Comment.Math.Univ.Carolin. 32,2 (1991)213–218

Computation of rigidity of order $\frac{n^2}{r}$ for one simple matrix

Pavel Pudlák, Zdeněk Vavřín

Abstract. We shall compute the exact value of rigidity of the triangular matrix with entries 0 and 1.

Keywords: rigidity of matrices, lower bounds to complexity

Classification: 15A03, 68Q15

Let F be an arbitrary field, let M be a square matrix of type n. The rigidity of M is the function depending on $r \in \{0, 1, \dots, n\}$, defined by

$$R_M^F(r) = \min\{|B|, M = A + B, r(A) \leq r\},$$

where $|B|$ denotes the number of nonzero elements in B and $r(A)$ denotes the rank of A. Intuitively, $R_M^F(r)$ is the minimal number of changes in M needed to reduce the rank to a value less or equal to r. The concept of rigidity was introduced J. Valiant [3] in connection with lower bounds to the size of circuits. He showed that a sufficiently large lower bound to the rigidity of a matrix implies that the transformation determined by the matrix cannot be computed by a linear size circuit. It is an open problem to find such matrices. So far only small lower bounds to the rigidity of explicitly given matrices have been proved. Razborov [2] proved an $\Omega(\frac{n^2}{r})$ lower bound to the rigidity of the matrix of the generalized Fourier transform and the inverse matrix of the Vandermonde matrix, Alon [1] proved an $\Omega(\frac{n^2}{r^2})$ for Hadamard matrices.

We shall determine the exact value of the rigidity of the triangular matrix

$$T_n = (\, t_{ij}\,)_{i,j=1}^n, \qquad t_{ij} = \begin{cases} 1, & i \geq j, \\ 0, & i < j. \end{cases}$$

Theorem 1. *Let $r < n$ be given and determine k and Δ by*

$$\begin{aligned} n &= k(2r+1) + r + \Delta = \\ &= r(2k+1) + k + \Delta, \\ & k \geq 0, 1 \leq \Delta \leq 2r+1. \end{aligned} \tag{1}$$

Then

$$R_{T_n}^F(r) = \frac{(n - r + \Delta)(n + r - \Delta + 1)}{2(2r+1)}.$$

Note that for n, r large but r small in comparison with n,

$$R^F_{T_n}(r) \approx \frac{n^2}{4r}.$$

We shall say that

$$M = A + B$$

is a decomposition (of rank r, if $r(A) = r$), $|B|$ is the number of changes, $|b_i|$ is the number of changes in the i-th row, if b_i is the i-th row of B.

If $|B| = R^F_M(r)$, we shall say that the decomposition is optimal.

Speaking of linear dependence of rows of a decomposition we mean linear dependence of the rows of A.

The proof of Theorem 1 is based on the following lemma:

Lemma 1. *Let $r < n$ and let k be given by* (1)*. Then in any decomposition of T_n of rank at most r there is a row containing at least $k+1$ changes.*

We shall also determine the optimal decomposition of T_n.

Theorem 2. *All optimal decompositions of rank r of the matrix T_n have the form* (2), (3) *given in the proof of Theorem 1 below.*

The proof of Theorem 2 is based on the following lemmas:

Lemma 2. *Let n and $r < n$ be given, let k be determined by* (1) *and let an optimal decomposition of T_n be given. Then $k+1$ is the maximum number of changes in a row.*

Lemma 3. *Let an optimal decomposition of T_n be given. Then deleting a row with the maximal number of changes and the corresponding column with the same index leads to an optimal decomposition of T_{n-1}.*

Proofs.

Proof of Lemma 1: Let $T_n = A + B$ be a decomposition of rank r. Let t_j, resp. a_j,b_j be the j-th row of T_n, resp. A, B. Suppose for contradiction that the maximal number of changes in a row is k. Let us take $r+1$ rows with indices belonging to the set

$$S = \{k+1, k+1+1(2k+1), k+1+2(2k+1), \dots, k+1+r(2k+1)\}.$$

These rows must be linearly dependent, i.e.

$$\sum_{j \in S'} \alpha_j a_j = 0$$

for some $0 \neq S' \subset S, |S'| = s' \leq r+1, \quad \alpha_j \neq 0$ for all $j \in S'$. Then

$$\sum_{S'} \alpha_j t_j = \sum_{S'} \alpha_j b_j$$

and, consequently,

$$|\sum_{S'} \alpha_j t_j| \leq \sum_{S'} |\alpha_j b_j| \leq s'k.$$

Denote $N = |\sum_{S'} \alpha_j t_j|$. The vector $\sum_{S'} \alpha_j t_j$ has the form

$$(c_1, \dots, c_1, c_2, \dots, c_2, \dots, c_{s'}, \dots, c_{s'}, 0, \dots, 0),$$

where the length of each constant section is at least $2k+1$ except for the first section $c_1, \dots, c_1$ which can have the length $k+1$. Observe that the last section $c_{s'}, \dots, c_{s'}$ cannot consist of zeros and that it is not possible that two consecutive sections consist of zeros. It follows that:

1. With exception of the case when the first section $c_1, \dots, c_1$ consists of nonzero elements and has length $k+1$,

$$N \geq \frac{s'}{2}(2k+1) > s'k,$$

which is a contradiction.

2. In the remaining case,

$$N \geq k+1+\frac{s'-1}{2}(2k+1) = \\ = \frac{2s'k+s'+1}{2} > s'k$$

and the same contradiction appears again. □

Proof of Theorem 1: For $m = n, n-1, \dots, r+1$ let us proceed in the following way:

Having any decomposition $T_m = A+B$ of rank at most r, we find a row containing at least $k+1$ changes ($m = k(2r+1)+r+\Delta$) and reduce the matrices T_m, A, B by deleting this row and the corresponding column with the same index. Thus, we obtain a decomposition of T_{m-1} of rank at most r.

This procedure applied to any decomposition of T_n (of rank at most r) shows that the total number of changes is at least

$$\Delta(k+1)+(2r+1)k+(2r+1)(k-1)+\dots+(2r+1)1 =$$

$$= (2r+1)\frac{k(k+1)}{2}+\Delta(k+1) = \frac{(n-r+\Delta)(n+r-\Delta+1)}{2(2r+1)}$$

(due to (1)).

Now consider the concrete decomposition

$$T_n = A+B \tag{2}$$

such that

(3)

$$B = \begin{pmatrix}
+1 &&&&&&&&&&&&& \\
+1 & +1 &&&&&&&&&&&& \\
\vdots && \ddots &&&&&&&&&&& \\
+1 && \dots & +1 &&&&&&&&&& \\
&&&& 0 & -1 & -1 & \dots & -1 &&&&& \\
&&&&& 0 & -1 && -1 &&&&& \\
&&&&&& \ddots & \ddots & \vdots &&&&& \\
&&&&&&&& -1 &&&&& \\
&&&&&&&& 0 &&&&& \\
&&&&&&&&& \ddots &&&& \\
&&&&&&&&&& +1 &&& \\
&&&&&&&&&& +1 & +1 && \\
&&&&&&&&&& \vdots && \ddots & \\
&&&&&&&&&& +1 && \dots & +1
\end{pmatrix}.$$

This means, B is a block diagonal and the diagonal blocks are alternatively lower triangular, with all entries in the triangular equal to $+1$, and "sharp" upper triangular, with zeros on the diagonal and "-1's" in the upper triangle. The number of diagonal blocks is $2r+1$. We shall speak rather of nonzero triangles (the "-1"-triangles considered without zero diagonals) than of the whole diagonal blocks. Any $2r+1-\Delta$ of the nonzero triangles have dimension k and the remaining Δ triangles have dimension $k+1$.

This form of B ensures that the matrix A has the form of r "steps" and, thus, $r(A) = r$.

Evidently

$$\begin{aligned}
|B| &= (2r+1-\Delta)\frac{k(k+1)}{2} + \Delta\frac{(k+1)(k+2)}{2} = \\
&= \frac{(n-r+\Delta)(n+r-\Delta+1)}{2(2r+1)},
\end{aligned}$$

due to (1). Thus the lower and upper bounds for $R^F_{T_n}(r)$ are determined precisely. $\square$

Note that the precise lower bound is given without any knowledge of the form of the optimal decomposition.

Proof of Lemma 2: Suppose that there is a row containing at least $k+2$ changes. Deleting this row and the column with the same index in all the three matrices T_n, A and B, we obtain a decomposition of T_{n-1} (of rank at most r), the number of changes of which is less than the minimum given by Theorem 1. $\square$

Proof of Lemma 3: It follows directly from Theorem 1 and Lemmas 1 and 2. $\square$

Proof of Theorem 2: We shall proceed by induction on n:

1) $n = 1, r = 0:$

$$B = (+1).$$
$$n = 0(2r+1) + r + 1.$$

B has $\Delta = 1$ nonzero triangle of dimension $k+1 = 1$, $2r+1-\Delta = 0$ nonzero triangles of dimension $k = 0$.

2) $n - 1 \to n$

Let n fulfil (1) and let the i-th row contain $k+1$ changes. The induced decomposition of the $(n-1)$ by $(n-1)$ matrix which arises by deleting the i-th row and column, is an optimal decomposition (Lemma 3) and thus has the form (2), (3). Having this in mind, we can show schematically all the variants of the rows $i_0 - 1$, i_0 and $i_0 + 1$, with the changes in the $(i_0 - 1)$st and $(i_0 + 1)$st rows shown by the signs x:

$$\begin{array}{r ccccccccccccc}
 & 1 & 1 & x & x & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
(i)(a) & 1 & 1 & \underline{1} & \underline{1} & \underline{1} & \underline{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & 1 & 1 & x & x & x & x & x & 0 & 0 & 0 & 0 & 0 & 0
\end{array}$$

$$\begin{array}{r ccccccccccccc}
 & 1 & 1 & 1 & 1 & 1 & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
(b) & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & 1 & 1 & 1 & 1 & 1 & 1 & x & 0 & 0 & 0 & 0 & 0 & 0
\end{array}$$

$$\begin{array}{r ccccccccccccc}
 & 1 & 1 & 1 & 1 & 1 & x & x & x & x & x & 0 & 0 & 0 \\
(c) & 1 & 1 & 1 & 1 & 1 & 1 & \underline{0} & \underline{0} & \underline{0} & \underline{0} & 0 & 0 & 0 \\
 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & x & x & x & 0 & 0 & 0
\end{array}$$

$$\begin{array}{r ccccccccccccc}
 & 1 & 1 & x & x & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
(ii)(a) & 1 & 1 & \underline{1} & \underline{1} & \underline{1} & \underline{1} & \overline{0} & \overline{0} & \overline{0} & \overline{0} & 0 & 0 & 0 \\
 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & x & x & x & 0 & 0 & 0
\end{array}$$

$$\begin{array}{r ccccccccccccc}
 & 1 & 1 & x & x & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
(b) & 1 & 1 & \underline{1} & \underline{1} & \underline{1} & \underline{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & 1 & 1 & 1 & 1 & 1 & 1 & x & x & x & x & 0 & 0 & 0
\end{array}$$

$$\begin{array}{r ccccccccccccc}
 & 1 & x & x & x & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
(c) & 1 & 1 & 1 & 1 & 1 & 1 & \underline{0} & \underline{0} & \underline{0} & \underline{0} & 0 & 0 & 0 \\
 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & x & x & x & 0 & 0 & 0
\end{array}$$

It is evident that the changes of the i-th row shown by underline (resp. overline) are optimal. The situation $(i)(b)$ cannot occur since there are no changes in the i-th row needed. Neither $(i)(a), (c)$ can occur since the i-th row would not be a row with the maximal number of changes. Thus only the variants $(ii)(a), (b), (c)$ remain. The situation $(ii)(b)$ means the increase of an "(+1)-triangle", $(ii)(c)$ means the increase of a "(−1)-triangle" and $(ii)(a)$ enables both of them.

In each case, the form (2), (3) of the decomposition of T_n is kept.

References

[1] Alon N., *On the rigidity of Hadamard matrices*, manuscript.
[2] Razborov A.A., *On rigid matrices* (in Russian), preprint.
[3] Valiant L.G., *Graph-theoretic arguments in low-level complexity*, Proc. Math. Found. Comp. Sci., Springer (1977) 162–176.

Institute of Mathematics, Czechoslovak Academy of Sciences, Žitná 25, 115 67 Praha 1, Czechoslovakia

(*Received* November 13, 1990, *revised* February 13, 1991)