Matrix Rigidity

Introduction

Sasha Golovnev

August 31, 2020

Recap

- Non-rigid = Sparse + Low-Rank

Recap

- Non-rigid $=$ Sparse $+$ Low-Rank
- Rigid $\neq$ Sparse $+$ Low-Rank

Recap

- Non-rigid $=$ Sparse $+$ Low-Rank
- Rigid $\neq$ Sparse $+$ Low-Rank
- Proving Valiant's result:
  rigid matrices require log-depth circuits
  of super-linear size

Rigidity Implies Circuit Lower Bounds

Theorem (Val77)

Let $\mathbb{F}$ be a field, and $A \in \mathbb{F}^{n \times n}$ be a family of matrices for $n \in \mathbb{N}$.

If $\mathcal{R}_A^{\mathbb{F}}(\varepsilon n) > n^{1+\delta}$ for constant $\varepsilon, \delta > 0$, then any $O(\log n)$-depth linear circuit computing $x \to Ax$ must be of size $\Omega(n \cdot \log \log n)$.

Depth Reduction

Lemma (EGS75)

Let G be an acyclic digraph with s edges and of depth $d = 2^k$.

There exists a set of $s/\log d$ edges in G such that after their removal, the longest path in G has length at most $d/2$.

Rigidity Implies Circuit Lower Bounds

Theorem (Val77)

If $\mathcal{R}_A^{\mathbb{F}}(\varepsilon n) > n^{1+\delta}$ *for constant* $\varepsilon, \delta > 0$*, then any* $O(\log n)$*-depth linear circuit computing* $x \to Ax$ *must be of size* $\Omega(n \cdot \log\log n)$.

Theorem (Val77)

If $\mathcal{R}_A^{\mathbb{F}}(\varepsilon n) > n^{1+\delta}$ for constant $\varepsilon, \delta > 0$, then any $O(\log n)$-depth linear circuit computing $x \to Ax$ must be of size $\Omega(n \cdot \log\log n)$.

Lemma (EGS75)

Let G be an acyclic digraph with s edges and of depth $d = 2^k$.

There exists a set of $s/\log d$ edges in G such that after their removal, the longest path in G has length at most $d/2$.

$\exists$ circuit C computing A.

$\forall$ c_d. If $\mathrm{depth}(C) \le c_d \log n$,

then $\mathrm{size}(C) \ge c_s \cdot n \log\log n$,

where $c_s = \dfrac{\varepsilon}{\log c_d + \log(1/\delta)} = s$.

G – the graph of C, dag.

Apply Edge Remova Lemma

t times, $t = \log c_d + \log(1/\delta)$

	depth(C)	# removed edges
	$c_d \log n$	0
1	$c_d \log n/2$	$\frac{s}{\log d}$
2	$\frac{c_d \log n}{2^2}$	$\frac{s}{\log(d/2)}$
– – –	– – –	– – –
t	$\frac{c_d \log n}{2^t}$	$\frac{s}{\log d - t}$

After t steps:

depth $\frac{d}{2^t}$

$\theta(\log n)$

$d = c_d \log n$

is constant

$t = \log c_d + \log(\frac{1}{\delta})$

$$\text{depth} \le \frac{d}{2^t} = \frac{c_d \log n}{c_d \cdot (1/\delta)} = \delta \log n$$

Total # of removed edges

$$\boxed{t \cdot \frac{s}{\log d - t}}$$

t - constant

$s \sim \varepsilon n \log \log n$

$d \sim \log n$

$\log d - t \ge \log(d/2)$

$$t \cdot \frac{s}{\log d - t} \le \frac{ts}{\log(d/2)}$$

$$= \frac{(\log c_d + \log(\frac{1}{\delta})) \cdot \frac{\varepsilon}{\log c_d + \log(\frac{1}{\delta})} n \log \log n}{\log(d/2)}$$

$\circ \le \varepsilon n$

G of depth $d = c_d \log n$

and size $s \le c_s \cdot n \log\log n$.

We apply Edge Removal Lemma

$t = \Theta(1)$ times

We end up with a G'

of depth $\le \delta \log n$

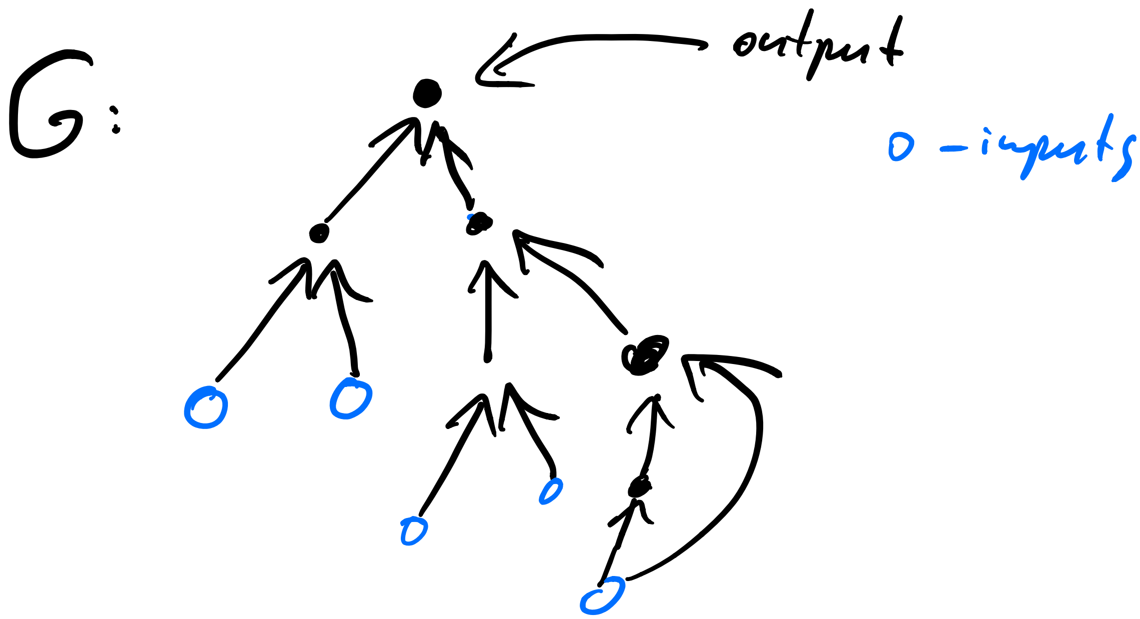
We've removed $\le \varepsilon n$ edges

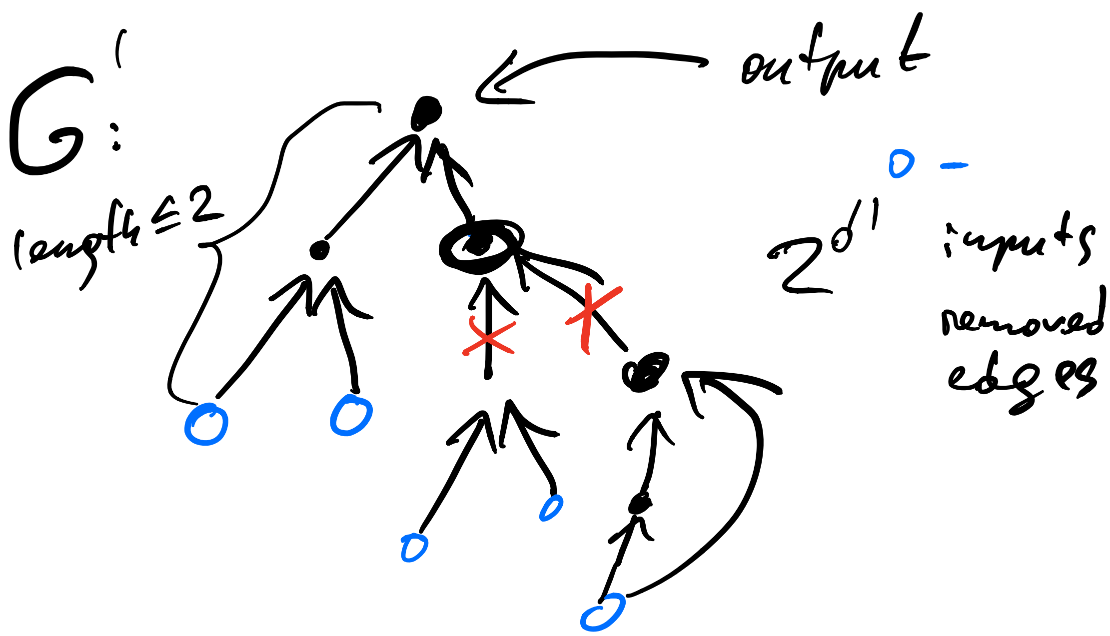
Every output of G' depends on

$\le n^\delta$ inputs

AND

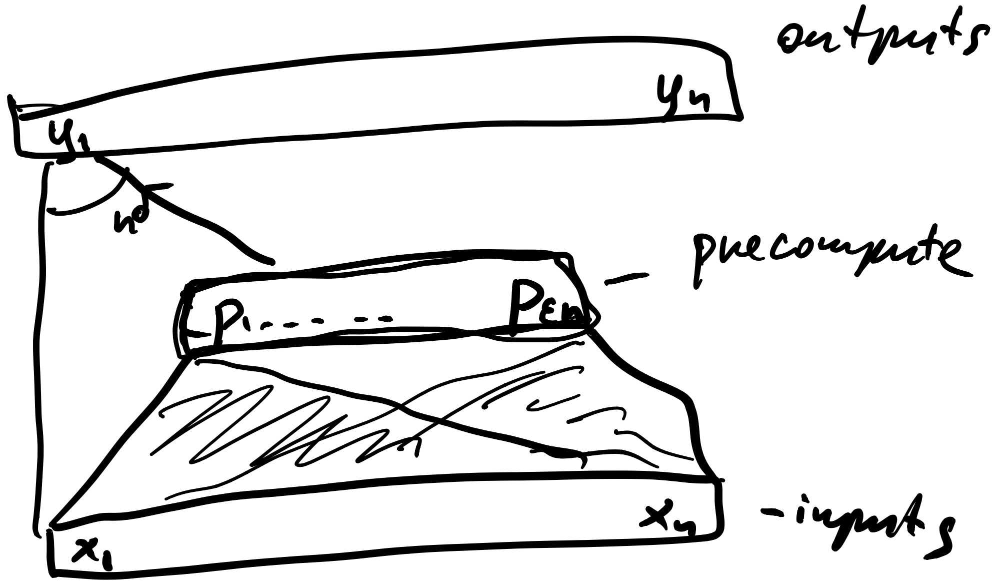
$\le n^\delta$ "removed edges"


G:
output
o - inputs


G':
output
length ≤ 2
o - $2^{d'}$ inputs
removed edges

common bits model

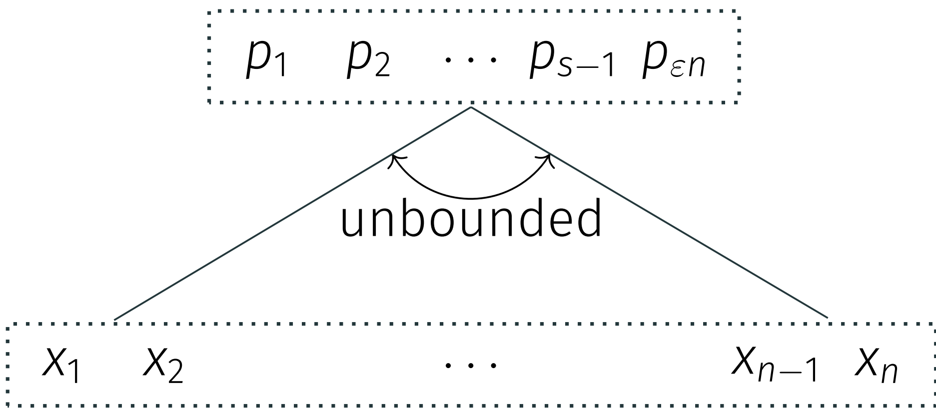
εn - edges



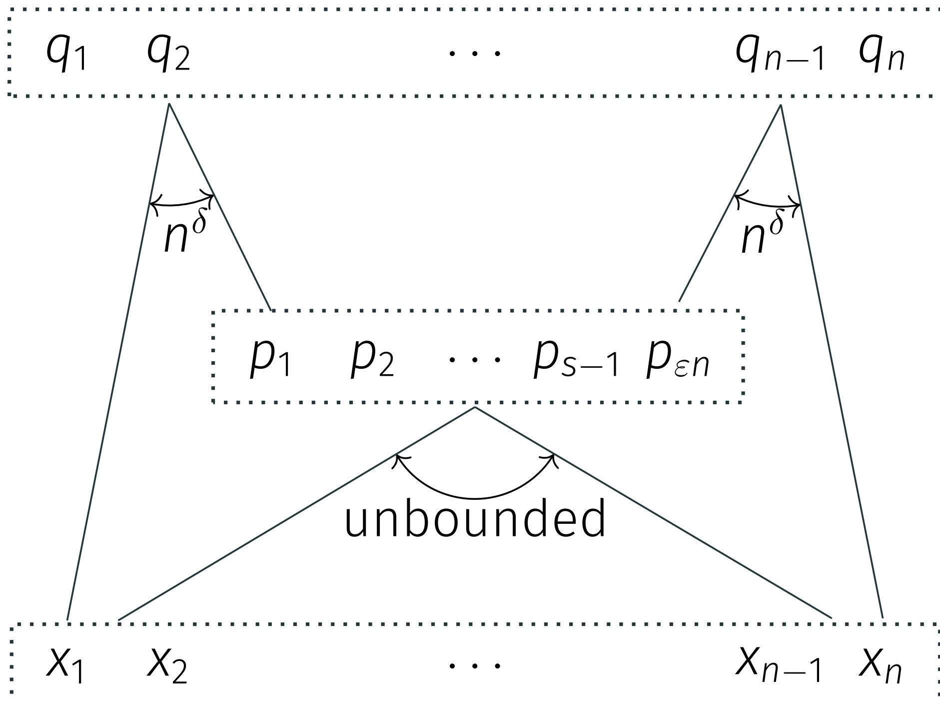
Linear-Size Log-Depth Circuits [Val77]

$x_1 \quad x_2 \quad \cdots \quad x_{n-1} \quad x_n$

Linear-Size Log-Depth Circuits [Val77]



Linear-Size Log-Depth Circuits [Val77]



Small Circuits are Not Rigid

- A linear circuit computes Mx for input $x \in \mathbb{F}^n$ where $M \in \mathbb{F}^{m \times n}$

Small Circuits are Not Rigid

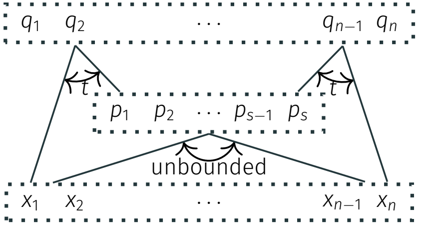
- A linear circuit computes Mx for input $x \in \mathbb{F}^n$ where $M \in \mathbb{F}^{n\times n}$
- For a circuit of size $O(n)$ and depth $O(\log n)$,

Small Circuits are Not Rigid

- A linear circuit computes Mx for input $x \in \mathbb{F}^n$ where $M \in \mathbb{F}^{m \times n}$

$x \to Mx$

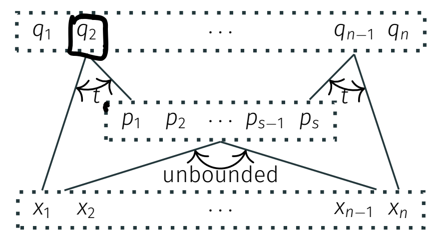
- For a circuit of size $O(n)$ and depth $O(\log n)$,



Small Circuits are Not Rigid

- A linear circuit computes Mx for input $x \in \mathbb{F}^n$ where $M \in \mathbb{F}^{m \times n}$
- For a circuit of size $O(n)$ and depth $O(\log n)$,

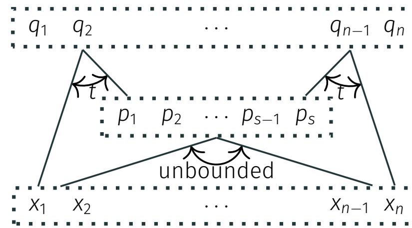
$$M = \overset{o/i}{A} + \underline{\overset{o/p}{C} \cdot \overset{p/i}{D}}$$



Small Circuits are Not Rigid

- A linear circuit computes Mx for input $x \in \mathbb{F}^n$ where $M \in \mathbb{F}^{m \times n}$
- For a circuit of size $O(n)$ and depth $O(\log n)$,

$$\overset{\cancel{m}\,n \times n}{M} = \overset{\cancel{m}\,n \times n}{A} + \overset{\cancel{m}\,n \times \varepsilon n}{C} \cdot \overset{\varepsilon n \times n}{D}$$

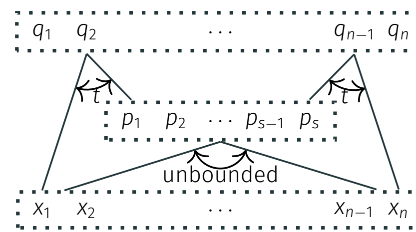


Small Circuits are Not Rigid

- A linear circuit computes Mx for input $x \in \mathbb{F}^n$ where $M \in \mathbb{F}^{m\times n}$
- For a circuit of size $O(n)$ and depth $O(\log n)$,

$$\overset{m\times n}{M} = \overset{m\times n}{A} + \overset{m\times \varepsilon n}{C} \cdot \overset{\varepsilon n\times n}{D}$$

sparse



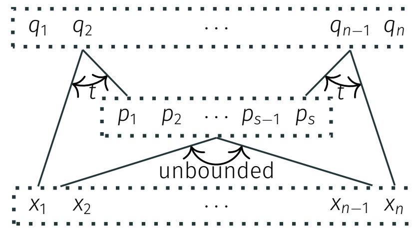
Small Circuits are Not Rigid

- A linear circuit computes Mx for input $x \in \mathbb{F}^n$ where $M \in \mathbb{F}^{m\times n}$
- For a circuit of size $O(n)$ and depth $O(\log n)$,

$$\overset{m \times n}{M} = \overset{m \times n}{A} + \overset{m \times \varepsilon n}{C} \cdot \overset{\varepsilon n \times n}{D} = A + \boxed{B}$$

sparse sparse

low-rank



Small Circuits are Not Rigid

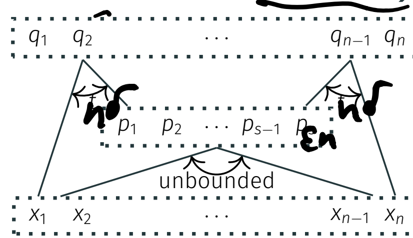
- A linear circuit computes $\underline{Mx}$ for input $x \in \mathbb{F}^n$ where $M \in \mathbb{F}^{m \times n}$

$$x \longrightarrow Mx$$

- For a circuit of size $\underline{O(n)}$ and depth $O(\underline{\log n})$,

$$\underbrace{\overset{m \times n}{M}} = \overset{m \times n}{A} + \overset{m \times \varepsilon n}{C} \cdot \overset{\varepsilon n \times n}{D} = A + B$$

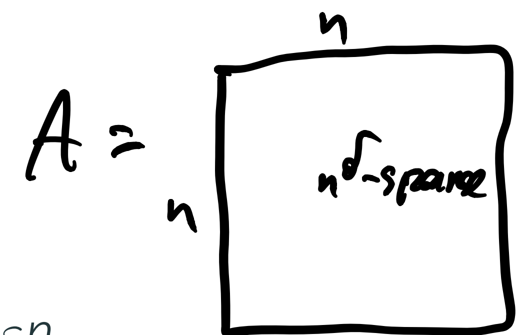
$A + C \cdot D$: sparse; A: sparse; B: low-rank



- $M \in \mathbb{F}^{m \times n}$ is not rigid:

$$M = A + B$$

A: s-sparse $= \leq n^{1+\delta}$; B: $\operatorname{rk} \leq \varepsilon n$



Rigidity for rank $n/100$ and sparsity $n^{1.01}$ implies super-linear circuit lower bounds

Existence of Rigid Matrices

Minimal and Maximal Rigidity

- We know there are matrices of rigidity 0

Minimal and Maximal Rigidity

- We know there are matrices of rigidity 0
- What is maximal rigidity? (Do rigid matrices even exist?)

Minimal and Maximal Rigidity

- We know there are matrices of rigidity 0
- What is maximal rigidity? (Do rigid matrices even exist?)
- What is "typical" rigidity?

Bounds on Rigidity

- First, we show that $\mathcal{R}_A^{\mathbb{F}}(r) \leq (n-r)^2$.

  (Which is much larger than what we need for circuit lower bounds.)

$R = \varepsilon n \Rightarrow \mathcal{R}(R) \geq n^{1+\delta}$

Bounds on Rigidity

- First, we show that $\mathcal{R}^{\mathbb{F}}_{A}(r) \leq (n-r)^2$.

  (Which is much larger than what we need for circuit lower bounds.)

- Then we show that most matrices achieve this bound!

Rigidity Upper Bound

Theorem

For any $\mathbb{F}, A \in \mathbb{F}^{n \times n}, 0 \leq r \leq n$,

$$\mathcal{R}_A^{\mathbb{F}}(r) \leq (n-r)^2 \ .$$

Case 1. $rk(A) < R$

$$R_A^F(R) = 0 \le (n-R)^2$$

<u>Case 2.</u> $rk(A) \geq R \Rightarrow \exists B \in F^{R \times R}$

$rk(B) = R$, B – submatrix of A.

Wlog

$$A = \begin{array}{c|c|c|} & R & n-R \\ \hline R & B & A_{12} \\ \hline n-R & A_{21} & A_{22} \\ \hline \end{array}$$

Every row of A_{21} is a <u>unique</u> linear comb. of rows of B.

<u>Change</u> entries A_{22}, so that they're same lin comb of A_{12}

Every row of the new matrix is a lin comb of the first R rows. $\Rightarrow R_A^F(R) \le (n-R)^2$

Existence of Rigid Matrices

Theorem

For any field $\mathbb{F}$,

- *if $\mathbb{F}$ is infinite, then for all $0 \leq r \leq n$ there exists a matrix $M \in \mathbb{F}^{n \times n}$ of rigidity*

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

- *if $\mathbb{F}$ is finite, then for all $0 \leq r \leq n - \Omega(\sqrt{n})$ there exists a matrix $M \in \mathbb{F}^{n \times n}$ of rigidity*

$$\mathcal{R}_M^{\mathbb{F}}(r) = \Omega\left((n-r)^2 / \log n\right) .$$

Proof: $M_{R,S} = \{ M \in \mathbb{F}^{n\times n} : R^{\mathbb{F}}_{M}(R) \le S \}$

~ set of non-rigid matrices

$|M_{R,S}| <<$ "the size" of the set of all matrices

$M \in M_{R,S}$

$M = L + S$,

$rk(L) \le R$; $\|S\|_0 \le S$

$$L = \begin{array}{c|cc} & R & n-R \\ \hline R & L_{11} & \\ n-R & & \end{array}$$

$rk(L_{11}) = rk(L)$

After one of $\binom{n}{R}^2$ permut. of (rows & cols $\le 2^{2n}$

Apply same per to M:

$$M = \begin{array}{c|cc} & R & n-R \\ \hline R & M_{11} & M_{12} \\ n-R & M_{21} & M_{22} \end{array}$$

Fix one of $\binom{n^2}{S}$ choices of non-zeros of S

$M_{22} = M_{21} \cdot M_{11}^{-1} \cdot M_{12}$

Case 1. $|F| = q < \infty$

$$M = \begin{array}{c|c|c|} & k & n-k \\ \hline k & M_{11} & M_{21} \\ \hline n-k & M_{12} & M_{22} \\ \hline \end{array}$$ is uniquely det.

1. One of $\binom{n}{k}^2 \leq 2^{2n}$ permutations

2. s-tuple of non-zeros in S — describe S

$\binom{n^2}{s}$

3. q^s values of non-zeros in S

4. All the entries in M_{11}, M_{12}, M_{21}

$q^{n^2-(n-k)^2}$

$$|M_{k,s}| \leq 2^{2n} \cdot \binom{n^2}{s} \cdot q^s \cdot q^{n^2-(n-k)^2}$$

$$<< q^{n^2}$$

$$|M_{R,S}| \leq 2^{2n} \cdot \binom{n^2}{s} \cdot q^s \cdot q^{n^2-(n-R)^2}$$

$$\ll \underline{q^{n^2}}$$

$$2^{2n} \cdot n^{2s} \cdot q^s \ll q^{(n-R)^2}$$

IF $\boxed{\begin{array}{l} R \leq n - 10\sqrt{n} \\ S \leq \dfrac{(n-R)^2}{10 \log n} \end{array}}$

Then

$$2^{2n} \cdot n^{2s} \cdot \boxed{q^S} \ll q^{(n-R)^2}$$

$$q^{(n-R)^2} \geq q^{100n}$$

$$2^{2n} \cdot n^{2s} \leq 2^{2n} \cdot 2^{2s \log n} \ll$$

$$\ll q^{(n-R)^2/2}$$

Case 2. Infinite Fields

$$R_A^F(r) = (n-r)^2 \text{ for } A.$$

$M \in M_{r,s}$

$$\begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix}$$

Fix perm one of finite # of perm

Fix one of finite # of ways to choose s-tuple

M_{22} - is a rational fn of M_{11}, M_{12}, M_{21}

rational fn

$$p : \mathbb{F}^{n^2-(n-r)^2+s} \longrightarrow \mathbb{F}^{n^2}$$

$$s < (n-r)^2$$

$$\mathbb{F}^{n^2-1} \longrightarrow \mathbb{F}^{n^2}$$

Outputs of p are alg dependent.

$\exists$ poly of n^2 variables $\equiv 0$

3 funs of 2 var.

x

y^2 alg dep.

$\underline{x^3+y^7}$

$$p(t_1,t_2,t_3) = (t_3 - t_1^3)^2 - t_2^7$$

$t_1 = x$

$t_2 = y^2$ $\Rightarrow p \equiv 0$

$t_3 = x^3+y^7$

n^2 funs of n^2-1 inputs are alg dep $\Rightarrow \exists$ poly

n^2 funs are root of this poly

After fixed perm & s-tuple:

All $\overset{\text{non-rigid}}{\text{matrices}}$ are outputs of $F^{n^2-1} \to F^{n^2}$; roots of a fixed poly.

Multiply finite # of polys $\Rightarrow$ polys