Matrix Rigidity

On Explicitness

Sasha Golovnev

September 2, 2020

Recap

- Rigid $\neq$ Sparse $+$ Low-Rank

Recap

- Rigid $\neq$ Sparse $+$ Low-Rank
- Moderately rigid matrices would imply circuit lower bounds

Recap

- Rigid $\neq$ Sparse $+$ Low-Rank
- Moderately rigid matrices would imply circuit lower bounds
- Extremely rigid matrices exist

Constructing Rigid Matrices

- We'll construct two families of very rigid matrices

Constructing Rigid Matrices

- We’ll construct two families of very rigid matrices
- The constructions will now be satisfying

Constructing Rigid Matrices

- We'll construct two families of very rigid matrices
- The constructions will now be satisfying
- Notion of Explicitness

Construction I. Algebraically Independent Numbers

Linearly Independent Numbers

Definition

$x_1, \ldots, x_n \in \mathbb{R}$ are linearly independent over $\mathbb{Q}$ if they do not satisfy any non-trivial linear equation with coefficient in $\mathbb{Q}$:

$$k_1 x_1 + \ldots + k_n x_n \neq 0 \,.$$

except for

for all $k_1, \ldots, k_n \in \mathbb{Q}$ $k_1 = \ldots = k_n = 0$.

Linearly Independent Numbers

Definition

$x_1, \ldots, x_n \in \mathbb{R}$ are linearly independent over $\mathbb{Q}$ if they do not satisfy any non-trivial linear equation with coefficient in $\mathbb{Q}$:

$$k_1 x_1 + \ldots + k_n x_n \neq 0 \,.$$

for all $k_1, \ldots, k_n \in \mathbb{Q}$ $k_1 = \ldots = k_n$.

Example

$\{1, \alpha\}$ are linearly independent over $\mathbb{Q}$ iff α is irrational.

$1 \cdot q_1 = \alpha \cdot q_2 \iff$

$\alpha = \frac{q_1}{q_2} \in \mathbb{Q}$

Examples

Theorem (Besicovitch)

Let $a_1, a_2, \ldots, a_m$ be m distinct square roots of square-free integers, then they are all linearly independent over $\mathbb{Q}$.

$\sqrt{2} \notin \mathbb{Q}$ $\{1, \sqrt{2}\}$

$\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}\}$

Not an ex: $\sqrt{8} = 2\sqrt{2}$

Algebraically Independent Numbers

Definition

$x_1, \ldots, x_n \in \mathbb{R}$ are algebraically independent over $\mathbb{Q}$ if they do not satisfy any non-trivial polynomial equation with coefficient in $\mathbb{Q}$.

Algebraically Independent Numbers

Definition

$x_1, \ldots, x_n \in \mathbb{R}$ are algebraically independent over $\mathbb{Q}$ if they do not satisfy any non-trivial polynomial equation with coefficient in $\mathbb{Q}$.

Examples

- $\{\pi, e^\pi\}$ are algebraically independent over $\mathbb{Q}$

Algebraically Independent Numbers

Definition

$x_1, \ldots, x_n \in \mathbb{R}$ are algebraically independent over $\mathbb{Q}$ if they do not satisfy any non-trivial polynomial equation with coefficient in $\mathbb{Q}$.

Examples

- $\{\pi, e^\pi\}$ are algebraically independent over $\mathbb{Q}$
- $\{\sqrt{e+7}, e^3+1\}$ are not algebraically independent over $\mathbb{Q}$

Algebraically Independent Numbers

Definition

$x_1, \ldots, x_n \in \mathbb{R}$ are algebraically independent over $\mathbb{Q}$ if they do not satisfy any non-trivial polynomial equation with coefficient in $\mathbb{Q}$.

Examples

- $\{\pi, e^\pi\}$ are algebraically independent over $\mathbb{Q}$
- $\{\sqrt{e+7}, e^3+1\}$ are not algebraically independent over $\mathbb{Q}$

  $\{e, \pi\}$—open question!

Perron's Theorem

Theorem

Any set $p_1, \ldots, p_{n+1} \in \mathbb{F}[x_1, \ldots, x_n]$ *of* $n+1$ *polynomials of* n *variables is algebraically dependent.*

Perron's Theorem

Theorem

Any set $p_1, \ldots, p_{n+1} \in \mathbb{F}[x_1, \ldots, x_n]$ *of* $n+1$ *polynomials of* n *variables is algebraically dependent.*

Example

$$p_1 = (x+y)^3$$

$$p_2 = x + y + y^2$$

$$p_3 = y$$

$$A(p_1, p_2, p_3) = (p_2 - p_3^2)^3 - p_1 \equiv 0$$

Lindemann–Weierstrass theorem

Theorem (Lindemann–Weierstrass)

If $x_1, \ldots x_n$ are linearly independent over $\mathbb{Q}$, then $e^{x_1}, \ldots, e^{x_n}$ are algebraically independent over $\mathbb{Q}$.

$$(e^{x_1})^3 + (e^{x_2})^7 + (e^{x_3}) \cdot (e^{x_4})^{10}$$

Lindemann–Weierstrass theorem

Theorem (Lindemann–Weierstrass)

If $x_1, \ldots x_n$ are linearly independent over $\mathbb{Q}$, then $e^{x_1}, \ldots, e^{x_n}$ are algebraically independent over $\mathbb{Q}$.

Example

$e^{\sqrt{2}}, e^{\sqrt{3}}, e^{\sqrt{5}}, e^{\sqrt{6}}, \ldots$ are *algebraically independent.*

Rigidity from Algebraic Independence

Lemma

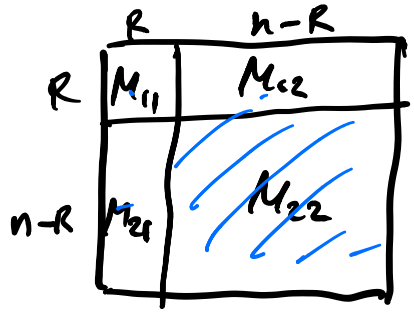
Let $M \in \mathbb{R}^{n\times n}$ *be a matrix where all* n^2 *elements are algebraically independent over* $\mathbb{Q}$*. Then for every* $0 \le r \le n$,

$$\mathcal{R}_M^{\mathbb{R}}(r) = (n-r)^2 \ .$$

Pf. Contrary:

$\exists$ s-sparse matrix S, $s=(n-R)^2-1$

$\mathrm{Rank}(M+S) \le R.$



All entries of M_{22} will be polys of $M_{11}, M_{12}, M_{21}, S$

M polys of $\boxed{M_{11}, M_{12}, M_{21}, S}$

#variables: $n^2-(n-R)^2+s \le n^2-1$

#polys $= n^2$

$\Rightarrow$ $\exists$ poly P satisfied by n^2 polys.

$\Rightarrow$ n^2 entries are <u>not</u> alg ind.

Short descr: $e^1 \quad e^{\sqrt{2}} \quad e^{\sqrt{3}}$ $\square$

Cannot decimal repres.:

Construction II.
Exponential Time

Existence

Theorem (Last Lecture)

Let

$$q = |\mathbb{F}| < \infty\,,$$
$$r = n - \Theta(\sqrt{n})\,,$$
$$s = \Theta((n - r)^2 / \log n)\,.$$

There exists a matrix $M \in \mathbb{F}^{n \times n}$:

$$\mathcal{R}_M^{\mathbb{F}}(r) \geq s\,.$$

Algorithm

- For every $M \in \mathbb{F}^{n \times n}$
  - If for every s-sparse $S \in \mathbb{F}^{n \times n}$
  - $\quad \mathbf{rank}(M + S) \geq r$
  - Then $\mathcal{R}_M^{\mathbb{F}}(r) \geq s$

Algorithm

- For every $M \in \mathbb{F}^{n \times n}$
  - If for every s-sparse $S \in \mathbb{F}^{n \times n}$
  - $\textbf{rank}(M + S) \geq r$
  - Then $\mathcal{R}_M^{\mathbb{F}}(r) \geq s$

Correctness

Follows from existence.

Algorithm

- For every $M \in \mathbb{F}^{n \times n}$
  - If for every s-sparse $S \in \mathbb{F}^{n \times n}$
  - $\quad \mathbf{rank}(M + S) \geq r$
  - Then $\mathcal{R}_M^{\mathbb{F}}(r) \geq s$

Correctness

Follows from existence.

Running time

$q^{n^2} \cdot q^{n^2} \cdot n^{O(1)} = q^{O(n^2)}$

Infinite Fields

- Brute force doesn’t work

Infinite Fields

- Brute force doesn't work
- We'll prove that there exists a rigid (over $\mathbb{R}$) matrix $M \in \{0,1\}^{n \times n}$

Infinite Fields

- Brute force doesn't work
- We'll prove that there exists a rigid (over $\mathbb{R}$) matrix $M \in \{0,1\}^{n\times n}$
- We'll show that one can check rigidity of a matrix $M \in \mathbb{R}^{n\times n}$ in time $2^{O(n^2)}$

Infinite Fields

- Brute force doesn't work
- We'll prove that there exists a rigid (over $\mathbb{R}$) matrix $M \in \{0,1\}^{n \times n}$
- We'll show that one can check rigidity of a matrix $M \in \mathbb{R}^{n \times n}$ in time $2^{O(n^2)}$

Zero-patterns

Definition

For a set of *t*-variate polynomials $F = \{f_i\}_{i \in [m]}$, its set of *zero-patterns* is the of all sequences of zero-non-zero outputs of functions from F:

$M = 01010$ iff $\exists x$: $f_1(x) = 0$; $f_2(x) \neq 0$ $f_3(x) = 0$ ...

$$Z(F) = \{M \in \{0,1\}^m : \ \exists x \in \mathbb{F}^t \ \forall i \in [m], \ M_i = \mathbf{1}_{f_i(x) \neq 0}\}.$$

ZERO-PATTERNS

Definition

For a set of t-variate polynomials $F = \{f_i\}_{i \in [m]}$, its set of *zero-patterns* is the of all sequences of zero-non-zero outputs of functions from F:

$$Z(F) = \{M \in \{0,1\}^m : \exists x \in \mathbb{F}^t \ \forall i \in [m],\ M_i = \mathbf{1}_{f_i(x) \neq 0}\}.$$

Lemma (RBG01)

$$|Z(F)| \leq \binom{t+dm}{t}.$$

$\approx (dm)^t \ll$ compare 2^m

$$|Z(F)| \le \binom{t+dm}{t}.$$

Poly method ♡

Pf. $N = |Z(F)|$

$\underline{x}_1, \dots, \underline{x}_N \in \mathbb{R}^t$ "witness"

N distinct zero-patterns of F.

1000 $\quad \exists\, \underline{x}_1 \in \mathbb{R}^t$

$f_1(x_1) \ne 0 \quad f_2(x_1) = f_3(x_1) \dots = f_m(x_1) = 0$

0101 $\quad x_2$

$\underline{i} \in [N]$. $\quad S_i \subseteq [m]$ — the set of (indices of) polys from F which are **not** zeros at x_i

$$\underline{g_i} = \prod_{k \in S_i} f_k \qquad \boxed{g_i(x_i) \ne 0}$$

N polys g_i $\quad$ Later say $N \le \dots$

$g_i(x_j) = 0$ iff $\exists f_k \in S_i \setminus S_j$

.

$g_i(x_j) = 0$ iff $\exists f_k \in S_i \setminus S_j$

Which polys are 0 at point x_j

$S_j \equiv$ polys which are **not** zeros

All but polys from S_j $= 0$ at x_j.

$g_i = \prod_{f \in S_i} f$ $\quad g_i(x_j) = 0$ $\quad \exists f_k \in S_i \setminus S_j$

$$g_i(x_j) = 0 \text{ iff } S_i \not\subseteq S_j$$

All polys g_i are linearly ind.

$\exists a_1 \dots a_N \in \mathbb{R}$:

$$\sum_{i \in [N]} a_i g_i \equiv 0 \quad \exists a_i \neq 0$$

$$i^* = \operatorname{argmin}_{i \in [N],\, a_i \neq 0} |S_i|$$

$$\sum_{i \in [N]} a_i g_i (x_{i*}) = 0$$

$$g_{i*}(x_{i*}) \neq 0 \Rightarrow a_{i*} g_{i*}(x_{i*}) \neq 0 \checkmark$$

$$\forall a_i \neq 0, \; S_i \nsubseteq S_{i*} \Leftrightarrow g_i(x_{i*}) = 0 \checkmark$$

N linearly ind polys of t variables, each of degree dm

$d = 1$

x_1
⋮
x_t

t lin polys.

$d = 2$

$x_1^2 \quad x_1 x_2 \quad x_1 x_3 \cdots \quad x_t x_{t-1}, \; x_t^2$

---

comb (with repet.)

$$\left(\!\!\binom{t}{dm}\!\!\right) = \binom{t + dm - 1}{t} \qquad \square$$

Binary Rigid Matrix

Theorem (PR94)

For all large enough n, there exists a matrix $M \in \{0,1\}^{n\times n}$ such that

$$\mathcal{R}_M^{\mathbb{R}}\left(\frac{n}{200}\right) \geq \frac{n^2}{100} .$$

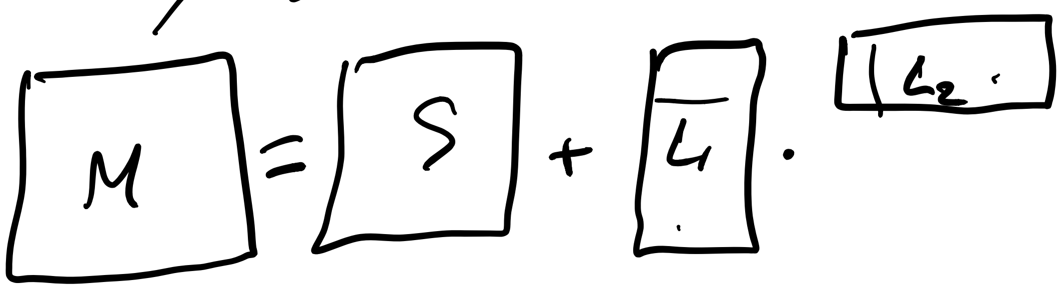
$M \in \{0,1\}^{n\times n}$

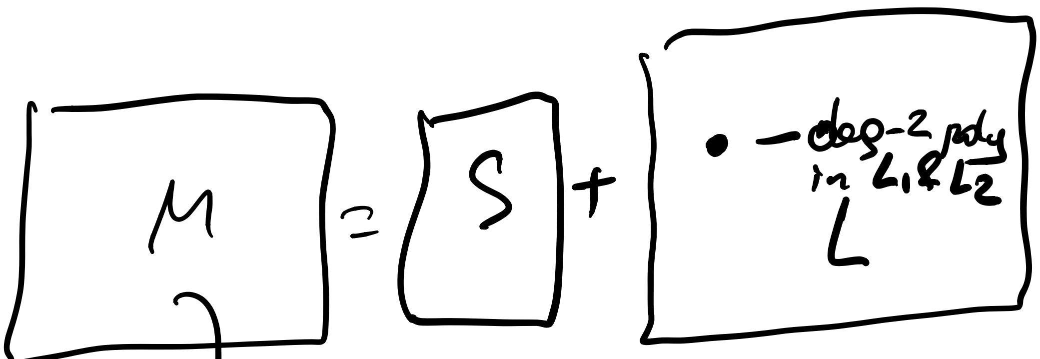
$M = S + L = S + L_1 \cdot L_2$

$\|S\|_0 = s$ $\quad$ $\mathrm{rk}(L) \le R$ $\quad$ $L_1 \in \mathbb{R}^{n\times R}$ $\quad$ $L_2 \in \mathbb{R}^{R\times n}$

s var $\quad$ n^2 var

deg-1 in S, L





deg-2 poly in S, L_1, L_2

$s + nR + nR$

Lemma (RBG01)

$$|Z(F)| \leq \binom{t+dm}{t}.$$

$R = \frac{n}{200}$ $S = \frac{n^2}{100}$

M - deg-2 in $S+2Rn$ vars.

$m = n^2$ polys

$d = 2$ - degree

$t = S + 2Rn \leq \frac{n^2}{100} + \frac{n^2}{100} = \frac{n^2}{50}$ vars

$$|Z(F)| \leq \binom{t+dm}{t} \approx \binom{2n^2 + \frac{n^2}{50}}{\frac{n^2}{50}}$$

$$\leq 2^{n^2(2+\frac{1}{50})\cdot \varepsilon} << 2^{n^2/10}$$

upper bound on $\{0,1\}$ non-rigid matrices.

$\#$ non-rigid matrices $\leq$ $\#$ zero-patterns $\cdot \binom{n^2}{\leq S}$

$$\leq 2^{n^2/10} \cdot \binom{n^2}{\frac{n^2}{100}} << 2^{n^2/2}$$

Total $\#$ matrices 2^{n^2} $\square$

Infinite Fields

- Brute force doesn't work
- We'll prove that there exists a rigid (over $\mathbb{R}$) matrix $M \in \{0,1\}^{n\times n}$
- We'll show that one can check rigidity of a matrix $M \in \mathbb{R}^{n\times n}$ in time $2^{O(n^2)}$

Checking Rigidity

Theorem

One can decide whether a system of m degree-2 polynomials of n variables with $\{0,1\}$-coefficients has a solution in time $O(m^{O(1)}2^{O(n)})$.

degree-d polys

$O(m \cdot d^{O(n)})$ arithmetic op.

length poly(input length, m, d)

Checking Rigidity

Theorem

One can decide whether a system of m degree-2 polynomials of n variables with $\{0,1\}$-coefficients has a solution in time $O(m^{O(1)} 2^{O(n)})$.

Theorem

Let $M \in \{0,1\}^{n \times n}$, and r and s be non-negative integers. Then one can decide whether $\mathcal{R}_M^{\mathbb{R}}(r) > s$ in time $2^{O(n^2)}$.

Theorem 1

One can decide whether a system of m degree-2 polynomials of n variables with $\{0,1\}$-coefficients has a solution in time $O(m^{O(1)}2^{O(n)})$.

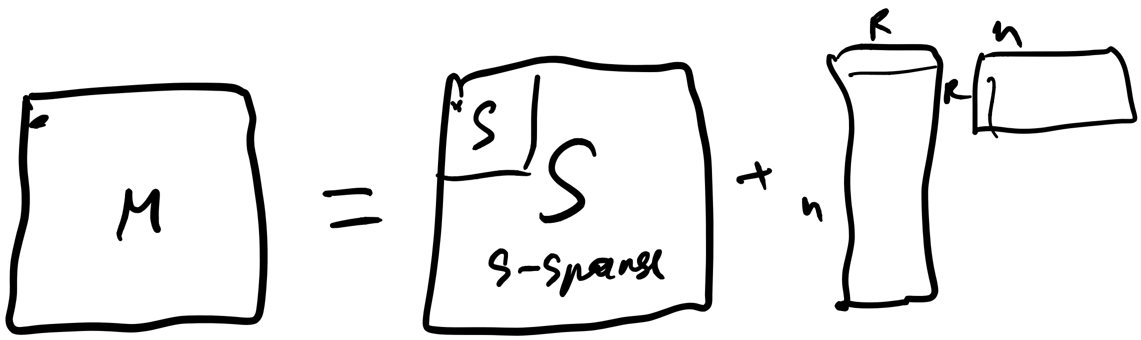
Theorem

Let $M \in \{0,1\}^{n \times n}$, and r and s be non-negative integers. Then one can decide whether $\mathcal{R}_M^{\mathbb{R}}(r) > s$ in time $2^{O(n^2)}$.

Pf. $M = S + L = S + L_1 \cdot L_2$ (S: sparse, L: small)

iff

M is non-rigid



For one $\binom{n^2}{s}$ choices of non-zeros in S:

n^2 entries of M = degree 2-poly equations.

vars, S, L_1, L_2. check $\exists$ sol Thm 1

#vars $s + n \cdot R + n \cdot R$

time $2^{O(n^2)} \cdot \binom{n^2}{s} = 2^{O(n^2)}$ □

Constructing Rigid Matrices

- We'll construct two families of very rigid matrices
- The constructions will now be satisfying
- Notion of Explicitness

Super-exp.

2^{n^2}

$2^{O(n)} \in E$

CCB for E | Even E^{NP}

Explicit matrices $=$ have algorithms outputting all their entries in polynomial time

Summary

rigidity	field	running time

Summary

rigidity	field	running time
$\frac{(n-r)^2}{\log n}$	$\lvert\mathbb{F}\rvert < \infty$	existence

Summary

rigidity	field	running time
$\frac{(n-r)^2}{\log n}$	$\lvert\mathbb{F}\rvert < \infty$	existence
$(n-r)^2$	$\lvert\mathbb{F}\rvert = \infty$	existence

SUMMARY

rigidity	field	running time
$\frac{(n-r)^2}{\log n}$	$\lvert\mathbb{F}\rvert < \infty$	existence
$(n-r)^2$	$\lvert\mathbb{F}\rvert = \infty$	existence
$(n-r)^2$	$\mathbb{R}$	alg ind ent

SUMMARY

rigidity	field	running time
$\frac{(n-r)^2}{\log n}$	$\lvert\mathbb{F}\rvert < \infty$	existence
$(n-r)^2$	$\lvert\mathbb{F}\rvert = \infty$	existence
$(n-r)^2$	$\mathbb{R}$	alg ind ent
$\frac{(n-r)^2}{\log n}$	$\lvert\mathbb{F}\rvert < \infty$	$2^{O(n^2)}$

SUMMARY

rigidity	field	running time
$\frac{(n-r)^2}{\log n}$	$\lvert\mathbb{F}\rvert < \infty$	existence
$(n-r)^2$	$\lvert\mathbb{F}\rvert = \infty$	existence
$(n-r)^2$	$\mathbb{R}$	alg ind ent
$\frac{(n-r)^2}{\log n}$	$\lvert\mathbb{F}\rvert < \infty$	$2^{O(n^2)}$
$(n-r)^2$	$\mathbb{R}$	$2^{O(n^2)}$

Overview

- Next week: Explicit constructions

Overview

- Next week: Explicit constructions
- Next month: Less explicit but more rigid constructions