COMS 6998: Algebraic Techniques in TCS (Fall'21) Nov.9, 2021

Lecture 8: Rigidity Lower and Upper Bounds

Instructor: *Josh Alman* Scribe notes by: *Alex Lindenbaum, Yunya Zhao*

Disclaimer: This draft may be incomplete or have errors. Consult the course webpage for the most up-to-date version.

1 A random matrix is very likely to be rigid

Valiant-rigid (Recall from last lecture) A matrix $M \in \mathbb{R}^{N\times N}$ is Valiant-rigid if there is an $\varepsilon > 0$ such that

$$\mathscr{R}_M\big(\frac{N}{\log\log N}\big) > N^{1+\varepsilon}.$$

A random 0/1 matrix is Valiant-rigid with high probability. This means most of the Boolean matrices are in fact Valiant-rigid.

Proposition 1. *If N is large enough, a random matrix $M \in \mathbb{F}_2^{N\times N}$ has $\mathscr{R}_M(\frac{N}{4}) \geq \frac{N^2}{20}$ with high probability.*

Proof. Suppose $M \in \mathbb{F}_2^{N\times N}$ has $\mathscr{R}_M(\frac{N}{4}) < \frac{N^2}{20}$, then we can write M as a low-rank matrix plus a sparse matrix: $M = L + S$, where $\text{rank}(L) \leq \frac{N}{4}$, $\text{sparsity}(S) \leq \frac{N^2}{20}$. Now we count the total number of such L and S.

- Since the rank of L is at most $\frac{N}{4}$, we can write $L = A \times B^\top$ where $A, B \in \mathbb{F}_2^{N\times N/4}$, so

$$\#(L) \leq 2^{2\times N\times (N/4)} = 2^{N^2/2}.$$

- Since the sparsity of S is at most $\frac{N^2}{20}$,

$$\#(S) = \sum_{i=0}^{N^2/20} \binom{N^2}{i} \leq N^2 \cdot \binom{N^2}{\frac{N^2}{20}} \leq N^2 \cdot (20e)^{N^2/20} \leq 2^{0.4N^2}.$$

Therefore we know the number of such M is

$$\#(M) \leq \#(L)\cdot\#(S) \leq 2^{(0.5+0.4)N^2} = 2^{0.9N^2}.$$ □

Since there are in total 2^{N^2} matrices in $\mathbb{F}_2^{N\times N}$, a random matrix $M \in \mathbb{F}_2^{N\times N}$ has $\mathscr{R}_M(\frac{N}{4}) \geq \frac{N^2}{20}$ with probability at least $1 - 2^{-0.1N^2}$.

2 Lower bound(s) for rigidity of Walsh-Hadamard Matrix H_n

Recall that the Walsh-Hadamard matrix is defined as

$$H_n = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}^{\otimes n} \in \{-1, 1\}^{2^n \times 2^n}.$$

Equivalently, we can view the columns and rows of H_n to be indexed by n-bit binary strings: for $x, y \in \{0,1\}^n$,

$$H_n[x, y] = (-1)^{\langle x, y \rangle}.$$

Naive H_n rigidity lower bound. Let $N = 2^n$. We observe that H_n has full rank. For any matrix, changing one of its entries can decrease its rank by at most 1. So a straightforward lower bound can be given (when working over a ring where the characteristic of the ring $\neq 2$, e.g., the ring $\mathbb{R}$ or $\mathbb{F}_m$)

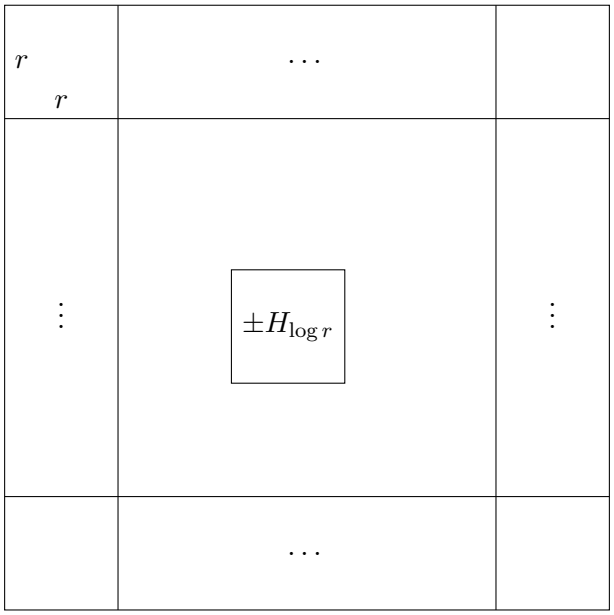
$$\mathscr{R}_{H_n}(r) \geq N - r.$$

We will give better lower bounds below.

(Slightly better) H_n rigidity lower bound. Assume r is a power of 2.

$$\mathscr{R}_{H_n}(r-1) \geq \frac{N^2}{r^2}.$$

Proof. Divide H_n into blocks of size $r \times r$, and there are $\frac{N}{r} \times \frac{N}{r}$ such blocks.

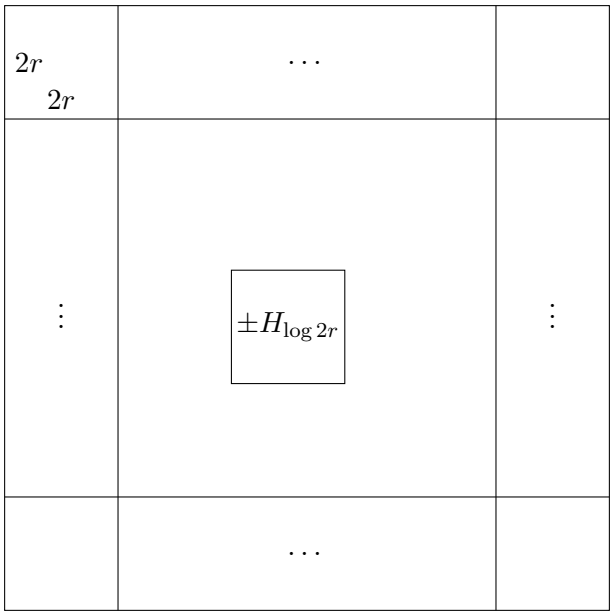


Because of the recursive nature of H_n, each block is $\pm H_{\log r}$. Since $H_{\log r}$ is a full rank matrix, this means each block has full rank. We need to change 1 entry in each block in order to reduce the rank of H_n to $r - 1$. Thus the number of entries we need to change is at least $\frac{N^2}{r^2}$. □

(Better than above) H_n rigidity lower bound.

$$\mathscr{R}_{H_n}(r) \geq \frac{N^2}{4r}.$$

Proof. We use a similar approach as above.



This time, we divide H_n into blocks of size $2r \times 2r$, and there are $\frac{N}{2r} \times \frac{N}{2r}$ such blocks. Again, all these blocks are $\pm H_{\log 2r}$, and they are all full-rank. We need to change r entries in each block to reduce the rank of H_n to r. Thus the total number of entries changed is $\frac{N^2}{4r^2} \times r = \frac{N^2}{4r}$. □

This is the best lower bound we know so far.

3 Lower bound on rigidity of Discrete Fourier Transform F_p

Let p be a prime number. Recall that the discrete Fourier transform matrix $F_p \in \mathbb{C}^{p \times p}$ is defined as

$$F_p[a, b] = \omega_p^{a \cdot b}, \quad \text{where } \omega_p = e^{-\frac{2\pi i}{p}}.$$

Not every submatrix of the Hadamard matrix has full rank, e.g., the middle 2×2 submatrix of $H_2 \in \{-1, 1\}^{4\times 4}$ has rank 1. However, we will show that every submatrix of the discrete Fourier matrix has full rank, and this will lead to a slightly stronger rigidity lower bound.

Lemma 2. *For any r, any $S \subseteq \{0, 1, ..., p-1\}$ of size $|S| = r$, any $0 \leq k < p - r$, the submatrix $F_p|_{a\in S, b\in\{k,k+1,...,k+r-1\}}$ has full rank.*

Proof. Assume to the contrary that the submatrix is not full-rank, then there exist constants $c_k, \cdots, c_{k+r-1}$ such that $\forall a \in S$,

$$\sum_{b=k}^{k+r-1} c_b \cdot F_p[a, b] = 0 \iff \sum_{b=k}^{k+r-1} c_b \cdot (\omega_p^a)^b = 0.$$

We can rewrite this as a polynomial to which we would plug in ω_p^a:

$$p(x) = \sum_{b=k}^{k+r-1} c_b \cdot x^b.$$

Properties of $p(x)$ include:

- p is non-zero.
- ω_p^a is a root of p for all r choices of $a \in S$.

However, since the degree of p is $(k+r-1)$, and 0 is a root with multiplicity k, there can only be $(r-1)$ other roots, which is a contradiction with the second property of $p(x)$. □

What if b is not a continuous subset? Let $b \in T$, where T is an arbitrary size-r subset of $\{0, ..., p-1\}$. The polynomial will become

$$p(x) = \sum_{b \in T} c_b \cdot x^b.$$

It turns out the lemma still holds because of the following theorem, which we state here without proof.

Theorem 3. *Any polynomial $p : \mathbb{C} \to \mathbb{C}$ with r monomials has $< r$ roots of unity as roots.*

Using this theorem and a similar proof as that of the lemma, we can show that any submatrix of F_p has full rank.

Lower bound on rigidity of F_p. We have shown that any submatrix of F_p has full rank, therefore, in order to hit all of the $(r+1) \times (r+1)$ submatrices, the number of entries we need to change is

$$\mathscr{R}_{F_p}(r) \geq \frac{N(N-r)}{2(r+1)} \log \frac{N}{r}, \quad \text{(where } N = p\text{)}.$$

Plug in $r = \frac{N}{\log \log N}$, we have

$$\mathscr{R}_{F_p}(\frac{N}{\log \log N}) \geq N \cdot \log \log N \cdot \log \log \log N.$$

Note that this still does not reach the Valiant rigidity of $\mathscr{R}_M(\frac{N}{\log \log N}) \geq N^{1+\varepsilon}$. This is the best known lower bound for any explicit matrix family. If we were to push this bound, we would need to exploit other properties of the matrices than just the full-rank submatrices, this is because there is an explicit family for which this bound is already tight.

4 Upper bound on rigidity for R_n

Recall that in Homework 2 we defined the family of matrices $R_n \in \{0,1\}^{2^n \times 2^n}$ by

$$R_n[x, y] = 1 \iff \langle x, y \rangle = 0.$$

We can show that R_n is not Valiant-rigid.

Lemma 4. *$\forall \delta > 0$, we can change $\leq 2^{\delta n}$ entries per row or column of R_n to make its rank $\leq 2^{n(1-\Theta(\delta^2))}$.*

Since $2^{\delta n} = N^{\delta}$, this means we can change $N^{1+\delta}$ entries of R_n to decrease its rank to $N^{1-c\delta^2}$, so R_n is not Valiant-rigid.

Proof. The idea is to repeatedly apply low-rank updates until the resulting matrix is very sparse. Let k be a number whose value will be determined at the end of the proof. The procedure goes as follows:

- For each $x \in \{0,1\}^n$, if $|x| \leq k$ then set row x of R_n to all zeros.
- For each $y \in \{0,1\}^n$, if $|y| \leq k$ then set column y of R_n to all zeros.

Changing one row (column) corresponds to decreasing the rank of the matrix by at most one. Thus, the total rank change was at most twice the number of n-bit strings with at most k ones:

$$\text{rank changes by } \leq 2 \cdot \sum_{i=0}^{k} \binom{n}{i}.$$

How many rows did our procedure not zero out? Any such row x would satisfy $|x| > k$. How many non-zero entries remain in a fixed row x? y must satisfy

1. $R_n[x,y] = 1$, i.e. $\langle x, y \rangle = 0$, and
2. $|y| > k$, otherwise we would have set that entry to 0.

y must have at least $|x|$ zeros in order for property 1 to hold. Therefore, $k+1 \leq |y| \leq n - |x|$. The number of such y's is

$$\sum_{i=k+1}^{n-|x|} \binom{n-|x|}{i}.$$

Let $k = (\frac{1}{2} - \epsilon)n$. Then the rank change is at most

$$2 \cdot \sum_{i=0}^{(1/2-\epsilon)n} \binom{n}{i} \leq 2 \cdot n \cdot \binom{n}{(1/2-\epsilon)n} \leq 2^{n(1-\Theta(\epsilon^2/\log\frac{1}{\epsilon}))},$$

and the number of non-zero entries per row is at most

$$\begin{aligned}
\sum_{i=(1/2-\epsilon)n}^{(1/2+\epsilon)n} \binom{(1/2+\epsilon)n}{i} &= \sum_{i=(1/2-\epsilon)n}^{(1/2+\epsilon)n} \binom{(1/2+\epsilon)n}{(1/2+\epsilon)n - i} \\
&= \sum_{i=0}^{2\epsilon n} \binom{(1/2+\epsilon)n}{i} \\
&\leq n \cdot \binom{(1/2+\epsilon)n}{2\epsilon n} \leq 2^{O(\epsilon)n}.
\end{aligned}$$

Picking ϵ such that $\delta = O(\epsilon)$, the lemma is proven. □

5 Upper bound on rigidity for Walsh-Hadamard transform

The Walsh-Hadamard Matrix H_n is also not Valiant-rigid. The proof relies on this fact:

Lemma 5. *There is a diagonal matrix $D \in \mathbb{F}_2^{2^n \times 2^n}$ such that*

$$H_n = R_n \times D \times R_n.$$

To see how this implies that H_n is not rigid, observe that $R_n = L + S$ for some low-rank and sparse matrices L and S, respectively. More specifically,

$$\text{rank}(L) = r \leq 2^{n(1-\Theta(\epsilon^2))},$$

and the row-column sparsity of S is

$$\text{rc-sparse}(S) = s \leq 2^{\epsilon n}.$$

Expanding the formula for H_n, we get that

$$H_n = LD(L+S) + SDL + SDS.$$

The rank of $LD(L+S)$ is the minimum rank between L, D, and $L+S$, which is at most r. The rank of SDL is also at most r. And the row-column sparsity of SDS is at most s^2. So H_n is a sum of a low-rank and low-sparsity matrix!

Proof of Lemma 5. We let D be an arbitrary diagonal matrix and try to characterize R_nDR_n. For any $x, y \in \{0,1\}^n$,

$$\begin{aligned} R_nDR_n[x,y] &= \sum_{z \in \{0,1\}^n} R_n[x,z] \cdot D[z,z] \cdot R_n[z,y] \\ &= \sum_{\substack{z \in \{0,1\}^n \\ \langle z,x \rangle = \langle z,y \rangle = 0}} D[z,z] \\ &= \sum_{\substack{z \in \{0,1\}^n \\ \langle z, x \vee y \rangle = 0}} D[z,z] = \sum_{z \in \{0,1\}^n} R_n[x \vee y, z] \cdot D[z,z]. \end{aligned}$$

Say $D = \text{diag}(d)$ for some $d \in \mathbb{F}_2^{2^n}$. Then this is equal to

$$\sum_{z \in \{0,1\}^n} R_n[x \vee y, z] \cdot d[z] = (R_n \times d)[x \vee y].$$

If we pick d such that $(R_d \times d)[z] = (-1)^{|z|}$, then

$$(R_n \times d)[x \vee y] = (-1)^{|x \vee y|} = (-1)^{n - |\bar{x} \wedge \bar{y}|} = (-1)^n \cdot H_n[\bar{x}, \bar{y}],$$

where $\bar{x}$ denotes the complement of x, i.e., $\bar{x}_i = 1 - x_i$.

Since $H_n[x,y] = (-1)^{|x \wedge y|}$, R_nDR_n is just a scaled permutation of H_n. □