Problems and results in Extremal Combinatorics- II

Noga Alon *

Dedicated to Miki Simonovits, for his 60^{th}*-birthday*

Abstract

Extremal Combinatorics is one of the central areas in Discrete Mathematics. It deals with problems that are often motivated by questions arising in other areas, including Theoretical Computer Science, Geometry and Game Theory. This paper contains a collection of problems and results in the area, including solutions or partial solutions to open problems suggested by various researchers. The topics considered here include questions in Extremal Graph Theory, Polyhedral Combinatorics and Probabilistic Combinatorics. This is not meant to be a comprehensive survey of the area, it is merely a collection of various extremal problems, which are hopefully interesting. The choice of the problems is inevitably biased, and as the title of the paper suggests, it is a sequel to a previous paper [2] of the same flavour, and hopefully a predecessor of another related future paper. Each section of this paper is essentially self contained, and can be read separately.

1 Introduction

Extremal Combinatorics deals with the problem of determining or estimating the maximum or minimum possible value of an invariant of a combinatorial object that satisfies certain requirements. Problems of this type are often related to other areas including Computer Science, Information Theory, Number Theory and Game Theory. This branch of Combinatorics has been very active during the the last few decades, see, e.g., [5], [11], and their many references.

This paper contains a collection of problems and results in the area, including solutions or partial solutions to open problems suggested by various researchers. The questions considered include problems in Extremal Graph Theory, Polyhedral Combinatorics and Probabilistic Combinatorics. This is not meant to be a comprehensive survey of the area, but rather a collection of several extremal problems, which are hopefully interesting. The techniques used include combinatorial, probabilistic and algebraic tools. Each section of this paper is essentially self contained, and can be read separately.

*Schools of Mathematics and Computer Science, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv 69978, Israel. Email: noga@math.tau.ac.il. Research supported in part by a USA-Israeli BSF grant, by the Israel Science Foundation and by the Hermann Minkowski Minerva Center for Geometry at Tel Aviv University.

2 Balanced subgraphs in dense graphs

As mentioned below the title, this paper is dedicated to Miki Simonovits, one of the founders of modern Extremal Graph Theory. It is therefore natural to start with a problem he raised, together with Erdős, more than thirty years ago in [8]. A graph is called *D-balanced* if the ratio between the maximum degree of a vertex in it and the minimum degree of a vertex in it is at most D. In [8] Erdős and Simonovits prove that for every fixed $\alpha > 0$, there exists a finite $D = D(\alpha)$ such that if $n > n_0(\alpha)$, then any graph with n vertices and at least $n^{1+\alpha}$ edges contains a D-balanced subgraph with m vertices and at least $\frac{2}{5}m^{1+\alpha}$ edges, where $m \geq n^{\alpha(1-\alpha)/(1+\alpha)}$. They apply this fact to prove, among other things, that the maximum number of edges in a graph on n vertices that contains no copy of the graph of the 3-cube is at most $O(n^{8/5})$ - a result that is not known to be tight but is still the best known upper estimate for this question.

They conclude their paper by raising the following question.

Problem (Erdős-Simonovits [8]): Is it true that there are absolute constants $\epsilon > 0$ and D, such that the following holds: For every m there is some $n_0 = n_0(m)$ such that any graph with $n > n_0$ vertices and at least $n \log_2 n$ edges contains a D-balanced subgraph with m vertices and at least $\epsilon m \log_2 m$ edges ?

In this section we show that this is not true. The proof is probabilistic, and is based on a modification of the technique of Pyber, Rödl and Szemerédi, who proved in [15] that there are graphs with n vertices and $\Omega(n \log \log n)$ edges that contain no 3-regular subgraphs. For simplicity of presentation, we omit in this section all floor and ceiling signs, whenever these are not crucial. We make no attempt to optimize the various absolute constants that appear in the proof. All logarithms in this section are in base 2.

Proposition 2.1 *For every $D > 1$ and every $n > 10^5$, there is a graph G with at most $2n$ vertices and at least $2n \log(2n)$ edges such that the following holds. For any m and d, if there is a subgraph H of G with m vertices, average degree at least d, and maximum degree at most Dd, then $d < 36(4\sqrt{\log m} + \log(64D) + 18)$.*

Proof: Let G be a random bipartite graph constructed as follows. Let A be a set of n vertices. For each i satisfying $4 \leq i \leq \frac{1}{2}\log n$, and each j satisfying $1 \leq j \leq 8$, let $B_{i,j}$ be a set of $\frac{n}{2^i}$ vertices, where all the sets A and $B_{i,j}$ are pairwise disjoint. Let $B = \cup_{i,j} B_{i,j}$ be the union of all sets $B_{i,j}$. The two classes of vertices of of G are the sets A and B. The edges of G are chosen randomly; for each i, $4 \leq i \leq \frac{1}{2}\log n$, and for each j, $1 \leq j \leq 8$, each vertex of A is connected to one random, uniformly chosen vertex of $B_{i,j}$, where all choices are independent. Note that $|A| = n$, $|B| = 8\sum_{i=4}^{\log n/2} \frac{n}{2^i} < n$ and the degree of each vertex of A is $8(\frac{1}{2}\log n - 3)$ (which is larger than $2\log(2n)$ for $n > 10^5$).

Claim: The following holds almost surely (that is, with probability that tends to 1 as n tends to infinity). Let $m \leq n$ and r be positive integers satisfying $r \geq 4\sqrt{\log m} + 16$ and suppose $A' \subset A$ and $B' \subset B$ satisfy $|A'| \leq m, |B'| \leq m$. Suppose, further, that $B \subset \cup_{i \in I} \cup_{1 \leq j \leq 8} B_{i,j}$, where

$$I = \{i : \ 4 \leq i \leq \frac{1}{2}\log n, \ \frac{n}{2^i} \geq m2^r\}.$$

Then the number of edges of the induced subgraph of G on $A' \cup B'$ is smaller than mr.

Proof of Claim: It suffices to show that almost surely there are no subsets $A' \subset A$, $B' \subset B$ of cardinality precisely m each, that span at least mr edges (since we can always add vertices to these sets, if needed). There are less than $\binom{n}{m}^2$ ways to choose two such sets A', B'. Having chosen these sets, there are $\binom{m^2}{mr}$ ways to choose a set of mr edges connecting a vertex of A' with one of B'. For each such fixed choice of edges, the probability that all of them are edges of the random graph G is zero in case two of these edges connect the same vertex of A' to two distinct members of the same set $B_{i,j}$. In any other case, this probability is at most $(\frac{1}{m2^r})^{mr}$, and also at most $(\frac{1}{\sqrt{n}})^{mr}$. Indeed, each of these edges is chosen as an edge of G with probability $\frac{1}{|B_{i,j}|}$ for some $i \in I$, and all these choices are mutually independent. Since $|B_{i,j}| \geq max\ (\sqrt{n}, m2^r)$ for each $i \in I$, the above two estimates indeed hold. It therefore follows that the probability that there are A', B' violating the conclusion of the claim is at most

$$(\binom{n}{m})^2 \binom{m^2}{mr} (\frac{1}{\sqrt{n}})^{mr}, \tag{1}$$

and also at most

$$(\binom{n}{m})^2 \binom{m^2}{mr} (\frac{1}{m2^r})^{mr}. \tag{2}$$

Suppose, first, that $m \leq n^{1/4}$. Since $r \geq 16 > e^2$, the quantity in (1) is at most

$$(\frac{en}{m})^{2m} (\frac{em}{r})^{mr} \frac{1}{n^{mr/2}} \leq n^{2m} m^{mr} n^{-mr/2} \leq 2^{2m \log n - (mr \log n)/4} \leq 2^{-(mr \log n)/8} \leq \frac{1}{n^{2m}}.$$

For $m > n^{1/4}$, the quantity in (2) is at most

$$(\frac{en}{m})^{2m} (\frac{em}{r})^{mr} (\frac{1}{m2^r})^{mr} < n^{2m} 2^{-mr^2} \leq 2^{2m \log n - 4m \log n} = \frac{1}{n^{2m}},$$

where here we used the fact that $r \geq 4\sqrt{\log m} \geq 2\sqrt{\log n}$. It follows that the probability that the assertion of the lemma fails is at most

$$\sum_{m \geq 1} \frac{1}{n^{2m}} < \frac{2}{n^2},$$

which tends to zero as n tends to infinity, completing the proof of the claim. □

Returning to the proof of the proposition, assume that our randomly constructed G satisfies the assertion of the claim. We show that this implies that it satisfies the conclusion of the Proposition as well. Given m and d, let H be a subgraph of G with m vertices, average degree at least d and maximum degree at most Dd. Let V' denote the set of all vertices of H and put $A' = A \cap V'$.

The number of vertices of H in sets $B_{i,j}$ with $\frac{n}{2^i} \leq \frac{m}{64D}$ is at most the total number of vertices in all such sets, which is at most $\frac{m}{4D}$. The total number of edges incident with these vertices is therefore at most $\frac{m}{4D} Dd = \frac{md}{4}$.

Define $r = 4\sqrt{\log m} + 16$. The number of edges of H connecting any single set $B_{i,j}$ to A' is at most $|A'|$, and hence the total number of edges of H incident with vertices in sets $B_{i,j}$ with $\frac{m}{64D} \leq \frac{n}{2^i} \leq m2^r$ is at most $8|A'|(r + \log(64D) + 2) \leq 8m(r + \log(64D) + 2)$.

Finally, the number of edges of H incident with vertices in sets $B_{i,j}$ with $\frac{n}{2^i} > m2^r$ is smaller than mr, by the Claim. As the total number of edges of H is at least $md/2$, we conclude that

$$\frac{md}{2} \leq \frac{md}{4} + 8m(r + \log(64D) + 2) + mr,$$

implying that

$$d \le 32(r + \log(64D) + 2) + 4r < 36(r + \log(64D) + 2) \le 36(4\sqrt{\log m} + \log(64D) + 18).$$

This completes the proof. $\Box$

Proposition 2.1 clearly supplies a negative answer to the problem of [8] mentioned in the beginning of the section.

3 Graphs with the Turán Property

A graph G *has the Turán Property (or TP, for short)*, if for every induced subgraph G' of G and every integer $r > 0$, the maximum number of edges in a K_{r+1}-free subgraph of G' is equal to the maximum number of edges in an r-colorable subgraph of it. The reason for the name is the fact that the famous theorem of Turán [19], which is often considered to be the starting point of Extremal Graph Theory, can be stated as the assertion that complete graphs satisfy TP.

The definition of graphs that satisfy TP was suggested by Kalai [12], who noticed that if a graph satisfies the property then it must be perfect, and also noticed that not every perfect graph satisfies TP; indeed, any graph obtained from an even cycle by adding to it two new vertices joined by edges to the two ends u, v of an edge of the cycle is perfect, and yet does not satisfy TP. This is because omitting the edge uv we get a triangle-free subgraph, but at least two edges have to be deleted to get a bipartite subgraph.

Kalai [12] raised the problem of characterizing all graphs that satisfy the Turán Property. This is a subclass of the class of all perfect graphs, and its characterization seems interesting. In particular, he asked if line-graphs of bipartite graphs satisfy the Turán Property. In this section we show that this is the case.

Theorem 3.1 *Let H be the line-graph of a bipartite graph $G = (V, E)$. Then for every integer $r > 0$, the maximum number of edges in a K_{r+1}-free subgraph of H is equal to the maximum number of edges in an r-colorable subgraph of H.*

Since induced subgraphs of line-graphs of bipartite graphs are themselves line-graphs of bipartite graphs, this shows that indeed line graphs of bipartite graphs satisfy TP. Turán's Theorem is the special case of the above theorem obtained by letting G be a star.

Proof of Theorem 3.1: Let G and H be as above, and let $r > 0$ be an integer.

Claim: It is possible to color the edges of G by r colors $\{1, 2, \ldots, r\}$, such that for every vertex v of G, the numbers of edges of each color incident with v are nearly equal. That is, if the degree of G is d, then for every $i \in \{1, \ldots, r\}$, the number of edges of color i incident with v is either $\lfloor d/r \rfloor$ or $\lceil d/r \rceil$.

To prove the claim argue as follows. First split vertices of G, if needed, to make its maximum degree at most r. This is done as follows. As long as there is a vertex v of G of degree $d > r$, modify it using the following procedure. Define $k = \lceil d/r \rceil$ and replace v by k new vertices $v_1, v_2, \ldots, v_k$, called its *descendants*. Let $vu_1, vu_2, \ldots vu_d$ be an arbitrary enumeration of all edges of G incident with v. For each i, $1 \le i \le k$, let the edges incident with the new vertex v_i be the edges $v_i u_j$ for all

j satisfying $(i-1)r < j \leq min(d, ir)$. This process terminates with a bipartite graph in which all degrees are at most r. By König's Theorem (cf., e.g., [5]) the edges of this graph can be properly colored by the r colors $\{1, 2, \ldots, r\}$. By collapsing all descendants of each vertex v back, keeping the colors of the edges, we obtain a coloring $f : E \mapsto \{1, 2, \ldots, r\}$ of the edges of the original graph G by r colors satisfying the assertion of the claim.

Returning to the proof of the theorem, let H' be the spanning subgraph of H consisting of all edges connecting two adjacent vertices of H (which are edges of G with the same end-point) iff their f-values differ. That is, for $e, e' \in E$ which have a common end-point in G (and are thus adjacent in H), ee' is an edge of H' if and only if $f(e) \neq f(e')$. Obviously H' is an r-colorable subgraph of H. We claim that no $K_{r+1}-$free subgraph H'' of H can contain more edges than H'. Indeed, the line graph H consists of $|V|$ pairwise edge disjoint cliques corresponding to the vertices of the graph G. In each such clique of d vertices (corresponding to a vertex of degree d of G), the graph H'' cannot contain more edges than the Turán number $t(d, r)$ which is the number of edges in a complete r-colorable graph on d vertices with nearly equal color classes. This follows from Turán's Theorem. However, this is exactly the number of edges of this clique that the graph H' contains, by the construction and the property of the coloring f. As H is a union of edge-disjoint cliques, it follows that H' contains at least as many edges as H", completing the proof of the theorem. □

Kalai's problem of characterizing all graphs with the Turán Property remains open. The recent proof of the strong Perfect Graph Theorem [7] provides a simple characterization of all perfect graphs in terms of forbidden induced subgraphs, and it will be interesting to find a similar characterization of all graphs satisfying the Turán Property.

4 The oriented choice number of a matching

The *(oriented) choice number* $och(G)$ of a matching $G = (V, E)$ on n directed edges (u_i, v_i), $(1 \leq i \leq n)$, is the minimum number k such that for any assignment of a list $S(v)$ of k colors to each vertex in $V = \cup_{i=1}^{n}\{u_i, v_i\}$ there is a proper vertex coloring of G, $c : V \mapsto \cup_{v \in V} S(v)$ satisfying

$$c(v) \in S(v) \text{ for all } v \in V \tag{3}$$

and

$$\text{There are no colors } a, b \in \cup_{v \in V} S(v) \text{ and } i, j \text{ with } c(u_i) = c(v_j) = a \text{ and } c(v_i) = c(u_j) = b. \tag{4}$$

This notion (which is a special case of a more general one defined for arbitrary graphs) was introduced by A. Sali and G. Simonyi in [17], where they show, among other things, that for every integer k there is an integer n such that for a matching G on n edges, $och(G) > k$. Let $g(k)$ denote the minimum number n such that this holds. Trivially, $g(1) = 1$, and Tuza and Voigt [20] proved that $g(2) = 12$. Here we consider the asymptotic behaviour of the function $g(k)$ and show that $\log_2 g(k) = (1 + o(1))k^2$.

Theorem 4.1 *There exists an absolute constant c such that for every k,*

$$2^{k^2-1} < g(k) \leq 2^{k^2+ck}$$

Before presenting the proof it is convenient to observe that for a matching of n edges G and for lists of colors $S(v)$ as above, there is a proper coloring c satisfying conditions (3) and (4) if and only if there is a tournament T whose set of vertices is the set of all colors $\cup_{v \in V} S(v)$, and a mapping from the vertices of G to those of T mapping each vertex to a color in its list such that each directed edge of G is mapped to a directed edge (with the same direction) of T.

Proposition 4.2 *For all $k \geq 1$, $g(k) \geq 2^{k^2-1}$.*

Proof: Let $G = (V, E)$ be a directed matching with $n < 2^{k^2-1}$ edges (u_i, v_i), $(1 \leq i \leq n)$, where $V = \cup_{i=1}^n \{u_i, v_i\}$, and let $S(v), v \in V$ be lists of k colors each. Put $S = \cup_{v \in V} S(v)$ and let T be a random tournament on the set of vertices S. To complete the proof it suffices to show that with positive probability the following holds: for every i between 1 and n there are distinct $a_i \in S(u_i)$ and $b_i \in S(v_i)$ such that (a_i, b_i) is a directed edge of T. Fix an index i. If $|S(u_i) \cap S(v_i)| \geq 2$ there are always a_i, b_i as above. Otherwise, the probability there are no such a_i, b_i is at most $2^{-(k^2-1)}$. Therefore, the expected number of indices i for which we do not have colors a_i, b_i as needed is at most $n 2^{-(k^2-1)} < 1$, and hence with positive probability we can map the vertices so that all edges are mapped as needed, completing the proof. $\Box$

The upper bound is slightly more complicated.

Proposition 4.3 *Let N, k and g be positive integers satisfying*

$$N \binom{\frac{N-1}{2}}{k} \geq k \binom{N}{k} \tag{5}$$

and

$$2^{\binom{N}{2}} \left(1 - \frac{1}{\binom{N}{k}}\right)^g < 1. \tag{6}$$

Then $g(k) \leq g$.

Proof: Let N, k, g be as above, and let S be a set of N colors. Let $G = (V, E)$ be a matching consisting of g directed edges (u_i, v_i), $(1 \leq i \leq g)$. For each such i, let $S(u_i)$ and $S(v_i)$ be random subsets of cardinality k of S, chosen uniformly among all k-subsets, where all $2g$ choices are mutually independent. To complete the proof we have to show that with positive probability there is no proper coloring of G, $c : V \mapsto S$ satisfying (3) and (4). As explained after the statement of Theorem 4.1, this is equivalent to proving that with positive probability the following holds: For every tournament T on the set of vertices S, there is some i, $1 \leq i \leq g$, such that all edges connecting a member of $S(u_i)$ with a member of $S(v_i)$ are directed from $S(v_i)$ to $S(u_i)$.

Let T be a fixed tournament on S. Let K denote the bipartite graph with two classes of vertices of size k each, and all k^2 directed edges from a vertex of the first class to one of the second.

Claim: T contains at least $\binom{N}{k}$ copies of K.

Proof of Claim: We apply the technique of [13]. Let $d_1, d_2, \ldots, d_N$ be the outdegrees of all vertices of T. Then the average value of d_i is $(N-1)/2$. Let R denote the graph consisting of k edges emanating from a single vertex, called the *apex* of R, to k distinct vertices, called the *leaves* of R. The number of copies of R in T is $\sum_{i=1}^N \binom{d_i}{k}$. By convexity it follows that this number is at least

$$N \binom{(N-1)/2}{k} \geq k \binom{N}{k},$$

where the last inequality is simply (5). We can now classify the copies of R in T according to their sets of leaves. For each k-subset B of S, let x_B denote the number of copies of R in T whose set of leaves is B. By the inequality above, the average value of x_B is at least k. Note that there are precisely $\binom{x_B}{k}$ copies of K in T in which the second vertex class is B. Thus, the total number of copies of K in T is $\sum_B \binom{x_B}{k} \geq \binom{N}{k}$, where the last inequality follows from the fact that the average value of x_B is at least k. This completes the proof of the claim. □

Returning to the proof of Proposition 4.3 note that by the claim, for every fixed directed edge of G, (u_i, v_i), the probability that all edges of T connecting a vertex of $S(u_i)$ and a vertex of $S(v_i)$ are directed from $S(v_i)$ to $S(u_i)$ is at least $1/\binom{N}{k}$. Indeed, this is precisely the probability that the two random sets $S(v_i), S(u_i)$ form a copy of K in T. As all sets are chosen independently, the probability that this does not happen for any edge (u_i, v_i) of G is at most

$$(1 - \frac{1}{\binom{N}{k}})^g.$$

As the total number of tournaments on the labelled set S is $2^{\binom{N}{2}}$, it follows, by (6), that with positive probability, for every tournament T on S there is an edge (u_i, v_i) of G such that all edges of T connecting a vertex of $S(u_i)$ and a vertex of $S(v_i)$ are directed from $S(v_i)$ to $S(u_i)$. This implies that $g(k) \leq g$, completing the proof of the proposition. □

It is easy to check that for every $\epsilon > 0$ and all $k > k_0(\epsilon)$, $N = \lceil (1+\epsilon)k2^k \rceil$ and

$$g = \binom{N}{k}\binom{N}{2}\log_e 2 < (eN/k)^k N^2$$

satisfy (5) and (6), implying that $g(k) \leq 2^{k^2+O(k)}$. This, together with the assertion of Proposition 4.2, complete the proof of Theorem 4.1. □

5 Extreme points in a model of optimal persuasion rules

Let $X = X_1 \times X_2$ where X_i are finite sets. Let A be a subset of X, and define $B = X \setminus A$. Let M be the set of all real functions $m : X \mapsto R$ satisfying the following two conditions:
(i) $m(x, y) \in [0, 1]$ for all $(x, y) \in X$.
(ii) *The* 3*-path condition:* $m(a, c) + m(a, b) + m(d, b) \geq 1$ for all triples $(a, b) \in A$, $(a, c) \in B$ and $(d, b) \in B$

Note that this means that M is the set of all fractional covers of the 3-uniform hypergraph whose vertices are all edges of the complete bipartite graph with vertex classes X_1, X_2, and whose (hyper)edges are all edge-sets of paths of length 3 in this bipartite graph in which the edges belong to B, A and B in this order. An extreme point of M is a member of M which is not a convex combination of other members of M.

J. Glazer and A. Rubinstein studied in [9] the extreme points of M. The motivation for their work is a model for optimal persuasion rules. In this model a speaker is trying to persuade a listener to accept a certain request. The conditions under which it will be accepted depend (in a way known to both of them) on the values of two aspects, known only to the speaker. In order to persuade the listener, the speaker is allowed to send him a message in which he states (not necessarily truthfully) the values of his two aspects. The listener can then check the value of at most one of them (possibly chosen randomly) and then he either accepts or rejects the request (again, possibly using randomization). The speaker is trying to maximize the probability that the listener will accept the request, while the listener, who only knows the probability distribution over all possible pairs of values of the two aspects, is trying to minimize the probability of taking a wrong decision, that is, accepting when he should reject or rejecting when he should accept. Here X_1, X_2 are the sets of possible values of the two aspects. A is the set of pairs of aspects on which the listener should accept, and B the set on which he should reject. The quantity $m(x, y)$ is the probability the listener takes a wrong action, assuming the actual pair of values of the aspects is (x, y), and assuming the speaker sends a message that maximizes the probability the request will be accepted. See [9] for more details.

The authors of [9] raised the following conjecture.

Conjecture 5.1 (Glazer and Rubinstein) *If m is an extreme point of M then*
$m(x, y) \in \{0, 1\}$ *for all* $(x, y) \in A$ *and*
$m(x, y) \in \{0, 1/2, 1\}$ *for all* $(x, y) \in B$

The conjecture as stated is not valid. A counter example is given below. However, the intuition of Glazer and Rubinstein that the extreme points of M have a simple structure was fully justified, and a slight variation of the conjecture is true, as stated in the following theorem.

Theorem 5.2 *If $m \in M$ is an extreme point of M then m is half-integral, that is, $m(x, y) \in \{0, 1/2, 1\}$ for all $(x, y) \in X$.*

This implies that in the persuasion game described above,there is always an optimal strategy for the listener in which all the random choices he makes (accepting or rejecting, and deciding which aspect to check) are made with probability 0, 1/2 or 1. More details and some interesting examples can be found in [9].

In the next subsection we describe a counter example to Conjecture 5.1. The subsequent subsection contains the proof of Theorem 5.2. The proof provides some additional information about the extreme points of M.

5.1 A counter example

Define $X_1 = \{1, 2, 3, 4\}$, $X_2 = \{a, b, c, d\}$, $A = \{(1, b), (2, c), (3, d), (3, a)\}$.

Let m be the following member of M: $m(1, a) = m(2, b) = m(3, c) = 1/2$, $m(4, d) = 0$, $m(3, d) = 1/2$, $m(1, b) = m(2, c) = m(3, a) = 0$, and $m(x, y) = 1$ for all other $x \in X$.

We claim that this point is an extreme point of M (and as $m(3, d) = 1/2$ it provides a counter example to the conjecture above.) Indeed, suppose this is false and $m = \sum_{v \in V} c_v v$ with $c_v > 0$ for all v, where $\sum_{v \in V} c_v = 1$ and with $V \subset M$.

Obviously $v(1, b) = v(2, c) = v(3, a) = 0$ for all $v \in V$. Therefore, by summing over the appropriate paths, $v(1, a) + v(2, b) + v(3, c) \geq 3/2$ for all $v \in V$. Since, however, $m(1, a) + m(2, b) + m(3, c) = 3/2$, it follows that in fact $v(1, a) + v(2, b) + v(3, c) = 3/2$ for all $v \in V$, and hence also, since the sum of each pair of these three numbers is at least 1, that $v(1, a) = v(2, b) = v(3, c) = 1/2$ for all

$v \in V$. In addition, $v(4,d) = 0$ for all $v \in V$, and by considering the path $\{(3,c),(3,d),(4,d)\}$ this implies that $v(3,d) \geq 1/2$ for all $v \in V$. As $m(3,d) = 1/2$ it follows that in fact $v(3,d) = 1/2$ for all $v \in V$. As for each $(x,y) \in X$ besides the ones considered already, $m(x,y) = 1$, it follows that $m(x,y) = v(x,y) = 1$ for each such x and all $v \in V$, implying that $m = v$ for all $v \in V$. This completes the proof of the claim and shows that the above conjecture is false.

5.2 Extreme points are half-integral

We need the following lemma.

Lemma 5.3 *Let $C = (c_{ij})$ be a nonsingular square matrix, where $c_{i,j} \in \{0,1,-1\}$ for all i,j, and suppose that each row of C contains at most two nonzero entries. Then, for any integral vector b, the unique solution y of the system of equations $Cy = b$ is half-integral, that is, each entry of $2y$ is an integer.*

Proof: Let s denote the number of rows of C. Note that by assumption, each row of C contains either one nonzero entry (which is 1 or -1) or two nonzero entries (in $\{-1,1\}$.) Let G be the graph on the set of vertices $\{1,2,\ldots,s\}$ in which for each row i of C there is an edge e_i defined as follows: if there is a unique j such that $c_{ij} \neq 0$, then e_i is a loop at the vertex j, and if there are two distinct indices j,k such that $c_{ij}, c_{ik} \neq 0$ then e_i is an edge connecting j and k. Obviously, G has s vertices and s edges. In addition, since C is nonsingular, it follows that in each connected component of G the number of vertices is equal to the number of edges, and it thus contains precisely one cycle (which may be a loop). When solving the system $Cy = b$, we actually solve for the variables corresponding to the vertices in each connected component separately. In each such component, the determinant of the coefficients matrix is 1 or -1, in case the unique cycle in the component is a loop, and is 2 or -2 in case the cycle is longer. The result now follows from Cramer's rule. □

Proof of Theorem 5.2: Let $m : X \mapsto R$ be an extreme point of M. Since it is an extreme point, it is the unique solution of a system of $|X|$ linear equations in the $|X|$ unknowns $m(x,y)$, where each equation is either an equation of the form $m(x,y) = 0$ or $m(x,y) = 1$ or $m(a,c)+m(a,b)+m(d,b) = 1$ with $(a,b) \in A$ and $(a,c) \in B$, $(d,b) \in B$. It is convenient to denote the restriction of m to A by f, and the restriction of m to B by g. Therefore, $f = m_{|A} : A \mapsto R$ and $g = m_{|B} : B \mapsto R$, with $f(x,y) = m(x,y)$ for all $(x,y) \in A$ and $g(x,y) = m(x,y)$ for all $(x,y) \in B$. With this notation, the pair of functions f, g form the unique solution to a system of linear equations in which each equation is either an equation of the form

$$f(x,y) = \epsilon \quad with \quad \epsilon \in \{0,1\} \tag{7}$$

or of the form

$$g(x,y) = \epsilon \quad with \quad \epsilon \in \{0,1\} \tag{8}$$

or of the form

$$g(x,u) + f(x,y) + g(v,y) = 1. \tag{9}$$

Let Y denote this system of linear equations. Let Y' be the system obtained from Y by substituting the value of each variable $f(x, y)$ for which there is an equation of the form (7) in Y in each equation it appears. Thus, the system Y' has only equations of the form (8) and (9) or equations of the form

$$g(x, u) + g(v, y) = \epsilon \quad with \quad \epsilon \in \{0, 1\} \tag{10}$$

(obtained from equations of the form (9) in which the value of $f(x, y) \in \{0, 1\}$ has been substituted.) It is obvious that this new system still has a unique solution. Let Y" be the system of equalities obtained from Y' as follows. Each equation of the form (8) or of the form (10) in Y' is taken to the system Y" as it is. For each pair of edges $(a, b), (c, d) \in B$, if $m(a, b) = m(c, d)$ then we add the corresponding equality, that is

$$g(a, b) - g(c, d) = 0. \tag{11}$$

Finally, for each fixed edge $(x, y) \in A$ which participates in some equalities of the form (9), we include an arbitrarily chosen one of them. Note that since we have added all equalities between the g-values of B-edges, if this chosen equality holds, then so do all other equalities of the form (9) involving $f(x, y)$. This is because in all these equalities, $g(x, u)$ must be the smallest g-value of a B-edge incident with x, and similarly, $g(v, y)$ must be the smallest g-value of a B-edge incident with y.

Therefore, the solution to the system Y" is also unique, and supplies immediately a solution to Y. Observe that in Y", for each A-edge (x, y), $f(x, y)$ appears in at most one equality.

We now construct a system Z of equalities and inequalities in the variables $g(x, y)$. This is done using Y" as follows. Each equation involving only variables $g(x, y)$ (and not $f(x', y')$) in Y" is taken to the system Z as it is. This includes equalities of form (8), (10) and (11). For each equation of the form (9) of Y", we add the inequality

$$g(x, u) + g(v, y) \leq 1$$

to Z. Finally, we also add the inequalities

$$0 \leq g(x, y) \leq 1 \tag{12}$$

for all $(x, y) \in B$. Note that this system has a solution: in fact, the function $g(x, y) = m_{|B}(x, y)$ as defined above, where m is our original extreme point, clearly satisfies each constraint in Z. We can thus take an extreme solution, and call it $\overline{g}$. An extreme solution is determined by a subset of the inequalities, taken as equalities. Note that by Lemma 5.3 this solution is half integral, and hence, by (12), satisfies $\overline{g}(x, y) \in \{0, 1/2, 1\}$ for all admissible (x, y). Now define, for each equation of the form (9) in Y",

$$\overline{f}(x, y) = 1 - \overline{g}(x, u) - \overline{g}(v, y).$$

(Since there is at most one such equation with each $f(x, y)$, we can simply solve it and there will be no contradictions.) This gives a solution to Y" in which all $\overline{g}$ and all $\overline{f}$-values lie in $\{0, 1/2, 1\}$, and as this solution is unique, this is the case with our original g and f as well. (Note that this also implies that the solution to the system Z is unique, and there is no need to take an extreme point in it. Moreover, there is even no need to include the additional inequalities of the form $g(x, u)+g(v, y) \leq 1$, as the solution would have been unique without them as well. The argument is, however, simpler with these inequalities)

The solution to Y" is a solution to Y', by the discussion above, and can be easily extended to a solution to Y in a unique way, keeping all f and g values in the set $\{0, 1/2, 1\}$. This shows that indeed in the original solution m (described by f and g) all coordinates lie in $\{0, 1/2, 1\}$, and completes the proof. □

6 A graph coupon collector process

Let $G = (V, E)$ be a graph with n vertices. Consider the following stochastic process executed on G. Initially all vertices are uncovered. In each step, pick a vertex at random and if it has an uncovered neighbor, cover a random uncovered neighbor. Else, do nothing. This can be viewed as a coupon collector process on G. Let $cc(G)$ denote the expected number of steps required to cover all vertices of G. The authors of [1] proved, motivated by the study of a question on load balancing in peer-to-peer networks, that if G is the graph of the k-cube, then $cc(G) = O(n)$. Here we give a short proof of the following.

Theorem 6.1 *For any d-regular graph on n vertices $cc(G) \geq n - \frac{n}{d} + \frac{n}{d}\log_e(n/d)$.*

We further show that if $d >> 1$ and G is a sufficiently strong expander (for example, an appropriately defined nearly d-regular random graph), then the above lower estimate is essentially tight. In particular, if $d >> \log n$ then $cc(G) = (1 + o(1))n$.

More interesting is the fact that the last equality holds for any d-regular expander with a sufficiently small second eigenvalue (and in particular, for the known families of explicit expanders).

An $(n, d, \lambda)-$*graph* is a d-regular graph $G = (V, E)$ on n vertices, such that the absolute value of every eigenvalue of the adjacency matrix of G, besides the largest one, is at most λ. If $\lambda \leq 2\sqrt{d-1}$, then G is called *Ramanujan*.

Theorem 6.2 *For any $(n, d, \lambda)-$graph G, $cc(G) \leq n + n(\frac{\lambda}{d})^2(\log_e n + 1)$.*

In particular, for any Ramanujan d-regular graph G on n vertices, $\lambda \leq 2\sqrt{d-1}$, implying that $cc(G) \leq n + 4n(\log_e n + 1)/d$. Therefore, if $d >> \log n$ then $cc(G) = (1 + o(1))n$. Explicit constructions of such graphs are known whenever $d - 1$ is a prime power, see [14].

Proof of Theorem 6.1: Consider the process on a d-regular graph G. For each i, $1 \leq i \leq n$, let X_i be the random variable counting the number of steps the process performs starting from the time there are exactly i uncovered vertices, until there are $(i-1)$ uncovered vertices. If U_i denotes the set of uncovered vertices when there are i of them, and $N(U_i)$ denotes the set of all their neighbors in G, then X_i simply counts the number of random vertices the process chooses until it hits a vertex of $N(U_i)$. Therefore, X_i is a geometric random variable with success probability $p_i = |N(U_i)|/n$. Since $|N(U_i)| \leq d|U_i| = di$, it follows that the expected value of X_i is $1/p_i \geq \frac{n}{di}$. It is also obvious that for each i, the expectation of X_i is at least 1. By linearity of expectation we conclude that

$$cc(G) \geq \sum_{i=1}^{n/d} \frac{n}{di} + \sum_{i>n/d} 1 \geq n - \frac{n}{d} + \frac{n}{d}\log_e(n/d).$$

□

For the proof of Theorem 6.2 we need the following lemma, which follows, for example, from Lemma 9.2.4 in [3].

Lemma 6.3 *Let C be a set of vertices in an (n,d,λ)-graph $G=(V,E)$, and let $B=V-N(C)$ be the set of all its non-neighbors, $|B|=bn$. Then $|C|b^2d^2 \le \lambda^2 b(1-b)n$, and hence*

$$|N(C)| = (1-b)n \ge \frac{|C|}{|C|/n + (\lambda/d)^2}.$$

□

Proof of Theorem 6.2. Let G be an (n,d,λ) graph, and let X_i and U_i be as in the proof of Theorem 6.1. By Lemma 6.3, $|N(U_i)| \ge \frac{i}{i/n+(\lambda/d)^2}$. Therefore, X_i is a geometric random variable with success probability $p_i = |N(U_i)|/n \ge \frac{i}{i+n(\lambda/d)^2}$.

By linearity of expectation it follows that

$$cc(G) \le \sum_{i=1}^{n} \frac{i+n(\lambda/d)^2}{i} = n + n(\frac{\lambda}{d})^2 \sum_{i=1}^{n} \frac{1}{i} \le n + n(\frac{\lambda}{d})^2(\log_e n + 1).$$

□

Remarks.

1. The last proof implies that if the expansion in G is stronger (as it is, for example, in random nearly d-regular graphs), then the expectation is in fact at most $n+(1+o(1))n\log_e n/d$. Therefore, for such graphs the lower bound in Theorem 6.1 is nearly tight. It may be interesting to decide if it is also nearly tight for the k-cube, that is, if the expected number of steps there is $(1+\log_e 2+o(1))n$.
2. The proof of Theorem 6.2 implies that the same upper bound holds even if after each step an adversary, whose objective is to delay the termination as much as he can, is allowed to shift the uncovered vertices to any place he wishes, keeping their number. This might be useful in applications. In particular, the upper bound holds for a modified process in which we always cover the first uncovered neighbor of the random vertex picked, if there is such a neighbor.
3. It seems plausible to conjecture that the maximum possible value of $cc(G)$, as G ranges over all d-regular graphs with n vertices, is obtained for the union of pairwise disjoint $(d+1)$ cliques (assuming $(d+1)$ divides n.) This would imply, in particular, that for every d-regular G on n vertices $cc(G) \le n + O(n \log n/d)$.
4. It is easy to see that for non-regular graphs G on n vertices, $cc(G)$ may be $\tilde{\Omega}(n^2)$, even if the minimum degree is at least $\log n$, as shown, for example, by a complete bipartite graph with classes of vertices of sizes $d=\log n$ and $n-d$.
5. Standard techniques can be used to show that with high probability the process on G does not take much longer than its expectation, that is, the number of steps is highly concentrated around its mean.

7 A hats game puzzle and generalized covers

In this section we consider a version of a hats game puzzle that has first been considered in [4] and has also been the subject of an article in the Science section of the NY Times [16]. The game is played by a team of n players, and (say) a TV host. After the team enters the game room, the host places either a green hat or a red hat on each player's head. Every player can see the other players' hats, but not his own. Shortly after getting the hat, each player has to declare ”my hat is green”, "my hat is red", or "I pass". These declarations have to be simultaneous, and no communication is allowed between the players after the game starts. They are allowed, however, to coordinate their strategies beforehand. The team wins a big prize if at least one player guesses his hat color right, and none guesses it wrong. Otherwise, they lose. Assuming a uniform distribution of hat combinations, a trivial strategy gives the team a 1/2 probability of winning; simply let the first player guess, and let everybody else pass. Can they do better ? The results in [4] imply that they can do much better. Using the properties of the Hamming code, they can in fact ensure that the probability of losing will only be $(1 + o(1))/n$. The situation is more complicated when the number of possible colors of the hats, denoted by q, is larger than 2. Here, too, there is a strategy for which the probability of losing tends to zero as the number of players, n, tends to infinity and q is fixed, but the asymptotic behaviour of the probability of losing for the optimal strategy is not known.

Lenstra and Seroussi [18] showed that this probability is at most $O(n^{-1/e \log q})$. Here we improve this estimate and show that it is at most $O((q \log n)/n)$. It is not difficult to see that this probability is at least $\Omega(q/n)$, and it will be interesting to close the gap between the upper and lower bound. All logarithms in this section are in the natural basis e.

It is convenient to formulate the problem in terms of the existence of a certain code. Let $Q = \{1, 2, \ldots, q\}$ denote the set of possible colors of a hat, and let Q^n denote the set of all possible assignments of hats to the n players. Fix a strategy for the players, let $W \subset Q^n$ be the set of all winning configurations under this strategy, and let $C = Q^n \setminus W$ be the set of all losing configurations.

Claim: For every vector $w = (w_1, w_2, \ldots, w_n) \in W$ there is an i, $1 \leq i \leq n$, such that for every $u \in Q - \{w_i\}$ the vector $w_u = (w_1, w_2, \ldots, w_{i-1}, u, w_{i+1}, \ldots, w_n)$ lies in C.

Note that for $q = 2$ this simply means that C is a binary code of covering radius 1, that is, each binary n-vector lies within Hamming distance 1 of C.

To prove the claim note that if $w \in W$ then there is at least one player, say, player number i, that guesses w_i when the configuration is w, and as his guess will be the same for all the modified vectors w_u, all these vectors must represent losing configurations, as claimed.

The converse of the above claim also holds, that is, if $W \subset Q^n$ satisfies the condition in the claim, then there is a strategy in which all configurations in W are winning configurations; indeed, if player number i, who knows the value of w_j for all $j \neq i$, sees that there is some $a \in Q$ such that w_u as defined above is not in W for all $u \neq a$, then he guesses that $w_i = a$. It is easy to see that all guessing players will indeed guess correctly on members of W. It thus follows that the problems of estimating the probability of losing in the optimal strategy is equivalent to the problem of minimizing the cardinality of C in a partition $Q^n = W \cup C$ of Q^n into two disjoint sets, satisfying the property of the claim. The following theorem shows that there is a strategy ensuring a losing probability of at most $\frac{(q-1)\log n+1}{n} + (\frac{q-1}{q})^n$.

Theorem 7.1 *Let $q > 1$ be an integer, and put $Q = \{1, 2, \ldots, q\}$. Then there is a partition of Q^n into two disjoint sets W and C such that*

$$|C| \leq \frac{(q-1)\log n + 1}{n} q^n + (q-1)^n$$

and such that for every vector $(w_1, w_2, \ldots, w_n) \in W$ there is an i, $1 \leq i \leq n$, such that for every

$u \in Q - \{w_i\}$ *the vector* $(w_1, w_2, \ldots, w_{i-1}, u, w_{i+1}, \ldots, w_n) \in C$.

Proof: We apply a probabilistic argument illustrating the so called alteration method, see, e.g., [3], Chapter 3. Define

$$m = \lceil \frac{q^n \log n}{(q-1)^{n-1} n} \rceil.$$

For a vector $(x_1, x_2, \ldots, x_n) \in Q^n$, let $B(x)$ denote the set of all vectors $(y_1, \ldots, y_n) \in Q^n$ for which $y_i \neq x_i$ for every i. Let $x^{(1)}, \ldots, x^{(m)}$ be m random, independent (not necessarily distinct) members of Q^n. For a fixed vector $(y_1, y_2, \ldots, y_n) \in Q^n$ and a vector $z \in Q^n$, we say that z *covers* y if the Hamming distance between z and y is precisely $n-1$. Notice that if this is the case then there exists an index i such that for every $u \in Q - \{y_i\}$, the vector $(y_1, \ldots, y_{i-1}, u, y_{i+1}, \ldots, y_n)$ lies in $B(z)$. Note also that for every fixed vector y, if z is chosen randomly and uniformly in Q^n, then the probability that z covers y is precisely $p = \frac{n(q-1)^{n-1}}{q^n}$. It follows that the probability that no vector among the vectors $x^{(1)}, \ldots, x^{(m)}$ covers y is $(1-p)^m \leq e^{-pm} \leq 1/n$. By linearity of expectation, the expected number of vectors y which are not covered by at least one vector $x^{(i)}$ is at most q^n/n. Therefore, there exists at least one choice for the vectors $x^{(1)}, \ldots, x^{(m)}$ such that the set Z of all vectors $y \in Q^n$ which are not covered by any $x^{(i)}$ satisfies $|Z| \leq q^n/n$. Fixing such vectors $x^{(i)}$, define $C = \cup_{i=1}^m B(x^{(i)}) \cup Z$, $W = Q^n - C$, and observe that C and W satisfy the assertion of the theorem, and that

$$|C| \leq m(q-1)^n + q^n/n \leq \frac{(q-1)\log n + 1}{n} q^n + (q-1)^n,$$

completing the proof. □

Remark: By an easy counting argument it follows that the minimum possible cardinality of a set C satisfying the properties in Theorem 7.1 is at least $\frac{q^n(q-1)}{n+q-1}$. For fixed q and large n, the upper bound here exceeds this lower bound by a factor of roughly $\log n$. For $q=2$ it is known that the lower bound gives the correct asymototic behaviour, and it will be interesting to decide if this is the case for every fixed q, and in particular, for $q=3$.

8 Monotone broadcast digraphs

Let $D = (V, E)$ be an acyclic directed graph on the set $V = \{0, 1, 2, \ldots, n-1\}$ of n vertices, where for every directed edge (i, j) of D, $i < j$. Suppose, further, that if (i, j) is in E, then so is (i, k) for all k between i and j, and that for every two vertices a, b with $a < b$, there is a directed path of length at most d from a to b.

Motivated by an attempt to prove the optimality of a certain broadcast encryption scheme, Dani Halevy and Adi Shamir [10] conjectured that for every fixed d, there is some $c(d) > 0$ such that the minimum possible number of edges in such a digraph on n vertices is at least $c(d)n^{1+1/d}$. This is proved in the following theorem.

Theorem 8.1 *There is an absolute positive constant* b *such that in the notation above,* D *must have at least* $b\frac{n^{1+1/d}}{d^2}$ *directed edges.*

We note that there are simple examples of digraphs D with the above property and at most $O(dn^{1+1/d})$ edges.

Proof of Theorem 8.1: To simplify the presentation, we omit all floor and ceiling signs whenever these are not crucial. Let $D = (V, E)$ be as above, without loss of generality assume that $n = t^d$, and write every vertex of D in base t; therefore each vertex is represented by a vector $(x_1, x_2, \ldots, x_d)$, with $0 \leq x_i < t$ for all i, where here x_1 is the most significant digit. To prove the theorem, we assume that the number of edges of D is at most, say, $\frac{n^{1+1/d}}{4e^2d^2} = \frac{t^{d+1}}{4e^2d^2}$, and show that in this case D cannot satisfy the assumptions.

Claim: There exists a vector $x = (x_1, x_2, \ldots, x_d)$ satisfying the following conditions:
(i) $x_j \leq t(1 - \frac{2}{d})$ for all j.
(ii) For every vertex $y = (y_1, y_2, \ldots, y_d)$ for which $y_j = x_j$ for all $j = 1, 2, \ldots, i$, the outdegree of y is at most $\frac{t^{d-i+1}}{2d}$.

Proof of Claim: There are $t^d(1 - \frac{2}{d})^d$ vectors that satisfy (i). Among those, the number of vertices y that violate (ii) for i is at most

$$\frac{|E|}{\frac{t^{d-i+1}}{2d}} \cdot t^{d-i}(1 - \frac{2}{d})^{d-i} < \frac{t^d}{2de^2}.$$

Summing over all possible values of i we conclude that there is a vertex satisfying (i) that does not violate (ii) for any i. □

Let x satisfy the conclusion of the claim. We show that there is no directed path of length at most d starting at x and ending at n. To do so we first show, by induction on $j \leq d - 1$, that any directed path of length j starting at x, ends at a vertex $(z_1, z_2, \ldots, z_d)$ such that $z_k = x_k$ for all $k \leq d - j$. For $j = 1$ this follows from the fact that $x_d \leq t(1 - \frac{2}{d})$ together with the fact that the outdegree of x is at most $\frac{t}{2d}$, implying that the first edge cannot increase the value of x by more than $\frac{t}{2d}$, and hence (as there is no carry), implying the required assertion for $j = 1$.

Assuming the assertion holds for $j < d - 1$, we prove it for $j + 1$. By assumption, the first j edges of any path starting at x end at a vertex $z = (z_1, \ldots, z_d)$ for which $z_k = x_k$ for all $k \leq d - j$. As x satisfies the conclusions of the claim, the outdegree of z is a most $\frac{t^{d-(d-j)+1}}{2d} = \frac{t^{j+1}}{2d}$. As $z_{d-j} = x_{d-j} \leq t(1 - \frac{2}{d})$ this implies that after adding to z a number that does not exceed $\frac{t^{j+1}}{2d}$ all digits $z_1, z_2, \ldots, z_{d-j-1}$ stay the same. This completes the proof of the induction. In particular, every path of length $d - 1$ starting at x ends at a vertex z whose first digit is $x_1 < t(1 - \frac{2}{d})$. As the outdegree of z is at most $\frac{t^d}{2d}$ this implies that no path of length at most d starting at x can end at a vertex whose most significant digit exceeds, say, $t(1 - \frac{1}{d})$. In particular, there is no directed path of length at most d from x to n, contradicting the assumption and hence showing that the number of edges exceeds $\frac{n^{1+1/d}}{4e^2d^2}$.

This completes the proof. □

Acknowledgment: I would like to thank Gil Kalai, Ariel Runbinstein and Gadiel Seroussi for helpful discussions and useful comments on various parts of this article.

References

[1] M. Adler, E. Halperin, R. Karp and V. Vazirani, A stochastic process on the hypercube with applications to peer-to-peer networks, STOC 2003, 575-584.

[2] N. Alon, Problems and results in extremal combinatorics- I, Discrete Math. 273 (2003), 31-53.

[3] N. Alon and J. H. Spencer, *The Probabilistic Method*, Second Edition, Wiley, New York, 2000.

[4] J. Aspnes, R. Beigel, M. Furst and S. Rudich, The expressive power of voting polynomials, Combinatorica 14 (1994), no. 2, 135–148.

[5] B. Bollobás, *Extremal Graph Theory*, Academic Press, London, 1978.

[6] B. Bollobás, *Random Graphs*, Academic Press (1986).

[7] M. Chudnovsky, N. Robertson, P.D. Seymour and R. Thomas, The Strong Perfect Graph Theorem, to appear.

[8] P. Erdős and M. Simonovits, Some extremal problems in graph theory, Colloq. Math. Soc. J. Bolyai 4, Combinatorial theory and its applications I, North-Holland, Amsterdam, 1970, pp. 377–390.

[9] J. Glazer and A. Rubinstein, A model of optimal persuasion rules, to appear.

[10] D. Halevy and A. Shamir, The LSD Broadcast Encryption Scheme, CRYPTO 2002, Lecture Notes in Computer Science, vol. 2442 (2002), pp. 47-60.

[11] S. Jukna, *Extremal Combinatorics*, Springer-Verlag, Berlin, 2001.

[12] G. Kalai, Private communication, 2002.

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

[14] M. Morgenstern, Existence and explicit Construction of q+1-regular Ramanujan graphs for every prime power q, *J. Combinatorial Theory* **B** 62 (1994), 44–62.

[15] L. Pyber, V. Rödl and E. Szemerédi, *Dense Graphs without 3-regular Subgraphs* , J. Combinatorial Theory Ser. B 63 (1995), 41-54.

[16] S. Robinson, Why mathematicians now care about their hat color, New York Times, Science Section, April 10, 2001.

[17] A. Sali and G. Simonyi, Oriented list colorings of undirected graphs, Contemporary trends in discrete mathematics , DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 49, Amer. Math. Soc., Providence, RI, 1999, 307–316.

[18] G. Seroussi, Private communication, 2001.

[19] P. Turán, Eine Extremalaufgabe aus der Graphentheorie, *Mat. Fiz Lapok* **48** (1941), 436–452.

[20] Zs. Tuza and M. Voigt, Oriented list colorings of graphs, J. Graph Theory 36 (2001), 217–229.