open. In this note we study the Turán numbers of complete bipartite graphs (the "Zarankiewicz problem").

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 gave the following upper bound for an arbitrary fixed t and $s \geq t$:

$$\mathrm{ex}(n, K_{t,s}) \leq c_{t,s} n^{2-\frac{1}{t}}, \tag{1}$$

where $c_{t,s}>0$ is a constant depending on t and s. The right hand side is conjectured to give the correct order of magnitude. However, the best general lower bound, obtained by the probabilistic method, yields only

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

Mathematics Subject Classification (1991): 05 C 35, 14 A 25.

[1] Research supported in part by NSF Grants DMS-8707320 and DMS-9102866.

[2] Research supported in part by Hungarian National Foundation for Scientific Research Grant T016503.

where c' is a positive absolute constant. (Cf. [8], p.61, proof of inequality (12.19).)

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

The optimality of the order of magnitude (up to a constant factor) of the upper bound (1) has been established via explicit constructions for $t=2,3$ and all $s \ge t$. The incidence graphs of projective planes demonstrate this order of magnitude for $t=2$ (this was observed by E. Klein, as reported by Erdős [6]). In this case, however, even the asymptotic order of magnitude is known:

$\mathrm{ex}(n,K_{2,2}) = \frac{1}{2}n^{3/2} + O(n^{4/3})$ (Erdős, Rényi, T. Sós [7], Brown [5]),

and for general $s \ge 2$,

$\mathrm{ex}(n,K_{2,s}) = \frac{\sqrt{s-1}}{2}n^{3/2} + O(n^{4/3})$ (Füredi [9]).

The optimality of the upper bound (1) for $t=3$ was established by W. G. Brown [5], hence $\mathrm{ex}(n,K_{3,3}) = \Theta(n^{5/3})$. His construction is the "unit distance graph" in the 3-dimensional affine space over finite fields of order $q \equiv -1 \mod 4$.

Here we give an explicit construction which demonstrates the optimality, up to a constant factor, of the upper bound (1) for all values of $t \ge 2$ and $s \ge t!+1$.

For more details and references on these problems we refer to Chapter VI, Section 2 of Bollobás [3] and to Füredi [9].

2. The norm-graph

Let q be a prime-power and $t > 1$ be an integer. We define the *norm-graph* $G = G_{q,t}$ as follows.

The set of vertices $V(G)$ of G is $GF(q^t)$, the finite field with q^t elements. For $a \in GF(q^t)$ let $N(a)$ denote the $GF(q^t)/GF(q)$-norm of a, i.e. $N(a) = a \cdot a^q \cdots a^{q^{t-1}} = a^{(q^t-1)/(q-1)} \in GF(q)$. Now let two vertices $a \ne b \in V(G) = GF(q^t)$ of G be adjacent iff $N(a+b) = 1$. The number of solutions in $GF(q^t)$ of the equation $N(x) = 1$ is $\frac{q^t-1}{q-1}$. (For this and other basic facts about finite fields the reader is referred to Lidl–Niederreiter [10].) Thus, if we write $n = q^t$ for the number of vertices of G, then the number of edges is at least $\frac{1}{2}q^t(\frac{q^t-1}{q-1} - 1) \ge \frac{1}{2}q^{2t-1} = \frac{1}{2}n^{2-\frac{1}{t}}$. We formulate now the main result of the paper.

Theorem 2.1. *The graph $G = G_{q,t}$ contains no subgraph isomorphic to $K_{t,t!+1}$.*

Corollary 2.2. *For $t \ge 2$ and $s \ge t!+1$ we have*

$$\mathrm{ex}(n, K_{t,s}) \ge c_t \cdot n^{2-\frac{1}{t}},$$

where $c_t > 0$ is a constant depending on t; we may choose $c_t = 2^{-t}$. For every t and $s \ge t$, the inequality holds with $c = 1/2$ for infinitely many values of n.

The Corollary follows from Theorem 2.1 in view of the fact that there is a prime power q between $(1/2)n^{1/t}$ and $n^{1/t}$. The union of $\lfloor n/q^t \rfloor$ disjoint copies of $G_{q,t}$ will have the appropriate number of edges. Better estimates for the gaps between consecutive prime powers yield improved constants.

3. The proof

The statement of Theorem 2.1 is a direct consequence of the following: if $d_1, d_2, \ldots, d_t$ are t distinct elements from $GF(q^t)$, then the system of equations

$$
\begin{aligned}
N(x+d_1) &= (x+d_1)(x^q+d_1^q)\ldots(x^{q^{t-1}}+d_1{}^{q^{t-1}}) = 1\\
N(x+d_2) &= (x+d_2)(x^q+d_2^q)\ldots(x^{q^{t-1}}+d_2^{q^{t-1}}) = 1\\
&\vdots\\
N(x+d_t) &= (x+d_t)(x^q+d_t^q)\ldots(x^{q^{t-1}}+d_t^{q^{t-1}}) = 1
\end{aligned}
\tag{3}
$$

has at most $t!$ solutions $x \in GF(q^t)$.

We shall infer this by considering a more general system of equations.

Theorem 3.3. *Let K be a field and $a_{ij}, b_i \in K$ for $1 \le i,j \le t$ such that $a_{ij_1} \ne a_{ij_2}$ if $j_1 \ne j_2$. Then the system of equations*

$$
\begin{aligned}
(x_1-a_{11})(x_2-a_{21})\ldots(x_t-a_{t1}) &= b_1,\\
(x_1-a_{12})(x_2-a_{22})\ldots(x_t-a_{t2}) &= b_2,\\
&\vdots\\
(x_1-a_{1t})(x_2-a_{2t})\ldots(x_t-a_{tt}) &= b_t
\end{aligned}
\tag{4}
$$

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

This indeed suffices to prove Theorem 2.1 because system (3) is a special case of system (4) ($K = GF(q^t)$, $a_{ij} = -d_j^{q^{i-1}}$, $x_i = x^{q^{i-1}}$, $b_j = 1$). ∎

We put $f_j = f_j(x_1, x_2, \ldots, x_t) := (x_1 - a_{1j})(x_2 - a_{2j}) \cdots (x_t - a_{tj})$ $(1 \le j \le t)$ for the polynomials on the left-hand side of the system (4). Let us define the regular map $F\colon K^t \to K^t$ by $F(x_1, x_2, \ldots, x_t) := (f_1(x_1, \ldots, x_t), \ldots, f_t(x_1, \ldots, x_t))$. Theorem 3.3 claims that $|F^{-1}(b)| \le t!$ holds for every $b \in K^t$.

It is straightforward to verify that $|F^{-1}(0)| = t!$. The second half of our proof will in essence establish that all roots of the equation $F(x_1, \ldots, x_t) = 0$ are simple. The structure to be established in the first half of the proof then will allow the $t!$ bound to carry over from $b = 0$ to all b. This conclusion will rest on the following result (see Theorem 3 in [14, Chap. II, Sec. 6.3, p.143]; in the first edition of [14], it is stated as Theorem 6 in [Chap. II, Sec. 5]). For some of the definitions, see below.

Fact. *Let K be an algebraically closed field, $A = K[x_1,\dots,x_t]$, $f_j \in A$, $B = K[f_1,\dots,f_r]$, and define $F:K^t \to K^r$ by $F(x)=(f_1(x),\dots,f_r(x))$ $(x\in K^t)$. Assume B is integrally closed in its field of quotients and that A is finite over B and has rank d over B. Then for all $b\in K^r$, $|F^{-1}(b)|\le d$.* ∎

To establish Theorem 3.3, we shall assume without loss of generality that K is algebraically closed. We write $A=K[x_1,x_2,\dots,x_t]$ for the polynomial ring with indeterminates x_i over K. As before, let f_j $(1\le j\le t)$ denote the polynomials on the left-hand side of the system (4). Let $B=K[f_1,f_2,\dots,f_t]$ be the K-subalgebra of A generated by the polynomials f_j.

Recall that a ring R is *finite* over a subring $S\subseteq R$ if R is a finitely generated S-module. (We assume S contains the identity element of R.) Finiteness of R over S is equivalent to the following two conditions: (i) R is a finitely generated algebra over S; (ii) R is integral over S (every element of R is a root of a monic polynomial over S).

An integral domain R *has rank* r over a subring $S\subseteq R$ if the field of quotients $QF(R)$ of R is a degree-r extension of the field of quotients $QF(S)$ of S. For the basics of commutative algebra we refer to [2], [4], [12]; especially [2, Chap. 5].

Lemma 3.4. *A is finite over B and has rank $t!$ over B.*

From the Lemma we infer that the transcendence degree of B over K is t, hence the f_j are algebraically independent over K. This implies that B is isomorphic to A, and therefore integrally closed (in its field of quotients). Hence an application of the Fact (above) yields $|F^{-1}(b)|\le t!$. ∎

It remains to prove the Lemma.

Finiteness. We prove by induction on t that A is an integral extension of B. If $t=1$ then $A=B$ and integrality is obvious. Suppose that $t>1$ and let $M=QF(A)$ be the field of quotients of A. Theorem 10.4 of [12] states that the integral closure of a subring C of M is the intersection of all valuation rings $R\le M$ which contain C. (Recall that a valuation ring R of M is a subring of M such that for every element $y\in M$ either $y\in R$ or $y^{-1}\in R$.) Thus, to verify the integrality of A over B, we show that if R is a valuation ring of M containing B, then $R\ge A$.

Write I for the (unique) maximal ideal of the valuation ring R. By symmetry it is enough to prove that $x_t\in R$. We do this by showing that the assumption $x_t\notin R$ leads to contradiction. If $x_t\notin R$ then $x_t-a_{tj}\notin R$ and hence $1/(x_t-a_{tj})\in I$ and $g_j:=f_j/(x_t-a_{tj})\in I$ for $j=1,\dots,t$.

By the inductive hypothesis, the elements $x_1,\dots,x_{t-1}$ are integral over $C=K[g_1,\dots,g_{t-1}]$. This together with $C\le R$ implies that $K[x_1,\dots,x_{t-1}]\le R$.

Next observe that the polynomials $g_1,\dots,g_t$ have no common zero in K^{t-1}. By Hilbert's Nullstellensatz this implies that they generate the ideal (1) in $K[x_1,\dots,x_{t-1}]$: there exist polynomials $h_j\in K[x_1,\dots,x_{t-1}]$ such that $\sum g_jh_j=1$. This relation leads to a contradiction because $g_j\in I$, $h_j\in R$ and hence the left-hand side belongs to I, while $1 \notin I$. The finiteness of A over B now follows since A is a finitely generated algebra over B (actually even over K).

Computing the rank. We have to show that $\dim_{QF(B)} QF(A) = t!$. Since $|F^{-1}(0)| = t!$, an application of the Fact shows that the dimension is at least $t!$.

Let $\mathfrak{m}$ denote the ideal $(f_1, \dots, f_t)$ of B. Let $B_\mathfrak{m}$ denote the corresponding local ring and $A_\mathfrak{m}$ the corresponding $B_\mathfrak{m}$-algebra.

First we establish that $\mathfrak{m}A$ is a finite intersection of maximal ideals of A. For a permutation $\sigma \in S_t$ let I_σ be the (maximal) ideal $(x_1 - a_{1\sigma(1)}, x_2 - a_{2\sigma(2)}, \dots, x_t - a_{t\sigma(t)})$ of A. We show that $\mathfrak{m}A = \prod_{\sigma \in S_t} I_\sigma$. Obviously we have $\mathfrak{m}A \subseteq I_\sigma$ for every $\sigma \in S_t$ hence $\mathfrak{m}A \subseteq \cap_{\sigma \in S_t} I_\sigma = \prod_{\sigma \in S_t} I_\sigma$.

Now let $f = f_1 f_2 \cdots f_t$, $f_\sigma = \prod_{i=1}^t (x_i - a_{i\sigma(i)})$ and $g_\sigma = f / f_\sigma$. We observe first that the polynomials f_j $(1 \le j \le t)$ and g_σ $(\sigma \in S_t)$ have no common zero. Indeed a common zero of the polynomials f_j is of the form $(a_{1\tau(1)}, a_{2\tau(2)}, \dots, a_{t\tau(t)})$ for some $\tau \in S_t$, which is not a zero of g_τ. Again by the Nullstellensatz, for suitable polynomials $h_j, h_\sigma \in A$ we have $\sum h_j f_j + \sum h_\sigma g_\sigma = 1$. Now let $g \in \prod_{\sigma \in S_t} I_\sigma$. We have $\sum h_j f_j g + \sum h_\sigma g_\sigma g = g$ and $\sum h_j f_j g \in \mathfrak{m}A$. We show that $g_\sigma g \in \mathfrak{m}A$ which implies that $g \in \mathfrak{m}A$.

The polynomial g can be written as a sum of terms of the form $g^* = g' \cdot \prod_{\tau \in S_t} m_\tau$ where $g' \in A$ and $m_\tau \in \{x_1 - a_{1\tau(1)}, x_2 - a_{2\tau(2)}, \dots, x_t - a_{t\tau(t)}\}$. Now if $m_\sigma = x_i - a_{i\sigma(i)}$, then $g^* g_\sigma$ is divisible in A by $f_{\sigma(i)}$, giving that $g^* g_\sigma \in \mathfrak{m}A$ and $g \in \mathfrak{m}A$.

By the Chinese remainder theorem

$$A/\mathfrak{m}A = A / \cap_{\sigma \in S_t} I_\sigma \cong \oplus_{\sigma \in S_t} A/I_\sigma \cong \oplus_{\sigma \in S_t} K$$

and therefore $\dim_K A/\mathfrak{m}A = t!$.

It is elementary localization that $A/\mathfrak{m}A$ and $A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m}$ are isomorphic as K-algebras. We obtain that $\dim_K A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m} = t!$. In other words, the K-space $A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m}$ can be generated by $t!$ elements.

A is a finite B-module, thus $A_\mathfrak{m}$ is a finitely generated module over the local ring $B_\mathfrak{m}$. Nakayama's Lemma implies that $A_\mathfrak{m}$ can also be generated by at most $t!$ elements as a $B_\mathfrak{m}$-module. Let $X = \{u_1, \dots, u_p\}$ be one such generating set with $u_i \in A_\mathfrak{m}$ and $p \le t!$.

Now we prove that $\{u_1, \dots, u_p\}$ generates $QF(A)$ as linear space over $QF(B)$.

Let $x/y \in QF(A)$, $x, y \in A$, $y \ne 0$. Here y is integral over B, hence there exists an element $0 \ne z \in A$, such that $yz \in B$. For $xz \in A \subseteq A_\mathfrak{m}$ we have $xz = \sum_{i=1}^p w_i u_i$ for some $w_i \in B_\mathfrak{m}$. Then $x/y = xz/yz = \sum_{i=1}^p (w_i/yz) u_i$, where $w_i/yz \in QF(B)$, hence X is indeed a linear generating set of $QF(A)$ over $QF(B)$.

We have $\dim_{QF(B)} QF(A) \le |X| \le t!$ and this concludes the proof of the Lemma and the Theorems. ∎

4. Concluding remarks

Remark 1. We sketch here the geometric version of the proof of the finiteness of F, which shows the simple ideas behind the algebraic arguments.

Let $\mathbf{A}^t$ denote the affine t-space over K. There exists a projective variety X such that $\mathbf{A}^t \subset X$ and F extends to a morphism $F': X \to \mathbf{P}^t$ (where $\mathbf{P}^t$ denotes the projective t-space over K). We can also assume that the embedding $u: \mathbf{A}^t \hookrightarrow \mathbf{P}^t$ extends to a morphism $u': X \to \mathbf{P}^t$.

If F is not finite, then there exists a point $x \in (X - \mathbf{A}^t)$ such that $F'(x) \in \mathbf{A}^t$. One can choose a smooth pointed curve $y \in C$ and a morphism $p: C \to \mathbf{P}^t$ such that $p(y) = x$ and $p(U - y) \subset \mathbf{A}^t$ for a suitable neighborhood $y \in U \subset C$.

We can pass to the completion of the local ring of C at y. This is isomorphic to the ring of formal power series $K[[z]]$, where z is a variable. $u' \circ p: C \to \mathbf{P}^t$ has a power series-expansion $(g_0(z) : \ldots : g_t(z))$. After dividing by g_0 one can consider this in affine coordinates. We have the local expansion $h_i(z) = g_i(z)/g_0(z)$ of $u' \circ p: C \to \mathbf{A}^t$, where the h_i are formal Laurent series. By construction $p(y) = x \in (X - \mathbf{A}^t)$, implying that one of these series, say h_1, has a pole at y.

By construction, the j^{th} coordinate function of $F' \circ u' \circ p$ is $\prod_i (h_i(z) - a_{ij})$, and it does not have a pole at y since $F'(x) \in \mathbf{A}^t$. Thus, for every $1 \le j \le t$ there is a $i = i(j) > 1$ such that $h_i(0) - a_{ij} = 0$. This leads to a contradiction because $i(j_1) \ne i(j_2)$ if $j_1 \ne j_2$, and the values of i are restricted to $i = 2, \ldots, t$. ∎

Remark 2. We can say more about the embedding $B \hookrightarrow A$ than what is stated in the Lemma. In fact, A is a free B-module. The local condition for flatness in Theorem 23.1 from Matsumura [12] is applicable, giving that A is locally free and hence projective over B. Now the Quillen-Suslin theorem [13], [15] implies that A is a free module over B. ∎

Remark 3. The bound obtained for the number of solutions of the original system (3) of equations may not be sharp. It is conceivable that $G_{q,t}$ does not contain $K_{t,s}$ for an s much smaller than $t!$, possibly as small as $O(2^t)$. Note that for $q = 2$ the bound $2^t - t$ would be tight (all nonzero elements have norm 1).

Remark 4. It would be interesting to see explicit constructions for graphs with large edge density and without $K_{t,t}$, even if the density is far worse than that guaranteed by the probabilistic lower bound (2). Motivation for such constructions comes especially from the theory of computing (cf. [1]).

The first explicit examples of graphs with $n^{2-\epsilon}$ edges which do not contain certain fixed bipartite graphs were given by A. E. Andreev [1]. He constructed bipartite graphs with n vertices on each side, with $n^{2-1/t}$ edges, and without

$K_{r(t),s(t)}$ where both $r(t)$ and $s(t)$ are greater than $(2t)^{t(t-1)/2}$. Our result reduces these parameters to $r(t)=t$ and $s(t)=t!+1$.

Remark 5. In connection with the preceding problem it may be interesting to study the subgraphs $K_{r,s}$ in $G_{q,t}$ for $t<r\le s$. In particular, does there exist and absolute constant C such that $G_{q,t}$ does not contain $K_{r,r}$ for some $r\le t^C$?

Acknowledgements. Helpful discussions with Laci Babai, Ferenc Bródy, William Fulton, and Burt Totaro are gratefully acknowledged. One of the authors (Rónyai) visited the Department of Computer Science of the University of Chicago in June-July 1995; it was this visit that made most of these discussions possible. The hospitality of the University of Chicago is gratefully acknowledged. We would like to thank Laci Babai for numerous improvements of the manuscript.

Note added in proof. With the techniques of the paper we obtained a slight improvement of Corollary 2.2 recently. It is valid for $s\ge(t-1)!+1$. In particular we have $\mathrm{ex}(n,K_{4,7})\ge c\cdot n^{2-\frac{1}{4}}$.

References

[1] A. E. Andreev: On a family of Boolean matrices, *Vestnik Mosk. Univ.* Ser. 1 (mat.-mech.) **41** (1986), 97–100 (in Russian), English translation: *Moscow Univ. Math. Bull.* **41** (1986), 79–82.

[2] M. F. Atiyah, I. G. Macdonald: *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[3] B. Bollobás: *Extremal Graph Theory*, Academic Press, 1978.

[4] N. Bourbaki: *Algèbre Commutative*, Hermann, 1961–1965.

[5] W. G. Brown: On graphs that do not contain a Thomsen graph, *Canad. Math. Bull.*, **9** (1966) 281–289.

[6] P. Erdős: On sequences of integers no one of which divides the product of two others and on some related problems, *Isvestija Nautshno-Issl. Inst. Mat. i Meh. Tomsk* 2, (1938) 74–82, *(Mitteilungen des Forschungsinstitutes für Math. und Mechanik Univ. Tomsk)*.

[7] P. Erdős, A. Rényi, V. T. Sós: On a problem of graph theory, *Studia Sci. Math. Hungar.* 1, (1966), 215–235.

[8] P. Erdős, J. Spencer: *Probabilistic Methods in Combinatorics*, Academic Press, London — New York, Akadémiai Kiadó, Budapest, 1974.

[9] Z. Füredi: Turán type problems, in: *London Math. Soc. Lecture Note Series 166*, (ed.: A. D. Keedwell), Cambridge University Press, 1991, 253–300.

[10] R. Lidl, H. Niederreiter: *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1986.

[11] T. Kővári, V. T. Sós, P. Turán: On a problem of K. Zarankiewicz, *Colloquium Math.*, **3** (1954), 50–57.

[12] H. MATSUMURA: *Commutative ring theory*, Cambridge University Press, 1989.

[13] D. QUILLEN: Projective modules over a polynomial ring, *Inventiones Mathematicae*, **36** (1976), 167–171.

[14] I. R. SHAFAREVICH: *Basic Algebraic Geometry*, 2nd revised and expanded ed., Springer Verlag, Berlin, 1994.

[15] A. A. SUSLIN: Projective modules over a polynomial ring are free, *Soviet Math. Dokl.*, **17** (1976), 1160–1164.

János Kollár

Department of Mathematics,
University of Utah
Salt Lake City, UT 84112
kollar@math.utah.edu

Lajos Rónyai

Computer and Automation Institute,
Hungarian Academy of Sciences
lajos@nyest.ilab.sztaki.hu

Tibor Szabó

Department of Mathematics,
The Ohio State University
and
Eötvös Loránd University,
Budapest, Hungary
szabote@math.ohio-state.edu