COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA 12 (2) (1992) 221–226

A COMBINATORIAL APPROACH TO COMPLEXITY

P. PUDLÁK and V. RÖDL

Received July 20, 1989

We present a problem of construction of certain intersection graphs. If these graphs were explicitly constructed, we would have an explicit construction of Boolean functions of large complexity.

In Boolean complexity one can investigate graphs instead of Boolean functions. Suppose we have a Boolean function with an even number of variables $f : \{0,1\}^{2n} \to \{0,1\}$. Then we can identify in a natural way f with a bipartite graph $G = (P, Q, E)$. $E \subseteq P \times Q$, with $|P| = |Q| = 2^n$. This transition is the essence of the communication complexity, however the complexity of graphs has been investigated also from the point of view of Boolean complexity [4], [5]. Here we shall show that if f has small complexity, more precisely, if f can be computed by small branching programs, then G can be represented as an intersection graph where vertices are subspaces of a low dimensional vector space. Thus the minimal dimension in which G can be represented in this way gives an interesting characteristic of the graph. We shall prove some basic facts about it, however we are not able to construct explicitly graphs which require large dimension.

Definition 1. Let G be as above. If we can assign a subspace $v(r)$ of some vector space V to each vertex $r \in P \cup Q$ so that for every pair of vertices $p \in P$, $q \in Q$

$$(p,q) \in E \text{ iff } v(p) \cap v(q)$$

is a nontrivial subspace, then we say that G *has a projective representation in* V.
2. For a given field k we denote by

$$\mathrm{pdim}_k G$$

the minimal dimension of a vector space in which G has a projective representation; it will be called *the projective dimension of* G.
3. Similarly we define an *affine representation* in V by taking affine subspaces instead of vector subspaces and requiring

$$(p,q) \in E \text{ iff } v(p) \cap v(q) \neq \emptyset;$$

AMS Subject Classification code (1991): 68 R 10

the corresponding characteristic, *affine dimension*, will be denoted by

$$\operatorname{adim}_k G.$$

Theorem 1. *Suppose $f : \{0,1\}^{2n} \to \{0,1\}$ can be computed by a branching program of size d, let G be the graph associated with f, let k be an arbitrary field. Then G has a projective representation over k^{d+2}, i.e.*

$$\operatorname{pdim}_k G \leq d + 2.$$

Proof. The proof uses the idea of representation of graphic matroids as regular matroids.

Let B be a branching program computing f. B has one source vertex, say v_0, one accepting vertex v_+ and one rejecting vertex v_-. An input string a determines the subgraph H_a of B, (two disjoint trees with roots v_+ and v_-) consisting of all edges that are open for this input. B accepts the input iff there is an unoriented path from v_0 to v_+ in this subgraph. We identify $\{0,1\}^{2n}$ with $P \times Q$. Now let $a = (p,q) \in P \times Q$. Then p determines a subgraph H_p and q determines a subgraph H_q so that $H_a = H_p \cup H_q$. Hence we have

$$f(p,q) = 1 \text{ iff there is a path from } v_0 \text{ to } v_+ \text{ in } H_p \cup H_q.$$

By a simple modification of the branching program we can ensure that, for no p and q, there is a path connecting v_0 to v_+ in either H_p or H_q. Namely we can add a new source with both edges directed to the old source and with a label from the other half of inputs than is the label of the old source. Also we can remove vertex v_-. Now we identify (glue) v_0 with v_+. Then

$$f(p,q) = 1 \text{ iff there is a cycle in } H_p \cup H_q.$$

By the property above we also know that such a cycle must contain edges from both subgraphs. Next step is to replace edges by vectors. Take a vector space over k whose dimension is the number of vertices of B and choose a basis of it. Assign an element e_v of the basis to each vertex v of B. Then the vector subspace assigned to an $r \in P \cup Q$ is defined by

$$v(r) = \{e_u - e_w | (u,w) \in H_r\}.$$

Hence to each edge (u,w) we assign vector $e_u - e_w$. (If the characteristic of k is different from 2 we must consider directed edges.) Under this assignment the cycles in graphs are translated onto cycles in vector spaces. Thus if there is a cycle in $H_p \cup H_q$, then we have a set of vectors from $v(p) \cup v(q)$ summing to 0 which cannot be reduced and, by the property of B, must contain vectors from both subspaces. In the other direction, any nonzero vector in $v(p) \cap v(q)$ can be used to construct a cycle in $v(p) \cup v(q)$ consisting of vectors which correspond to the edges of B, hence also a cycle in $H_p \cup H_q$.

The size d of the branching program is the number of vertices which are not sinks. Thus the dimension of the vector space is $d + 2$. ∎

In the sequel we denote by

$$N = |P| = |Q|,$$

which is 2^n, if the graph G corresponds to a $2n$ argument Boolean function. An easy counting gives the following

Proposition 1. *For k a fixed finite field*

$$\max_{G \subseteq N \times N} \operatorname{pdim}_k G = \Omega(N^{\frac{1}{2}}). \qquad \blacksquare$$

Thus, theoretically, one can obtain an $\Omega(2^{n/2})$ lower bound for the branching program complexity of some Boolean function. We give a less trivial result now.

Theorem 2. *For the real field $\mathbb{R}$*

$$\max_{G \subseteq N \times N} \operatorname{pdim}_{\mathbb{R}} G = \Omega\left(\left(\frac{N}{\log N}\right)^{\frac{1}{2}}\right).$$

Proof. Let a projective representation v of $G = (P, Q, E)$ in k^d be given, let $N = |P| = |Q|$. We must first construct a representation which is in a sense uniform.

Lemma 1. *There exists a projective representation v' of G in $\mathbb{R}^{2d}$ such that for every $r \in P \cup Q$ the dimension of $v'(r)$ is exactly d.*

Proof. First extend $\mathbb{R}^d$ to $\mathbb{R}^{3d}$. Then we can use d dimensions to extend each $v(p)$, $p \in P$, so that its dimension is exactly d and similarly the other dimensions for vertices $q \in Q$. Finally we reduce the dimension of the whole space to $2d$ while preserving the dimensions of the intersections by taking a projection of the representation onto a subspace of dimension $2d$ in general position. $\blacksquare$

For each $r \in P \cup Q$ take a $2d \times d$ matrix $M(r)$ of some basis vectors of $v(c)$. Then we have

$$(p, q) \in E \quad \text{iff} \quad v'(p) \cap v'(q) \neq \{0\} \quad \text{iff} \quad \det(M(p), M(q)) = 0.$$

Since the number of pairs (p, q) is finite, we can choose an $\varepsilon > 0$ such that

$$(p, q) \in E \quad \text{iff} \quad (\det(M(p), M(q)))^2 - \varepsilon < 0,$$
$$(p, q) \notin E \quad \text{iff} \quad (\det(M(p), M(q)))^2 - \varepsilon > 0.$$

Now think of $(\det(M(p), M(q)))^2 - \varepsilon$ as a polynomial evaluated on some real numbers. Then we see that E is determined by the signs of N^2 polynomials of degree $4d^2$ with $2d^2 \cdot 2N$ variables. Thus each graph of projective dimension at most d is determined in such a way. The number of possible sign sequences can be bounded by the degree of polynomials the number of polynomials and the number of variables. We shall use a bound proved by Warren [8]:

Lemma 2. *Let $p_1, \ldots, p_m$ be polynomials of degree at most s and with t variables, $s \geq 1$, $m \geq t$. Then the number of sequences*

$$(\operatorname{sgn} p_1(x), \ldots, \operatorname{sgn} p_m(x)),$$

where x ranges over all sequences of reals for which no polynomial is equal to 0, is bounded by

$$\left(\frac{4esm}{t}\right)^t. \qquad \blacksquare$$

It follows that the number of graphs of dimension d is bounded by

$$\left(\frac{16ed^2N^2}{4d^2N}\right)^{4d^2N} = (4eN)^{4d^2N}.$$

If each graph can be represented in dimension d then this number must be greater or equal to N^2, which gives us

$$d \geq \left(\frac{N}{4 \cdot \log_2 4eN}\right)^{\frac{1}{2}}. \qquad \blacksquare$$

Motived by our results Razborov [5] proved the following relation between affine dimension and formula size.

Theorem 3. *For any field k*

$$\operatorname{adim}_k G \leq L(f),$$

where G is the graph corresponding to a Boolean function f and L is the formula size in basis $\{\neg, \&, \vee\}$. $\blacksquare$

In fact he proved more. In terms of graph complexity (see [4]) it means that

$$\operatorname{adim}_k G \leq L_{\mathcal{B}}(G).$$

Roughly speaking this means that it is necessary to use at least $\operatorname{adim}_k G$ unions and intersections in order to construct G from complete bipartite graphs. We shall show some relations between the projective dimension and affine dimension.

Proposition 2.
(1) *For every field k*

$$\operatorname{adim}_k G \leq (\operatorname{pdim}_k G)^2.$$

(2) $\operatorname{adim}_{\mathbb{R}} G + 1 \leq \operatorname{pdim}_{\mathbb{R}} G$.

Proof.

(1) Let v be a projective representation of G in k^d. We construct an affine representation v' of G in k^{d^2} as follows:

$$v'(r) = \{A | A \quad \text{is a} \quad d \times d\text{-matrix whose row space is a subspace of } v(r) \text{ and with } Sp(A) = 1\}.$$

We shall show that v' represents the same graph as v. Suppose w is a nonzero vector in $v(r_1) \cap v(r_2)$. Let B be a $d \times d$-matrix with one row equal to w and all other equal to 0. Since w is nonzero, we can choose the nonzero row so that $Sp(B)$ is nonzero. Then clearly $(Sp(B)^{-1}) \cdot B$ is in $v'(r_1) \cap v'(r_2)$. If $A \in v'(r_1) \cap v'(r_2)$ and $Sp(A) = 1$ then there is at least one nonzero row in A and it must belong to $v(r_1) \cap v(r_2)$.

(2) In the real field $\mathbb{R}$ an affine representation is obtained from a projective one simply by intersecting it by a hyperplane in a general position. $\blacksquare$

The following result of Lovász implies that there is no such simulation of affine representations by projective ones for the field of reals. For finite fields Razborov [5] has shown that

$$\operatorname{pdim}_k(G) \leq \operatorname{adim}_k(G)^{0(\operatorname{adim}_k(G))}.$$

Theorem 4. *There exists $\varepsilon > 0$ such that if G is the complement of an N to N matching, then*

$$\mathrm{pdim}_k G > \varepsilon \cdot \log N,$$

for every field k of characteristic different from 2. ∎

Corollary. *There exist graphs G_N such that*

$$\mathrm{adim}_{\mathbb{R}} G = 2 \quad \textit{and} \quad \mathrm{pdim}_{\mathbb{R}} G = \Omega(\log N).$$

Proof. Take the complements of matchings. Then the second half is just Theorem 4 and the first half is trivial. ∎

We shall give a proof of Theorem 4 for the case $k = \mathbb{R}$, since it shows an interesting relation with some concepts studied elsewhere.

Definition. A *scalar product representation* of a graph G in $\mathbb{R}^d$ is a mapping $w : P \cup Q \to \mathbb{R}^d$ such that

$$(p, q) \in E \quad \text{iff} \quad w(p) * w(q) = 0,$$

where $*$ denotes the scalar product of vectors.

Scalar product representations has been used by Lovász [1]; Paturi and Simon [3] used a similar concept in communication complexity; Reiterman, Rödl and Šiňajová [6], [7] and Parsons and Pisanski [2] studied another similar concept.

Proposition 3. *Every bipartite graph G has a scalar representation in $\mathbb{R}^d$, where*

$$d = \binom{2 \dim_{\mathbb{R}} G}{\dim_{\mathbb{R}} G}.$$

Proof. For each $r \in P \cup Q$ take $2d' \times d'$-matrix $M(r)$, where $d' = \dim_{\mathbb{R}} G$, as in the proof of Theorem 2. Thus

$$(p, q) \in E \quad \text{iff} \quad \det(M(p), M(q)) = 0.$$

Clearly we can write $\det(M(p), M(q))$ in the form

$$\sum_{i \in I, j \in J} a_i b_j,$$

where a_i are $\mp$ determinants of $d' \times d'$ submatrices of $M(p)$, b_j are determinants of $d' \times d'$ submatrices of $M(q)$, and $|I| = |J| = \binom{2d'}{d'}$. ∎

Proposition 4. *The complement of an N to N matching does not have a scalar product representation in $\mathbb{R}^d$ for $d < N$.*

Proof. Let $u_1, \ldots, u_N, w_1, \ldots, w_N \in \mathbb{R}^d$ be such that $u_i * w_j = 0$ for $i \neq j$. Suppose that $d < N$. Then some u_i is a linear combination of $u_1, \ldots, u_{i-1}$. Hence also $u_i * w_i = 0$. Thus this cannot be a representation of the complement of a matching. ∎

Proof of Theorem 4. By propositions 2 and 3 we get

$$\binom{2d}{d} \geq N,$$

whenever d is the projective dimension over $\mathbb{R}$ of the complement of an N to N matching. This gives the bound of Theorem 4. ∎

Conclusions. The most important open problem is to find explicit examples of graphs with large projective and affine dimensions. The largest lower bounds that we know of are only $\Omega(\log N)$. In order to improve the best lower bound to the branching program complexity of an explicitly defined Boolean function (due to Nečiporuk), we need a lower bound for projective dimension larger than $(\log N)^2/\log\log N$.

References

[1] L. LOVÁSZ: On the Shannon capacity of graphs, *IEEE Transactions of Information theory*, **IT–25** (1979), 1–7.

[2] T. D. PARSONS, and T. PISANSKI: Vector representations of graphs, to appear in *Discrete Math.* **78** (1989), 143–154.

[3] R. PATURI, and J. SIMON: Probabilistic communication complexity, *25-th FOCS* (**1984**), 118–126.

[4] P. PUDLÁK, V. RÖDL, and P. SAVICKÝ: Graph complexity, *Acta Informatica* **25** (1988), 515–535.

[5] A. A. RAZBOROV: Applications of matrix methods for the theory of lower bounds in computational complexity, *Combinatorica* **10** (1990), 81–93.

[6] J. REITERMAN, V. RÖDL, and E. ŠIŇAJOVÁ: Geometrical embeddings of graphs, *Discrete Math.* **74** (1989), 291–319.

[7] J. REITERMAN, V. RÖDL, and E. ŠIŇAJOVÁ: Embeddings of graphs in euclidean spaces, *Discrete Comput Geom.* **4** (1989), 349–364.

[8] H. E. WARREN: Lower bounds for approximations by nonlinear manifolds, *Transactions AMS* **133** (1968), 167–178.

P. Pudlák

Mathematical Institute, ČSAV
11 567 Praha 1, Žitná ul. 25
Czech and Slovak Federal Republic

V. Rödl

Department of Mathematics
Emory University, Atlanta
GA 30322, USA