Matrix Rigidity

Natural Proofs, Inapproximability of Rigidity

Sasha Golovnev

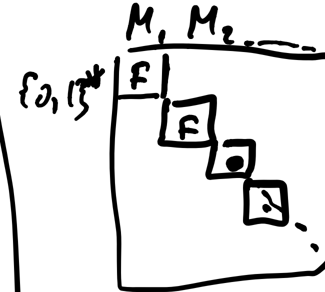
November 16, 2020

Natural Proofs

$f: \{0,1\}^n \to \{0,1\}$

- Property of Boolean functions P

- Relativization



- Algebraization

- Natural Proofs

Natural Proofs

- Property of Boolean functions P
- n^c-usefulness:

$$\boxed{P(f) = 0} \text{ for every } f \in \mathrm{SIZE}(n^c) .$$

Need to find $g : \{0,1\}^n \to \{0,1\}$ $P(g) = 1$

$P(f) = \exists$ a set of $n - n^\varepsilon$ variables, and assignment to them that makes f constant $\Rightarrow P(F) = 0$

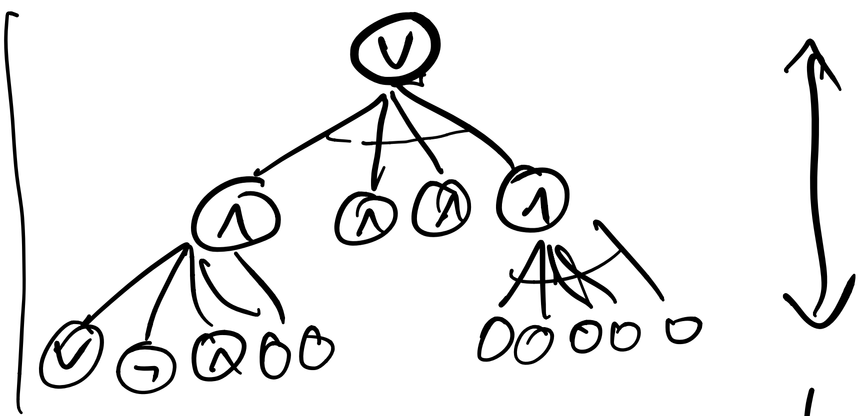
OW $\Rightarrow P(f) = 1$

$2^{O(n)}$

Ex. $P(f)$ = can f be approximated by a poly of deg $\sqrt{n}$

Ex. $P(F)$ = Can not f be computed by a circuit of size n^c

Hastad's switching lemma:



depth $= d =$
$= O(1)$

For every fn computable by a depth-d circuit $\exists$ an assignment of $n - n^{\varepsilon}$ variables ($\varepsilon \in (0,1)$) s.t. the function becomes 0 or 1.

$$F(\underset{\overset{\uparrow}{0}}{x_1}, x_2, \underset{\overset{\uparrow}{1}}{x_3}, \underset{\overset{\uparrow}{0}}{\ldots}, x_n)$$

$$g(y_1, \ldots, y_{n^{\varepsilon}}) = 0$$

$$\quad\quad\quad 0 \; 1 \; 0$$

$$h(x_1, \ldots, x_n) = \underline{x_1 \oplus \ldots \oplus x_n}$$

$$h_2(y_1, \ldots, y_{n^{\varepsilon}}) = \underline{y_1 \oplus \ldots \oplus y_{n^{\varepsilon}}} \, (\oplus 1) \neq 0/1$$

Natural Proofs

- Property of Boolean functions P
- n^c-usefulness:

$$P(f) = 0 \text{ for every } f \in \mathrm{SIZE}(n^c)\,.$$

- Constructiveness: Given the truth table of $f\colon \{0,1\}^n \to \{0,1\}$, one can compute $\boxed{P(f)}$ in time $2^{O(n)}$

TT(F)

Natural Proofs

- Property of Boolean functions P
- n^c-usefulness:

$$P(f) = 0 \text{ for every } f \in \mathrm{SIZE}(n^c).$$

- Constructiveness: Given the truth table of $f\colon \{0,1\}^n \to \{0,1\}$, one can compute $P(f)$ in time $2^{O(n)}$
- Largeness: At least $1/n^{100}$ fraction of all functions $f\colon \{0,1\}^n \to \{0,1\}$ satisfy P

$\boxed{P(f) = 1}$ for many functions f.

You prove CLB for some $\boxed{f} : \{0,1\}^n \to \{0,1\}$

Let's take a random fn $g : \{0,1\}^n \to \{0,1\}$

$h = f \oplus g$

$$h(x) = f(x) \oplus g(x) \iff \boxed{f(x)} = \underline{g}(x) \oplus \underline{h}(x)$$

At least of g & h
requires large circuits

$$\frac{\boxed{g \text{ is random}}}{\boxed{h \text{ is random}}}$$

You proved CLB for f

$\Rightarrow$ implies CLB for a half of all fns

Natural Proofs Limitation

Theorem (RR94)

Suppose that subexponentially strong one-way functions exist. Then there exists a constant c such that there is no n^c-useful natural predicate P.

$\Rightarrow P \neq NP$

$\Rightarrow \exists$ crypto

$f : \{0,1\}^n \to \{0,1\}^n$

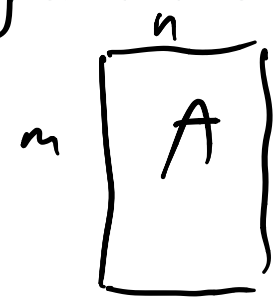
s.t. compute f in poly(n)

cannot invert in time 2^{n^ε} $\quad \varepsilon \in (0,1)$

Max LIN-SAT

$m = \Theta(n)$

Parameters m, n, k. A matrix $\boxed{A \in \mathbb{F}_2^{m \times n}}$ and the distribution



$$D_k^{(A)} = Av + e,$$

$v \in \mathbb{F}_2^n$ is a random vector, $e \in \mathbb{F}_2^m$ is a random vector of Hamming weight $\underline{\underline{k}}$.

best running time $\approx \binom{n}{k} \gg \text{poly}(n)$ for $k = \omega(1)$

Say, $k = n^{\varepsilon}$

$A \in \mathbb{F}_2^{m \times n}$

$v \in \mathbb{F}_2^n$ random

$x = \boxed{A \cdot v} \in \mathbb{F}_2^m$

Given x, I can verify in poly time whether $\left(\boxed{x} = A \cdot v\right)$ for some v

---

Given $\cancel{x}$, check whether

$$x = \boxed{A \cdot v} + \boxed{e}, \text{ where}$$

$e \in \mathbb{F}_2^m$ of Ham weight 1.

In time m, I brute force Ham weight 1, then check whether

$$x - e = A \cdot v$$

Given x,

$x = Av + e$, Hw of e is k.

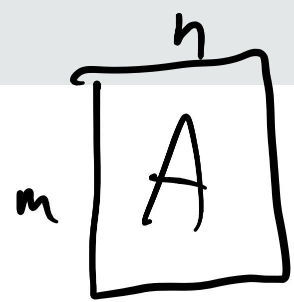
$\binom{n}{\le k} \cdot \mathrm{poly}(n)$

Average LIN-SAT

Conjecture [Ale03]

For every $m(n) = \Theta(n)$, there exists a family of $m(n) \times n$ matrices $A = \{A_n\}$, such that for every function $k(n)$ which satisfies $n^{\varepsilon} < k(n) < n^{1-\varepsilon}$ for some constant $\varepsilon > 0$, any polynomial-time algorithm can distinguish $D_k(A)$ and $D_{k+1}(A)$ only with negligible (in n) probability.

$\underline{D_k(A)}$ & $\underline{D_{k+1}(A)}$



$\underline{D_k(A)} = A \cdot v + e_k$

e_k - random vector of HW k.

$\underline{D_{k+1}(A)} = A \cdot v + e_{k+1}$

e_{k+1} -- of HW $k+1$

$k = n^{\varepsilon}$

$\approx \binom{n}{k} >> \mathrm{poly}(n)$

$\boxed{\text{Conj.}}$ No poly time alg sees the difference between these two distributions

Inapproximability of Rigidity

Theorem (Ale03)

This $\boxed{\text{Conjecture}}$ implies that for every fixed $\varepsilon, \delta > 0$ one cannot distinguish with in poly time *non-negligible probability the following two cases:*

(Yes instance) Any $M \in \{0,1\}^{n \times n}$ such that

$$\boxed{\mathcal{R}_M^{\mathbb{F}_2}(\varepsilon n) < n^{1+\delta}.}$$

low rigidity

(No instance) Any $M \in \{0,1\}^{n \times n}$ such that

$$\boxed{\mathcal{R}_M^{\mathbb{F}_2}(\varepsilon n) \geq \Omega(n^2).}$$

high rigidity

rigidity $\in [n, n^2]$

Our alg:

– Is it true that every $k \times k$ submatrix has full rank?

don't know how to check this in poly time

– Is this matrix a generator of a good code?

don't know (impossible) to solve in poly time.

Inapproximability:

It's known Matrix Rigidity is NP-hard. Under reasonable assumption, you cannot $\boxed{n^{1-\delta}}$ approximate it