Rigidity of a simple extended lower triangular matrix

Meena Mahajan [a] Jayalal Sarma M.N. [a]

[a] *The Institute of Mathematical Sciences, Chennai 600 113, India.*

Abstract

For the all-ones lower triangular matrices, the upper and lower bounds on rigidity are known to match [13]. In this short note, we apply these techniques to the all-ones extended lower triangular matrices, to obtain upper and lower bounds with a small gap between the two; we show that the rigidity is $\theta(\frac{n^2}{r})$.

Key words: combinatorial problems, computational complexity, matrix rank

For a square matrix over any field, the rigidity function is defined as

$$R_M(r) \stackrel{def}{=} \inf_N \{\text{support}(N) : \text{rank}(M+N) \leq r\}$$

where $\text{support}(N) = \#\{(i,j) \mid N[i,j] \neq 0\}$. The rigidity of a matrix is thus the minimum number of entries that need to be changed to bring down the rank below a given value. A folklore result is that over any field, $R_M(r) \leq (n-r)^2$. The notion of rigidity was introduced by Valiant [16] and was independently proposed by Grigoriev [6].

The main motivation for studying rigidity is that good lower bounds on rigidity give important complexity-theoretic results in various computational models, such as linear algebraic circuits and communication complexity. An important result in this direction, established by Valiant [16], says that if for some $\epsilon > 0$ there exists a $\delta > 0$ such that an $n \times n$ matrix M_n has rigidity $R_{M_n}(\epsilon n) \geq n^{1+\delta}$ over a field $\mathbb{F}$, then the transformation $x \rightarrow Mx$ cannot be computed by linear size logarithmic depth linear circuits. See [2] for a survey of this result. Razborov [14] proves that good lower bounds on rigidity over a finite field imply strong separation results in communication complexity: For an explicit infinite sequence of (0,1)-matrices $\{M_n\}$ over a finite field F, if $R_M(r) \geq$

Email addresses: meena@imsc.res.in (Meena Mahajan), jayalal@imsc.res.in (Jayalal Sarma M.N.).

$\frac{n^2}{2^{(\log r)^{o(1)}}}$ for some $r \geq 2^{(\log \log n)^{\omega(1)}}$, then there is an explicit language $L_M \notin \mathsf{PH}^{cc}$, where PH^{cc} is the analog of PH in the communication complexity setting. See [3,8] for surveys.

However, obtaining explicit bounds on the rigidity of special family of matrices is surprisingly elusive, and thus has received a lot of attention [4,5,8,9,12,15] Recently, Lokam [10] proved the first unconditional super-linear (in fact, quadratic) lower bound for rigidity for an explicit family of matrices (over $\mathbb{C}$). However, similar results are not known for $\mathbb{Q}$ or for finite fields $\mathbb{F}_q$ for any $q \geq 2$. The rareness of matching, or even close, lower and upper bounds correlates well with the lack of upper bounds on the computational version of rigidity [11]. Due to the difficulty in obtaining non-trivial bounds, the exploration of combinatorial techniques that may lead to such bounds becomes interesting.

A rare case where a closed-form expression has been obtained for rigidity is for the all-ones lower triangular matrices T_n. By all-ones we mean that any entry permitted to be non-zero is one. That is, T_n is the matrix of dimension n with $j \leq i \implies T_n[i,j] = 1$, $j > i \implies T_n[i,j] = 0$. It is shown in [13] that over any field,

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

where $n = 2rk + r + k + \Delta$ for $k \geq 0$, $1 \leq \Delta \leq 2r+1$.

In this note we consider all-ones extended lower triangular (*elt*) matrices. In an elt matrix M, the first diagonal above the main diagonal can be non-zero, but all other elements above the diagonal must be 0. (That is, $M[i,j] \neq 0 \implies j \leq i+1$.) It is worthwhile noting that elt matrices can capture a lot of information: it is known that determinant/permanent computation of elt matrices is as hard as the general case, see [1,7]. An all-ones elt matrix EL_n of dimension n is an elt matrix satisfying $j \leq i+1 \implies M[i,j] = 1$, and has rank $n-1$. Even with this small extension beyond T_n, we are unable to obtain a closed-form expression for rigidity. However, applying a slight modification of the proof of [13], we show lower and upper bounds differing by an additive factor of roughly n/r.

What we find interesting is that though the modification to the matrix family considered in [13] is extremely slight, we are not able to match the lower and upper bounds. Nor does the proof indicate indicate where the slack is: which of the bounds is less likely to be tight. We believe that exploring such combinatorics can help in improving lower bounds.

Theorem 1 *Given n and r such that $r \leq n-2$, define the following quantities: $k = \left\lfloor \frac{n-r-1}{2r+1} \right\rfloor$; $\delta = n - r - k(2r+1)$; $\Gamma = \frac{(k+1)}{2}(n-r+\delta)$; $\ell = \left\lfloor \frac{n-r}{2r+1} \right\rfloor$. Now, over any field,*

(1) If $n \leq 3r$, then $R_{EL_n}(r) = n - r - 1$.
(2) If $n \geq 3r + 1$, then $\Gamma \leq R_{EL_n}(r) \leq \Gamma + \ell - 1$.

Asymptotically, $R_{EL_n}(r) \in \theta(\frac{n^2}{r})$.

Our upper bound proof directly mimics that of [13]. Our lower bound proof mimics that of [13] to obtain one bound, and then further tightens it when $n = 3r + 1$. A combinatorial argument that can provide a similar tightening at all $n = r + k(2r + 1)$ would completely close the gap between the upper and lower bounds, but we do not see how to obtain this.

Upper Bound: Define $\tau = n - r - (2r + 1)\ell$. We will show that

$$R_{EL_n}(r) \leq \frac{(\ell + 1)}{2}(n - r + \tau) + \ell - 1$$

This immediately yields the claimed upper bound when $n \leq 3r$, since $l = 0$ in this case. When $n \geq 3r + 1$, consider two cases:

Case 1: $\ell = k$. Then $\tau = \delta$ and so $\Gamma = \frac{(k+1)}{2}(n - r + \delta) = \frac{(\ell+1)}{2}(n - r + \tau)$.
Case 2: $\ell = k + 1$. Then $\tau = 0$, $\delta = 2r + 1$, and $n = 2r\ell + r + \ell = \delta\ell + r$. So

$$\begin{aligned}
\Gamma &= \tfrac{(k+1)}{2}(n - r + \delta) \\
&= \tfrac{(\ell+1)}{2}(n - r + \delta) - \tfrac{1}{2}(n - r + \delta) \\
&= \tfrac{(\ell+1)}{2}(n - r + \tau) + \tfrac{(\ell+1)}{2}(\delta) - \tfrac{1}{2}(\delta\ell + \delta) \\
&= \tfrac{(\ell+1)}{2}(n - r + \tau)
\end{aligned}$$

Thus in either case, the upper bound holds.

Now we establish the upper bound in terms of ℓ and τ.

We start with the matrix EL_n, which has rank $n - 1$. In particular, the first $n - 1$ rows are linearly independent. Thus to bring the rank down to r or less, at most r of these rows can remain unchanged. We can view the changes as being made sequentially, and track the ranks of matrices along the way, beginning with $n - 1$ and ending with $r' \leq r$. Since changing a single entry of any matrix changes the rank by at most 1, the optimal way to reduce rank will have $r' = r$. Our upper bound assumes that the r linearly independent rows in the final matrix are in fact unchanged rows of EL_n. (It is possible that a better upper bound exists, that does not use this assumption. But we were unable to derive one, and we think it is unlikely.)

We identify r linearly independent rows $R_{j_1}, \ldots R_{j_r}$ which we will keep intact, so the rank of the resulting matrix is still at least r. We will change each of the other rows to one of these rows by changing some entries. But to minimize

the number of entries changed, we adopt the following general strategy used in [13] for T_n. Let n_0 be the first set of rows which we will explicitly make zero. Similarly, n_{2i-1} is the number of rows just above R_{j_i} which are changed to R_{j_i} by changing the appropriate 0s to 1s, and n_{2i} is the number of rows below the row R_{j_i} which are changed to R_{j_i} by changing the appropriate 1s to 0s. Now the total number of changes is a function of these n_i's, as described below, and the natural idea for minimizing the number of changes be to make the contribution of each n_i roughly equal. In particular, this evenly spaces out the rows to be preserved. In detail:

$$\begin{aligned}
\#\text{ of changes in } n_0\text{-block} &= \textstyle\sum_{t=1}^{n_0}(t+1) &&= \tfrac{n_0(n_0+3)}{2} \\
\#\text{ of changes in } n_{2i-1}\text{-block} &= \textstyle\sum_{t=1}^{n_{2i-1}} t &&= \tfrac{n_{2i-1}(n_{2i-1}+1)}{2} \\
\#\text{ of changes in } n_{2i}\text{-block} &= \textstyle\sum_{t=1}^{n_{2i}} t &&= \tfrac{n_{2i}(n_{2i}+1)}{2}) \\
\#\text{ of changes in } n_{2r}\text{-block} &= n_{2r} - 1 + \textstyle\sum_{t=1}^{n_{2r}-1} t &&= \tfrac{(n_{2r}+2)(n_{2r}-1)}{2}
\end{aligned}$$

and we want to minimize the total number of changes.

Intuitively, the optimal choice to achieve this should be to make all the n_i's equal, except n_0 which should be one less. This is because for each $i \notin \{0, r\}$, some row needs n_i changes, and for the extreme blocks the maximum change needed is $n_0 + 1$ and $n_{2r} - 1$ respectively, due to the elt structure. We just try to minimize this maximum change per block. While we cannot show that this strategy is indeed optimal, we use it to obtain our upper bound. When $\tau = 2r$; we set $n_0 = \ell$, $n_i = \ell + 1$ for $i \geq 1$. When $\tau < 2r$, some of the blocks other than n_0 will also have size ℓ rather than $\ell + 1$. Thus the last τ blocks will have size $\ell + 1$, and the first $(2r + 1 - \tau)$ will be of size ℓ. Thus,

$$\begin{aligned}
\text{Total number of changes} &= \tfrac{\ell(\ell+1)}{2}(2r+1) + \ell - 1 + (\ell+1)\tau \\
&= \tfrac{(\ell+1)}{2}\left[n - r + \tau\right] + \ell - 1
\end{aligned}$$

Lower Bound: The lower bound when $n \leq 3r$ is easy to see: for decreasing the rank of any matrix, at least one entry has to be changed.

The lower bound when $n \geq 3r + 1$ is a little more tricky. In [13], the corresponding lower bound for lower triangular matrices T_n is obtained by first showing that if $T_n + B_n$ has rank bounded by r, then some row of B_n has at least $k + 1$ non-zero entries. Deleting this row and column yields $T_{n-1} + B_{n-1}$ also of rank bounded by r. Applying this argument repeatedly, the total number of changes is bounded by a certain sum, yielding the result. Our proof follows the same outline, and differs in essentially two places: (a) Deleting any row i and column $i + 1$ of EL_n yields EL_{n-1}. (b) At $n = 3r + 1$ a tighter bound is possible.

Lemma 2 below shows that some row has lots of changes. Lemma 3 shows that when $n = 3r + 1$, at least $2r + 1$ changes are needed. Using these lemmas we can establish the lower bound. When $n \geq 3r + 2$, apply Lemma 2 repeatedly, eliminating one dense row each time, preserving the ELT structure, until n comes down to $3r + 1$. Now Lemma 3 says that $2r + 1$ more changes are necessary. Thus the total number of changes is at least $\delta(k+1) + (2r+1)k + (2r+1)(k-1) + \ldots + (2r+1)3 + (2r+1)2 + (2r+1) = \frac{(k+1)}{2}(n - r + \delta)$, giving the lower bound.

We now proceed to state and prove the lemmas.

Note that k and δ are functions of n and r. If we fix r and vary n, then $k(2r+1) + r + 1 \leq n \leq k(2r+1) + 3r + 1$. The value of k remains unchanged for $2r + 1$ successive values of n, during which δ ranges over 1 to $2r + 1$.

If $r + 2 \leq n \leq 3r + 1$, there is a row with at least 1 change. Now, for a general n, assuming that $EL_n + B_n$ has rank bounded by r, repeated applications of the following lemma show that B_n has reasonable row-wise density.

Lemma 2 *Let $r \leq n-2$, and let B_n be a matrix such that rank$(EL_n+B_n) \leq r$. Then some row in B_n, other than the last row, has at least $(k+1)$ non-zeroes.*

Proof: This proof is similar to that in [13]. Assume to the contrary that every row of B_n (possibly other than row n) has fewer non-zeroes than required. Let $A_n = EL_n + B_n$. The idea is to choose a set S of $r+1$ rows which exclude row n (and hence are linearly independent in EL_n), and are linearly dependent in A_n, and to then show that one of the rows from S in B_n has many non-zeroes. We choose S as follows

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

Since rank$(A_n) \leq r$, the rows indexed by S are linearly dependent in A_n; hence for some non-empty subset S' of S, we have non-zero α_j's satisfying

$$\sum_{j \in S'} \alpha_j a_j = 0 \qquad \text{and hence} \qquad \sum_{j \in S'} \alpha_j l_j = -\sum_{j \in S'} \alpha_j b_j$$

Here a_j, l_j, b_j refer to the jth row vectors of A_n, EL_n and B_n respectively. By our assumption, the vector on the right-hand-side RHS has at most $s'k$ non-zero entries ($s' = |S'|$). Exploiting the special structure of the matrix, we show that the left-hand-side LHS has more non-zero terms than the RHS and get a contradiction. Due to the structure of EL_n, the LHS is of the form $(c_1, c_1 \ldots c_1, c_2, c_2 \ldots c_2, \ldots c_{s'} \ldots c_{s'}, 0 \ldots 0)$. Each c_i section is of size at least $2k + 1$, except the c_1 section, which has size at least $k + 1$. Two consecutive sections cannot be zeros since $\alpha_j \neq 0$ for all j. And the last section necessarily has $c_{s'} \neq 0$.

Case 1: $s' = 2t+1$ for some t. Now consider the LHS. There are at least $t+1$ blocks of non-zeroes. At most one of these (the first) is of size $k+1$; all the rest have size $2k+1$. Hence the number of non-zero elements on the LHS is at least $(2k+1)t + k + 1 = (2t+1)k + t + 1 > s'k$.

Case 2: $s' = 2t$ with $t \neq 0$. There are at least t blocks of non-zeros. Furthermore, if the first block is a non-zero block, then in fact there must be $t+1$ non-zero blocks. Thus there are at least t blocks of non-zeros of size $2k+1$. Thus the number of non-zeroes on the LHS is at least $t(2k+1) > s'k$. □

Lemma 3 *$R_{EL_n}(r) \geq 2r+1$ when $n = 3r+1$.*

Proof: Suppose not; assume that $2r$ changes suffice to bring the rank of $E = EL_{3r+1}$ to r or less. That is, there is a matrix B with at most $2r$ non-zero entries such that $A = B + E$ has rank r or less. Since there are $3r+1$ rows, at least $r+1$ of them are left unchanged. These must be linearly dependent to achieve $\text{rank}(A) \leq r$, so they must include rows $n-1$ and n of E (all other rows of E are linearly independent) and exactly $r-1$ other rows.

Let S be the set of indices of preserved rows; $|S| = r+1$ and $\{n-1, n\} \subseteq S$. Let $S' = [n] \setminus S$; then $|S'| = 2r$. Each row of B in S' has at least one non-zero. But since there are only $2r$ non-zeroes overall, each row of B in S' has, in fact, exactly one non-zero.

For each $i \in S'$, row i is dependent on S and on $S \setminus \{n\}$. (With a single change per row, no row cannot be zeroed out.) Let $U = S \setminus \{n\} \cup \{i\}$. Then, as in the proof of Lemma 2, there exists $U' \subseteq U$: $i \in U'$, and for each $u \in U'$, $\exists \alpha_u \neq 0$ such that

$$\sum_{u \in U'} \alpha_u e_u = -\sum_{u \in U'} \alpha_u b_u.$$

The RHS has a single non-zero in row i since rows of B from S are zero. The LHS is of the form is of the form $(c_1, c_1 \ldots c_1, c_2, c_2 \ldots c_2, \ldots c_{u'} \ldots c_{u'}, 0 \ldots 0)$ where $c_{u'} \neq 0$. To get just one non-zero on the LHS, $c_{u'}$ must be a block of size 1, and all other c_j's must be zero. Thus $\exists k : U' = \{k-1, k\}$, and $\alpha_k + \alpha_{k-1} = 0$. But, we know that α_i must be non-zero, since this is the row we are expressing as a combination of rows in S. Hence U' must be either $\{i-1, i\}$ or $\{i, i+1\}$. Thus, for each row $i \in S'$, either row $i-1$ or row $i+1$ is in S. So rows in S can be separated by at most 2 rows of S'. Since rows $n = 3r+1$ and $n-1 = 3r$ are in S, the 3rd last row of S is at least $3r-3$, the 4th last row of S is at least $3r-6$, and so on; the first row of S is at least row 3. But then row 1 does not have a neighbouring row in S, a contradiction. □

Acknowledgments

We gratefully acknowledge the constructive comments from the anonymous referees, that helped us to improve the readability of this note.

References

[1] E. Allender, V. Arvind, and M. Mahajan. Arithmetic complexity, Kleene closure, and formal power series. *Theory Comput. Syst.*, 36(4):303–328, 2003.

[2] M. Cheraghchi. On matrix rigidity and the complexity of linear forms. Technical Report TR05-70, ECCC, 2005.

[3] B. Codenotti. Matrix rigidity. *Linear Algebra and its Applications*, 304(1–3):181–192, 2000.

[4] B. Codenotti, P. Pudlák, and G. Resta. Some structural properties of low-rank matrices related to computational complexity. *Theoretical Computer Science*, 235(1):89–107, 2000.

[5] J. Friedman. A Note on matrix rigidity. *Combinatorica*, 13(2):235–239, 1993.

[6] D. Y. Grigoriev. Using the notions of seperability and independence for proving the lower bounds on the circuit complexity. Notes of the Leningrad branch of the Steklov Mathematical Institute, Nauka, 1976. in Russian.

[7] L. Li. Formal power series: An algebraic approach to the GapP and #P functions. In *Proc. 7th Structure in Complexity Theory Conference*, pages 144–154, 1992.

[8] S. V. Lokam. Spectral methods for matrix rigidity with applications to size-depth tradeoffs and communication complexity. In *Proc. 36th Annual IEEE Symposium on Foundations of Computer Science*, pages 6 – 15, 1995. JCSS 63(3):449-473, 2001.

[9] S. V. Lokam. Note on rigidity of Vandermonde matrices. *Theoretical Computer Science*, 237(1-2):477–483, 2000.

[10] S. V. Lokam. Quadratic lower bounds on matrix rigidity. In *Proc. Theory and Applications of Models of Computation TAMC, LNCS 3959*, pages 295–307, 2006.

[11] M. Mahajan and J. Sarma M.N. On the Complexity of Matrix Rank and Rigidity. In *Proceedings of 2nd International Computer Science Symposium in Russia (CSR)*, volume 4649 of *Lecture Notes in Computer Science*, pages 269–280, 2007. Preliminary Techreport appeared as ECCC-TR06-100, Aug 2006.

[12] P. Pudlak and V. Rodl. Some combinatorial-algebraic problems from complexity theory. *Discrete Mathematics*, 136:253–279, 1994.

[13] P. Pudlak and Z. Vavrin. Computation of rigidity of order n^2/r for one simple matrix. *Comment. Nath. Univ. Carolinae.*, 32(2):213–218, 1991.

[14] A. A. Razborov. On rigid matrices. manuscript in russian, 1989.

[15] D. A. Spielman, M. A. Shokrollahi, and V. Stemann. A remark on Matrix Rigidity. *Information Processing Letters*, 64(6):283–285, 1997.

[16] L. G. Valiant. Graph theoretic arguments in low-level complexity. In *Proc. 6th MFCS*, volume 53 of *LNCS*, pages 162–176. Springer, Berlin, 1977.