BOLETIM
DA SOCIEDADE BRASILEIRA DE MATEMÁTICA

Bol. Soc. Bras. Mat., Vol. 20, No. 1, 87-99

Singular spaces of matrices and their application in combinatorics

László Lovász

Abstract. We study linear spaces of $n \times n$ matrices in which every matrix is singular. Examples are given to illustrate that a characterization of such subspaces would solve various open problems in combinatorics and in computational algebra. Several important special cases of the problem are solved, although often in disguise.

1. The problem

Let $\mathcal{A}$ be a linear subspace of the space $\mathbb{R}^{n \times n}$ of real $n \times n$ matrices. We say that $\mathcal{A}$ is *singular* if every matrix in $\mathcal{A}$ is singular. We are interested in the problem of characterizing singular spaces of matrices, and in obtaining an efficient algorithm to determine if a space of matrices (given by a linear basis) is singular. Unfortunately, we cannot give a complete solution to these problems, but special cases with combinatorial applications will be solved.

Geometrically, $\det X = 0$ defines a surface in $\mathbb{R}^{n \times n}$ and we are interested in the linear subspaces contained in this surface. Clearly, we may restrict our attention to the *maximal* singular subspaces.

The problem arose in differential geometry (see Room (1938)), but my interest in this problem stems from its connection to matching problems and other fundamentals problems in combinatorics. In this context, the problem was formulated by Edmonds (1967), who pointed out its relevance to combinatorial algorithms and to the theory of computational complexity.

We may slightly generalize the problem by considering a linear subspace $\mathcal{A}$ of real $n \times m$ matrices. We define the *generic rank* $\mathrm{gr}(\mathcal{A})$ of such a subspace as the maximum rank of matrices in it, and want to find an efficient way to compute this generic rank, given (say) a basis for $\mathcal{A}$. (Unfortunately, no really efficient algorithm is known for this problem, at least if we do not allow randomization.)

Received 14 January 1989.
Research supported by Hungarian National Research Fund No. 1812.

However, it is easy to reduce this seemingly more general problem to the problem of characterizing singular matrix spaces.

A trivial upper bound on the generic rank is the *column range rank* $\operatorname{lrr}(\mathcal{A})$ of the matrix space, defined as the dimension of the subspace spanned by all the columns of all the matrices in $\mathcal{A}$. This number is easy to compute if we have a basis of $\mathcal{A}$. Similarly, we can use the *row range rank* $\operatorname{rrr}(\mathcal{A})$ as an upper bound on the generic rank.

We mention two further ways to formulate the problem, which are both useful in some way. First, let $A_1, \dots, A_k$ generate our space $\mathcal{A}$, and let $x_1, \dots, x_k$ be variables. Then $A(x) = x_1A_1 + \cdots + x_kA_k$ is a matrix, each entry of which is a linear form in these variables. So $\det A(x)$ is a polynomial in these variables and we want to determine those matrices of linear forms for which this determinant is identically 0. Let us remark immediately that if the determinant is not identically 0 then it is non-zero for almost all choices of the variables. In particular, if we choose transcendental values for the x_i which are algebraically independent over the field generated by the entries of the A_i, then for this particular substitution $\det A(x)$ will be 0 if and only if it is identically 0. Unfortunately, this condition is of little use, since there is no way to evaluate a determinant with transcendental entries.

On the other hand, the observation that if $\det A(x)$ is not identically 0 then almost all substitutions give a non-zero value *is* of algorithmic interest. If we are given the matrices $A_1, \dots, A_k$, we can generate random values for $x_1, \dots, x_k$ (say, from a uniform distribution on $[0, 1]$) and evaluate the resulting numerical determinant. If the result is non-zero, we conclude that $\det A(x)$ is not identically zero. If the result is zero, we conclude that $\det A(x)$ is identically zero.

This conclusion is of course not quite legitimate: we may err. If $\det A(x)$ is identically 0, then we of course come to this conclusion. But if it is not identically 0, we may be unlucky enough to hit a root, and come to the wrong conclusion. However, the probability of this to happen is 0.

Of course, in practice we can not generate random real numbers and compute with them. If we generate, say, a random integer between 0 and N for each x_i then, no matter how large is N, there will be a positive probability of error. However, this probability will be very small (see Schwartz 1980), so we may still regard the problem as practically solved. (Whether one can generate a random integer in a given interval, or even a random bit, is a difficult question with physical or even philosophical overtones, and we shall not discuss it here.)

Unfortunately, the above – randomized – algorithm does not give any insight into the structure of such subspaces. In what follows we shall try to attack this more theoretical question.

Finally, we can also formulate the problem like this: let $A = (a_{ijk})$ be a $k \times n \times m$ "3-dimensional matrix", i.e., a tensor with 3 indices. This defines a trilinear form $\alpha(x, y, z)$. We want to find the maximum rank of a bilinear form obtained by fixing (say) the first variable x. This formulation will lead us to an interesting open question (see section 5).

2. Examples

Let us discuss some classes of singular subspaces. The first is the most natural one and is discussed, e.g., in Room (1938).

Example 1. Let U and V be two subspaces of $\mathbb{R}^n$ such that $\dim U = \dim V + 1$. Let $\mathcal{A}$ consist of all $n \times n$ matrices A for which $AU \subseteq V$. Clearly, $\mathcal{A}$ is a linear subspace of matrices and every member of it is singular.

This example contains as special cases several other constructions that occur in a natural way:

- let A be a singular matrix and consider all matrices of the form AX $(X \in \mathbb{R}^{n\times n})$;
- consider all matrices with 0's in their first row; more generally, all $n \times n$ matrices with a fixed $k \times (n - k + 1)$ block of 0's.

A more general way to put this example is the following: Let $\mathcal{A}$ be any space of $n \times n$ matrices. For $n \times n$ matrices B and C, let $B\mathcal{A}C$ denote the space of all matrices BAC, $A \in \mathcal{A}$. Then

$$\operatorname{gr}(\mathcal{A}) \le \operatorname{gr}(B\mathcal{A}C) + 2n - \operatorname{rk}(B) - \operatorname{rk}(C).$$

In the example, and we can choose B and C trivially so that $B\mathcal{A}C = 0$ and $\operatorname{rk}(B) + \operatorname{rk}(C) > n$. Then the inequality gives $\operatorname{gr}(\mathcal{A}) < n$.

This idea can be used, more generally, to construct new matrix spaces with low generic rank from a given matrix space with low generic rank. Let $\mathcal{A}$ be a space of $n \times m$ matrices of generic rank r. Let $\mathcal{A}'$ be the set of all $n \times (m + k)$ matrices that arise from some matrix in $\mathcal{A}$ by adding k new columns arbitrarily. Then $\mathcal{A}'$ is a matrix space of generic rank $r + k$.

There is of course a dual form of this construction, corresponding to adding new rows to a matrix.

Example 2. If n is odd then the space $\mathcal{S}_n$ of all skew symmetric $n \times n$ matrices is singular. More generally, if a space $\mathcal{A}$ of skew symmetric matrices has odd column range rank then

$$\operatorname{gr}(\mathcal{A}) < \operatorname{lrr}(\mathcal{A}) - 1.$$

The next example gives a construction to combine matrix subspaces with a low generic rank into a new subspace of such kind.

Example 3. Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be matrix spaces of the same dimensions. Define $\mathcal{A}_1 + \mathcal{A}_2 = \{A_1 + A_2 \colon A_i \in \mathcal{A}_i\}$. Then

$$\operatorname{gr}(\mathcal{A}_1 + \mathcal{A}_2) \leq \operatorname{gr} \mathcal{A}_1 + \operatorname{gr} \mathcal{A}_2.$$

Our last example we give is of a somewhat different, more special kind. We will see, however, that it also has important applications.

Example 4. Let $A_1, \dots, A_k$ be skew symmetric $n \times n$ matrices. Let $\mathcal{A}$ consist of all $n \times n$ matrices that arise in the form $[A_1 x, \dots, A_n x]$, where x ranges through $\mathbf{R}^n$. Then $\mathcal{A}$ is a singular space of matrices. To see this, observe that each matrix $A = [A_1 x, \dots, A_n x]$ in $\mathcal{A}$ satisfies $x^T A = 0$. More generally, it is not difficult to show that if such a matrix space $\mathcal{A}$ is not the 0 space then

$$\operatorname{gr}(\mathcal{A}) \leq \operatorname{lrr}(\mathcal{A}) - 1$$

We could generalize this construction: let $A_1, \dots, A_p$ be skew symmetric $n \times n$ matrices, $b_1, \dots, b_p \in \mathbf{R}^m$, arbitrary vectors. Consider all matrices of the form $\sum_{i=1}^p A_i x b_i^T$, where $x \in \mathbf{R}^n$. Clearly, these form a matrix space in which each matrix has rank less than n.

3. Some results

A complete characterization of singular matrix spaces seems to be unknown. There are, however, some results that show that under certain restrictions, singular (or low generic rank) matrix spaces arise by the constructions described in the previous section. As we shall see, these results were first obtained in a combinatorial framework, and correspondingly, the assumptions one has to make on the matrices involved concern some properties of the matrices generating the subspace. It is possible that there are conditions of an entirely different nature under which analogous results can be obtained.

Theorem 1. *Assume that the singular matrix space $\mathcal{A}$ is generated by rank 1 matrices. Then it arises by the construction in Example 1 above.*

There is a slightly more general way to formulate this theorem:

Theorem 1*. *Let $\mathcal{A} \subseteq \mathbf{R}^{n \times m}$ be a matrix space generated by rank 1 matrices. Then*

$$\operatorname{gr}(\mathcal{A}) = \min\{n - \dim U + \dim(\mathcal{A}U) \mid U \subseteq \mathbf{R}^m\}.$$

This theorem follows quite easily from the the Matroid Intersection Theorem of Edmonds (1970). In fact, we only need the special case when the matroids in

question are linear, which can be formulated without any reference to matroids:

Theorem 2. (Edmonds 1970.) *Let $a_1, \dots, a_p \in \mathbf{R}^k$ and $b_1, \dots, b_p \in \mathbf{R}^l$. The maximum number s os indices $1 \leq i_1 \leq \dots \leq i_s \leq p$ such that both sets of vectors $\{a_{i_1}, \dots, a_{i_s}\}$ and $\{b_{i_1}, \dots, b_{i_s}\}$ are linearly independent is given by*

$$s = \min\{\dim \operatorname{lin}\{a_j \colon j \in J\} + \dim \operatorname{lin}\{b_j \colon j \in \{1, \dots, n\} \setminus J\} \colon J \subseteq \{1, \dots, n\}\}.$$

To derive Theorem 1* from Theorem 2, consider the rank 1 matrices generating the space: these can be written as $a_1 b_1^T, \dots, a_p b_p^T$. Let s denote the largest integer such that there are s linearly independent vectors among the a_i such that the corresponding b_i are also linearly independent. Without loss of generality we may assume that these are $a_1, \dots, a_s$ and $b_1, \dots, b_s$, respectively. Now the matrix $a_1 b_1^T + \dots + a_s b_s^T$ has rank s by elementary linear algebra, and so $\operatorname{gr} \mathcal{A} \geq s$. On the other hand, Theorem 3 implies that there exists a subset $J \subseteq \{1, \dots, n\}$ such that

$$s = \dim \operatorname{lin}\{a_j \colon j \in J\} + \dim \operatorname{lin}\{b_j \colon j \in \{1, \dots, p\} \setminus J\}.$$

Now denote $U = \{x \in \mathbf{R}^n \colon a_j^T x = 0 \text{ for all } j \in J\}$. Then $\mathcal{A}U \subseteq \operatorname{lin}\{b_j \colon j \in \{1, \dots, n\} \setminus J\}$. So

$$n - \dim U + \dim \mathcal{A}U = n - (n - \dim \operatorname{lin}\{a_j \colon j \in J\}) + \dim \operatorname{lin}\{b_j \colon j \in J\} = s.$$

Hence, $\operatorname{gr} \mathcal{A} \geq n - \dim U + \dim \mathcal{A}U$. Since the opposite inequality is obvious, this proves the theorem.

Our next theorem shows that if the matrix space is generated by rank 2 skew symmetric matrices then its generic rank is still determined by the constructions given in the previous section:

Theorem 3. *Let $\mathcal{A} \subseteq \mathbf{R}^{n \times n}$ be a matrix space generated by skew symmetric matrices with rank 2. Then*

(a) *If B is any $n \times n$ matrix and $\mathcal{A}_1, \dots, \mathcal{A}_k$ are spaces of skew symmetric $n \times n$ matrices with odd column range rank such that*

$$B^T \mathcal{A} B \subseteq \mathcal{A}_1 + \dots + A_k,$$

then we have

$$\operatorname{gr}(\mathcal{A}) \leq 2 \operatorname{rk}(B) - 2n + \sum_i (\operatorname{lrr}(\mathcal{A}) - 1).$$

(b) *There exists $\mathcal{A}_1 \dots, \mathcal{A}_k$ and B for which equality holds in* (a).

This theorem again follows from a combinatorial result (Lovász 1980a-b), which is sometimes called the "matroid parity theorem".

Theorem 4. *Let $a_1, b_1, a_2, b_2, \dots, a_n, b_n \in \mathbf{R}^n$. Then the maximum number*

s of indices $1 \le i_1 \le \cdots \le i_s \le p$ such that $a_{i_1}, b_{i_1}, \ldots, a_{i_s}, b_{i_s}$ are linearly independent is given by

$$s = \min\left\{\dim W + \sum_{i=1}^{k}\left\lfloor \frac{\dim\langle H_1 \cup W\rangle - \dim W}{2}\right\rfloor\right\},$$

where W ranges over all subspaces of $\mathbf{R}^n$, $\{H_1, \ldots, H_k\}$ ranges over all partitions of $\{1, \ldots, p\}$, and $\langle H_i \cup W\rangle$ denotes the subspace generated by $\{a_i : i \in H_i\}$, $\{b_i : i \in H_i\}$ and W.

This theorem remais valid if we replace the real field by any other field. On the other hand, it is *not* valid in general for matroids. In fact, to compute the maximum in the theorem takes exponencial time (Lovász 1980c, Jensen and Korte 1982). But there are some classes of matroides to which it extends. The following version can be formulated without using matroid theoretical notions: *if we replace the vector space by an algebraically closed field, linear independence by algebraic independence, dimension by transcendence degree, and subspace by algebraically closed subfield, then the result corresponding to* Theorem 4 *holds* (Dress and Lovász 1987). For a discussion of those matroids for which this min-max result extends, see also Björner and Lovász (1987).

To derive Theorem 4 from Theorem 3, consider the rank 2 skew symmetric matrices generating the space. These can be written as

$$a_1 b_1^T - b_1 a_1^T, \ldots, a_p b_p^T - b_p a_p^T$$

Let $a_{i_1}, b_{i_1}, \ldots, a_{i_s}, b_{i_s}$ be a largest family of pairs a_i, b_i that are collectively linearly independent. It is obvious that the matrix space spanned by $a_{i_1} b_{i_1}^T$, ..., $a_{i_s} b_{i_s}^T$ has generic rank $2s$. On the other hand, consider the subspace W and the partition $\{H_i\}$ for which the minimum in the Theorem 4 is attained. If we choose any $n \times n$ matrix with null space W as B, and the space generated by the matrices $\{B^T(a_j b_j^T - b_j a_j^T)B : j \in H_i\}$ as $\mathcal{A}_i$, then equality is attained in (a).

We state one more class of matrix spaces for which the generic rank can be determined. These are the subspaces considered in Example 5, again with the restriction that the matrices in the definition have rank 2:

Theorem 5. *Let $A_1, \ldots, A_p$ be skew symmetric $n \times n$ matrices of rank 2. Let $\mathcal{A}$ consist of all $n \times n$ matrices that arise in the form $[A_1 x, \ldots, A_p x]$, where x ranges through $\mathbf{R}^n$. For every partition $\mathcal{P} = J_1 \cup \cdots \cup J_k$ of the index set $\{1, \ldots, p\}$, let $\mathcal{A}_i$ denote the matrix space formed by the columns in J_i. Then*

$$\operatorname{gr} \mathcal{A} = \min\left\{\sum_i (\operatorname{lrr}(\mathcal{A}_i) - 1)\right\}.$$

Again, there is a corresponding result in matroid theory that implies this

theorem. Variants of this were discovered by Edmonds (1970), Mason (1976) and Lovász (1977); see also Mason (1981). Let us say that a hyperplane H is in *general position* with respect to a family $\mathcal{F}$ of subspaces if there exists a subfield K of $\mathbf{R}$ such that each of the given subspaces has a basis with coordinates in K and H is defined by an equation $\sum_i \alpha_i x_i = 0$, where the coefficients α_i are algebraically independent over K.

Theorem 6. *Let $\mathcal{F}$ be a family of subspaces of $\mathbf{R}^n$ and H, a hyperplane in general position with respect to $\mathcal{F}$. Let Q be the subspace spanned by all subspaces of the form $A \cap H$, $A \in \mathcal{F}$. Then*

$$\dim Q = \min_{\{\mathcal{F}_1, \ldots, \mathcal{F}_k\}}\{\sum_{1 \le i \le k}(\dim\langle \mathcal{F}_i\rangle - 1)\},$$

where $\{\mathcal{F}_1, \ldots, \mathcal{F}_k\}$ ranges over all partitions of $\mathcal{F}$.

4. Combinatorial applications

a) Matchings. Perhaps the nicest combinatorial applications of the methods and results from the previous sections are in matching theory. The fundamental problem in this field is the following: given a graph G, decide whether or not it has a *perfect matching*, i.e., a set of disjoint edges covering every node. This problem, by no means easy, has both mathematically beautiful and practically efficient solutions. For these, we refer e.g. to the monograph Lovász and Plummer (1987).

However, the connection between linear algebra and the matching problem has gone through a reverse route. The first necessary and sufficient condition for the existence of a perfect matching in a bipartite graph was formulated in terms of linear algebra and proved using methods from linear algebra by Frobenius (1917). The problem itself grew out from the study of determinants. It was König (1916) who (in connection with an earlier, related result of Frobenius) observed that determinant problems can be formulated and handled in terms of graphs. (For more on the history of this basic theorem, see Lovász and Plummer 1986). Besides the necessary and sufficient condition which now occurs in every graph theory book (and is called the Marriage Theorem or the König-Hall Theorem), the work of König also implied the following (easy) result. Let G be a bipartite graph with bipartition $\{A, B\}$. Since we are interested in perfect matchings, we assume that $|A| = |B|$. Consider a variable x_e for each edge e. Let $F_G = \{f_{ij}\}$ denote the matrix shose rows are indexed by the elements of A, whose columns are indexed by the elements of B and

$$f_{ij} = \begin{cases} x_e, & \text{if } e = ij \in E(G), \\ 0, & \text{if } i \text{ and } j \text{ are non-adjacent} \end{cases}$$

Theorem 7. *A bipartite graph G has a perfect matching if and only if* $\det(F_G)$ *is not identically* 0.

Note that the matrices obtained by substituting for the x_e in all possible ways form a matrix space generated by the rank 1 matrices having a single 1 in a position corresponding to an edge. Theorem 7 says that the graph has a perfect matching iff this matrix space is non- singular.

As Edmonds (1967) points out, this theorem can be used to obtain an easy randomized algorithm for bipartite matching: substitute random numbers for the variables and evaluate the determinant. This algorithm does not directly supply us with a perfect matching; but if we have a test for the existence of a perfect matching, it is easy to actually find one: for a given node v, we look for an adjacent node u such that $G-u-v$ has a perfect matching (such a node u must exist if G itself has a perfect matching). Then we put the edge uv in the perfect matching and, recurrently, find a perfect matching in $G-u-v$. (This last trivial procedure breaks down in a parallel environment, as we shall see soon.)

It was remarked in Lovász (1979) that the preceding algorithm can be extended to non-bipartite graphs, using a result in the groundbreaking paper of Tutte (1947). The main result of his paper is a celebrated combinatorial condition on the existence of a perfect matching, but along the lines Tutte also proved the following algebraic condition. Given a graph G, associate again a variable x_e with each edge e. Let $T_G=(t_{ij})$ denote the skew symmetric matrix whose rows and columns are indexed by the node set $V(G)=\{1,\dots,n\}$, and

$$t_{ij}=\begin{cases} x_e, & \text{if } e=ij\in E(G) \text{ and } i<j \\ -x_e, & \text{if } e=ij\in E(G) \text{ and } i>j \\ 0, & \text{if } i \text{ and } j \text{ are non-adjacent.}\end{cases}$$

Theorem 8. *The graph G has a perfect matching if and only if* $\det(T_G)$ *is not identically* 0.

Again, the matrices obtained from T_G by substitution form a matrix space; in this case, this matrix space is generated by rank 2 skew symmetric matrices.

One can derive the Marriage Theorem and Tutte's Theorem from Theorems 1 and 3, respectively; but the proofs obtained are lengthy and not too attractive. Also, one can use the remarks in section 1 to design a rather simple algorithm to test a graph for the existence of a perfect matching. The worst case running time of this algorithm (if we use advanced determinant evaluation techniques), is comparable with the best implementations of Edmonds' blossom algorithm and other combinatorial algorithms (about $n^{2.5}$). But due to the facts that they

are *always* this slow, use randomization, and that numerical difficulties also arise, these algorithms remained curiosities until the study of parallel algorithms became fashionable. It turns out that determinant evaluation can be parallelized essentially optimally: a polynomial number of processors can solve the problem in polylog time (Csanky 1976). Every algorithm known to date to test the existence of a perfect matching that is well parallelizable is based on this linear algebraic formulation of the problem.

Let us remark that even if this test tells us that the graph has a perfect matching, it does not give us one. There is a trivial recursive procedure to use this test in an algorithm to find a perfect matching, but this is not parallelizable. Karp, Upfal and Wigderson (1985) show in a very general setting that (with a further randomization) this weighted matching algorithm can be used to actually find a perfect matching (if it exists) in parallel. Mulmuley, Vazirani and Vazirani (1986) illustrated the power of linear algebraic techniques, by designing a very nice and simple, more direct algorithm to find a perfect matching in a graph in polylog time, using a polynomial number of processors.

b) Structural rigidity. Let G be a graph. We want to realize G by a bar-and-joint structure: the nodes of G will be represented by flexible joints, adjacent nodes must be connected by rigid bars. Will the resulting structure be rigid?

This question is not yet well defined, since we can place the points in many positions. Let us assume that we place them now in general position, say, their coordinates are algebraically independent real numbers (in a sense this is the most "rigid" situation, but I do not want to go into the details of this theory). It is easy to see that the rigidity of this "general position" structure does not depend on the choice of these coordinates.

Let us give a heuristic argument for the translation of this problem into linear algebra; the arguments can be made precise by using elements of the theory of differential equations. Suppose that we are working in the plane. Also suppose that our structure is not rigid, and consider a motion of it. Let $x_v(t)$ denote the position of node v at time t. Then the fact that the bars are rigid says that for every edge $uv\in E(G)$,

$$(x_u(t)-x_v(t))^2=\text{const}.$$

Differentiating, we get

$$(x_u-x_v)(\dot{x}_u-\dot{x}_v)=0$$

This may be viewed as a system of homogeneus linear equations on the velocity vectors $\dot{x}_v$ of the nodes. This system always has non-trivial solutions, e.g. we can take $\dot{x}_u$ the same for all nodes: this corresponds to translating the structure. We also obtain a solution from rotating the structure. If the structure is non-rigid,

we obtain further solutions, i.e., the solution space of the system is more than 3-dimensional. Conversely, one can show that if the solution space has dimension larger than 3, then the structure is non-rigid.

If we write out the matrix of the above system, we obtain an $m \times 2n$ matrix, where m is the number of edges and n is the number of nodes of the graph. There is one row corresponding to each edge and two columns corresponding to each node, one for the x-coordinate and one for the y-coordinate. The row corresponding to an edge uv has $x_v - x_u$ in the position corresponding to $x_v, x_u - x_v$ in the position corresponding to $x_u, y_v - y_u$ in the position corresponding to $y_v, y_u - y_v$ in the position corresponding to y_v and 0 elsewhere. If we substitute all possible values for the x_u and y_u, we obtain a matrix space $\mathcal{A}_G$, and the structure is rigid if and only if $\mathrm{gr}(\mathcal{A}_G) = 2n - 3$. (Exercise: show by algebra that $\leq$ always holds.)

This matrix space has a very special structure. Consider its transpose, and the column corresponding to the edge $e = uv$. We introduce an orientation of this graph just for reference purposes. Let b_e denote the oriented incidence vector of this edge, i.e., the vector indexed by the nodes in which the u-th coordinate is 1, the v-th is -1, and the rest 0. Let x and y denote the column vectors formed by the first and second coordinates of the nodes, respectively. Then the column corresponding to e is

$$\begin{pmatrix} b_e b_e^T x \\ b_e b_e^T y \end{pmatrix}.$$

Clearly, matrices arising in this way form a linear space. Moreover, we can write the e-th column in the following form:

$$\begin{pmatrix} 0 & b_e b_e^T \\ -b_e b_e^T & 0 \end{pmatrix} \begin{pmatrix} -x \\ y \end{pmatrix}.$$

So this matrix space has the structure of Example 4, with the A_i having rank 2. Hence Theorem 5 can be applied. We do not go through the details (see Lovász and Yemini (1982)), but formulate only the condition derived from this theorem (essentially equivalent to the results of Laman (1970)):

Theorem 9. *A graph G is generic rigid in the plane if and only if it has the following property: adding any new edge, the resulting graph has two edge-disjoint spanning trees.*

c) Polynomial identities. Let $f(x_1, \ldots, x_n)$ be a polynomial with integral coefficients. Is f identically 0? This question has a trivial answer, taught in high schools: the polynomial is identically 0 iff eliminating all parentheses, all terms cancel. While for simple identities this is a very useful decision procedure, it may take exponential time, (measured in the length of the formula for f). For

example, if we want to verify the trivial identity

$$\prod_{1 \leq i \leq j \leq n} (x_i + x_j) - \prod_{1 \leq i \leq j \leq n} (x_i + x_j) = 0$$

by eliminating the parentheses, then we obtain exponentially many terms (before they all cancel).

It is not known whether there exists a polynomial time procedure to verify polynomial identities! (If we allow randomization, then there is one: just substitute random values for the x_i). One can show, however, that the problem reduces to the singular subspace problem. In fact, Valiant (1979) describes a construction that represents every polynomial as the determinant of a matrix in which each entry is either a variable or a constant. Moreover, the construction can be carried out in polynomial time. After a trivial homogenization, this gives a matrix space and the polynomial is identically 0 iff this space is singular.

Note that the determinant of every matrix space is of course a polynomial in variables $x_1, \ldots, x_n$ if we represent the typical matrix in the space as $x_a A_1 + \cdots + x_n A_n$, where the A_i are the generators of the space. This polynomial however cannot be written in general as polynomial of polynomial length (at least no such formula is known, and it is conjectured that no such formula exists). So matrix spaces arising in this construction are of a special kind.

5. Open problems

a. The central problem in this area is, of course, to characterize singular matrix spaces (or, more generally, to characterize the generic rank of a matrix space). If the matrix space is given by its generators, and these generators are, say, integral matrices, then the problem of deciding whether the space is non-singular is, trivially, in $\mathcal{NP}$ from the point of view of complexity theory: if the space is non-singular then this is easily exhibited by specifying a linear combination of the generators that is non-singular. Theorems 1, 3 and 5 are special cases when the problem is also in co-$\mathcal{NP}$. There is no hope to prove that the problem is $\mathcal{NP}$-complete, since as remarked at the beginning, there is a simple polynomial time randomized algorithm to solve it, i.e., the problem is in the class $\mathcal{RP}$ (and it is believed that $\mathcal{RP} \neq \mathcal{NP}$).

b. A more modest program is to find further special cases for which the problem is in co-$\mathcal{NP}$ or in $\mathcal{P}$. Perhaps the most important from the point of view of applications would be to extend the application to rigidity theory to dimension 3. Which graphs have the property that the generic joint-and-bar structure realizing them in 3-space is rigid? (Of course, one could extend the problem to any dimension.)

The discussion generalizes from the plane and yields that the task is to determine the generic rank of the space of matrices with 3 mod $V(G)$ rows and $|E(G)|$ columns of the form

$$\begin{pmatrix} \cdots & b_e b_e^T x & \cdots \\ \cdots & b_e b_e^T y & \cdots \\ \cdots & b_e b_e^T z & \cdots \end{pmatrix}$$

Unfortunately, no way is known to transform this matrix space into one of the types that are known to be solvable.

c. It is natural to ask if any of the solvable classes described in section 3 can be generalized. For example, can one characterize singular matrix spaces generated by rank 2 matrices? Or can one give a formula for the generic rank of a matrix space in the second (generalized) construction in Example 5, where the A_i are rank 2 skew symmetric matrices?

d. A very important special case is the problem of polynomial identities, discussed in section 4. Is there a good way to recognize which polynomials are identically 0? Do matrix spaces arising from polynomials have a more natural description?

e. Note that if we formulate theorems 3 and 5 in terms of 3-tensors, we obtain that they concern essentially the same class of tensors. Namely, they concern those 3-dimensional arrays $(a_{i,j,k})$ in which fixing i we obtain a rank 2 skew symmetric matrix. In one case, however, we consider the matrix space $\sum_i a_{ijk}x_i$ while in the other, we consider $\sum_j a_{ijk}x_j$. But there is no immediate connection between the two results. Is there a connection between the matrix spaces $\sum_i a_{ijk}x_i$ and $\sum_j a_{ijk}x_j$ for a general 3-dimensional array? Assuming we can compute the generic rank of one, does it help in computing the generic rank of the other?

References

A. Björner and L. Lovász (1987), *Pseudomodular lattices and continuous matroids*, Acta Sci. Math. Szeged **51**, 295-308.

L. Csánsky (1976), *Fast parallel matrix inversion algorithms*, SIAM J. Comput. **5**, 618-623.

A. Dress, L. Lovász (1987), *On some combinatorial properties of algebraic matroids*, Combinatorica **7**, 39-48.

J. Edmonds (1967), *Systems of distinct representatives and linear algebra*, J. Res. Nat. Bur. Standards Sect. **B 71B**, 241-247.

J. Edmonds (1970), *Submodular functions, matroids, and certain polyhedra*, in: Combinatorial Structures and their Appl. (ed. R. K. Guy, H. Hanani, N. Sauer and J. Schönheim), Gordon and Breach, New York, 69-87.

G. Frobenius (1982), *Über zerlegbare Determinanten,*, Sitzungsber. Königl. Preuss. Akad. Wiss., XVIII, 1917, 274-277.

P. M. Jensen and B. Korte (1982), *Complexity of matroid property algorithms*, SIAM J. Comput., **11**, 184-190.

R. M. Karp, E. Upfal and A. Wigderson (1986), *Constructing a perfect matching is in random NC*, Combinatorica **6**, 35-48.

D. König (1916), *Über Graphen und ihre Anwendung auf Determinantentheorie und Mengenlehre*, Math. Annalen **77**, 453-465.

G. Laman (1970), *On graphs and rigidity of plane skeletal structures*, J. Engrg. Math. **4**, 331-340.

N. Linial, L. Lovász and A. Wigderson (1988), *Rubber bands, convex embeddings, and graph connectivity*, Combintorica **8**, 91-102.

L. Lovász (1977), *Flats in matroids and geometric graphs*, in: Combinatorial Surveys, Proc. 6th Britsh Comb. Conf., Academic Press, 45-86.

L. Lovász (1979), *Determinants, matchings, and random algorithms*, in: Fundamentals of Computation theory, FCT'79 (ed. L. Budach), Akademie-Verlag Berlin, 565-574.

L Lovász (1980a), *Selecting independent lines from a family of lines in a space*, Acta Sci. Math. Szeged **42**, 121-131.

L. Lovász (1980b), *Matroid matching and some applications*, J. Comb. Theory **B 28**, 208-236.

L. Lovász (1980c), *The matroid matching problem*, in: Algebraic Methods in Graph Theory (ed. L. Lovász and V. T. Sós), Coll. Math. Soc. J. Bolyai 25, North–Holland, 495-517.

L. Lovász and M. D. Plummer (1986), *Matching Theory*, Akadémiai Kiadó, Budapest – North-Holland, Amsterdam.

L. Lovász, Y. Yemini (1982), *On generic rigidity in the plane*, SIAM J. Alg. Discr. Methods **1**, 91-98.

J. H. Mason (1977), *Matroids as the study of geometric configurations*, in: Higher Combinatorics (ed. M. Aigner), Reidel, 133-176.

J. H. Mason (1981), *Glueing matroids together: a stude of Dilworth truncations and matroid analogues of exterior and symmetric powers*, in: Algebraic Methods in Graph Theory (ed. L. Lovász and V. T. Sós), Coll. Math. Soc. J. Bolyai **25**, North-Holland, 519-561.

K. Mulmuley, U. Vazirani and V. Vazirani (1987), *Matching is as easy as matrix inversion*, Combinatorica **7**, 105-113.

T. G. Room (1938), *The geometry of determinantal loci*, Cambridge Univ. Press.

J. T. Schwartz (1980), *Fast probabilistic algorithms for verification of polynomial identities*, J. ACM **27**, 701-717.

W. T. Tutte (1947), *The factorization of linear graphs*, J. London Math. Soc. **22**, 107-111.

L. G. Valiant (1979), *The complexity of computing the permanent*, Theor. Comp. Sci., **8**, 189-201.

László Lovász
Department of Computer Science
Eötvös Loránd University
Budapest, H-1088 Hungary