Extremal Bipartite Graphs and Superpolynomial Lower Bounds for Monotone Span Programs *

László Babai † Anna Gál‡ János Kollár§ Lajos Rónyai¶ Tibor Szabó‖
Avi Wigderson**

Abstract

This paper contains two main results. The first is an explicit construction of bipartite graphs which do not contain certain complete bipartite subgraphs and have maximal density, up to a constant factor, under this constraint. This construction represents the first significant progress in three decades on this old problem in *extremal graph theory*. The construction beats the previously known probabilistic lower bound on density. The proof uses the elements of commutative algebra and algebraic geometry (theory of ideals, integral extensions, valuation rings).

The second result concerns *monotone span programs*. We obtain the first superpolynomial lower bounds for explicit functions in this model. The best previous lower bound was $\Omega(n^{5/2})$ by Beimel, Gál, Paterson (FOCS'95); our analysis exploits a general combinatorial lower bound criterion from that paper. We give two proofs of superpolynomial lower bounds; one based on the construction in the first part, the other based on an analysis of Paley-type bipartite graphs via Weil's character sum estimates.

A third result demonstrates the power of monotone span programs by exhibiting a function computable in this model in linear size while requiring superpolynomial size monotone circuits and exponential size monotone formulae[1].

1 Introduction

1.1 Paley-type bipartite graphs

Let q be a prime power and $k|q-1$. We define the Paley-type bipartite graph $\Gamma = P(q,k)$ as follows. The two parts of the vertex set are $V_1 = V_2 = GF(q)$ (the finite field of order q); and two vertices $x \in V_1$ and $y \in V_2$ are adjacent if $(x+y)^{(q-1)/k} = 1$ (in $GF(q)$). These bipartite graphs are regular of degree $(q-1)/k$. (For this and other elementary facts about finite fields we refer the reader to Lidl–Niederreiter [LN].)

For $x \in V_1$, let $\Gamma(x)$ denote the set of neighbors of x. The set system $\{\Gamma(x) : x \in V_1\}$ has remarkable intersection properties which have been analysed via André Weil's character sum estimates. The first paper describing such an analysis in combinatorics is by Graham-Spencer [GS]; constructions of k-wise nearly independent random variables have been analysed in a similar spirit (cf. [AGHP], [AMN]).

While Weil's inequalities yield asymptotically tight estimates of the sizes of r-wise intersections of the sets $\Gamma(x)$ up to the point when the intersection sizes become about $\sqrt{q}$ (this occurs around $r \approx \log q/(2\log k)$), the large error term in Weil's estimates renders them useless for higher intersections.

We introduce a subclass of the Paley-type bipartite graphs, to be called *norm-graphs*, for which entirely

*Part of this work was done while two of the authors, Gál and Rónyai, were visiting the University of Chicago.

†Department of Computer Science, University of Chicago, Chicago IL 60637-1504. E-mail: laci@cs.uchicago.edu

‡Institute for Advanced Study, Princeton N.J. 08540. Email: panni@math.ias.edu. – Research supported by NSF Grant DMS-9304580.

§Department of Mathematics, University of Utah, Salt Lake City, UT 84112. E-mail: kollar@math.utah.edu. – Research supported in part by NSF Grants DMS-8707320 and DMS-9102866.

¶Computer and Automation Institute, Hungarian Academy of Sciences, Budapest, Lágymányosi u. 11, Hungary H-1111. E-mail: lajos@nyest.ilab.sztaki.hu. – Research supported in part by Hungarian National Foundation for Scientific Research Grant T016503.

‖Department of Mathematics, The Ohio State University, Columbus, Ohio 43210. Email: szabote@math.ohio-state.edu .

**Institute of Computer Science, Hebrew University, Jerusalem, Israel. Currently visiting the Institute for Advanced Study, Princeton, N.J. 08540 and Princeton University. Research supported by the Sloan Foundation, American-Israeli BSF grant 92-00106, and the Wolfson Research Awards, administered by the Israel Academy of Sciences. Email: avi@cs.huji.ac.il .

[1] This paper arose from the merger of two papers, one by Kollár, Rónyai, Szabó on the Zarankiewicz problem [KRS], and a subsequent paper by Babai, Gál, and Wigderson on span programs [BGW]. The journal versions will be published separately.

different techniques enable us to control r-wise intersection sizes up to $r \approx \log q / \log k$, when the expected r-wise intersection size becomes bounded (and most $(r+1)$-wise intersections empty).

The norm-graphs are defined by setting $q = q_1^t$ and $k = q_1 - 1$, where q_1 is a prime power and $t \geq 2$. The techniques required for the strong analysis involve the elements of commutative algebra and algebraic geometry. As a result we make progress on the "Zarankiewicz problem" which will be described in the next section.

Explicit combinatorial constructions are scarce and in great demand in the theory of computing. Specifically, explicit constructions for the Zarankiewicz problem have been applied by several authors to the monotone circuit complexity of the "Boolean sums" problem ([Ne, Me, Pi]). A lower bound of $n^{2-o(1)}$ was first achieved by Andreev [An] via his explicit construction of graphs of large density for the Zarankiewicz problem. The gap between the trivial upper bound $n^{2-1/r}$ and Andreev's lower bound is a factor of $r^{\Theta(r^2)}$; norm-graphs reduce this gap to $(r+2)!$ where the parameter r may grow as a function of n.

As a more significant indication of the relevance of the norm-graphs to lower bounds, our first superpolynomial lower bound in the *monotone span program* model (see Section 1.3) was based on the norm-graphs. We subsequently observed that an even stronger lower bound follows from the analysis of middle-range intersections of Paley-type graphs via Weil's estimates. We present both techniques.

1.2 The Zarankiewicz problem

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 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. One of our goals in this paper is the study of the Turán numbers of complete bipartite graphs (the "Zarankiewicz problem").

Let t, u be positive integers with $t \leq u$. We denote by $K_{t,u}$ the complete bipartite graph with $t+u$ vertices and tu edges. Kővári, T. Sós, and Turán [KST] gave the following upper bound for an arbitrary fixed t and $u \geq t$:

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

where $c_{t,u} > 0$ is a constant depending on t and u. 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

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

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

Note that for all t, u such that $2 \leq t \leq u$, we have $\frac{t+u-2}{tu-1} > \frac{1}{t}$, 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 $u \geq t$ [Er38, Br].

The incidence graphs of projective planes demonstrate this order of magnitude for $t = 2$ (this was observed by Esther Klein, as reported by Erdős in [Er38]). 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 [ERS], Brown [Br]), and for general $u \geq 2$,

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

The situation for $t \geq 3$ seems more difficult. The optimality of the upper bound (1) for $t = 3$ was established by W. G. Brown [Br], 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 $q \equiv -1 \bmod 4$.

In spite of its considerable interest to combinatorics and to the theory of computing (cf. [Ne, Me, Pi, ES, Bol, An, Fü]) no substantial progress on this problem has been made since W.G. Brown's 1966 paper [Br]. In particular, for no pair (t, u) with $4 \leq t \leq u$ has the probabilistic lower bound been improved.

In this paper we present an *explicit construction* which demonstrates the optimality, up to a constant factor, of the upper bound (1) for all values of $t \geq 2$ and $u \geq t! + 1$:

Theorem 1.1 *For $t \geq 2$ and $u \geq t! + 1$ we have*

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

where $c_t > 0$ is a constant depending on t. We may choose $c_t = 2^{-t}$ for every n, and $c_t = 1/2$ for infinitely many values of n.

Note in particular that this bound beats the order of magnitude of the probabilistic lower bound for every pair (t, u) under consideration. Both the *explicitness* of the construction and the *optimality* of the exponent are essential for our application to span programs.

We should mention that 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

[An]. He constructed bipartite graphs with n vertices on each side, with $n^{2-1/r}$ edges, and without $K_{t(r),u(r)}$ where both $t(r)$ and $u(r)$ are greater than $(2r)^{r(r-1)/2}$. These parameters are far too large for our application. Our result reduces these parameters to $t(r) = r$ and $u(r) = r! + 1$, thus improving Andreev's result for all $r \geq 2$.

For more details and references on the Zarankiewicz problem we refer to Chapter VI, Section 2 of Bollobás [Bol] and to Füredi [Fü].

1.3 Monotone span programs

Karchmer and Wigderson [KW] introduced span programs as a linear algebraic model for computing Boolean functions.

Let us consider a linear space W over some field K; let $w \neq 0$ be a specified vector called the *root*. A *span program* takes a set of n variable symbols $x_1, \ldots, x_n$ and their negations, together called *literals*, and associates a subspace with each of the $2n$ literals. Such a program defines a Boolean function $f(x_1, \ldots, x_n)$ in the following way: let $U = U(\alpha_1, \ldots, \alpha_n)$ denote the span of those subspaces corresponding to TRUE literals under a given truth-assignment $x_i := \alpha_i$ $(i = 1, \ldots, n; \alpha_i \in \{0, 1\})$. We set $f(\alpha_1, \ldots, \alpha_n) = 1$ precisely if $w \in U$.

The *size* of a span program is the sum of the dimensions of the subspaces associated with the literals. Note that the size of the span program is not less, and at most by a factor of $2n$ greater, than the dimension of W (assuming, as we may w.l.o.g., that those subspaces span all of W). Thus, as far as superpolynomial bounds are concerned, size and dimension are equivalent complexity measures.

A span program is called *monotone* if only the positive literals $\{x_1, \ldots, x_n\}$ are associated with subspaces (negated variables correspond to the $\{0\}$ subspace). Monotone span programs compute monotone Boolean functions, even though the computation uses non-monotone linear algebraic operations.

We denote by $\mathrm{SP}_K(f)$ (and $\mathrm{mSP}_K(f)$) the size of the smallest span program (monotone span program, resp.) over the field K that computes f.

The class of Boolean functions with polynomial size span programs is equivalent to the class of functions with polynomial size counting branching programs [BDHM, KW]. Span program size is a lower bound on the size of symmetric branching programs [KW]. The model of symmetric branching programs is essentially the same as that of (undirected) contact schemes (for definitions, see [KW]). Lower bounds for span programs also imply lower bounds for formula size.

Span programs can be viewed as a model of *parallel computation.* Indeed, functions with polynomial size span programs over finite fields belong to NC^2. (This is immediate from the fact that linear algebra is in (non-uniform) NC^2 [Ber, BDHM, KW, Mu]). As we shall see, the monotone analog of this statement fails badly; functions admitting polynomial size monotone span programs do not necessarily have polynomial size or even polylog depth monotone circuits (cf. Theorem 1.2 below).

The reduction in [KW] from symmetric branching programs to span programs preserves monotonicity, and thus lower bounds for monotone span programs imply lower bounds for monotone symmetric branching programs and for monotone formula size.

Lower bound techniques for monotone circuits and formulae are well known (e.g. Razborov [Ra1, Ra2, Ra3], Haken [Ha] for circuits, Karchmer-Wigderson [KW1], Raz-Wigderson [RW] for formulae). These techniques, however, do not appear to be adaptable to the study of monotone span programs. Indeed, the following separation result demonstrates the power of monotone span programs vs. monotone circuits and formulae.

Theorem 1.2 *There exists a family $\{f_n\}$ of monotone Boolean functions in n variables such that f_n can be computed by a monotone span program of size $O(n)$ (and dimension $O(\sqrt{n})$) over $GF(2)$ but requires monotone Boolean circuits of size $n^{\Omega(\log n)}$, and monotone formulae of size $\exp(\Omega(\sqrt{n}))$.*

A different motivation for studying monotone span programs comes from a cryptographic tool called *"secret-sharing schemes."* This connection is reviewed in detail by Beimel, Gál, and Paterson [BGP]. Without giving the definitions, we should mention that most known secret sharing schemes are "linear," and lower bounds for the total size of "shares" in linear secret sharing schemes are equivalent to lower bounds for monotone span programs. Our main result can therefore be interpreted as a *superpolynomial lower bound for linear secret sharing schemes.* For details we refer to the survey by Stinson [St] and to the extensive literature listed in [BGP].

The best known lower bound for *general* secret sharing schemes is $\Omega(n^2/\log n)$ (Csirmaz [Cs]). This immediately implies the same lower bound for monotone span programs for explicit functions. This by-product of [Cs] was improved by Beimel, Gál, and Paterson [BGP] to an $\Omega(n^{5/2})$ lower bound for monotone span programs; they prove this bound for the 6-clique function. (Here n denotes the number of variables.) More importantly, [BGP] exhibits a combinatorial criterion which we shall be able to exploit to obtain superpolynomial lower bounds. We state our main result.

Theorem 1.3 *For every reasonable function* $2 \leq t(n) \leq \log n / \log\log n$*, there exists a family of explicit monotone Boolean functions* f_n *in* n *variables such that*

$$\mathrm{mSP}_K(f_n) = n^{\Omega(t(n))}$$

over any field K*. The function family* $\{f_n\}$ *belongs both to* NP *and to* $\mathrm{DSPACE}(t(n) \cdot \log n)$*. – We call* $t(n)$ *"reasonable" if it is monotone nondecreasing and computable in* $O(\log n)$ *space.*

2 Monotone span programs vs. monotone circuits and formulae

Here we give the proof of Theorem 1.2, a result that may be interpreted as an indication why lower bounds for monotone span programs may be hard to come by.

We consider the following function f_n on $n = v^2$ variables: the input is a $v \times v$ (0,1)-matrix representing a bipartite graph X with v vertices in each part. X is accepted if it has an *odd factor*, i.e., a spanning subgraph such that all vertices have odd degree in the subgraph. Note that X is rejected exactly if it has a component with an odd number of vertices.

It is easy to construct a monotone span program of size n over $GF(2)$ for this function. Indeed, let $V = V_1 \cup V_2$ be the vertex set and let W denote the $2v$-dimensional space over $GF(2)$ generated by the basis $\{u_i : i \in V\}$. The variables are $x_{i,j}$ ($i \in V_1, j \in V_2$). Let $x_{i,j}$ correspond to the one-dimensional subspace spanned by $u_i + u_j$. The root is the "all-ones" vector $w = \sum_{i \in V} u_i$. It should be clear that the root is the sum of a set of vectors of the form $u_i + u_j$ precisely if the corresponding edges (i, j) form an odd factor.

Despite the simplicity of this span program (as well as the trivial sequential algorithm) for this function, it has close affinity to the perfect matching problem, which makes it as difficult for monotone Boolean models. Specifically, note that every perfect matching is an odd factor, and should be accepted. For rejected graphs, identify every 2-coloring of V (say red and blue) with the graph of all monochromatic edges. This graph has two connected components. Note that an odd 2-coloring (in which each color occupies an odd number of vertices) has two odd components, and thus is rejected by our function.

Now for circuit size, we observe that Razborov's proof [Ra2] provides an $n^{\Omega(\log n)}$ lower bound on any monotone circuit that accepts all perfect matchings, and rejects any constant fraction of *all* 2-colorings. As odd 2-colorings constitute half of all 2-colorings, the above argument suffices.

For the formula size (equivalently circuit depth) lower bound we use a similar method to the one used by Raz and Wigderson in [RW], which is based on the communication complexity approach of Karchmer and Wigderson [KW1]. Define the disjointness function on a pair x, y of u-bit vectors by DISJ $(x, y) = 1$ iff the sets represented by these vectors are disjoint.

Theorem 2.1 *([KS, Ra4], cf. [BFS]) Any* $1/3$ *error probabilistic communication protocol for* DISJ *requires* $\Omega(u)$ *communication bits.*

We will reduce DISJ to the following communication problem ODDFACTOR (m, c) on the set V where $v = 4u$. The first player has a perfect matching m from V_1 to V_2. The second player has an odd coloring of V. They have to compute an edge $e \in m$ which is 2-colored by c. As this is the monotone relation capturing f_n, if this problem requires t bits to solve deterministically, the monotone formula size of f_n is $\exp(\Omega(t))$. Assuming a t-bit deterministic protocol here, we derive a probabilistic protocol of the same complexity for DISJ.

We shall use the following "gadget." Let (a_1, a_2, a_3, a_4) and (b_1, b_2, b_3, b_4) be ordered quadruples of distinct vertices in V_1 and in V_2, resp. Define two matchings

$$M_1 = \{(a_1, b_1), (a_2, b_2), (a_3, b_3), (a_4, b_4)\}$$

and

$$M_0 = \{(a_1, b_2), (a_2, b_1), (a_3, b_4), (a_4, b_3)\}\ .$$

Also define two 2-colorings (red is the complement of blue in each) by $B_1 = \{a_1, b_2, a_3, b_4\}$ and $B_0 = \{a_1, a_2, b_1, b_2\}$.

Now assume our players have the inputs x and y, resp., for the disjointness problem, and they share a random string r. They interpret r as a partition of V into u pairs of quadruples of vertices of the type described above, with a uniform distribution over all partitions and orderings. The player holding x constructs the matching m by taking from the ith part of the partition the matching M_{x_i}, for all $i \in [u]$. Similarly, the player holding y constructs a 2-coloring c' using B_{y_i} for all $i \in [u]$. Since this coloring c' is even, he then flips the color of a random vertex w in V to produce his final odd coloring c. On obtaining a bichromatic edge e by the assumed protocol, the players answer 1 iff $w \in e$.

Observe that if DISJ $(x, y) = 1$ then the coloring c' makes each edge of the matching m monochromatic, and there is exactly one bichromatic edge in m under the coloring c. Therefore the players will make no error on disjoint pairs (x, y).

On the other hand if (x, y) intersect in k places, then (m, c') is uniformly distributed over all such pairs having $4k$ bichromatic edges. Since the protocol returning e is deterministic, and w is random, the players will now err with probability $\leq 1/(4k+1) \leq 1/5$. $\square$

3 The lower bounds for monotone span programs

3.1 The BGP Lower Bound Condition

We shall make use of a technique introduced by Beimel, Gál, and Paterson [BGP], to prove lower bounds for monotone span programs. The idea is to show that if a small monotone span program accepts all the minterms of the function f then it must also accept an input that does not contain any minterms, a contradiction. This approach can be viewed as an application of the "fusion method" [Ra3, Ka, Wi].

A *minterm* of a monotone Boolean function is a minimal set of variables which, if assigned the value 1, force the function to take the value 1 regardless of the values assigned to the remaining variables.

It will be convenient to use the language of *set systems* (hypergraphs) rather than Boolean functions. The correspondence is established by the bijection between $\{0,1\}^n$ and the power-set of a universe X of n elements. The Boolean function f will then correspond to the set system $f^{-1}(1)$. Clearly, monotone Boolean functions correspond to *filters*, i.e., set systems closed under supersets. The minterms correspond to the minimal elements of this filter (with respect to inclusion).

A *Sperner family* is a family of sets none of which contains any other member of the family. The minimal elements of a filter form a Sperner family; and each Sperner family $\mathcal{F}$ uniquely defines a filter (consisting of all not necessarily proper supersets of the members of $\mathcal{F}$).

Given a Sperner family $\mathcal{F}$, we shall denote by $f_{\mathcal{F}}$ the corresponding monotone Boolean function.

Given a set system $\mathcal{F} \subset 2^X$ over the universe X, we say that a set $A \subseteq X$ *determines* a member $H \in \mathcal{F}$ if H is the unique member of $\mathcal{F}$ containing A. Next we define is a key concept introduced in [BGP].

Definition 3.1 *We call a Sperner family $\mathcal{F}$* self-avoiding *if one can associate a set $D(H)$ with each $H \in \mathcal{F}$, called the* core *of H, such that*

(i) $D(H)$ determines H (with respect to $\mathcal{F}$); and

(ii) for any $H \in \mathcal{F}$ and any subset $T \subseteq D(H)$, the set

$$S(T) := \bigcup_{G \in \mathcal{F}, G \cap T \neq \emptyset} G \setminus T,$$

does not contain any member of $\mathcal{F}$. (We call $S(T)$ the spread *of T.)*

(This definition is equivalent to a special case of "critical families" defined in [BGP, Sec. 2.2].)

The following result summarizes the BGP lower bound technique.

Theorem 3.2 (Beimel, Gál, Paterson [BGP]) *Let $\mathcal{F}$ be a Sperner family over a universe of n elements and $f_{\mathcal{F}}$ the corresponding monotone Boolean function in n variables. If $\mathcal{F}$ is self-avoiding then for every field K we have*

$$\mathrm{mSP}_K(f_{\mathcal{F}}) \geq |\mathcal{F}| \ .$$

3.2 A sufficient condition for self-avoidance

We shall use the following general scheme to construct self-avoiding Sperner families.

Take a bipartite graph Γ with vertex set $V_1 \cup V_2$.

Notation 3.3 For a vertex x, we denote by $\Gamma(x)$ the set of neighbors of x; and for a subset A of the vertex set, we denote by $\Gamma(A)$ the set of common neighbors of A, i.e., $\Gamma(A) = \cap_{x \in A} \Gamma(x)$. Let moreover $\Delta(A) = A \cup \Gamma(A)$.

Notation 3.4 An *r-set* is a set of r elements. For a set X and an integer $r \geq 0$ we shall use $\binom{X}{r}$ to denote the *set* of all r-subsets of X.

Now fix an integer $t > 1$ and a subset $\mathcal{S} \subseteq \binom{V_1}{t-1}$. Set

$$\mathcal{F} = \mathcal{F}(\Gamma, \mathcal{S}) := \{\Delta(A) : \ A \in \mathcal{S}\}. \qquad (3)$$

Let $m(t) = m(\Gamma, t) := \max\{|\Gamma(B)| : \ B \in \binom{V_1}{t}\}$.

Lemma 3.5 *If $|\Gamma(A)| > (t-1) \cdot m(t)$ for all $A \in \mathcal{S}$ then $\mathcal{F}$ is self-avoiding.*

Proof. First, $\mathcal{F}$ is a Sperner family since all $A \in \mathcal{S}$ have the same cardinality $(t-1)$.

We define the core function as $D(\Delta(A)) = A$. This clearly satisfies item (i) in Def. 3.1. We need to verify item (ii).

Assume that $A \in \mathcal{S}$. Let $T \subseteq A$, and consider the *spread* $S(T)$ defined in Def. 3.1. Assume for a contradiction that $\Delta(A^*) \subseteq S(T)$ holds for some $A^* \in \mathcal{S}$.

By the definition of $S(T)$ and our construction, every vertex $y \in S(T) \cap V_2$ must be adjacent to some vertex $x(y) \in T$. This is true in particular for each $y \in \Gamma(A^*)$. Let x_0 be the most frequently occurring $x(y)$ for $y \in \Gamma(A^*)$; then x_0 is adjacent to more than $(t-1) \cdot m(t)/|T| \geq m(t)$ vertices in $\Gamma(A^*)$. In other words,

$$|\Gamma(A^* \cup \{x_0\})| > m(t),$$

in contradiction with the definition of $m(t)$ since $|A^* \cup \{x_0\}| = t$ (which in turn holds because $A^* \cap T = \emptyset$). $\square$

3.3 An intersection property of the norm-graphs

The *norm-graphs* are the explicit bipartite graphs to be constucted in Section 5. The properties of these graphs, to be verified in Section 5.2 and critical to the span program application, are summarized in the following theorem.

Theorem 3.6 *Given a prime power q and positive integers t, s where $s = t!$, there exists an explicit bipartite graph $\Gamma = \Gamma(q, t)$ with the following properties:*

(i) Γ has $2n := 2q^t$ vertices, equally partitioned among the two classes V_1 and V_2;

(ii) Γ is regular of degree $(q^t - 1)/(q - 1)$;

(iii) Any t distinct vertices in V_1 have at most s common neighbors.

From the properties listed, we deduce an additional property of Γ.

Lemma 3.7 *Any graph Γ possessing properties (i)–(iii) listed in Theorem 3.6 also has the following property:*

($\star$) At least a $\frac{1}{2s-1}$ fraction of the sets $A \in \binom{V_1}{t-1}$ have $|\Gamma(A)| \geq q/2$ common neighbors.

We defer the combinatorial proof to Section 4.1.

3.4 Large self-avoiding Sperner families: first construction

We use the bipartite graph Γ discussed in Theorem 3.6 to construct a Sperner family. We make an additional **assumption** on the parameters:

$$q > 2ts. \tag{4}$$

Let $\mathcal{S} = \{A \in \binom{V_1}{t-1} : |\Gamma(A)| \geq q/2\}$. We apply our general construction $\mathcal{F} = \mathcal{F}(\Gamma, \mathcal{S})$ (eqn. 3). (So we shall have $2n$ Boolean variables, an insignificant change in notation).

We now have $m(t) \leq s$ by item (iii) in Theorem 3.6. Our assumption (4) therefore implies the inequality $|\Delta(A)| > t \cdot m(t)$ for all $A \in \mathcal{S}$. By Lemma 3.5 we conclude that $\mathcal{F}$ is self-avoiding.

Moreover, from Lemma 3.7, we have $|\mathcal{F}| \geq \binom{n}{t-1}/(2s-1)$. For $s = t!$, the latter quantity is approximately $n^{t-1}/((t+1)!)^2$. We need to choose the parameters such that $q > 2ts$.

Choosing $q := \Omega(ts)$ we obtain

$$t = t(n) = O(\sqrt{\log n / \log\log n}).$$

In view of Theorem 3.2, this proves our first superpolynomial lower bound $n^{\Omega(t(n))}$ for monotone span programs, confirming Theorem 1.3 up to $t(n) \leq \sqrt{\log n / \log\log n}$. $\square$

3.5 Large self-avoiding Sperner families: second construction

The following well known lemma guarantees a tight control of the intersection sizes of vertex neighborhoods in the Paley-type graphs $\Gamma = P(q, k)$. We use the notation introduced in Section 1.1. For real numbers b, c we use the notation $b \pm c$ to denote a quantity between $b - c$ and $b + c$.

Lemma 3.8 *Let $a_1, \ldots, a_t$ be distinct elements of the finite field $GF(q)$ and $k|q-1$ $(k, t \geq 2)$. Then the number of solutions $x \in GF(q)$ to the system of equations $(a_i + x)^{(q-1)/k} = 1$ $(i = 1, \ldots, t)$ is $q/k^t \pm t\sqrt{q}$.*

In Section 4.2 we state the relevant character sum estimate of A. Weil and show how to deduce Lemma 3.8 along the lines of [GS].

Restated in our combinatorial setting, we obtain that for $A \in \binom{V_1}{t}$ we have $|\Gamma(A)| = q/k^t \pm t\sqrt{q}$.

It follows that as long as q/k^t is much larger than $\sqrt{q}$, the $(t-1)$-wise intersections are almost uniformly k-times larger than the t-wise intersections. In view of Lemma 3.5, this suggests the following constraints on the choice of the ranges of the parameters in the following lemma.

Lemma 3.9 *If $k \geq 3t$ and $q > 4t^4 k^{2t-2}$ then the system $\mathcal{F} = \{\Delta(A) : A \in \binom{V_1}{t-1}\}$ is self-avoiding.*

(In the notation of Section 3.2, we have chosen $\mathcal{S} = \binom{V_1}{t-1}$.)

Indeed, $m(t) \leq q/k^t + t\sqrt{q}$ and for all $A \in \binom{V_1}{t-1}$, $|\Gamma(A)| \geq q/k^{t-1} - (t-1)\sqrt{q}$, both by Lemma 3.8. Combined with the assumption on the parameters, these inequalities guarantee that $|\Gamma(A)| > t \cdot m(t)$, hence Lemma 3.5 applies. $\square$

To achieve the best lower bound, i. e., to maximize $|\mathcal{F}| = \binom{q}{t-1}$, given q, we need to maximize t under the given constraints. Not all prime powers q will allow this, only those belonging to specific arithmetic progressions. Let us select t first, and then minimize q. W.l.o.g. assume t is odd (otherwise add 1); set $k := 3t$; and select q to be of the form $q := 2^{\ell\varphi(3t)}$ where φ denotes Euler's totient function. Such a choice guarantees that $k|q-1$. Since $1 < \varphi(3t) \leq 2t$, one can clearly choose ℓ such that q satisfies the inequalities $4t^4k^{2t-2} < q < 2^{2t} \cdot 4t^4k^{2t-2}$. With this choice, $t = \Theta(\log q/\log\log q)$, and the lower bound $|\mathcal{F}| = q^{\Theta(\log q/\log\log q)}$ on the monotone span program complexity of the monotone function in $2q$ variables, defined by $\mathcal{F}$, follows. $\square$

It may seem that this lower bound applies to infinitely many, but not to all values of n. Note, however, that for every sufficiently large n, an appropriate q can be found between $n/2$ and $\sqrt{n}$. Using our function augmented with $n-2q$ redundant variables, we still have a lower bound of the form $n^{\Theta(\log n/\log\log n)}$.

4 Proofs of the intersection lemmas

4.1 Typical intersections: proof of Lemma 3.7

The proof will follow by combining two auxiliary observations. Let $d = (q^t-1)/(q-1)$ denote the degree of the vertices of Γ. We shall use the inequality $d \geq q^{t-1}+t$, which holds assuming $t \geq 3$. (We may assume this for our application.) We shall use the E ("expected value") notation for *averages* over explicitely stated domains.

Claim 4.1 *For any k, $0 \leq k \leq t$, the average cardinality of $\Gamma(A)$ over all $A \in \binom{V_1}{k}$ is*

$$E(|\Gamma(A)|) = \frac{n \cdot \binom{d}{k}}{\binom{n}{k}} > n/q^k = q^{t-k}.$$

Proof. For $A \in \binom{V_1}{k}$ and $y \in V_2$, we count the number of inclusions $y \in \Gamma(A)$ in two ways. We obtain $\sum_A |\Gamma(A)|$ on the one hand, and $\sum_y \binom{|\Gamma(y)|}{k} = n \cdot \binom{d}{k}$ on the other hand. The inequality follows by observing that $\binom{d}{k} > (d-k+1)^k/k! > q^{(t-1)k}/k!$; and $\binom{n}{k} < n^k/k! = q^{tk}/k!$. $\square$

Claim 4.2 *Let $A \in \binom{V_1}{t-1}$. Then $|\Gamma(A)| < qs$.*

Proof. For any subset $B \subset V_2$ we have $|B| \cdot d = \sum_{x \in V_1} |\Gamma(x) \cap B|$ (by counting the edges between V_1 and B). We now apply this equation to $B = \Gamma(A)$. We split the sum on the right hand side according to whether $x \in A$ or not; in the former case, $\Gamma(x) \supset B$.

$$|B| \cdot d = |A| \cdot |B| + \sum_{x \in V_1 \setminus A} |\Gamma(x) \cap B|.$$

Consequently the average cardinality of $\Gamma(x) \cap B$ over $x \in V_1 \setminus A$ is $|B|(d-|A|)/(n-|A|) > |B|/q$. It follows that for some $x_0 \in V_1 \setminus A$ we have $|\Gamma(x_0) \cap B| > |B|/q$. But the left hand side here is the number of common neighbors of the t-tuple $A \cup \{x_0\}$; hence $s > |B|/q$, as stated. $\square$

Now we put these two claims together to prove Lemma 3.7. Let p denote the probability that $|\Gamma(A)| \geq q/2$ where A is a $(t-1)$-subset of V_1 chosen uniformly at random. Then, by Claim 4.2 we have

$$E(|\Gamma(A)|) \leq p \cdot qs + (1-p) \cdot q/2 = q((2s-1)p+1)/2. \tag{5}$$

On the other hand, we have $E(|\Gamma(A)|) > q$ by Claim 4.1 ($k = t-1$). A comparison with inequality (5) yields $p \geq 1/(2s-1)$, as desired. $\square$

4.2 Character sums: proof of Lemma 3.8

Let χ be a homomorphism of the multiplicative group $GF(q)^\times$ onto the group of k^{th} roots of unity. We extend the domain of χ to $GF(q)$ by setting $\chi(0) = 0$. The function χ is called a *multiplicative character of order* k over $GF(q)$.

Let $f(x)$ be a polynomial over $GF(q)$ which is not of the form $c \cdot (g(x))^k$ for any polynomial g over $GF(q)$ and scalar $c \in GF(q)$. Let t denote the number of distinct roots of f in the algebraic closure of $GF(q)$. Under these circumstances, Weil's theorem gives the following bound.

Theorem 4.3 (A. Weil)

$$\Big| \sum_{x \in GF(q)} \chi(f(x)) \Big| \leq (t-1)\sqrt{q}. \tag{6}$$

(See e.g. [Sch, p.43, Theorem 2C].)

Now we turn to the proof of Lemma 3.8. Let ω denote a primitive k^{th} root of unity and let g be a generator of the multiplicative group of $GF(q)$. Set $\chi(g^\ell) = \omega^\ell$. This is clearly a homomorphism onto the group of k^{th} roots of unity; add $\chi(0) = 0$ to obtain a character of order k. It is clear moreover that $\chi(g^\ell) = 1$ if and only if $k|\ell$, i.e., if and only if $x^{(q-1)/k} = 1$, where $x = g^\ell$.

Let X denote the set of those $x \in GF(q)$ which simultaneously satisfy $\chi(a_i + x) = 1$ for $i = 1, \ldots, t$. Our aim is to estimate the number $N = |X|$.

Consider the polynomial $h(z) = 1 + z + \ldots + z^{k-1} = (z^k-1)/(z-1)$. Clearly $h(1) = k$, $h(\omega^j) = 0$ for $j = 1, \ldots, k-1$, and $h(0) = 1$. Let now $H(x) = \prod_{i=1}^t h(\chi(a_i + x))$. We observe that if $x \in X$ then $H(x) = k^t$; if $x = -a_i$ for some i then $H(x) = 0$ or $H(x) = k^{t-1}$; and in the remaining cases, $H(x) = 0$.

Therefore the sum $S := \sum_{x\in GF(q)} H(x)$ satisfies

$$Nk^t \le S \le Nk^t + tk^{t-1}. \qquad (7)$$

$H(x)$ is the product of sums of k terms each. Let us expand the product to the sum of k^t terms. Let Ψ denote the set of the k^t functions $\psi : \{1,\dots,t\} \to \{0,1,\dots,k-1\}$ which will serve to index this sum. We have

$$S = \sum_{x\in GF(q)} \sum_{\psi\in\Psi} \prod_{i=1}^{t} (\chi(a_i+x))^{\psi(i)} = \sum_{x\in GF(q)} \sum_{\psi\in\Psi} \chi(f_\psi(x)), \qquad (8)$$

where $f_\psi(x) := \prod_{i=1}^t (a_i + x)^{\psi(i)}$.

Let $\psi_0(i) := 0$ for all i; hence $f_{\psi_0}(x) = 1$ for all $x \in GF(q)$. After switching the order of summation in equation (8), let us separate the term corresponding to ψ_0; clearly, this term will be q. This is the "main term"; we need to estimate the "error term" $R := S - q$. Let $\Psi^* = \Psi \setminus \{\psi_0\}$.

$$|R| \le \sum_{\psi\in\Psi^*} \Big| \sum_{x\in GF(q)} \chi(f_\psi(x)) \Big|.$$

We note that all roots of f_ψ belong to $GF(q)$, and it has at least one and at most $t-1$ distinct roots, each with multiplicity $\le k-1$. It follows that the conditions of Weil's theorem are satisfied and each inner sum has absolute value $\le (t-1)\sqrt{q}$. Consequently

$$|R| \le k^t(t-1)\sqrt{q}.$$

Combining this with equation (7), we obtain

$$\begin{array}{rclcl} N & = & S/k^t \pm t/k & = & q/k^t + R/k^t \pm t/k \\ & = & q/k^t \pm (t-1)\sqrt{q} \pm t/k & = & q/k^t \pm t\sqrt{q}. \quad \square \end{array}$$

5 The norm-graph

5.1 The construction

Let q be a prime-power and $t > 1$ be an integer. We define the *norm-graph* $G = G_{q,t}$ as the Paley-type bipartite graph $P(q^t, q-1)$. (Here we use q in the role of q_1 of Section 1.1.)

We have to explain the term "norm-graph." 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 two vertices $a \in V_1$ and $b \in V_2$ are adjacent iff $N(a+b) = 1$.

Let us write $n = |V_1| = |V_2| = q^t$ for the number of vertices in each half of the graph. Then the degree of each vertex is $(q^t-1)/(q-1) > n^{1-1/t}$.

The main technical contribution of this paper is the following:

Theorem 5.1 *The graph $G = G_{q,t}$ contains no subgraph isomorphic to $K_{t,t!+1}$.*

5.2 The proof

Theorem 5.1 is a direct consequence of the following statement: if $d_1, d_2, \dots, d_t$ are t distinct elements from $GF(q^t)$, then the system of equations

$$\begin{array}{rclcl} N(x+d_1) & = & (x+d_1)(x^q+d_1^q)\cdots(x^{q^{t-1}}+d_1^{q^{t-1}}) & = & 1 \\ N(x+d_2) & = & (x+d_2)(x^q+d_2^q)\cdots(x^{q^{t-1}}+d_2^{q^{t-1}}) & = & 1 \\ \vdots & & \vdots & & \vdots \\ N(x+d_t) & = & (x+d_t)(x^q+d_t^q)\cdots(x^{q^{t-1}}+d_t^{q^{t-1}}) & = & 1 \end{array} \qquad (9)$$

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

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

Theorem 5.2 *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*

$$\begin{array}{rcl} (x_1-a_{11})(x_2-a_{21})\cdots(x_t-a_{t1}) & = & b_1, \\ (x_1-a_{12})(x_2-a_{22})\cdots(x_t-a_{t2}) & = & b_2, \\ \vdots & & \vdots \\ (x_1-a_{1t})(x_2-a_{2t})\cdots(x_t-a_{tt}) & = & b_t \end{array} \qquad (10)$$

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

This indeed suffices to prove Theorem 5.1 because system (9) is a special case of system (10) ($K = GF(q^t)$, $a_{ij} = -d_j^{q^{i-1}}$, $x_i = x^{q^{i-1}}$, $b_j = 1$). $\square$

We put $f_j = f_j(x_1, x_2, \dots, x_t) := (x_1 - a_{1j})(x_2 - a_{2j})\cdots(x_t - a_{tj})$ $(1 \le j \le t)$ for the polynomials on the left-hand side of the system (10). Let us define the regular map $F : K^t \to K^t$ by $F(x_1, x_2, \dots, x_t) := (f_1(x_1,\dots,x_t), \dots, f_t(x_1,\dots,x_t))$. Theorem 5.2 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 $F(x_1,\dots,x_t) = 0$ are simple. The structure to be established in the first half of the proof will then allow the $t!$ bound to carry over from $b = 0$ to all b. This conclusion[2] will rest on the following result (see Theorem 3 in [Sha, Chap. II, Sec. 6.3, p.143]; in the first edition of [Sha], it is stated as Theorem 6 in [Chap. II, Sec. 5]). For some of the definitions, and the details of the proof, see Section 5.3 below.

[2]At first sight it would seem natural to apply Bézout's theorem [Sha] on intersections in projective space to the study of solutions of system (10). Note, however, that the projective closures of the hypersurfaces in (10) all contain the hyperplane $x_1 = 0$, hence their intersection is not proper.

Fact 5.3 *Let K be an algebraically closed field, $A = K[x_1, \dots, x_t]$, $f_i \in A$, $B = K[f_1, \dots, f_r]$, 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 $b \in K^r$, $|F^{-1}(b)| \le d$.* □

5.3 Integral extensions: proof of Theorem 5.2

To establish Theorem 5.2, 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_i $(1 \le i \le t)$ denote the polynomials on the left-hand side of the system (10). Let $B = K[f_1, f_2, \dots, f_t]$ be the K-subalgebra of A generated by the polynomials f_i.

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 of R is a degree-r extension of the field of quotients of S. For the basics of commutative algebra we refer to [AM], [Bou], [Ma]; especially [AM, Chap. 5].

Lemma 5.4 *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_i 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 Fact 5.3 yields $|F^{-1}(b)| \le t!$. □

It remains to prove Lemma 5.4.

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 denote the field of quotients of A. Theorem 10.4 of [Ma] 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 $\sum g_j h_j = 1$. 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. Let m denote the ideal $(f_1, \dots, f_t)$ of B. Let B_m denote the corresponding local ring and A_m the corresponding B_m-algebra.

It suffices to verify (cf. Bourbaki [Bou], Exercise 18, Chapter V, Section 2) that A_m/mA_m is a finite dimensional separable semisimple algebra over K and $\dim_K A_m/mA_m = t!$. Due to the isomorphism of K-algebras $A/mA \cong A_m/mA_m$, we can do this by proving the claims for A/mA.

As K is algebraically closed, semisimplicity and separability will be established if we show that mA 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 $mA = \prod_{\sigma \in S_t} I_\sigma$. Obviously we have $mA \subseteq I_\sigma$ for every $\sigma \in S_t$ hence $mA \subseteq \cap_{\sigma \in S_t} I_\sigma = \prod_{\sigma \in S_t} I_\sigma$.

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_i 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 $\sum h_j f_j g \in mA$. We show that $g_\sigma g \in mA$ which implies that $g \in mA$.

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 $m_\sigma = x_j - a_{j\sigma(j)}$, then $g^* g_\sigma$ is divisible in A by f_j, giving that $g^* g_\sigma \in mA$ and $g \in mA$.

By the Chinese remainder theorem

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

and therefore $\dim_K A/mA = t!$. This concludes the proof of Lemma 5.4 and Theorems 5.2 and 5.1. □

6 Open questions

Two open questions naturally arise in connection with Theorem 1.2. The first question asks to increase the gap established in Theorem 1.2; the second asks to reverse the direction of the gap.

Problem 6.1 Do there exist functions admitting polynomial size monotone span programs which require exponential size monotone circuits?

Problem 6.2 Do there exist functions admitting polynomial size monotone circuits which require superpolynomial size monotone span programs?

The fundamental question, of course, continues to be to find explicit functions which require superpolynomial size (non-monotone) span programs.

Acknowledgments

We thank Amos Beimel for his comments on the manuscript.

References

[AB] N. Alon and R. Boppana: The monotone circuit complexity of Boolean functions. *Combinatorica* 7 (1987), 1–22.

[AGHP] N. Alon, O. Goldreich, J. Håstad, R. Peralta: Simple constructions of almost k-wise independent random variables. *Random Structures and Algorithms* 3 (1992), 289–304.

[An] 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.

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

[AMN] Y. Azar, R. Motwani, J. Naor: Approximating probability distributions using small sample spaces. *Combinatorica,* to appear.

[BFS] L. Babai, P. Frankl, J. Simon: Complexity classes in communication complexity theory. In: *Proc. 27th IEEE FOCS,* 1986, pp. 337–347.

[BNS] L. Babai, N. Nisan, M. Szegedy: Multiparty protocols, pseudorandom generators for Logspace, and time-space tradeoffs. *J. Computer and Sys. Sci.* **45** (1992), 204–232.

[BGW] L. Babai, A. Gál, A. Wigderson: Superpolynomial lower bounds for monotone span programs, in preparation.

[BGP] A. Beimel, A. Gál and M. Paterson: Lower bounds for monotone span programs. In *Proc. 36th IEEE FOCS*, Milwaukee WI 1995, pp. 674–681.

[Ber] S. J. Berkowitz: On computing the determinant in small parallel time using a small number of processors. *Inform. Process. Lett.* 18 (1984), 147–150.

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

[Bou] N. Bourbaki: *Algèbre Commutative.* Hermann, Paris, 1961-1965.

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

[BDHM] G. Buntrock, C. Damm, H. Hertrampf, and C. Meinel: Structure and importance of the logspace-mod class. *Math. Systems Theory* 25 (1992), 223–237.

[Cs1] L. Csirmaz: The size of a share must be large. In A. De Santis, ed., *Advances in Cryptology – Eurocrypt'94, pre-proceedings*, 1994.

[Cs] L. Csirmaz: The dealer's random bits in perfect secret sharing schemes. Preprint, Mathematical Inst. Hungarian Acad. Sci., 1994.

[Er47] P. Erdős: Some remarks on the theory of graphs. *Bull. A. M. S.* bf 53 (1947), 292–294.

[Er38] 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).*

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

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

[Fü] Z. Füredi: New asymptotics for bipartite Turán numbers. *J. Comb. Theory-A*, to appear.

[GS] R. L. Graham, J. H. Spencer: A constructive solution to a tournament problem. *Canad. Math. Bull.* 14 (1971), 45–48.

[Ha] Armin Haken: Counting bottlenecks to show monotone P≠NP. In *Proc. 36th IEEE FOCS*, Milwaukee WI 1995, pp. 36–40.

[KS] B. Kalyanasundaram and G. Schnitger: The probabilistic communication complexity of set intersection. In *Proc. of Structure in Complexity Theory,* 1987, pp. 41-49.

[Ka] M. Karchmer: On proving lower bounds for circuit size. In *Proc. 8th Ann. Symp. Structure in Complexity Theory,* IEEE 1993, pp. 112–118.

[KW] M. Karchmer and A. Wigderson: On span programs. In *Proc. 8th Ann. Symp. Structure in Complexity Theory*, IEEE 1993, pp. 102–111.

[KW1] M. Karchmer and A. Wigderson: Monotone Circuits for Connectivity require Super-Logarithmic Depth. In *SIAM Journal on Discrete Mathematics*, Vol 3, No. 2, 1990, pp. 255-265.

[KRS] J. Kollár, L. Rónyai, T. Szabó: Norm-graphs and bipartite Turán numbers. *Combinatorica*, to appear.

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

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

[Ma] H. Matsumura: *Commutative Ring Theory*, Cambridge University Press, 1989.

[Me] K. Mehlhorn: Some remarks on Boolean sums. *Acta Inform.* 12 (1979), 371–375.

[Mu] K. Mulmuley: A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. *Combinatorica* 7 (1987), 101–104.

[Ne] E. I. Nečiporuk: On a Boolean matrix. *Problemy Kibernet.* 21 (1969), 237–240. English translation in *Systems Theory Res.*, 21 (1971) 236–239.

[Pi] N. Pippenger: On another Boolean matrix. *Theoretical Computer Science* 11 (1980), 49–56.

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

[RW] R. Raz and A. Wigderson: Monotone Circuits for Matching require Linear Depth. *Journal of the ACM*, Vol 39, 1992, pp. 736-744.

[Ra1] A. A. Razborov: Lower bounds for the monotone complexity of some Boolean functions. *Soviet Math. Doklady*, 31 (1985) 354–357.

[Ra2] A. A. Razborov: A lower bound on the monotone network complexity of the logical permanent. *Mat. Zametki* 37 (1985), 887-900.

[Ra3] A. A. Razborov: On the method of approximation. In *Proc. 21st ACM STOC*, 1989, pp. 167–176.

[Ra4] A. A. Razborov: On the distributional complexity of disjointness. *Theoretical Computer Science*, 106, 1992, No. 2, pp. 385-390.

[Sch] W. M. Schmidt: *Equations over Finite Fields: An Elementary Approach.* Lect. Notes in Math. vol. 536, Springer Verlag, 1976.

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

[St] D. R. Stinson: An explicitation of secret sharing schemes. *Design, Codes and Cryptography* 2 (1992), 357–390.

[Su] A. A. Suslin, Projective modules over a polynomial ring are free, *Soviet Math. Dokl.* 17 (1976), 1160-1164.

[We] I. Wegener: *The Complexity of Boolean Functions.* Wiley-Teubner 1987.

[Wi] A. Wigderson: The fusion method for lower bounds in circuit complexity. In: *Combinatorics, Paul Erdős is Eighty*, (Volume 1), D. Miklós, V. T. Sós, T. Szőnyi, eds., Bolyai Society Mathematical Studies 1, Budapest 1993, pp. 453–467.