Mathematical Notes, Vol. 63, No. 4, 1998

Improved Lower Bounds on the Rigidity of Hadamard Matrices

B. S. Kashin and A. A. Razborov

UDC 519.142, 517.984.4

ABSTRACT. We write $f = \Omega(g)$ if $f(x) \geq cg(x)$ with some positive constant c for all x from the domain of functions f and g. We show that at least $\Omega(n^2/r)$ entries must be changed in an arbitrary (generalized) Hadamard matrix in order to reduce its rank below r. This improves the previously known bound $\Omega(n^2/r^2)$. If we additionally know that the changes are bounded above in absolute value by some number $\theta \geq n/r$, then the number of these entries is bounded below by $\Omega(n^3/(r\theta^2))$, which improves upon the previously known bound $\Omega(n^2/\theta^2)$.

KEY WORDS: rigidity of matrices, Hadamard matrices, spectral methods, Hoffman–Wielandt inequality.

§1. Introduction

Let A be a matrix over a field k. By $R_A^k(r)$ we denote the *rigidity function of* A, defined to be the minimal number of entries that must be changed in A in order to reduce its rank below r. This notion was introduced by Valiant [1, 2]; independently a similar notion was suggested by Grigor'ev [3].

The main reason for introducing and studying this concept is that rigid matrices are known to be hard with respect to several important computational models for which no lower bounds are currently available. These models include, for example, linear algebraic circuits [2, 4] and computations with bounded alternation in communication complexity [5, 6]. In particular, any *explicit* example of an sufficiently rigid matrix would immediately give rise to the corresponding example of a computational problem which is hard for these models. That would be a major breakthrough in the area.

Despite numerous efforts, the best known lower bounds for $R_A^k(r)$ attained for specific $n \times n$ matrices A are only of the form $\Omega(n^2/(r\log(n/r)))$ for finite field k (Friedman [7]) and $\Omega(n^2/r)$ for the case in which k is infinite ($r \leq n/2$). The easiest way to prove the latter bound was independently observed by Grigor'ev and Nisan (unpublished): every *totally nonsingular* matrix A (i.e., a matrix in which all square submatrices are nonsingular) satisfies $R_A^k(r) \geq \Omega(n^2/r)$ (k is arbitrary and $r \leq n/2$). Other methods for obtaining the same bound $\Omega(n^2/r)$ applicable to various classes of matrices were proposed in [5, 8–10]; some of them are also valid for finite fields.

One class of matrices that seem to be good candidates for having large rigidity over $\mathbb{R}$ is that of Hadamard matrices. They are perfectly suitable for study by spectral methods, and the latter have already established themselves as an extremely useful tool for solving similar problems in complexity theory (see [11, 12] for typical examples). Pudlák, Razborov and Savický [13] established the bound $R_H^{\mathbb{R}}(r) \geq \Omega(n^2/(r^3\log r))$, where H is an arbitrary Hadamard matrix, and Alon [14] improved this to $R_H^{\mathbb{R}}(r) \geq \Omega(n^2/r^2)$. Motivated by the above-mentioned application to communication complexity, Lokam [6] introduced a restricted version of rigidity, $R_A^{\mathbb{C}}(r,\theta)$, by additionally requiring that the *absolute values* of the change be bounded by θ. In particular, he was able to show that $R_H^{\mathbb{C}}(n/2,\theta) \geq \Omega(n^2/\theta^2)$ for any (generalized) Hadamard matrix H.

In this note we present some improvements of these results. Namely, for an arbitrary (generalized) Hadamard matrix H and any $r \leq n/2$ we prove that $R_H^{\mathbb{C}}(r) \geq \Omega(n^2/r)$, and if θ is an additional parameter satisfying $\theta \geq n/r$, then $R_H^{\mathbb{C}}(r,\theta) \geq \Omega(n^3/(r\theta^2))$. Our bounds are too weak to give any nontrivial corollaries in complexity theory, and they do not penetrate through the n^2/r barrier. The main purpose of this note is to draw the experts' attention once again to the use of spectral methods in the area, since we strongly feel that their potential is far from being exhausted.

Translated from *Matematicheskie Zametki*, Vol. 63, No. 4, pp. 535–540, April, 1998.
Original article submitted December 1, 1997.

0001-4346/98/6334-0471 $20.00

§2. Matrix rigidity

Definition 1 [1, 2, 6]. For a matrix A over some field, let $\mathrm{wt}(A)$ be the number of nonzero entries of A. The *rigidity function* $R_A^k(r)$ of A is defined by

$$R_A^k(r) \rightleftharpoons \min_B\{\mathrm{wt}(A-B) \mid \mathrm{rk}(B) \le r\},$$

where B ranges over all matrices of the same size as A. If $k = \mathbb{C}$ and θ is a positive real, we also let

$$R_A^{\mathbb{C}}(r,\theta) \rightleftharpoons \min_B\{\mathrm{wt}(A-B) \mid \mathrm{rk}(B) \le r,\ |a_{ij}-b_{ij}| \le \theta\ \ \forall i,j\}. \tag{1}$$

Remark 1. Lokam [6] used the restriction $|b_{ij}| \le \theta$ instead of $|a_{ij}-b_{ij}| \le \theta$ in his definition of $R_A^{\mathbb{C}}(r,\theta)$. However, it seems to be more reasonable to bound the ℓ_∞-norm of the *changes* rather than of their result. In particular, with this definition one can also say something nontrivial in the range $\theta \ll 1$ (see Proposition 1 below).

Definition 2. An $n \times n$ complex matrix H is called a *generalized Hadamard matrix* if $|h_{ij}| = 1$ for all i,j and $HH^* = nI_n$, where H^* is the adjoint of H and I_n is the $n \times n$ identity matrix.

Proposition 1. *For any $n \times n$ generalized Hadamard matrix H and any $r \le n/2$,*

(a) $R_H^{\mathbb{C}}(r) \ge \Omega(n^2/r^2)$ *(see* [14, 6]*),*
(b) $R_H^{\mathbb{C}}(n/2,\theta) \ge \Omega(n^2/\theta^2)$, *where $\theta > 0$ is an arbitrary parameter (see* [6]*),*
(c) $R_H^{\mathbb{C}}(n/2,\theta) \ge \Omega(n^2/\theta)$ *provided that $\theta \le n/r$ (see* [6]*).*

Remark 2. Strictly speaking, Proposition 1, c), is stated in [6] for an even more restricted version of rigidity $R_A^+(r,\theta)$ obtained by adding the extra condition $|b_{ij}| \ge 1$ to (1). An easy inspection of Lokam's proof, however, reveals that this condition is redundant.

In this note we prove the following.

Theorem. *For any $n \times n$ generalized Hadamard matrix H and any $r \le n/2$,*

(a) $R_H^{\mathbb{C}}(r) \ge \Omega(n^2/r)$,
(b) $R_H^{\mathbb{C}}(r,\theta) \ge \Omega(n^3/r\theta^2)$ *provided that $\theta \ge n/r$.*

Part (b) of the theorem improves Proposition 1 by a factor of n/r in the range $\theta \ge n/r$. Both the statement and the proof can be also viewed as a "continuous extension" of Proposition 1 into that range.

§3. Matrix spectra

The *Frobenius norm* $\|A\|_F$ of a complex matrix A is defined by

$$\|A\|_F \rightleftharpoons \left(\sum_{i,j} |a_{ij}|^2\right)^{1/2}.$$

Let A be an $n \times n$ real symmetric matrix, and let $\lambda_1(A) \ge \cdots \ge \lambda_n(A)$ be its (real) eigenvalues. Then

$$\mathrm{Tr}(A) = \lambda_1(A) + \cdots + \lambda_n(A) \tag{2}$$

and

$$\|A\|_F^2 = \lambda_1^2(A) + \cdots + \lambda_n^2(A). \tag{3}$$

Let $r = \mathrm{rk}(A)$, so that exactly r eigenvalues of $\lambda_1(A), \ldots, \lambda_n(A)$ are nonzero. By Cauchy's inequality, (2) and (3) imply $\mathrm{Tr}(A)^2 \le \|A\|_F^2 \cdot r$. Thus, we have proved the following assertion.

Lemma 1. *For every real symmetric matrix A,*

$$\mathrm{rk}(A) \geq \frac{\mathrm{Tr}(A)^2}{\|A\|_F^2}.$$

We also recall the Hoffman–Wielandt inequality. Let $\sigma_i(A) \rightleftharpoons \sqrt{\lambda_i(AA^*)}$ be the *ith singular value* of a complex matrix A.

Proposition 2 [15; 16, §8.3]. *For any pair A, B of $n \times n$ complex matrices,*

$$\sum_{i=1}^{n} \bigl(\sigma_i(A) - \sigma_i(B)\bigr)^2 \leq \|A - B\|_F^2.$$

§4. Proof of the theorem

(a) Just as in the previous proofs [13, 14, 6], our strategy is to show that submatrices of any generalized Hadamard matrix are of sufficiently high rank (at least, on the average), so that the argument by Grigor'ev and Nisan for totally nonsingular matrices still can be carried through.

In fact, there is an abundant literature in functional analysis (e.g., see [17–20]) dealing with the following general question: How orthogonal are random submatrices of an orthogonal matrix? Since "sufficiently orthogonal" matrices are certainly nonsingular, we might directly apply the results from [19, 20]: this would yield the bound $R_H^{\mathbb{C}}(r) \geq \Omega(n^2/(r \log n))$. On the other hand, we need something much weaker than provided by the subtle machinery from [19, 20]. So, we replace it by the following simple lemma, which also allows us to get rid of the logarithmic factor in the denominator.

Throughout the paper we use the math boldface to denote random objects.

Lemma 2. *Let $q \leq n$, and let A be $q \times n$ complex matrix such that $|a_{ij}| = 1$ for all i, j and $AA^* = nI_q$. Let $\boldsymbol{B}$ be a randomly chosen $q \times q$ submatrix of A. Then for any r we have*

$$\mathsf{P}[\mathrm{rk}(\boldsymbol{B}) \leq r] \leq \frac{2r}{q}.$$

Proof. Denote $\boldsymbol{BB}^*$ by $\boldsymbol{C}$. Then $\boldsymbol{C}$ is a (positive definite) real symmetric $q \times q$ matrix that has all entries on the main diagonal equal to q (thus, $\mathrm{Tr}(\boldsymbol{C}) = q^2$) and satisfies $\mathrm{rk}(\boldsymbol{C}) \leq \mathrm{rk}(\boldsymbol{B})$. Therefore, by Lemma 1 (applied to $A := \boldsymbol{C}$), we have

$$\mathrm{rk}(\boldsymbol{B}) \leq r \implies \|\boldsymbol{C}\|_F^2 \geq \frac{q^4}{r}. \tag{4}$$

On the other hand, by Chebyshev's inequality,

$$\mathsf{P}\left[\|\boldsymbol{C}\|_F^2 \geq \frac{q^4}{r}\right] \leq \frac{r}{q^4} \cdot \mathsf{E}\bigl[\|\boldsymbol{C}\|_F^2\bigr]. \tag{5}$$

Let

$$\boldsymbol{\xi}_j \rightleftharpoons \begin{cases} 1 & \text{if the } j\text{th column is present in } \boldsymbol{B} \\ 0 & \text{otherwise;} \end{cases}$$

then $(\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_n)$ is uniformly distributed on the set of all vectors in $\{0,1\}^n$ that have exactly q ones, and $\boldsymbol{c}_{i_1 i_2} = \sum_{j=1}^{n} a_{i_1 j} a_{i_2 j} \boldsymbol{\xi}_j$. Hence

$$\|\boldsymbol{C}\|_F^2 = \sum_{i_1, i_2} (\boldsymbol{c}_{i_1 i_2} \boldsymbol{c}^*_{i_1 i_2}) = \sum_{i_1, i_2} \sum_{j_1, j_2} (a_{i_1 j_1} a_{i_2 j_1} a^*_{i_1 j_2} a^*_{i_2 j_2} \boldsymbol{\xi}_{j_1} \boldsymbol{\xi}_{j_2}) = \sum_{j_1, j_2} \left(\sum_{i_1, i_2} a_{i_1 j_1} a_{i_2 j_1} a^*_{i_1 j_2} a^*_{i_2 j_2} \right) \boldsymbol{\xi}_{j_1} \boldsymbol{\xi}_{j_2}.$$

Now we have

$$\mathsf{E}[\xi_{j_1}\xi_{j_2}] = \begin{cases} \dfrac{q}{n} & \text{if } j_1 = j_2 \\ \dfrac{q(q-1)}{n(n-1)} & \text{if } j_1 \neq j_2. \end{cases}$$

Therefore,

$$\begin{aligned}\mathsf{E}[\|C\|_F^2] &= \frac{q(q-1)}{n(n-1)} \sum_{j_1,j_2} \sum_{i_1,i_2} (a_{i_1 j_1} a_{i_2 j_1} a^*_{i_1 j_2} a^*_{i_2 j_2}) + \left(\frac{q}{n} - \frac{q(q-1)}{n(n-1)}\right) \sum_{j} \sum_{i_1,i_2} (a_{i_1 j} a_{i_2 j} a^*_{i_1 j} a^*_{i_2 j}) \\ &= \frac{q(q-1)}{n(n-1)} \|AA^*\|_F^2 + \left(\frac{q}{n} - \frac{q(q-1)}{n(n-1)}\right) nq^2 = q^2\left(q + \frac{q-1}{n-1}(n-q)\right) \le 2q^3. \end{aligned} \tag{6}$$

Now Lemma 2 readily follows from (4)–(6).

Corollary. *Let H be an $n \times n$ generalized Hadamard matrix, and $\boldsymbol{H}_0$ be a random $q \times q$ submatrix of H. Then* $\mathsf{E}[\mathrm{rk}(\boldsymbol{H}_0)] \ge q/8$.

Proof. The matrix $\boldsymbol{H}_0$ can be constructed in two steps: first we pick q rows at random, and then we pick q columns. Since the $q \times n$ matrix $\boldsymbol{A}$ obtained at the first step always satisfies the assumptions of Lemma 2, it follows that $\mathsf{P}[\mathrm{rk}(\boldsymbol{H}_0) \le q/4 \mid \boldsymbol{H}_0$ has rows $i_1, \ldots, i_q] \le 1/2$ for every particular choice of rows $1 \le i_1 < \cdots < i_q \le n$. Hence

$$\mathsf{P}[\mathrm{rk}(\boldsymbol{H}_0) \le q/4] \le 1/2, \qquad \mathsf{E}[\mathrm{rk}(\boldsymbol{H}_0)] \ge q/4 \cdot \mathsf{P}[\mathrm{rk}(\boldsymbol{H}_0) \ge q/4] \ge q/8.$$

Now we are in position to complete the proof of the Theorem. Namely, let H be an $n \times n$ generalized Hadamard matrix and $r \le n/2$. Since the bound $R^{\mathbb{C}}_H(n/2) \ge n/2$ is trivial, we can assume without loss of generality that $r \le n/16$. Let us choose a matrix A such that $\mathrm{rk}(H - A) \le r$. We set $q = 16r$ and pick a $q \times q$ submatrix $\boldsymbol{H}_0$ of H at random. Let $\boldsymbol{A}_0$ be the corresponding submatrix of A; then

$$\mathsf{E}[\mathrm{rk}(\boldsymbol{H}_0)] \le \mathsf{E}[\mathrm{rk}(\boldsymbol{H}_0 - \boldsymbol{A}_0)] + \mathsf{E}[\mathrm{rk}(\boldsymbol{A}_0)] \le r + \mathsf{E}[\mathrm{wt}(\boldsymbol{A}_0)] = r + \frac{q^2}{n^2}\,\mathrm{wt}(A).$$

On the other hand, $\mathsf{E}[\mathrm{rk}(\boldsymbol{H}_0)] \ge 2r$ by the corollary of Lemma 2. Combining these two inequalities, we get $\mathrm{wt}(A) \ge rn^2/q^2 = \Omega(n^2/r)$ which completes the proof of (a).

(b) Proposition 1, (c), was proved in [6] by applying the Hoffman–Wielandt inequality to the pair of matrices H, $\frac{1}{\theta}B$. We extend this to the range $\theta \ge n/r$ simply by varying the coefficient of B.

Namely, assume, as before, that H is an $n \times n$ generalized Hadamard matrix and $r \le n/2$. Let A be a matrix such that $\mathrm{rk}(H - A) \le r$ and $|a_{ij}| \le \theta$ for all i, j, where $\theta \ge n/r$ is another parameter. Applying Proposition 2 to the pair H, $\frac{r}{n}(H - A)$, we conclude by analogy with [6] that

$$\left\| H - \frac{r}{n}(H - A) \right\|_F^2 \ge n(n - r). \tag{7}$$

On the other hand,

$$H - \frac{r}{n}(H - A) = \left(1 - \frac{r}{n}\right) H + \frac{r}{n} A.$$

Hence, this matrix has at most $\mathrm{wt}(A)$ entries with absolute values bounded by $1 + r\theta/n$, whereas all other entries have absolute values $1 - r/n$. This implies the bound

$$\left\| H - \frac{r}{n}(H - A) \right\|_F^2 \le \mathrm{wt}(A)\left(1 + \frac{r\theta}{n}\right)^2 + \left(1 - \frac{r}{n}\right)^2 n^2. \tag{8}$$

By combining (7) and (8), we obtain

$$\mathrm{wt}(A)\left(1+\frac{r\theta}{n}\right)^2 \geq r(n-r).$$

Since $r \leq n/2$ and $\theta \geq n/r$, the desired bound $\mathrm{wt}(A) \geq \Omega(n^3/(r\theta^2))$ follows. This completes the proof of (b).

The research of the first author was supported by the Russian Foundation for Basic Research under grants No. 96-01-00094 and No. 96-15-96102 and by the INTAS Foundation under grant No. 93-1376. The research of the second author was supported by the Russian Foundation for Basic Research under grants No. 96-01-01222 and No. 96-15-96090.

References

1. L. G. Valiant, *Some Conjectures Relating to Superlinear Complexity Bounds*, Tech. Report No. 85, Univ. of Leeds (1976).
2. L. G. Valiant, *Graph-Theoretic Arguments in Low-Level Complexity*, Tech. Report No. 13-77, Univ. of Edinburgh, Dep. of Comp. Sci. (1977).
3. D. Yu. Grigor'ev, "An application of separability and independence notions for obtaining lower bounds of circuit complexity," *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (POMI)*, **60**, 38–48 (1976).
4. D. Yu. Grigor'ev, "Lower bounds in the algebraic computational complexity," *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (POMI)*, **118**, 25–82 (1982).
5. A. A. Razborov, *On Rigid Matrices* [in Russian], Manuscript (1989).
6. S. V. Lokam, "Spectral methods for matrix rigidity with applications to size-depth tradeoffs and communication complexity," in: *Proc. of the 36th IEEE Symposium on Foundations of Computer Science*, Los Alamitos (CA), 6–15 (1995).
7. J. Friedman, "A note on matrix rigidity," *Combinatorica*, **13**, No. 2, 235–239 (1993).
8. P. Pudlák and Z. Vavřín, "Computation of rigidity of order n^2/r for one simple matrix," *Comment. Math. Univ. Carolin.*, **32**, No. 2, 213–218 (1991).
9. P. Kimmel and A. Settle, *Reducing the Rank of Lower Triangular All-Ones Matrix*, Tech. Report CS 92-21, Univ. of Chicago (1992).
10. P. Pudlák, "Large communication in constant depth circuits," *Combinatorica*, **14**, No. 2, 203–216 (1994).
11. M. Krause and S. Waack, "Variation ranks of communication matrices and lower bounds for depth two circuits having symmetric gates with unbounded fan-in," in: *Proc. of the 32nd IEEE Symposium on Foundations of Computer Science*, Los Alamitos (CA), 777–782 (1991).
12. N. Nisan and A. Wigderson, "On the complexity of bilinear forms," in: *Proc. of the 27th ACM Symposium on the Theory of Computing*, New York, 723–732 (1995).
13. P. Pudlák, A. Razborov, and P. Savický, *Observations on Rigidity of Hadamard Matrices* [in Russian], Manuscript (1988).
14. N. Alon, *On the Rigidity of Hadamard Matrices*, Manuscript (1990).
15. A. J. Hoffman and H. W. Wielandt, "The variation of the spectrum of a normal matrix," *Duke Math. J.*, **20**, 37–39 (1953).
16. G. H. Golub and C. F. van Loan, *Matrix Computations*, John Hopkins Univ. Press (1983).
17. B. S. Kashin, "On some properties of matrices of bounded operators from the space ℓ_2^n into ℓ_2^m," *Izv. Akad. Nauk Arm. SSR Mat.*, **15**, No. 5, 379–394 (1980).
18. A. A. Lunin, "Operator norms of submatrices," *Mat. Zametki* [*Math. Notes*] **45**, No. 3, 248–252 (1989).
19. B. Kashin and L. Tzaffiri, *Some Remarks on the Restriction of Operators to Coordinate Subspaces*, Tech. Report No. 12, The Edmund Landau Center for Research in Math. Anal., Hebrew Univ., Jerusalem (1993/94).
20. M. Rudelson, "Almost orthogonal submatrices of an orthogonal matrix," *Israel J. Math* (to appear).

V. A. Steklov Mathematics Institute, Russian Academy of Sciences
E-mail address: kashin@mi.ras.ru, razborov@mi.ras.ru

Translated by A. A. Razborov