A note on monotone complexity and the rank of matrices

Anna Gál [a,1], Pavel Pudlák [b,2]

[a] *Department of Computer Science*
University of Texas at Austin
Austin, TX 78712, USA
E-mail: panni@cs.utexas.edu.

[b] *Mathemtical Institute*
Academy of Sciences of the Czech Republic
Prague, Czech Republic
E-mail: pudlak@math.cas.cz.

Abstract

We shall give simpler proofs of some lower bounds on monotone computations. We describe a simple condition on combinatorial structures, such that the rank of the matrix associated with these structures gives lower bounds on monotone span program size and monotone formula size. We also prove an upper bound on the rank of the corresponding matrices, and show that such structures can be constructed from self-avoiding families. As a corollary, we obtain an upper bound on the size of self-avoiding families, which solves a problem posed in [4].

Key words: Computational complexity, lower bounds, span programs.

Introduction

The rank of a matrix has been used a number of times to prove lower bounds on various types of complexity. In particular it has been used for the size of monotone formulas and monotone span programs. In [13] Razborov introduced

[1] Research supported in part by NSF CAREER Award CCR-9874862 and an Alfred P. Sloan Research Fellowship.
[2] Research supported in part by grants No. A1019901 of the Academy of Sciences of the Czech Republic, No. 201/01/1195 of the Grant Agency of the Czech Republic, and by project No. LN00A056 of the Ministry of Education of the Czech Republic

a method of proving lower bounds on formula size that is directly using the rank of certain matrices. In particular, he proved that any matrix A that has large rank, but at the same time a certain set of its submatrices have small rank, can be used to obtain lower bounds on formula size. (The submatrices that must have small rank are specified by a certain cover of the matrix, which in turn specifies the actual function for which we want to obtain lower bounds. See [13] for more details.)

Note that Razborov's condition can be applied to both monotone and non-monotone complexity, and rank over any field can be used. Unfortunately, in the nonmonotone case, as Razborov has shown in [13], this method cannot give superlinear lower bounds. In the monotone case, Razborov used this method to give $n^{\Omega(\log n)}$ lower bounds on monotone formula size of explicitly defined functions. He has also shown that in the case of 0/1 matrices and monochromatic covers his rank condition gives matrices with a gap between the deterministic and nondeterministic communication complexities of the associated function, thus the results relating deterministic and nondeterministic communication complexity [1] imply that one cannot obtain larger bounds working with 0/1 matrices and monochromatic covers.

For the model of monotone span programs two methods have been used for proving superpolynomial lower bounds. The first method, introduced in [5], uses the size of *self avoiding families* (see also [3],[4]). Using this method, an $\Omega(n^{5/2})$ lower bound was proved in [5] for monotone span programs over arbitrary fields computing the 6-clique function, and in [3], [4] $n^{\Omega(\log n/\log\log n)}$ lower bounds were obtained for monotone span programs over arbitrary fields computing explicit functions.

The other method, introduced in [6], is an extension of Razborov's rank argument to span programs. The constructions of explicit Boolean functions with $n^{\Omega(\log n)}$ monotone complexity in both [13] and [6] are defined using the so called *isolated neighbor condition* (cf. [6]), which can nicely be used to obtain matrices satisfying Razborov's rank condition. It has also been shown in [6] that the isolated neighbor condition is sufficient for obtaining large self-avoiding families, and $n^{\Omega(\log n)}$ lower bounds were obtained in [6] using the method of self-avoiding families as well. It remained open if larger than $n^{O(\log n)}$ self-avoiding families exist.

In this note we define a certain combinatorial structure that enables us to use rank lower bounds directly. We shall show that using these structures lower bounds on the depth of monotone circuits and the size of monotone span programs can be obtained in a simpler way. We shall prove an upper bound on the rank of the matrices associated with these structures. Then we shall show that our structures can be constructed from self-avoiding families. As a consequence we get that there are no self-avoiding families larger than $n^{O(\log n)}$, answering a question from [4], and showing that the method of [5] cannot yield larger than $n^{\Omega(\log n)}$ lower bounds on monotone span program size.

A combinatorial structure

We shall study the following type of set systems on $[n] = \{1, \dots, n\}$. A is a family of subsets of $[n]$, B is a family of k-tuples of nonempty subsets of $[n]$ and they satisfy:

(*) *for every $a \in A$ and every $(b_1, \dots, b_k) \in B$, a has a nonempty intersection with exactly one b_i.*

We will be mainly interested in $k = 2$.

Monotone depth

The depth (monotone and general) has been characterized by the communication complexity of Karchmer-Wigderson (KW) game [9]. Computing the communication complexity of the KW game in general is a difficult problem, because what is computed in the game is not a function, but only a relation. On the other hand, computing the (two party) communication complexity of a function is usually not difficult, thus the task of proving lower bounds can be considerably simplified, if one could replace the relation in the KW game by a function.

Let us consider the case of monotone circuit depth. The KW game for a monotone function f is defined as follows. One player gets a minterm of f, the other gets a maxterm of f. Think of the min- and maxterms as subsets of $[n]$. The goal of the players is to find an $i \in [n]$ in the intersection of the given minterm and the given maxterm. In general we know that each minterm intersects each maxterm, but there may be more than one element in the intersection. To require that the intersection be of size one is too restrictive: it is known that this would give functions with read-once monotone formulae [8].

Thus, instead, assume that we can divide each maxterm into two parts (more generally into k parts) so that every minterm intersects exactly one of the two parts of each maxterm. Then, instead of asking the players to find an element in the intersection, we will require only to decide in which part they intersect. Obviously, this is an easier task, thus we have reduced the lower bound on the

KW game to a lower bound on the two party communication complexity of a function.

We can further relax the condition by considering only certain minterms and maxterms. In fact, it is better not to look for a function with such a property, but rather for a combinatorial structure defined above. Below we shall show that there are structures for which this approach works, i.e., for which one can prove sufficiently large lower bounds on communication complexity. We will use the rank lower bound of [12] on communication complexity: the log of the rank of a matrix is a lower bound on the communication complexity of the associated function.

Let A, B satisfy (*). Let $z_1, \ldots, z_k \in F$ be arbitrary elements of a field F. Define a matrix $R = R_{A,B,\bar{z}} = \{r_{a,\bar{b}}\}$, where the indices of rows, resp. columns range over the elements of A resp. of B, by

$$r_{a,\bar{b}} = z_i \quad \text{where } i \text{ is such that } a \cap b_i \neq \emptyset$$

Thus we have shown:

Theorem 1 *Suppose a monotone circuit accepts all $a \in A$ and rejects all sets $[n] \setminus b_1 \cup \ldots \cup b_k$, for $\bar{b} \in B$. Then it has depth at least* $\log \operatorname{rank} R$.

By [9], this also implies that $\operatorname{rank} R$ is a lower bound on the monotone formula size of the corresponding function. This will also follow from the lower bounds on monotone span programs below, since (monotone) formula size is at least as large as (monotone) span program size.

Monotone span programs

The model of span programs was introduced in [10]. Let a field F be fixed. A *monotone span program* for n variable monotone functions is a matrix M and a row vector v_0 such that

(1) $v_0 \neq \vec{0}$;
(2) each row is labeled by some $l \in [n]$.

Inputs for a boolean function are elements of $\{0,1\}^n$, instead we shall use subsets of $[n]$. We say that the monotone span program accepts a subset $a \subseteq [n]$, if there exists a vector $\vec{c}$ such that

$$\vec{c}^{\perp} M = \vec{v}_0,$$

and $\vec{c}$ is nonzero only on rows indexed by $l \in a$.

The size of the monotone span program is the number of rows of M. In what follows, when we consider span programs over a field F, all arithmetic operations and the rank are over F, unless stated otherwise.

Theorem 2 *Let A, B satisfy (*). Suppose a monotone span program over F accepts all $a \in A$ and rejects all sets $[n] \setminus b_1 \cup \ldots \cup b_k$, for $\bar{b} \in B$. Then it has size at least* $\operatorname{rank} R$.

PROOF. Let the monotone span program be given by a matrix M and a target vector $\vec{v}_0$. Let m be the number of rows of M, which is the size of the span program.

For every $a \in A$, let $\vec{c}_a$ be a vector that witnesses that a is accepted, which means that $\vec{c}_a^{\perp} M = \vec{v}_0$. Let $\bar{b} \in B$. Since $[n] \setminus b_1 \cup \ldots \cup b_k$ is not accepted, no linear combination of vectors of M gives $\vec{v}_0$. Hence there exists a vector $\vec{u}_{\bar{b}}$ such that $\vec{v}^{\perp}\vec{u}_{\bar{b}} = 0$ for every row vector $\vec{v}$ of M that is labeled by an element of $[n] \setminus b_1 \cup \ldots \cup b_k$ and $\vec{v}_0^{\perp}\vec{u}_{\bar{b}} = 1$. Vector $\vec{d}_{\bar{b}}$ will be defined by modifying the vector $M\vec{u}_{\bar{b}}$ as follows. For every $i = 1, \ldots, k$ multiply the elements of $M\vec{u}_{\bar{b}}$ that correspond to the rows labeled by elements of b_i by the field element z_i; note that all other elements are 0. We claim that

$$r_{a,\bar{b}} = \vec{c}_a^{\perp}\vec{d}_{\bar{b}}. \tag{1}$$

Indeed, let i be such that $a \cap b_i \neq \emptyset$. Then the only coordinates on which both $\vec{c}_a$ and $\vec{d}_{\bar{b}}$ are nonzero are those that are labeled by elements of b_i. Hence

$$\vec{c}_a^{\perp}\vec{d}_{\bar{b}} = z_i \vec{c}_a^{\perp} M \vec{u}_{\bar{b}} = z_i \vec{v}_0^{\perp}\vec{u}_{\bar{b}} = z_i.$$

This proves (1). Since R is a matrix of scalar products of vectors of dimension m, $\operatorname{rank} R \leq m$.

Remark Using $k > 2$ we can get only little gain over the case $k = 2$. For every $i = 1, \ldots, k$ let B_i be the set of pairs $(b_i, \bigcup_{j \neq i} b_j)$ for $(b_1, \ldots, b_k) \in B$. Assign z_i to the first set and 0 to the second and let R_i be the matrix for A, B_i, z_i. Then $R = R_1 + \ldots + R_k$, hence $\operatorname{rank} R \leq k \max_i \operatorname{rank} R_i$. We can assume that only disjoint sets are allowed in each k-tuple of sets, because otherwise, if some j appears in several sets in some k-tuple, then no $a \in A$ can contain j, and we can leave j out from all the sets of the structure, without changing the intersection properties. Thus $k \leq n$. Therefore, the gain from using $k > 2$ is at most a factor of n.

Constructions

We shall show some constructions which demonstrate that our concept is quite natural.

Products Given two set systems A, B on $[n]$ and A', B' on $[m]$, satisfying the condition (*), one can take the product of them $A \times A', B \times B'$ on $[n] \times [m]$ defined by

$$A \times A' = \{a \times a';\ a \in A,\ a' \in A'\},$$
$$B \times B' = \{(b_i \times b'_j)_{i \in [k], j \in [k']};\ (b_1, \ldots, b_k) \in B,\ (b'_1, \ldots, b'_{k'}) \in B'\}.$$

Furthermore, if z_i and z'_j are the field elements assigned to b_i and b'_j, then we assign $z_i z'_j$ to $b_i \times b'_j$. One can easily check that the product satisfies condition (*) and the associated matrix is the tensor product of the matrices, hence its rank is the product of the ranks of these matrices. Thus one can get infinitely many examples starting from one. However, one cannot get superpolynomial bounds in this way.

When some field elements assigned to b_i's are the same, we can unite those sets without changing the corresponding matrix. Hence the product does not have to increase the parameter k. For instance, if we use only ± 1, then we can keep $k = 2$.

Geometric constructions Let V be a set of size $\geq 2k - 1$. Let $W = \binom{V}{k}$ (the set of k-element subsets of V). Define

$$A = \{\binom{X}{k};\ X \in \binom{V}{2k-1}\},$$

$$B = \{(\binom{Y}{k}, \binom{Z}{k});\ Y, Z \text{ a partition of } V\}.$$

Condition (*) is satisfied because exactly one of the following two statements is true $X \cap Y \geq k$, $X \cap Z \geq k$. The associated matrix (take $z_1 = 0, z_2 = 1$) has almost full rank, but we cannot get large bounds, since $|A| < |W|^2$.

This construction can be interpreted geometrically: think of the elements of A being k-dimensional faces of a simplex and elements of B being certain pairs of disjoint faces. A similar construction works with the octahedron and the dodecahedron.

The bipartite graph construction We shall show that our method generalizes the method of self-avoiding families used in [5], [3], [4], [6]. Hence all lower bounds that they get can be obtained also by our method. Still, it may be interesting to prove their best lower bound directly using our criterion. We will consider Boolean functions defined by bipartite graphs as in [3], [4], [6]. We will use the isolated neighbor condition similarly to [13], [6].

Let G be a bipartite graph on $U \times V$, $|U| = |V| = n/2$. We shall say it satisfies the *isolated neighbor condition for* k, if for every X, Y disjoint subsets of U of size at most k there exists a vertex $v \in V$ such that every vertex $u \in X$ is connected with v and no vertex $u \in Y$ is connected with v. For a bipartite graph satisfying this condition we define A to be the set of sets $a \subseteq U \cup V$ such that $|a \cap U| = k$ and $a \cap V$ is the set of all vertices that are joined to every vertex of $a \cap U$, i.e., maximal complete bipartite graph with the part in U of size k, and B to be the set of pairs (b_1, b_2) such that $b_1 \subseteq U$, $|b_1| \leq k$ and b_2 consists of all vertices of V that are not joined to any vertex of b_1. Since a induces a complete bipartite graph and b_1, b_2 an empty graph, a cannot intersect both b_1 and b_2. If $a \cap b_1 = \emptyset$, then the condition above guarantees that $a \cap b_2 \neq \emptyset$. Thus A, B satisfy (*). Take $z_1 = 0, z_2 = 1$. Since $b_1 \subseteq U$, the matrix $R_{A,B,\bar{z}}$ is the well-known disjointness matrix $D(n/2, k)$, the matrix in which rows are indexed by k–element subsets of $[n/2]$ and columns are indexed by at most k element subsets and the corresponding entry is 1 if the sets are disjoint and 0 otherwise. This matrix has full rank, see, eg., [7] or a more general Lemma 4 below. Thus we get a lower bound $\binom{n/2}{k}$.

There are several constructions that achieve $k = \Omega(\log n)$, see [2], the most popular is the Paley graph. Hence we obtain a lower bound of the form $n^{\Omega(\log n)}$.

An upper bound on the rank of the associated matrices

We shall show that the last mentioned construction gives asymptotically the largest rank that is possible for the matrices associated with structures satisfying (*). Thus using our approach we cannot obtain a larger lower bound than $n^{\Omega(\log n)}$.

Proposition 3 *Let A be a family of subsets of $[n]$, B a family of k-tuples of subsets of $[n]$ satisfying (*), and let $z_1, \ldots, z_k \in F$, $k \leq n$, F an arbitrary field. Then the rank of the matrix $R_{A,B,\bar{z}}$ is at most $n^{\Omega(\log n)}$.*

PROOF. By the remark above we can assume w.l.o.g. that $k = 2$. We shall show a little more, namely an upper bound on the cover number of the matrix $R_{A,B,\bar{z}}$. Consider the following $2n$ rectangles $R1_i$ and $R2_i$ for $i = 1, \ldots, n$. $R1_i$ is the rectangle with rows indexed by sets $a \in A$ such that i is contained in the set a, and columns indexed by pairs (b_1, b_2), such that i is contained in the set b_1. $R2_i$ is the rectangle with rows indexed by sets $a \in A$ such that i is contained in the set a, and columns indexed by pairs (b_1, b_2), such that i

is contained in the set b_2. Then all these rectangles are monochromatic: each entry of $R1_i$ is z_1, and each entry of $R2_i$ is z_2. The condition (*) implies that each $a \in A$ intersects at least one of the sets b_1 or b_2 for each column (in some point i). Thus, the $2n$ rectangles defined above form a monochromatic cover of R.

For a 0/1 matrix M, $C^0(M)$ ($C^1(M)$) denotes the smallest number of monochromatic rectangles needed to cover all the 0 entries (1 entries) of the matrix M. The nondeterministic communication complexity of the Boolean function corresponding to M is defined as $N^1(M) = \log_2 C^1(M)$. Similarly, the co-nondeterministic communication complexity is defined as $N^0(M) = \log_2 C^0(M)$. (See e.g. [11] for more on communication complexity.) It was proved in [1] that the deterministic communication complexity of the Boolean function associated with a 0/1 matrix M is at most $O(N^0(M)N^1(M))$. On the other hand, the log of the rank of a matrix is a lower bound on the deterministic communication complexity of the associated function [12]. Thus, we get that

$$\log_2 \operatorname{rank} R_{A,B,\bar{z}} \leq O(N^0(M)N^1(M)) \leq O((\log_2 n)^2) .$$

Hence the rank of $R_{A,B,\bar{z}}$ is at most $n^{O(\log n)}$.

A relation to self-avoiding families

A family A of subsets of V is called *self-avoiding* (cf. [5],[3],[4]) if, with each $a \in A$, one can associate a subset $T(a) \subseteq a$ such that for every $a, a' \in A$,

(1) if $T(a) \subseteq a'$ then $a = a'$,
(2) for every $y \subseteq T(a)$,

$$a' \not\subseteq \bigcup_{a'' \in A, a'' \cap y \neq \emptyset} a'' \setminus y.$$

Let us define

$$S(y) = \bigcup_{a'' \in A, a'' \cap y \neq \emptyset} a''.$$

Thus the second condition says that no a' is contained in $S(y) \setminus y$. In [5] they proved that every monotone span program that computes a monotone boolean function the minterms of which form a self-avoiding family has size at least the size of the family. Their proof actually gives such a lower bound for every monotone span program that accepts all sets $a \in A$ and rejects all sets of the form $V \setminus S(y)$ for $y \subseteq T(a)$, $a \in A$. We shall show that this can also be derived using our criterion, thus proving that our method is at least as general as the method of self-avoiding families.

We take A as it stands and define B as the set of pairs (b_1, b_2) such that for some $a \in A$, $b_1 \subseteq T(a)$ and $b_2 = V \setminus S(b_1)$. Let such a pair (b_1, b_2) be given and let $a' \in A$ be arbitrary. If $a' \cap b_1 \neq \emptyset$, then $a' \subseteq S(b_1)$, hence $a' \cap b_2 = \emptyset$. Thus a' intersects at most one of the sets. If $a' \cap b_1 = \emptyset$, then $a' \cap b_2 \neq \emptyset$, because otherwise $a' \subseteq S(b_1) \setminus b_1$ contradicting the definition of A. Thus also a' intersects at least one of the sets, hence we have condition (*). Take $z_1 = 0, z_2 = 1$, then the matrix $R_{A,B,\bar{z}}$ has full row rank by the following lemma (implicit in [5]).

Lemma 4 *Let A be a family of subsets that are incomparable by inclusion. For each $a \in A$, let $T(a) \subseteq a$ be such that for every $a, a' \in A$, if $T(a) \subseteq a'$ then $a = a'$. Let M be the matrix such that rows are indexed by the elements of A and columns are indexed by sets b such that $b \subseteq T(a)$ for some $a \in A$ and the entry corresponding to a and b is 1 if they have empty intersection and 0 otherwise. Then M has full row rank (over any field).*

PROOF. Recall that $D(n)$, the full disjointness matrix in which we take all subsets of $[n]$, has full rank (it can be proven easily by induction on n). Now consider M. Suppose that a row with index a can be expressed as a linear combination of others. Take the submatrix N of M consisting of columns indexed by $b \subseteq T(a)$. Clearly, the rows of N are rows of $D(|T(a)|)$, some of them repeated. Note that the row with index a is 1 in the column indexed by the empty set, and 0 in every other column in N, since $T(a) \subseteq a$. But the row indexed by a occurs in N only once, because of the way the sets $T(a)$ are defined, so it cannot be a linear combination of others.

Hence the size of every monotone span program that accepts all sets $a \in A$ and rejects all sets of the form $V \setminus S(y)$ for $y \subseteq T(a)$, $a \in A$ is at least rank $R_{A,B,\bar{z}} = |A|$.

Note that we have constructed a structure satisfying (*) from an arbitrary self-avoiding family so that the associated matrix has the rank equal to the size of the family. Hence we get the following corollary.

Corollary 5 *Every self-avoiding family of subsets of an n element set has size at most $n^{O(\log n)}$.*

References

[1] A. Aho, J. Ullman and M. Yannakakis: On notions of information transfer in VLSI circuits. In *Proc. of 15th ACM STOC*, 1983, pp. 133-139.

[2] 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.

[3] L. Babai, A. Gál, J. Kollár, L. Rónyai, T. Szabó, A. Wigderson, *Extremal bipartite graphs and superpolynomial lower bounds for monotone span programs*, STOC 1996, 603-611.

[4] L. Babai, A. Gál, A. Wigderson: Superpolynomial lower bounds for monotone span programs. *Combinatorica* 19 (3) (1999), pp. 301-319.

[5] A. Beimel, A. Gál, M. Paterson, *Lower bounds for monotone span programs.* Computational Complexity 6 (1996/97), 29-45.

[6] A. Gál, *A characterization of span program size and improved lower bounds for monotone span programs.* to appear in Computational Complexity, preliminary version in STOC 1998, 429-437.

[7] S. Jukna, *Extremal Combinatorics, With Applications in Computer Science.* Springer, (2000).

[8] M. Karchmer, N. Linial, I. Newman, M. Saks, A. Wigderson, *Combinatorial characterization of read-once formulae.* Discrete Mathematics, 114 (1993), 275-285.

[9] M. Karchmer and A. Wigderson, *Monotone circuits for connectivity require super-logarithmic depth.* SIAM J. on Discrete Math., 3/2, 1990, 255-265.

[10] M. Karchmer and A. Wigderson, *On span programs* Proc. 8th Ann. IEEE Symp. Structure in Complexity Theory, 1993, 102-111.

[11] E. Kushilevitz and N. Nisan, *Communication Complexity*, Cambridge University Press, 1997.

[12] K. Melhorn and E. Schmidt, *Las Vegas is better than determinism in VLSI and distributed computing.* Proc. 14-th STOC (1982), 330-337.

[13] A. A. Razborov, *Applications of matrix methods to the theory of lower bounds in computational complexity.* Combinatorica 10 (1990), 81-93.