Annals of Discrete Mathematics 16 (1982) 213–223
© North-Holland Publishing Company

BOUNDING THE INDEPENDENCE NUMBER OF A GRAPH

L. LOVÁSZ

Bolyai Institute, József Attila University, Szeged H-6720, Hungary

0. Introduction

The problem of computing the independence number of a graph is NP-complete; the matching number, on the other hand is computable in polynomial time. This difference in their computational complexity implies that, to attack these two problems, different strategies have to be applied. The matching problem may serve as a prototype of handling 'easy', i.e., polynomially solvable problems: find a good characterization, then a polynomial algorithm, describe the facets of associated polyhedra etc. None of these lines of attack holds out promises of success in the case of the independence number problem. So what scheme should one follow in the study of an NP-complete problem like independence number? Discouraged by the fact of NP-completeness, one might answer (or at least feel) that this problem is mathematically intractable and so one should not waste time on it. Others, who play down the relevance of polynomiality in algorithms, might say that all there is to do is to improve the (more or less trivial) exponential algorithms by heuristics, programming, data handling tricks, etc. These two extremes meet in the opinion that no further attempts to 'grip the essence' of the problem are needed.

In this paper we discuss an idea which *might* suggest some non-trivial approaches to NP-complete problems. Whether the sporadic phenomena collected here will ever fall into a pattern, and whether from this a unified approach to NP-complete problems can be learned, is beyond the guessing of this author.

Let $\alpha(G)$ denote the independence number of the graph G. If $\alpha(G)$ cannot be calculated efficiently, a next step is to ask for sharp bounds on it. There is a very significant difference between upper and lower bounds: A lower bound means to prove the *existence* of an independent set of some size, which is usually proved by more-or-less constructive methods (heuristics, random choice, etc.). On the other hand, an upper bound means the *non-existence* of an independent set of larger size—in this respect it is 'destructive'. Is there any practical value then in finding upper bounds? Potential applications of upper bounds are the following:

- In a branch-and-bound procedure, sharp upper bounds may cut down the size of the search tree considerably. (Question: is there any example in the case of an 'easy' problem where a polynomial-bounded algorithm is obtained by pruning a search tree with the help of an upper bound? Such an example might shed some light on the hitherto somewhat mysterious phenomenon that well-characterized problems tend to be polynomially solvable.)
- Given a reasonable upper bound, we may consider the class of those graphs for which this upper bound is attained, and then restrict the independence number problem to this class. There is a good chance that it is easier to solve that problem for this particular class of graphs, and such graphs may well be very interesting.
- Deriving sharper and sharper upper bounds, more and more insight could be gained into the nature of independence number (a procedure vaguely reminescent of the expansion of a function into, say, a Fourier series).

We shall survey some methods to obtain upper bounds on the independence number $\alpha(G)$ of a graph. We have left the precise notion of 'upper bound' open. The most natural choice, of course, is to look for a positive integer valued function φ defined on graphs, such that $\alpha(G) \leq \varphi(G)$ for every graph G and φ is polynomially computable. Sometimes we shall have to settle for less, e.g., the function φ should be such that $\varphi(G) \leq k$ is an NP-property of the pair (G, k). Putting things even more general, we shall be interested in methods which enable us to exhibit the relation $\varphi(G) \leq k$ for reasonably many pairs (G, k).

Let us remark that some of these results are easier to state in terms of $\tau(G) = |V(G)| - \alpha(G)$, the point-covering number of G. Also note that if $L(G)$ denotes the line-graph of G, then $\alpha(L(G))$ is the matching number of G, and so it is well-behaved. To what class of graphs generalizing line-graphs the successful theory of matchings can be extended is the motivation of some important current research [14, 16].

Finally, let us point out that complexity considerations concerning the independence number problem motivate, and may even initiate, research in fields like algebraic geometry, linear algebra and algebraic topology. Although these connections are in a very embryonic state, any link between graph theory (or combinatorial optimization) and these deep, classical fields of mathematics is, I feel, of particular interest.

1. Eigenvalues

We describe very briefly an upper bound on α which was discovered in connection with a problem of Shannon in coding theory.

Let G be a graph on $V(G)=\{1,\ldots,n\}$ and let $\mathscr{A}$ denote the set of $n\times n$ symmetric matrices $A=(a_{ij})$ such that $a_{ij}=1$ if $i=j$, or i and j are non-adjacent. Let $\Lambda(A)$ denote the largest eigenvalue of A. Define

$$\vartheta(G)=\min\{\Lambda(A)\colon A\in\mathscr{A}\}\,.$$

Since every $A\in\mathscr{A}$ contains a symmetric $\alpha(G)\times\alpha(G)$ submatrix J of all 1's, it follows that

$$\Lambda(A)\geqslant\Lambda(J)=\alpha(G)\,,$$

and so $\vartheta(G)\geqslant\alpha(G)$. What is important about ϑ is that it is polynomially computable. (More precisely, for every $\varepsilon>0$ a rational approximation of $\vartheta(G)$ with error less than ε can be computed in time polynomial in $|\log\varepsilon|$ and n. Note that ϑ may be irrational !) The idea of computing $\vartheta(G)$ is that $\Lambda(A)$ is a convex function of A on the affine subspace $\mathscr{A}$, and it can be minimized using the methods of Shor [17] and Yudin and Nemirovskii [18] (see also [4]).

As remarked before, this function ϑ gives rise to a class of graphs for which α is efficiently computable, namely the class of graphs with $\alpha(G)=\vartheta(G)$. This class is, however, rather ugly: it is in NP but it is also NP-complete. A nicer subclass is the class of perfect graphs. For perfect graphs the only known polynomial algorithm to compute $\alpha(G)$ is through computing $\vartheta(G)$ (see [4]).

It was also remarked that if a polynomially computable upper bound is found, then this can be used to prune branch and bound search trees. Experience shows that the use of ϑ does prune the search for maximum independent set considerably [3], but no theoretical results have been obtained so far concerning the size of the 'pruned' tree.

2. Algebraic geometry

The section title is perhaps somewhat immodest, but the flavor of the result of Li and Li [9], which is the starting point of our discussion, is indeed algebraic geometry.

Let G be a simple graph on $V(G)=\{1,\ldots,n\}$, and let us consider n variables $x_1,\ldots,x_n$. Form the polynomial

$$f(G;x_1,\ldots,x_n)=\prod_{\{i,j\}\in E(G)}(x_i-x_j)\,.$$

(This polynomial depends on the labelling of the points, but only up to its sign, which shall play no role.) Note the following simple fact.

Lemma 2.1. *$\alpha(G) \leq k$ iff, identifying $k+1$ variables in $f(G; x_1, \ldots, x_n)$ in all possible ways, we always obtain the zero polynomial.*

Let $X_k^n \subseteq C^n$ denote the set of those vectors which have at least $k+1$ equal coordinates, and let I_k^n denote the ideal of those polynomials in $C[x_1, \ldots, x_n]$ which vanish for every vector in X_k^n. Thus $\alpha(G) \leq k$ iff $f(G; x_1, \ldots, x_n) \in I_k^n$. To make use of this observation one needs a description of I_k^n which will enable us to exhibit 'easily' that a polynomial is in I_k^n. A natural approach is to find generators for I_k^n, and this was indeed accomplished by Li and Li [9]. Let $\mathscr{H}_k^n$ denote the set of those graphs on $\{1, \ldots, n\}$ which are unions of k disjoint complete graphs. Let $\bar{\mathscr{H}}_k^n$ denote the subset of $\mathscr{H}_k^n$ consisting of those graphs where the sizes of the components are as equal as possible (i.e., every graph in $\bar{\mathscr{H}}_k^n$ consist of $n - k\lfloor n/k \rfloor$ copies of a complete $\lceil n/k \rceil$-graph and $k\lceil n/k \rceil - n$ copies of a complete $\lfloor n/k \rfloor$-graph. Note that all members of $\bar{\mathscr{H}}_k^n$ are isomorphic, but we are considering labelled graphs !)

Theorem 2.2. *I_n^k is generated by the polynomials $f(H; x_1, \ldots, x_n)$ $(H \in \bar{\mathscr{H}}_k^n)$.*

Corollary 2.3. *A graph G satisfies $\alpha(G) \leq k$ iff there exist polynomials $g_H(x_1, \ldots, x_n)$ $(H \in \bar{\mathscr{H}}_k^n)$ such that*

$$f(G; x_1, \ldots, x_n) = \sum_{H \in \bar{\mathscr{H}}_k^n} g_H(x_1, \ldots, x_n) f(H; x_1, \ldots, x_n).$$

Of course, Theorem 2.2 and Corollary 2.3 remain true if $\bar{\mathscr{H}}_k^n$ is replaced by $\mathscr{H}_k^n$, and the main difficulty lies in proving these weaker conclusions.

Let us remark that if $(x_1, \ldots, x_n) \in C^n$ and $f(H; x_1, \ldots, x_n) = 0$ for every $H \in \bar{\mathscr{H}}_k^n$, then an easy argument shows that $(x_1, \ldots, x_n) \in X_k^n$. Hence, by the Nullstellensatz of Hilbert, there exist a natural number $p > 0$ and polynomials $g_H(x_1, \ldots, x_n)$ such that

$$f(G; x_1, \ldots, x_n)^p = \sum_{H \in \bar{\mathscr{H}}_k^n} g_H(x_1, \ldots, x_n) f(H; x_1, \ldots, x_n).$$

The main contents of Theorem 2.2 is that $p = 1$. This is somewhat reminiscent of the situation in integer linear programming, where a minimax formula for a linear relation follows in generality by the Duality Theorem, and one has to work hard and use special features of the problem to show that the denominators of the optimal solution of the linear program are 1's.

Why is this an upper bound on $\alpha(G)$? In the general sense mentioned in the introduction, $\alpha(G) \leq k$ can be proved by exhibiting polynomials g_H $(H \in \mathscr{H}_k^n)$ such that

$$(\mathrm{R}_1) \qquad f(G; x_1, \ldots, x_n) = \sum_{H \in \bar{\mathcal{H}}_k^n} g_H(x_1, \ldots, x_n) f(H; x_1, \ldots, x_n).$$

There are, however, three problems which arise here:

(1) The cardinality of $\bar{\mathcal{H}}_k^n$ is exponential in n; so (R_1) can be written down in polynomial time only if all but a polynomial number of the g_H are 0.

(2) It might happen that although (R_1) has only a polynomial number of terms, the coefficients g_H cannot be written down in polynomial space.

(3) Even if (R_1) is written down, there may not be any procedure to verify it in polynomial time.

Of these, the first problem is really serious and it limits the applicability of (R_1) to prove $\alpha(G) \leq k$ to special classes of graphs. (Question: can one *prove* that there exist graphs G for which every equation of type (R_1) has exponentially many terms on the right-hand side ?)

Objection (2) can be eliminated. I have proved that in (R_1) the coefficients g_H themselves may be chosen in the form $f(G_H; x_1, \ldots, x_n)$ with some graphs G_H. Thus the following theorem may be formulated.

Theorem 2.4. *A graph G has $\alpha(G) \leq k$ if and only if there exist graphs $G_1, \ldots, G_m$ on $V(G)$ such that each G_i can be partitioned into k cliques and*

$$(\mathrm{R}_2) \qquad f(G; x_1, \ldots, x_n) = \sum_{i=1}^{m} f(G_i; x_1, \ldots, x_n).$$

Finally, objection (3) is only moderately serious.

Of course, we cannot simply expand all polynomials occurring and then see if all terms cancel (as we learn at school), since the expansion of just $f(G; x_1, \ldots, x_n)$ contains exponentially many terms. But we may, say, generate values for $x_1, \ldots, x_n$ at random, substitute, and see if the two sides are equal. If they are not, then, of course, we know that (R_1) does not hold. If they are, then the probability that (R_1) is not an identity is negligible, but we have hit a choice of variables for which the two sides are equal. So the verification of (R_1) can be carried out at least in a 'random polynomial' framework. The problem of verifying a polynomial identity in deterministic polynomial time is an outstanding problem in the complexity theory of algebra. It may well be, however, that special identities like (R_2) can be verified easier.

Kleitman and the present author observed that a 'dual' version of the theorem of Li–Li is also true (in fact, it is easier to prove). Let $Y_k^n \subseteq C^n$ denote the set of those vectors which have at most k distinct entries, and let J_k^n denote the ideal of those polynomials which vanish for every vector in Y_k^n.

Lemma 2.5. *A graph G has chromatic number* $\geq k$ *if* $f(G; x_1, \ldots, x_n) \in J_k^n$.

The less trivial part is the following. Let $\mathscr{L}_k^n$ denote the set of those graphs on $\{1, \ldots, n\}$ whose edges form a complete k-graph (and which have, therefore, $n - k$ isolated points).

Theorem 2.6. *The polynomials* $f(L; x_1, \ldots, x_n)$ $(L \in \mathscr{L}_k^n)$ *generate the ideal* J_k^n.

Corollary 2.7. *A graph G satisfies* $\chi(G) \geq k$ *iff there exist polynomials* $g_L(x_1, \ldots, x_n)$ $(L \in \mathscr{L}_k^n)$ *such that*

$$f(G; x_1, \ldots, x_n) = \sum_{L \in \mathscr{L}_k^n} g_L(x_1, \ldots, x_n) f(L; x_1, \ldots, x_n).$$

Again, the following sharper version is true.

Theorem 2.8. *A graph G satisfies* $\chi(G) \leq k$ *iff there exist graphs* $G_1, \ldots, G_m$ *on* $V(G)$, *each containing a complete k-graph, such that*

$$f(G; x_1, \ldots, x_n) = \sum_{i=1}^{m} f(G_i, x_1, \ldots, x_n).$$

In this last form this result is reminiscent of a well-known result of Hajós [6], which also yields a 'pseudo-good' characterization of graphs with chromatic number $\geq k$. Define 3 operations on the set of graphs:

(α) add new points and/or lines,

(β) identify two non-adjacent points,

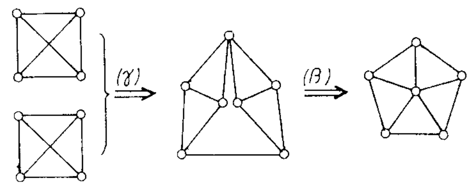
(γ) take two graphs G_1, G_2, delete two edges $x_1y_1 \in E(G_1)$ and $x_2y_2 \in E(G_2)$, identify x_1 with x_2 and join y_1 to y_2 by a new edge.

Theorem 2.9. *A graph G has* $\chi(G) \geq k$ *iff it can be constructed from complete k-graphs by the repeated application of steps* (α), (β) *and* (γ).

Again, the relation $\chi(G) \geq k$ can be proved for a graph G by carrying out the construction explicitly. Just how short this proof is, depends on the graph G. Perfect graphs can be obtained in one step. Are there other interesting classes for which the construction is short ? So far, Hajós' theorem was studied for its possible applications to planarity; its algorithmic complexity aspects are an unexplored territory (cf. Fig. 1).

To this approach to chromatic number the same remarks apply as to the Li–Li theorem on independence number.

Li and Li point out that by looking at the degrees of the polynomials, one



$$(x_1-x_2)(x_2-x_3)(x_3-x_4)(x_4-x_5)(x_5-x_1)(x_1-x_6)(x_2-x_6)(x_3-x_6)(x_4-x_6)(x_5-x_6)=$$
$$=(x_1-x_2)(x_2-x_3)(x_1-x_3)(x_1-x_6)(x_2-x_6)(x_3-x_6)(x_3-x_4)(x_4-x_5)(x_4-x_6)(x_5-x_6)$$
$$+(x_1-x_2)(x_2-x_3)(x_1-x_6)(x_2-x_6)(x_3-x_4)(x_4-x_5)(x_3-x_5)(x_3-x_6)(x_4-x_6)(x_5-x_6)$$

Fig. 1. Proving that the 5-wheel has chromatic number ≥ 4 by Hajós' construction and by the method of polynomials.

sees immediately that if $\alpha(G) \leq k$, then

$$|E(G)| = \deg f(G; x_1, \ldots, x_n) \geq \deg f(H; x_1, \ldots, x_n),$$

where $H \in \mathscr{H}_k^n$. This result is just Turán's theorem (for the complement of G). They also obtain generalizations of Turán's theorem this way, but we cannot go into the details of this.

The idea of using the degree of a polynomial to obtain combinatorial estimations also occurs in a paper by Brouwer and Schrijver [2], where they use it to calculate $\tau(H)$ for the hypergraph H formed by the lines of an affine plane over a finite field.

Let us conclude this section with the remark that Hilbert's Nullstellensatz may well be a source of other interesting 'good' or 'pseudo-good' characterizations in combinatorics. More generally, the duality between 'syntax' and 'semantics' comes up here (in the Nullstellensatz, the solvability of a system of algebraic equations—a 'semantical' problem—is characterized in terms of the non-expressability of 1 as an element of the ideal generated by the left-hand side—a syntactical property). So, e.g. Gödel's Completeness Theorem could be viewed as a 'pseudo-good' characterization of the consistency of a system of axioms: if it is inconsistent, we can exhibit this by deriving a contradiction, if it is consistent, we can exhibit a model. Of course, no polynomiality (or even finiteness) of these procedures is claimed. Whether polynomiality enters the picture in any reasonable way is not known.

3. Matroids

These results (see [10]) are best discussed in terms of the point-covering number $\tau(G)$. Let us assume that a matroid $(V(G), r)$ is introduced on $V(G)$. Then we may generalize the problem of determining $\tau(G)$ to determining $\tau(G, r)$, the minimum rank of a point-cover. In the special case where $(V(G), r)$ is the free matroid, we have $\tau(G, r) = \tau(G)$.

The gain in introducing this matroid structure on $V(G)$ is that we have more freedom in applying some reduction procedures. Let $v \in V(G)$, $r(v) = 1$ and assume that v is in the flat spanned by its neighbours. Delete v from the graph and contract v in the matroid. Then the resulting graph G' and matroid $(V(G'), r')$ satisfy

$$\tau(G', r') = \tau(G, r) - 1 . \tag{1}$$

If $v \in V(G)$ has rank $r(v) = 0$, then for the graph G' and rank function r' obtained similarly as above we have

$$\tau(G', r') = \tau(G, r) . \tag{2}$$

If $v \in V(G)$ is a coloop in the matroid, then let $(V(G), r'')$ be a new matroid which is obtained by deleting v, place a 'general' point on the flat spanned by its neighbours, and finally label this new point v.

Then

$$\tau(G, r'') = \tau(G, r) . \tag{3}$$

If $(V(G), r')$ is any weak map of the matroid $(V(G), r)$ (i.e., $r' \leqslant r$), then trivially

$$\tau(G, r') \leqslant \tau(G, r) . \tag{4}$$

Now these reductions enable us to prove the relation $\tau(G) \geqslant k$ for quite a few graphs. (It is not clear which are interesting classes for which this can be accomplished.) Fig. 2 shows how to exhibit, using reductions (1)–(4) that the graph G has $\tau(G) \geqslant 6$.

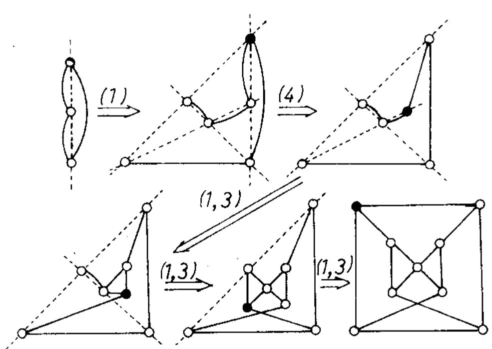


Fig. 2. Proving that the graph G has $\tau(G) \geqslant 6$ by the method of matroids. For brevity, (1) followed by (3) is depicted as one step, (1, 3).

So far, the main application of this method has been to develop a classification theory for τ-critical graphs (Lovász [11]). In the algorithmic context, an important problem which arises is handling the matroids. A natural approach is to restrict oneself to real representable matroids, and then handle them as real matrices. There are, however, many problems in connection with this, for example, how to construct a representation of a principal extension from a representation of the matroid? We cannot go into the complicated problems arising here.

4. Topology

The present author [12] proved the following lower bound on the chromatic number $\chi(G)$ of a graph. Let us define the neighbourhood complex $\mathcal{N}(G)$ of a graph G as the simplicial complex whose vertices are the points of G and whose simplices are those subsets of $V(G)$ which have a neighbour in common. Let us recall that a topological space T is called *k-connected* if for every $0 \leq r \leq k$, every continuous map of the r-sphere S^r into T extends to a continuous map of the $(r+1)$-ball B^{r+1} with boundary S^r into T. Thus 0-connected means arcwise connected, 1-connected means arcwise connected and simply connected (trivial fundamental group) etc.

Theorem 4.1. *If $\mathcal{N}(G)$ is k-connected, then $\chi(G) \geq k+3$.*

This theorem has been used to prove a conjecture of Kneser concerning the chromatic number of certain graphs. Its proof depends on the Borsuk–Ulam theorem on antipodal mappings of the sphere.

Schrijver and the present author have found the following lower bound on $\tau(G)$ of a somewhat similar character. Let G be a graph and define a simplicial complex $\mathcal{M}(G)$ whose vertices are those subsets X of $V(G)$ for which both X and $V(G)-X$ span at least one line. Let the simplices of $\mathcal{M}(G)$ be those sets of such subsets which are totally ordered with respect to inclusion.

Theorem 4.2. *If $\mathcal{M}(G)$ is k-connected, then $\tau(G) \geq k+3$.*

This result generalizes to hypergraphs without any essential change. Its proof depends on the Borsuk–Ulam theorem again.

The algorithmic aspects of these topological results are very much unexplored. It is likely that the k-connectivity of $\mathcal{N}(G)$ is an NP-property for every fixed k, since it means that the k-skeleton is contractible to a single point within the $(k+1)$-skeleton, and probably this contraction can be described in polynomial time. I could not, however, work out a rigorous proof. The situation is even more complicated with $\mathcal{M}(G)$, since this has exponentially many vertices. But we may replace $\mathcal{M}(G)$ by any simplicial complex which is homotopically equivalent. Is there such a complex which has only $|V(G)|^{\text{const}}$ vertices ? Is there one which can be constructed from G in polynomial time ? Probably these questions may be answered in the affirmative using some methods like the (homotopical) Crosscut Theorem of Mather [13] or other related results on topological spaces associated with posets, lattices, etc. (we also refer to [15] and [1]).

Conclusion. We have surveyed some methods to obtain upper bounds on $\alpha(G)$ (or, equivalently, lower bounds on $\tau(G)$), which use non-trivial tools from other parts of mathematics. We tried to show that complexity considerations in connection with these methods raise some interesting questions in other fields of mathematics.

Our selection has clearly not been representative for all approaches. We have to call the reader's attention to the work of, among others, Hammer and Simeone [7], Hansen [8] and Haemers [5], but we cannot discuss their approach in detail.

References

[1] K. Baclavski and A. Björner, Fixed points in partially ordered sets, Adv. in Math. 31 (1979) 263–287.

[2] A.E. Brouwer and A. Schrijver, The blocking number of an affine plane, J. Combin. Theory Ser. A 24 (1978) 251–253.

[3] I. Csonka, L. Lovász and G. Turán, to be published.

[4] M. Grötschel, L. Lovász and A. Schrijver, The ellipsoid method and its consequences in combinatorial optimization, Combinatorica 1 (1981) 169–197.

[5] W. Haemers, On some problems of Lovász concerning the Shannon capacity of a graph, IEEE Trans. Inf. Theory 25 (1980) 231–232.

[6] G. Hajós, Über eine Konstruktion nicht n-färbbarer Graphen, Wiss. Zeitschr. Martin-Luther Univ. Halle-Wittenberg A10 (1961) 116–117.

[7] P.L. Hammer and B. Simeone, Best linear upper bounds on quadratic 0-optimization, preprint.

[8] P. Hansen, Upper bounds for the stability number of a graph, Revue Roumaine de Math. Pures Appl. 24 (1979) 1195–1199.

[9] W.W. Li and S.R. Li, Independence numbers of graphs and generators of ideals, Combinatorica 1 (1981).

[10] L. Lovász, Flats in geometries and geometric graphs, in: P. Cameron, ed., Combinatorial Surveys (Academic Press, New York, 1977) pp. 45–86.

[11] L. Lovász, Some finite basis theorems in graphs theory, in: A. Hajnal and V.T. Sós, eds., Combinatorics, Coll. Math. Soc. J. Bolyai 18 (North-Holland, Amsterdam, 1978) pp. 717–729.

[12] L. Lovász, Kneser's conjecture, chromatic number, and homotopy, J. Combin. Theory A25 (1978) 319–324.

[13] J. Mather, Invariance of the homology of a lattice, Proc. Amer. Math. Soc. 17 (1966) 1120–1124.

[14] G. Minty, On maximal independent sets of vertices in claw-free graphs, J. Combin. Theory Ser. B 28 (1980) 284–304.

[15] G.-C. Rota, On the foundations of combinatorial theory I; theory of Möbius functions, Z. Wahrsch. Verw. Geb. 2 (1964) 340–368.

[16] N. Sbihi, Algorithme de recherche d'un stable de cardinalité maximum dans un graphe sans étoile, Discrete Math. 29 (1980) 53–76.

[17] N.Z. Shor, Convergence rate of the gradient descent method with dilatation of the space, Kibernetika 2 (1970) 80–85; (English translation: Cybernetics 6 (1970) 102–108).

[18] D.B. Yudin and A.S. Nemirovskii, Informational complexity and effective methods of solution for convex extremal problems, Ekonomika i Mat. Metody 12 (1979) 357–369; (English translation: Matekon: Transl. of Russian and East European Math. Economics 13(3) 24–45).