Lower Bounds on Matrix Rigidity via a Quantum Argument

Ronald de Wolf
CWI, Amsterdam
rdewolf@cwi.nl

Abstract

The *rigidity* of a matrix measures how many of its entries need to be changed in order to reduce its rank to some value. Good lower bounds on the rigidity of an explicit matrix would imply good lower bounds for arithmetic circuits as well as for communication complexity. Here we reprove the best known bounds on the rigidity of the Hadamard matrix, due to Kashin and Razborov, using tools from *quantum* computing. Our proofs are somewhat simpler than earlier ones (at least for those familiar with quantum) and give slightly better constants. More importantly, they give a new approach to attack this longstanding open problem.

1 Introduction

1.1 Rigidity

Suppose we have some $n \times n$ matrix M whose rank we want to reduce. The *rigidity* of M measures the minimal number R of entries we need to change in order to reduce its rank to r. Formally:

$$R_M(r) = \min\{\text{weight}(M - \widetilde{M}) \mid \text{rank}(\widetilde{M}) \leq r\},$$

where "weight" counts the number of non-zero entries. Here the rank could be taken over any field of interest; in this paper we consider the complex field. Roughly speaking, high rigidity means that M's rank is robust against changes: changes in few entries won't change the rank much.

Rigidity was defined by Valiant [22, Section 6] in the 1970s with a view to proving circuit lower bounds. In particular, he showed that an explicit $n \times n$ matrix M with $R_M(\varepsilon n) \geq n^{1+\delta}$ for $\varepsilon, \delta > 0$ would imply that log-depth arithmetic circuits that compute the linear map $M : \mathbb{R}^n \to \mathbb{R}^n$ need superlinear circuit size. Clearly, $R_M(r) \geq n - r$ for every full-rank matrix (reducing the rank by 1 requires changing at least 1 entry). This bound is optimal for the identity matrix, but usually far from tight. Valiant showed that most matrices have rigidity $(n-r)^2$, but finding an *explicit* matrix with high rigidity has been open for decades.

A very natural and widely studied candidate for such a high-rigidity matrix is the Hadamard matrix. This is an orthogonal $n \times n$ matrix H with entries $+1$ and -1; such matrices exist whenever n is a power of 2, but are conjectured to exist whenever n is a multiple of 4. Suppose we have a matrix $\widetilde{H}$ differing from H in R positions such that $\text{rank}(\widetilde{H}) \leq r$. The goal in proving high rigidity is to lower bound R in terms of n and r. Alon [5] proved $R = \Omega(n^2/r^2)$, which was reproved by Lokam [17] using spectral methods. Kashin and Razborov [11] improved this to $R = \Omega(n^2/r)$. This is currently the best known for the Hadamard matrix.

In view of the difficulty in proving strong lower bounds on rigidity proper, Lokam [17] also introduced a relaxed notion of rigidity. This limits the *size* of each change in entries to some parameter $\theta > 0$. Formally

$$R_M(r,\theta) = \min\{\text{weight}(M - \widetilde{M}) \mid \text{rank}(\widetilde{M}) \leq r, \parallel M - \widetilde{M} \parallel_\infty \leq \theta\},$$

where $\|\cdot\|_\infty$ measures the largest entry (in absolute value) of its argument. For the Hadamard matrix, Lokam proved the bound $R_H(r,\theta) = \Omega(n^2/\theta)$ if $\theta \leq n/r$ and $R_H(r,\theta) = \Omega(n^2/\theta^2)$ if $\theta > r/n$. In particular, if entries can change at most by a constant then the rigidity is $\Omega(n^2)$. For the case $\theta > r/n$, Kashin and Razborov [11] improved the bound to $R_H(r,\theta) = \Omega(n^3/r\theta^2)$. Study of this relaxed notion of rigidity is further motivated by the fact that stronger lower bounds would separate the communication complexity versions of the classes PH and PSPACE [17].

Apart from the Hadamard matrix, the rigidity of some other explicit matrices has been studied as well, sometimes giving slightly better bounds $R_M(r) = \Omega(n^2 \log(n/r)/r)$, for instance for Discrete Fourier Transform matrices [9, 21, 16]. Very recently, Lokam [18] showed a near-optimal rigidity bound $R_P(n/17) = \Omega(n^2)$ for the matrix P whose entries are the square roots of distinct primes, and proved an $\Omega(n^2/\log n)$ arithmetic circuit lower bound for the induced linear map $P : \mathbb{R}^n \to \mathbb{R}^n$. This matrix P, however, is "less explicit" than the Hadamard matrix and the rigidity bound has no consequences for communication complexity because P is not a Boolean matrix. Moreover, the same circuit lower bound was already shown by Lickteig [15] (see also [7, Exercise 9.5]) without the use of rigidity.

1.2 Our contribution

In this paper we give new proofs of the best known bounds on the rigidity of the Hadamard matrix, both the standard rigidity and the relaxed one:

- if $r \leq n/2$, then $R_H(r) \geq \dfrac{n^2}{4r}$
- $R_H(r,\theta) \geq \dfrac{n^2(n-r)}{2\theta n + r(\theta^2 + 2\theta)}$

Our constant in the former bound is a bit better than the one of Kashin and Razborov [11] (their proof gives $n^2/256r$). However, we feel our proof technique is more interesting than our precise result. As detailed in Section 2, the proof relies on interpreting an approximation $\widetilde{H}$ of the Hadamard matrix H as a *quantum communication system*, and then using quantum information theory bounds from [19] to relate the rank of $\widetilde{H}$ to the quality of its approximation.[1] Actually our bounds hold not just for the Hadamard matrix, but for every orthogonal matrix where all entries have the same magnitude. This includes for instance the Discrete Fourier Transform matrices. However, for definiteness we will state the results for the Hadamard matrix only.

This paper fits in a recent but fast-growing line of research where results about *classical* objects are proved or reproved using *quantum* computational techniques. Other examples of this are lower bounds for locally decodable codes and private information retrieval [13, 23], classical proof systems for lattice problems derived from earlier quantum proof systems [3, 4], strong limitations on classical

[1] The connection between the Hadamard matrix and quantum communication was also exploited in the lower bound for the communication complexity of inner product by Cleve et al. [8].

algorithms for local search [1] inspired by an earlier quantum computation proof, a proof that the complexity class PP is closed under intersection [2], formula size lower bounds from quantum lower bounds [14], and a new approach to proving lower bounds for classical circuit depth using quantum communication complexity [12].

It should be noted that the use of quantum computing is not strictly necessary for either of our results. The first is proved in two steps: (1) using the quantum approach we show that every $a \times b$ submatrix of H has rank at least ab/n and (2) using a non-quantum argument we show that an approximation $\widetilde{H}$ with small R contains a large submatrix of H and hence by (1) must have high rank. The result of (1) was already proved by Lokam [17, Corollary 2.2] using spectral analysis, so one may obtain the same result classically using Lokam's proof for (1) and our argument for (2). Either way, we feel the proof is significantly simpler than that of Kashin and Razborov [11], who show that a random $a \times a$ submatrix of H has rank $\Omega(a)$ with high probability. Our proof gives a better constant too: $1/4$ instead of $1/256$. In contrast, the quantum aspects of our proof for the bound on $R_H(r, \theta)$ cannot easily be replaced by a classical argument, but that proof is not significantly simpler than the one of Kashin and Razborov (which uses the Hoffman-Wielandt inequality) and the constant is essentially the same.

Despite this, we feel our quantum approach has merit for two reasons. First, it unifies the two results, both of which are now proved from the same quantum information theoretic idea. And second, using quantum computational tools gives a whole new perspective on the rigidity issue, and might just be the new approach we need to solve this longstanding open problem. Our hope is that these techniques not only reprove the best known bounds, but will also push them further.

2 Relation to quantum communication

Very briefly, an r-dimensional *quantum state* is a unit vector of complex amplitudes, written $|\phi\rangle = \sum_{i=1}^{r} \alpha_i |i\rangle \in \mathbb{C}^r$. Here $|i\rangle$ is the r-dimensional vector that has a 1 in its ith coordinate and 0s elsewhere. The inner product between $|\phi\rangle$ and $|\psi\rangle = \sum_{i=1}^{r} \beta_i |i\rangle$ is $\langle\phi|\psi\rangle = \sum_i \alpha_i^* \beta_i$. A (projective) *measurement* is an orthogonal set of projectors $\{P_i\}$. If this measurement is applied to some state $|\phi\rangle$, the probability of obtaining outcome i is given by the squared norm $\| P_i|\phi\rangle \|^2$. If $\{|v_i\rangle\}$ is an orthonormal basis, then a measurement in this basis corresponds to the projectors $P_i = |v_i\rangle\langle v_i|$. In this case the probability of outcome i is $\| P_i|\phi\rangle \|^2 = |\langle v_i|\phi\rangle|^2$. We refer to [20] for more details about quantum computing.

Our proofs are instantiations of the following general idea, which relates (approximations of) the Hadamard matrix to quantum communication. Let H be an $n \times n$ Hadamard matrix. Its rows, after normalization by a factor $1/\sqrt{n}$, form an orthonormal set known as the *Hadamard basis*. If Alice sends Bob the n-dimensional quantum state $|H_i\rangle$ corresponding to the normalized ith row of H, and Bob measures the received state in the Hadamard basis, then he learns i with probability 1.

Now suppose that instead of H we have some rank-r $n \times n$ matrix $\widetilde{H}$ that approximates H in some way or other. Then we can still use the quantum states $|\widetilde{H}_i\rangle$ corresponding to its normalized rows for quantum communication. Alice now sends the state $|\widetilde{H}_i\rangle$. Crucially, she can do this by means of an r-dimensional quantum state. Let $|v_1\rangle, \ldots, |v_r\rangle$ be an orthonormal basis for the row space of $\widetilde{H}$. In order to send $|\widetilde{H}_i\rangle = \sum_{j=1}^{r} \alpha_j |v_j\rangle$, Alice sends $\sum_{j=1}^{r} \alpha_j |j\rangle$ and Bob applies the unitary map $|j\rangle \mapsto |v_j\rangle$ to obtain $|\widetilde{H}_i\rangle$. He measures this in the Hadamard basis, and now his

probability of getting the correct outcome i is

$$p_i = |\langle H_i | \widetilde{H}_i \rangle|^2.$$

The "quality" of these p_i's correlates with the "quality" of $\widetilde{H}$: the closer the ith row of $\widetilde{H}$ is to the ith row of H, the closer p_i will be to 1.

Accordingly, Alice can communicate a random element $i \in [n]$ via an r-dimensional quantum system, with average success probability $p = \sum_{i=1}^{n} p_i/n$. But now we can apply the following upper bound on the average success probability, due to Nayak [19, Theorem 2.4.2] (see Appendix A):

$$p \leq \frac{r}{n}.$$

Intuitively, the "quality" of the approximation $\widetilde{H}$, as measured by the average success probability p, gives a lower bound on the required rank r of $\widetilde{H}$. Below we instantiate this idea in two different ways to get our two bounds.

3 Bound on $R_H(r)$

The next theorem was proved by Lokam [17, Corollary 2.7] using some spectral analysis. We reprove it here using a quantum argument.

Theorem 1 (Lokam) *Every $a \times b$ submatrix A of H has rank $r \geq ab/n$.*

Proof. Obtain rank-r matrix $\widetilde{H}$ from H by setting all entries outside of A to 0. Consider the a quantum states $|\widetilde{H}_i\rangle$ corresponding to the nonempty rows; they have normalization factor $1/\sqrt{b}$. For each such i, Bob's success probability is

$$p_i = |\langle H_i | \widetilde{H}_i \rangle|^2 = \left| \frac{b}{\sqrt{bn}} \right|^2 = \frac{b}{n}.$$

But we're communicating one of a possibilities using r dimensions, so Nayak's bound implies

$$\frac{1}{n} \sum_{i=1}^{n} p_i = p \leq \frac{r}{a}.$$

Combining both bounds gives the theorem. □

Surprisingly, Lokam's result allows us quite easily to derive Kashin and Razborov's [11] bound on rigidity, which is significantly stronger than Lokam's (and Alon's). We also obtain a slightly better constant than [11]: their proof gives 1/256 instead of our 1/4. This is the best bound known on the rigidity of the Hadamard matrix.

Theorem 2 *If $r \leq n/2$, then $R_H(r) \geq n^2/4r$.*

Proof. Consider some rank-r matrix $\widetilde{H}$ with at most $R = R_H(r)$ "errors" compared to H. By averaging, there exists a set of $a = 2r$ rows of $\widetilde{H}$ with at most aR/n errors. Now consider the submatrix A of $\widetilde{H}$ consisting of those a rows and the $b \geq n - aR/n$ columns that have no errors in

those a rows. If $b = 0$ then $R \geq n^2/2r$ and we are done, so we can assume A is nonempty. This A is errorfree, hence a submatrix of H itself, and the previous theorem implies

$$r = \mathrm{rank}(\widetilde{H}) \geq \mathrm{rank}(A) \geq \frac{ab}{n} \geq \frac{a(n - aR/n)}{n}.$$

Rearranging gives the theorem. □

4 Bound on $R_H(r, \theta)$

We now consider the case where the maximal change in entries of H is bounded by θ.

Theorem 3 $R_H(r, \theta) \geq \dfrac{n^2(n-r)}{2\theta n + r(\theta^2 + 2\theta)}$.

Proof. Consider some rank-r matrix $\widetilde{H}$ with at most $R = R_H(r, \theta)$ errors, and $\| H - \widetilde{H} \|_\infty \leq \theta$. As before, define the quantum states corresponding to its rows:

$$|\widetilde{H}_i\rangle = c_i \sum_{j=1}^{n} \widetilde{H}_{ij} |j\rangle,$$

where $c_i = 1/\sqrt{\sum_j \widetilde{H}_{ij}^2}$ is a normalizing constant. Note that $\sum_j \widetilde{H}_{ij}^2 \leq (n - \Delta(H_i, \widetilde{H}_i)) + \Delta(H_i, \widetilde{H}_i)(1+\theta)^2 = n + \Delta(H_i, \widetilde{H}_i)(\theta^2 + 2\theta)$, where $\Delta(\cdot, \cdot)$ measures Hamming distance. Bob's success probability p_i is now

$$p_i = |\langle H_i | \widetilde{H}_i \rangle|^2 \geq \frac{c_i^2}{n}(n - \theta\Delta(H_i, \widetilde{H}_i))^2 \geq c_i^2(n - 2\theta\Delta(H_i, \widetilde{H_i})) \geq \frac{n - 2\theta\Delta(H_i, \widetilde{H}_i)}{n + \Delta(H_i, \widetilde{H}_i)(\theta^2 + 2\theta)}.$$

Since p_i is a convex function of Hamming distance, we also get a lower bound for the average:

$$p \geq \frac{n - 2\theta R/n}{n + R(\theta^2 + 2\theta)/n}.$$

Nayak's bound implies $p \leq r/n$. Rearranging gives the theorem. □

For $\theta \geq n/r$ we obtain the second result of Kashin and Razborov [11]:

$$R_H(r, \theta) = \Omega(n^2(n-r)/r\theta^2).$$

If $\theta \leq n/r$ we get an earlier result of Lokam [17]:

$$R_H(r, \theta) = \Omega(n(n-r)/\theta).$$

5 Discussion

As mentioned in the introduction, this paper is the next in a recent line of papers about classical theorems with quantum proofs. So far, these results are somewhat *ad hoc* and it is hard to see what unifies them other than the use of some quantum mechanical apparatus. A "quantum method" in analogy to the "probabilistic method" [6] is not yet in sight but would be a very intriguing possibility. Using quantum methods as a mathematical proof tool shows the usefulness of the study of quantum computers, quantum communication protocols, etc., irrespective of whether a large quantum computer will ever be built in the lab. Using the methods introduced here to prove stronger rigidity lower bounds would enhance this further.

Most lower bounds proofs for $R_M(r)$ in the literature (including ours) work in two steps: (1) show that all or most submatrices of M have fairly large rank, and (2) show that if the number of errors R is small, there is some (or many) big submatrix of $\widetilde{M}$ that is uncorrupted. Such an uncorrupted submatrix of $\widetilde{M}$ is a submatrix of M and hence by (1) will have fairly large rank. As Lokam [16] observes, this approach will not yield much stronger bounds on rigidity than we already have: it is easy to show that a random set of $R = O(\frac{\max(a,b)n^2}{ab} \log(n/\max(a,b)))$ positions hits every $a \times b$ submatrix of an $n \times n$ matrix. Lokam's [18] recent $\Omega(n^2)$ rigidity bound for a matrix consisting of the roots of distinct primes indeed does something quite different, but unfortunately this technique will not work for matrices over $\{+1, -1\}$ like the Hadamard matrix.

One idea that would give a stronger lower bound for $R_H(r)$ is the following. We used the result that every $a \times b$ submatrix of H has rank at least ab/n. This bound is tight for some submatrices but too weak for others. We conjecture (or rather, hope) that submatrices for which this bound *is* more or less tight, are very "redundant" in the sense that each or most of its rows are spanned by many sets of rows of the submatrix. Such a submatrix can tolerate a number of errors without losing much of its rank, so then we don't need to find an uncorrupted submatrix of $\widetilde{H}$ (as in the current proof), but could settle for a submatrix with little corruption.

Acknowledgments

Thanks to Satya Lokam for sending me a draft of [18] and for some helpful explanations, and to Falk Unger for proofreading.

References

[1] S. Aaronson. Lower bounds for local search by quantum arguments. In *Proceedings of 35th ACM STOC*, pages 465–474, 2003. quant-ph/0307149.

[2] S. Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. quant-ph/0412187, 23 Dec 2004.

[3] D. Aharonov and O. Regev. A lattice problem in quantum NP. In *Proceedings of 44th IEEE FOCS*, pages 210–219, 2003. quant-ph/0307220.

[4] D. Aharonov and O. Regev. Lattice problems in NP∩coNP. In *Proceedings of 45th IEEE FOCS*, pages 362–371, 2004.

[5] N. Alon. On the rigidity of an Hadamard matrix. Manuscript. His proof may be found in [10, Section 15.1.2], 1990.

[6] N. Alon and J. H. Spencer. *The Probabilistic Method*. Wiley-Interscience, second edition, 2000.

[7] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1997.

[8] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp. Quantum entanglement and the communication complexity of the inner product function. In *Proceedings of 1st NASA QCQC conference*, volume 1509 of *Lecture Notes in Computer Science*, pages 61–74. Springer, 1998. quant-ph/9708019.

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

[10] S. Jukna. *Extremal Combinatorics*. EATCS Series. Springer, 2001.

[11] B. Kashin and A. Razborov. Improved lower bounds on the rigidity of Hadamard matrices. *Matematicheskie Zametki*, 63(4):535–540, 1998. In Russian. English translation available at Razborov's homepage.

[12] I. Kerenidis. Quantum multiparty communication complexity and circuit lower bounds, Apr 12, 2005. quant-ph/0504087.

[13] I. Kerenidis and R. de Wolf. Exponential lower bound for 2-query locally decodable codes via a quantum argument. In *Proceedings of 35th ACM STOC*, pages 106–115, 2003. quant-ph/0208062.

[14] S. Laplante, T. Lee, and M. Szegedy. The quantum adversary method and classical formula size lower bounds. In *Proceedings of 20th IEEE Conference on Computational Complexity*, 2005. To appear. quant-ph/0501057.

[15] T. Lickteig. Ein elementarer Beweis für eine geometrische Gradschanke für die Zahl der Operationen bei der Berechnung von Polynomen. Master's thesis, Diplomarbeit, Univ. Konstanz, 1980.

[16] S. Lokam. On the rigidity of Vandermonde matrices. *Theoretical Computer Science*, 237(1–2):477–483, 2000.

[17] S. Lokam. Spectral methods for matrix rigidity with applications to size-depth trade-offs and communication complexity. *Journal of Computer and Systems Sciences*, 63(3):449–473, 2001. Earlier version in FOCS'95.

[18] S. Lokam. A quadratic lower bound on rigidity. April 2005. Manuscript.

[19] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proceedings of 40th IEEE FOCS*, pages 369–376, 1999. quant-ph/9904093.

[20] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

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

[22] L. Valiant. Graph-theoretic arguments in low-level complexity. In *Proceedings of 6th MFCS*, volume 53 of *Lecture Notes in Computer Science*, pages 162–176. Springer, 1977.

[23] S. Wehner and R. de Wolf. Improved lower bounds for locally decodable codes and private information retrieval. In *Proceedings of 32nd ICALP*, 2005. To appear. quant-ph/0403140.

A Proof of Nayak's bound

For the sake of completeness, in this appendix we include Nayak's elegant proof of his upper bound on the average success probability of a low-dimensional quantum encoding [19, Theorem 2.4.2].

Consider an encoding $i \mapsto |\phi_i\rangle$ of $i \in [n]$ into an r-dimensional space with orthonormal basis $|1\rangle, \ldots, |r\rangle$. Let Q be the projector on this space. Suppose there is a measurement with orthogonal projectors $P_1, \ldots, P_n$ (possibly on a larger space) and success probabilities

$$p_i = \Pr[\text{measuring } |\phi_i\rangle \text{ gives outcome } i] = \| P_i|\phi_i\rangle \|^2.$$

Diagonalize $P_i = \sum_{j \in S_i} |v_{ij}\rangle\langle v_{ij}|$. Note that the set of all $|v_{ij}\rangle$ forms on orthonormal basis of the whole Hilbert space on which the measurement acts, hence $\sum_{i=1}^n \sum_{j \in S_i} |\langle\phi|v_{ij}\rangle|^2 = \| |\phi\rangle \|^2$ for every state $|\phi\rangle$ in this space. Now

$$p_i = \| P_i|\phi_i\rangle \|^2 = \sum_{j \in S_i} |\langle v_{ij}|\phi_i\rangle|^2 \leq \sum_{j \in S_i} \| Q|v_{ij}\rangle \|^2 = \sum_{j \in S_i} \sum_{k=1}^{r} |\langle k|v_{ij}\rangle|^2,$$

and

$$\sum_{i=1}^{n} p_i \leq \sum_{i=1}^{n} \sum_{j \in S_i} \sum_{k=1}^{r} |\langle k|v_{ij}\rangle|^2 = \sum_{k=1}^{r} \sum_{i=1}^{n} \sum_{j \in S_i} |\langle k|v_{ij}\rangle|^2 = \sum_{k=1}^{r} \| |k\rangle \|^2 = r.$$

This implies $p = \sum_{i=1}^n p_i/n \leq r/n$ for the average success probability.