Electronic Colloquium on Computational Complexity, Report No. 7 (2002)

Monotone complexity and the rank of matrices

(preliminary version)

Pavel Pudlák

December 28, 2001

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 most cases that this approach was used, there is not a single matrix associated with the function in question, but one has to minimize the rank over a set of matrices (eg., [8, 4]). Usually, this makes the techniques very difficult to apply. In this note we define a certain combinatorial structure that enables us to use the rank lower bound directly. We shall not prove new lower bound, we only show that some previous lower bounds on monotone span programs can be simply derived using this structure. It is open whether our approach can produce better lower bounds.

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 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 concerned with $k = 2$.

Monotone depth

The depth (monotone and general) has been characterized by the communication complexity of Karchmer-Wigderson (KW) game [6]. Computing the communication complexity of the KW game in general is a hard 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.

ISSN 1433-8092

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. We do not know whether under this restriction one can prove nontrivial lower bounds, but it is surely not good for our approach based on the rank. 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. Thus we have reduced the lower bound on the KW game to a lower bound on the 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, ie., for which one can prove sufficiently large lower bounds on communication complexity. For now we only mention that one can use the rank lower bound [7] on the communication complexity.

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* $\log \operatorname{rank} R$.

One can check that, in fact, $\operatorname{rank} R$ is a lower bound on the monotone formula size. However this will also follow from the lower bounds on monotone span programs below using well-known simulations.

Monotone span programs

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 $\{0,1\}^n$, 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 row indexed by $l \in a$.

The size of the monotone span program is the number of rows of M.

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, $\operatorname{rank} M \leq m$.

Remarks. 1. 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 $\operatorname{rank} R \leq k \max_i \operatorname{rank} R_i$.

2. Let t be an upper bound on the size of intersections $a \cap b_i$. Then $\operatorname{rank} M \leq kn^{t+1}$. By the remark above, we only need to bound $\operatorname{rank} R_i$ by n^{t+1}. Let S be the matrix $\{\chi_a^{\perp}\chi_{b_i}\}_{a,\bar{b}}$, where $a \in A, \bar{b} \in B$ and χ_X denotes the 0-1 characteristic vector of a subset $X \subseteq [n]$. Since S is a matrix of scalar products of vectors of length n, its rank is at most n. Let $f(x)$ be the polynomial of degree $t+1$ such that $f(0) = 0$ and $f(u) = z_i$ for $u = 1, \ldots, t$. Then the matrix $R_i = \{f(\chi_a^{\perp}\chi_{b_i})\}_{a,\bar{b}}$, hence

$$\operatorname{rank} R_i \leq (\operatorname{rank} S)^{t+1} \leq n^{t+1}.$$

Constructions

Products. Given two families A, B on $[n]$ and A', B' on $[m]$, 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. Similar construction works with the octahedron and the dodecahedron.

The bipartite graph construction We shall show that our method generalizes the method used in [2, 4]. 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.

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 $a \cap U$, ie., 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 $z_1 = 0, z_2 = 1$. Then the matrix $R_{A,B,\bar{z}}$ has full rank. This is because $R_{A,B,\bar{z}}$ is the well-known disjointness matrix $D(n/2, k)$[1]eg. [5] or a more general Lemma 1 below. Thus we get a lower bound $\binom{n/2}{k}$. There are several constructions that achieve $k = \Omega(\log n)$, see [1], the most popular being the Paley graph, hence we obtain a lower bound of the form $n^{\Omega(\log n)}$.

Relation to self-avoiding families

A family A of subsets of V is called *self-avoiding* (cf. [2]) if, no two elements of A are comparable by inclusion and 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 [3] 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 ours is at least as general as theirs.

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 $a' \subseteq S(b_1)$. 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 rank by the following lemma (implicit in [3]).

Lemma 1 *Let A be a family of subsets that are incomparable by inclusion. Let M be the matrix such that rows are indexed by the elements of A and columns are indexed by sets b such that $b \subseteq a$ for some $a \subseteq A$ and the entry corresponding*

[1] Recall that this is the matrix in which rows are indexed by k–element subsets of $[n]$ and columns are indexed by at most k element subsets and the corresponding entry is 1 if the sets are disjoint and 0 otherwise.

to a and b is 1 if they have empty intersection and 0 otherwise. Then M has full 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 $b \subseteq a$. Clearly, the rows of N are rows of $D(|a|)$, some of them repeated. But the row indexed by a occurs in N only once, so it cannot be a linear combination of others.

Hence the size of every monotone span program for 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 $\operatorname{rank} R_{A,B,\bar{z}} = |A|$.

Open problem

Does there exist sets A, B satisfying (*) such that the rank of the associated matrix is larger than $n^{O(\log n)}$?

References

[1] 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.

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

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

[4] A. Gál, *A characterization of span program size and improved lower bounds for monotone span programs.* STOC 1998, 429-437.

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

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

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

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