Matrix Rigidity

Rigidity of Hadamard

Sasha Golovnev

November 4, 2020

Hadamard Matrix

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} ,$$

$$H_N = \begin{pmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{pmatrix} \text{ for } N = 2^n > 2 \,.$$

Hadamard Matrix

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$H_N = \begin{pmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{pmatrix} \text{ for } N = 2^n > 2\,.$$

$$H_N = H_2^{\otimes n}\,.$$

Hadamard Matrix

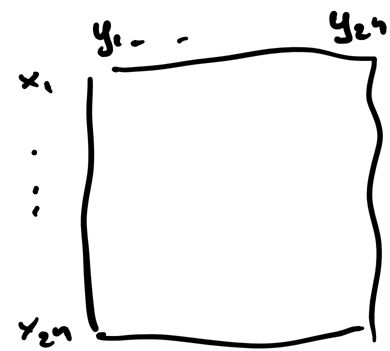
$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$H_N = \begin{pmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{pmatrix} \text{ for } N = 2^n > 2\,.$$

$$H_N = H_2^{\otimes n}\,.$$

$$H_{u,v} = \langle \cancel{u,v} \rangle \text{ for } u,v \in \{0,1\}^n\,.$$

$$H_{u,v} = (-1)^{\langle u,v \rangle}$$



$x_i \in \{0,1\}^n$ $\quad y_i \in \{0,1\}^n$

Known Lower Bounds

rigidity	reference
$\frac{n^2}{r^4 \log^2 r}$	Pudlák and Savickỳ, 88
$\frac{n^2}{r^3 \log r}$	Razborov, 88
$\frac{n^2}{r^2}$	Alon, 90
$\frac{n^2}{r^2}$	Lokam, 95
$\frac{n^2}{256r}$	Kashin and Razborov, 98
$\frac{n^2}{4r}$	de Wolf, 06

Lower and Upper Bounds

- We showed that $\mathcal{R}_H^{\mathbb{R}}(r) \geq \boxed{\frac{n^2}{4r}}$ for every $r \leq n/2$.

Lower and Upper Bounds

- We showed that $\mathcal{R}_H^{\mathbb{R}}(r) \geq \frac{n^2}{4r}$ for every $r \leq n/2$.
- We showed that for $r \geq n/2$, $\mathcal{R}_H^{\mathbb{R}}(r) \leq O(n)$.

Lower and Upper Bounds

- We showed that $\mathcal{R}_H^{\mathbb{R}}(r) \geq \frac{n^2}{4r}$ for every $r \leq n/2$.
- We showed that for $r \geq n/2, \mathcal{R}_H^{\mathbb{R}}(r) \leq O(n)$.
- We'll prove that H is not rigid for any $r = O(n)$.

Rigidity of Hadamard

Theorem (AW17)

For any field $\mathbb{F}$, $\delta > 0$, there exists $\delta' = \Omega\left(\delta^2 / \log^2 \frac{1}{\delta}\right)$ such that $\mathcal{R}^{\mathbb{F}}_{S_N}(N^{1-\delta'}) \leq \boxed{N^{1+\delta}}$ for any $N = 2^n$ large enough.

For CLB we want rigidity $N^{1+\delta}$
but for (essentially) linear rank

Binomial Coefficients

$$\frac{2^{n \cdot H(k/n)}}{n+1} \leq \binom{n}{k} \leq 2^{n \cdot H(k/n)},$$

Binomial Coefficients

$$\binom{n}{k} \approx \boxed{2^{n \cdot H(k/n)}}$$

$$\frac{2^{n\cdot H(k/n)}}{n+1} \leq \binom{n}{k} \leq 2^{n\cdot H(k/n)},$$

where

H(p) - binary Entropy function

$$✓ \quad H(p) = \boxed{p \log \frac{1}{p} + (1-p)\log\frac{1}{1-p}}.$$

$0 < p < 1$

$$\binom{n}{k} = \binom{n}{n-k}$$

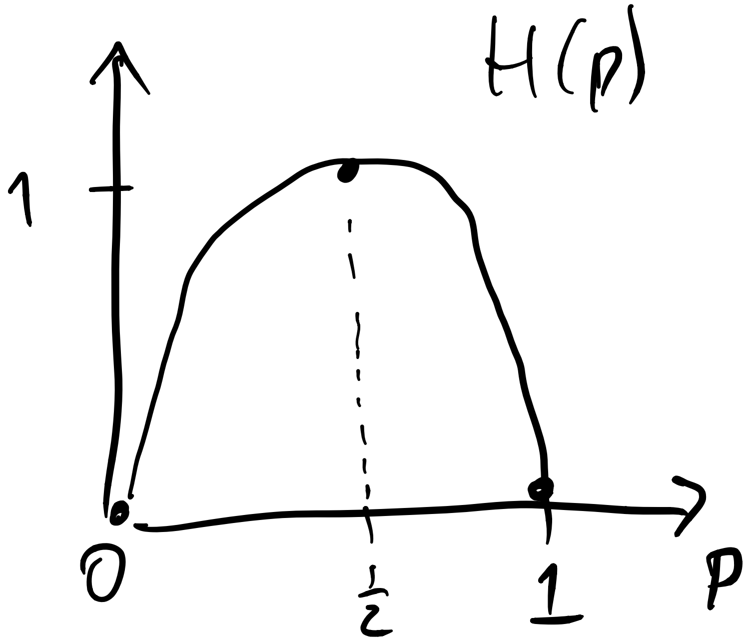
$$\Downarrow$$

$$H(p) = H(1-p)$$

$$\binom{n}{n/2} \approx \frac{2^n}{\sqrt{n}} \implies H(\tfrac{1}{2}) = 1$$

$$\binom{n}{0}, \binom{n}{n} = 1$$

$$H(0) = H(1) = 0$$



Taylor around $p = \frac{1}{2}$

$$H\left(\tfrac{1}{2}-\varepsilon\right) = 1 - \Theta(\varepsilon^2)$$

$\varepsilon \approx 0$

$$H(\varepsilon) = \varepsilon \log\left(\tfrac{1}{\varepsilon}\right) + (1-\varepsilon)\log\frac{1}{1-\varepsilon}$$

$$\approx \varepsilon \log\left(\tfrac{1}{\varepsilon}\right) + \log(1+\varepsilon)$$

$\log(1+x) \approx x - \Theta(x^2)$

$$\approx \boxed{\varepsilon \log\left(\tfrac{1}{\varepsilon}\right)} + \varepsilon = \Theta\left(\varepsilon \log\left(\tfrac{1}{\varepsilon}\right)\right)$$

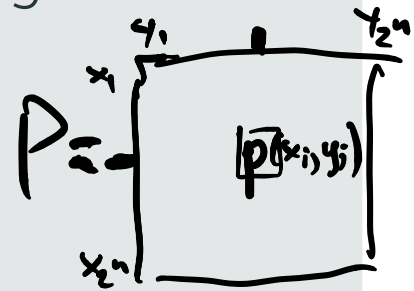
Low-degree Approximations

$$p(\underbrace{x_1, \dots, x_n}_{x}, \underbrace{y_1, \dots, y_n}_{y}) = \sum_{i \in [m]} c_i \cdot x_1 x_3^2 x_{n-3} y_2^4 y_{n/2}$$

Lemma

Let $p(x, y)$ for $x, y \in \mathbb{F}^n$ be a $(2n)$-variate polynomial with m monomials. Let $P \in \mathbb{F}^{2^n \times 2^n}$ be a matrix defined as $P_{x,y} = p(x, y)$ for every $x, y \in \{0, 1\}^n$. For any matrix $\boxed{M} \in \mathbb{F}^{2^n \times 2^n}$ that can be obtained from P by changing at most k columns and ℓ rows,

$$\underline{\operatorname{rank}(M) \le m + k + \ell\,.}$$



M = P but k+ℓ rows and cols are changed

$$p(x,y) = \sum_{i\in[m]} c_i \cdot f_i(x)\cdot g_i(y)$$

$$P_i = \begin{array}{c|ccc} & y_1 & y_t & y_{2^n} \\ \hline x_1 & & & \\ x_s & & f_i(x_s)\cdot g_i(y_t) & \\ x_{2^n} & & & \end{array} \qquad i\in[m]$$

$$\boxed{P_i} \quad \boxed{f_i(x)\cdot g_i(y)} \quad 1\le i\le m$$

$$P = \sum_{i\in[m]} c_i \cdot P_i$$

$$p = \sum_{i\in[m]} c_i \cdot p_i$$

$$P_i = 2^n \overset{1}{\begin{bmatrix} f_i(0\ldots0) \\ f_i(0\ldots1) \\ \vdots \\ f_i(1\ldots1) \end{bmatrix}} \cdot \; n \overset{2^n}{\begin{bmatrix} g_i(0\ldots0) & g_i(0\ldots1) & \cdots & g_i(1\ldots1) \end{bmatrix}}$$

$\text{rank}(P_i) \leq 1$

$$\text{rank}(P) \leq \text{rank}\Big(\sum_{i \in [m]} c_i P_i\Big)$$

$$\leq m$$

If you change $k+l$ rows & cols, then you increase rank by $k+l$

$$\Rightarrow \text{rank}(M) \leq$$

$$\leq \text{rank}(P) + k + l$$

$$\leq m + k + l \qquad \square$$

Proof Outline

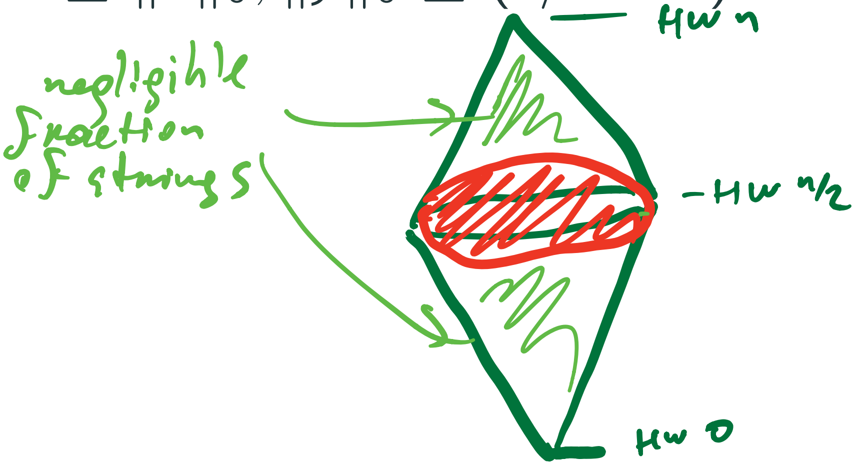
If a sparse poly "approximates" a matrix, then this matrix has low rank.

Proof Outline

$= (-1)^{\langle x,y \rangle}$

- It's sufficient to compute $H_{x,y}$ for $x, y \in \{0,1\}^n$:

$$(1/2 - \varepsilon)n \leq \|x\|_0, \|y\|_0 \leq (1/2 + \varepsilon)n\,.$$



Proof Outline

- It's sufficient to compute $H_{x,y}$ for $x, y \in \{0,1\}^n$:

$$(1/2 - \varepsilon)n \leq \|x\|_0, \|y\|_0 \leq (1/2 + \varepsilon)n\,.$$

- $\langle x, y \rangle$ is now in $[0, (1/2 + \varepsilon)n]$!

$\underbrace{[0, n]}$

x

$\boxed{0\;1\;0\;1\;0\;0\;0\;1\;1\;1}$ $\boxed{1\;0\;0\;1\;1\;0\;0\;1\;0\;1\;1}$

we expect $\langle x, y \rangle \approx \frac{n}{4}$

Proof Outline

- It's sufficient to compute $H_{x,y}$ for $x, y \in \{0,1\}^n$:

$$(1/2 - \varepsilon)n \leq \|x\|_0, \|y\|_0 \leq (1/2 + \varepsilon)n\,.$$

- $\langle x, y\rangle$ is now in $[0, (1/2+\varepsilon)n]$!

$\langle x, y \rangle \in [0, n]$

- We'll show that all but negligible fraction have $\langle x, y\rangle \geq 2\varepsilon n$. Now $\langle x, y\rangle \in [2\varepsilon n, (1/2+\varepsilon)n]$!

length of this interval

$n(\frac{1}{2} - \varepsilon)$

$H_{x,y} = (-1)^{\langle x,y\rangle}$

$F(t) = (-1)^t$ for $t \in [2\varepsilon n, (\frac{1}{2}+\varepsilon)n]$

$\deg F \leq \boxed{n(\frac{1}{2} - \varepsilon)}$

$H_{x,y} = F(x_1y_1 + x_2y_2 + \dots + x_ny_n) = (-1)^{\langle x,y\rangle}$

Proof Outline

- It's sufficient to compute $H_{x,y}$ for $x, y \in \{0,1\}^n$:

$$(1/2 - \varepsilon)n \leq \|x\|_0, \|y\|_0 \leq (1/2 + \varepsilon)n\,.$$

- $\langle x, y\rangle$ is now in $[0, (1/2 + \varepsilon)n]$!
- We'll show that all but negligible fraction have $\langle x, y\rangle \geq 2\varepsilon n$. Now $\langle x, y\rangle \in [2\varepsilon n, (1/2 + \varepsilon)n]$!
- There is a poly in $x_i y_i$ of degree $(1/2 - \varepsilon)n$ that correctly computes $\langle x, y\rangle$ in this range.

Proof Outline

- It's sufficient to compute $H_{x,y}$ for $x, y \in \{0,1\}^n$:

$$(1/2 - \varepsilon)n \le \|x\|_0, \|y\|_0 \le (1/2 + \varepsilon)n\,.$$

- $\langle x, y\rangle$ is now in $[0, (1/2+\varepsilon)n]$!
- We'll show that all but negligible fraction have $\langle x, y\rangle \ge 2\varepsilon n$. Now $\langle x, y\rangle \in \underline{[2\varepsilon n, (1/2+\varepsilon)n]}$!
- There is a poly in $x_i y_i$ of degree $(1/2 - \varepsilon)n$ that correctly computes $\langle x, y\rangle$ in this range.
- This gives a poly with $\binom{n}{(1/2-\varepsilon)n} = \boxed{2^{n(1-\varepsilon')}}$ monomials approximating Hadamard.

$f(t) = (-1)^t$ | $H_{x,y} = f(x_1y_1 + \cdots + x_ny_n)$

Number of Outliers

Even when considering x, y of HW $\approx \frac{n}{2}$,
we can focus x, y, s.t. $\langle x, y \rangle \geq 2\varepsilon n$

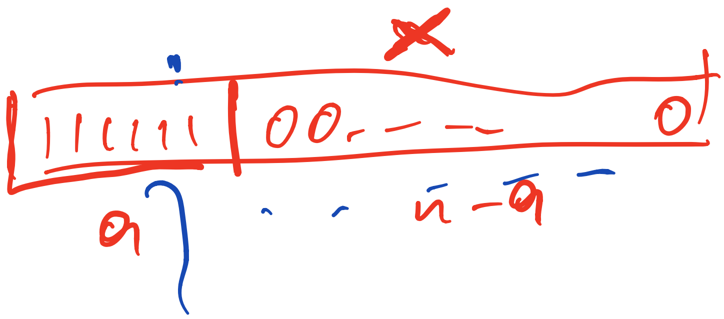
Lemma

Let $\varepsilon \in (0, \frac{1}{100})$. For any $x \in \{0,1\}^n$ such that $\|x\|_0 \in [(\frac{1}{2} - \varepsilon)n, (\frac{1}{2} + \varepsilon)n]$, there are at most $\boxed{2^{O(\varepsilon \log(1/\varepsilon) n)}}$ values of $y \in \{0,1\}^n$ such that $\|y\|_0 \in [(\frac{1}{2} - \varepsilon)n, (\frac{1}{2} + \varepsilon)n]$ and $\langle x, y \rangle < 2\varepsilon n$.

$a = \|x\|_0 \;;\; b = \|y\|_0 \;,\; s = \langle x, y \rangle$

Fixed x, how many such y do I have?

$$\sum_{b \in [(\frac{1}{2}-\varepsilon)n,\, (\frac{1}{2}+\varepsilon)n]} \; \sum_{s \le 2\varepsilon n} \binom{a}{s} \cdot \binom{n-a}{b-s}$$



Choose s ones from a ones

Choose $b-s$ ones from $n-a$

$$\le O(n^2) \cdot \binom{n(\frac{1}{2}+\varepsilon)}{2\varepsilon n} \cdot \binom{n(\frac{1}{2}+\varepsilon)}{n(\frac{1}{2}-3\varepsilon)}$$

$$O(n^2) \cdot \boxed{\binom{n(\frac{1}{2}+\varepsilon)}{2\varepsilon n} \cdot \binom{n(\frac{1}{2}+\varepsilon)}{n(\frac{1}{2}-3\varepsilon)}}$$

$$\lessapprox 2^{\frac{n}{2}H(4\varepsilon)} \cdot 2^{\frac{n}{2}H(8\varepsilon)}$$

$$\binom{n}{k} = \binom{n}{n-k} \quad \Bigg| \quad \binom{n(\frac{1}{2}+\varepsilon)}{n(\frac{1}{2}-3\varepsilon)} = \binom{n(\frac{1}{2}+\varepsilon)}{4\varepsilon n}$$

$$H(\varepsilon) \approx \varepsilon \log\left(\frac{1}{\varepsilon}\right)$$

$$= 2^{O\left(n\varepsilon \log\left(\frac{1}{\varepsilon}\right)\right)} \ll 2^n$$

$\square$

Approximating Hadamard

Lemma

Let $\mathbb{F}$ be a field, and $\varepsilon \in (0, \frac{1}{2})$. There exists a $(2n)$-variate multilinear polynomial $p(x, y)$ over $\mathbb{F}$ with at most $\boxed{2^{n-\Omega(\varepsilon^2 n)}}$ monomials such that

$<< 2^n$

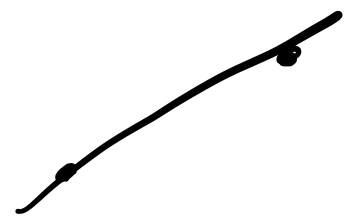
$$p(x, y) = (\mathbf{H}_{2^n})_{x,y} = (-1)^{\langle x,y \rangle}$$

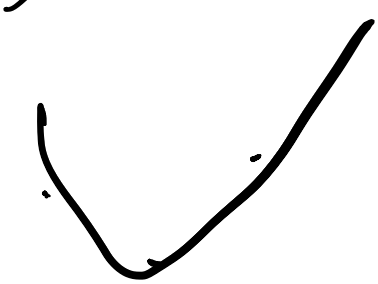
whenever $\langle x, y \rangle \in [2\varepsilon n, (\frac{1}{2} + \varepsilon)n]$.

points that matter

$$F(t) = (-1)^t \quad t \in [2\varepsilon n, n(\tfrac{1}{2} + \varepsilon)]$$

$$\deg F \le \boxed{n\left(\tfrac{1}{2} - \varepsilon\right)}$$





$$H_{x,y} = (-1)^{\langle x, y\rangle} =$$

$$= F(\langle x, y\rangle)$$

$$= F(x_1 y_1 + \dots + x_n y_n)$$

$z_i = x_i y_i$

$$= F(z_1 + z_2 + \dots + z_n)$$

$z^2 = z$

wlog F is multilinear

Multilinear

n vars

deg $\underline{n(\frac{1}{2}-\varepsilon)}$

$\underbrace{x_1 \cdots\cdots}$ x_n

$$\binom{n}{\leq n(\frac{1}{2}-\varepsilon)} \approx \binom{n}{n(\frac{1}{2}-\varepsilon)} \approx$$

$$\approx 2^{nH(\frac{1}{2}-\varepsilon)} = 2^{n(1-\varepsilon^2)} \ll$$

$$\ll 2^n$$

Rigidity of Hadamard

Theorem (AW17)

For any field $\mathbb{F}$, $\delta > 0$, *there exists* $\delta' = \Omega\left(\delta^2 / \log^2 \frac{1}{\delta}\right)$ *such that* $\mathcal{R}^{\mathbb{F}}_{S_N}(N^{1-\delta'}) \leq \boxed{N^{1+\delta}}$ *for any* $N = 2^n$ *large enough.*

Start with a poly that computes H at "all points that matter".

Poly p, corresponding matrix P.

$\mathrm{rk}(P) \leq 2^{n - \varepsilon^2 n}$. ✓

Computes $\boxed{H(x,y)}$ correctly for $\langle x, y \rangle \in [2\varepsilon n, n(\frac{1}{2}+\varepsilon)]$.

$M = P$, but "correct" in all rows/cols corresponding to x, y of HW <u>not</u> in $[n(\frac{1}{2}-\varepsilon), n(\frac{1}{2}+\varepsilon)]$

M differs from P $\binom{n}{n(\frac{1}{2}-\varepsilon)} = 2^{n-\varepsilon^2 n}$ rows & cols.

$$\mathrm{Rk}(M) \leq \mathrm{Rk}(P) + 2^{n-\varepsilon^2 n}$$
$$\leq 2^{n-\varepsilon^2 n}.$$

M computes H

1. if $\|x\|_0 \notin \frac{n}{2} \pm \frac{1}{2}\varepsilon n$
2. if $\|y\|_0 \notin \frac{n}{2} \pm \frac{1}{2}\varepsilon n$
3. if $\langle x,y\rangle \in [2\varepsilon n, n(\frac{1}{2}+\varepsilon)]$

~~It remains to compute~~ H

$$\boxed{x,y \in \frac{n}{2} \pm \frac{1}{2}\varepsilon n \;\; \& \;\; \langle x,y\rangle < 2\varepsilon n.}$$

$\boxed{M}$ differs from H only in $\underbrace{2^{n+n\varepsilon\log(\frac{1}{\varepsilon})}}$ pos.

$\Rightarrow$ H is not rigid $\square$