I Provable cryptography

OWF/OWP

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

1. Easy to compute:
   $x \to f(x)$ in $poly(n)$
2. Hard to invert (on average):
   $\forall$ poly-time alg A:

$X = \{x : A(f(x)) = x\}$

$|X| < \frac{2^n}{p(n)}$ $\forall$ poly $p(n)$.

E.g. $|X| = 1.9^n$ points.

---

1. Easy to compute
2. Hard to invert (in the worst-case)

$\forall$ poly-time alg A:

$|X| < 2^n$

Existence of these funs $\Rightarrow P \neq NP$

Provable crypto?

- Don't even know how to find a function which cannot invertable poly-time.

- Easy to compute: $2 \cdot n$
  Hard to invert: $10 \cdot n$

  Even this we don't know how to do:
  the best lower bounds we can prove $\approx 3n$.

- Easy to compute $\approx n$
  Hard to invert $\approx 3n$

  Almost.

We know:

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

can be computed by a circuit of size $\approx n$.

In order to invent f you have to have a circuit of size $\geq 2n$.

invent on ALL inputs

In fact, you can invent on $\frac{1}{2}$ of the inputs by a circuit of size $< n$.

Q: Design some f s.t. hard to invent even on $\frac{2^n}{n^{100}}$ inputs.

[Hiltgen 1994]

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

can compute in time $\approx n$

cannot invert in time $\approx \frac{3n}{2}$.

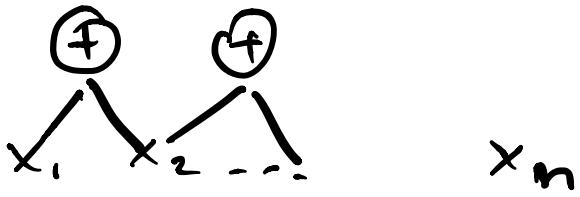
$F(x) = A \cdot x$ over $\mathbb{F}_2$.

$x \in \{0,1\}^n$

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

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$A \cdot x = \begin{bmatrix} x_1 + x_2 \\ x_2 + x_3 \\ x_3 + x_4 \\ \vdots \\ x_{n-1} + x_n \end{bmatrix}$$

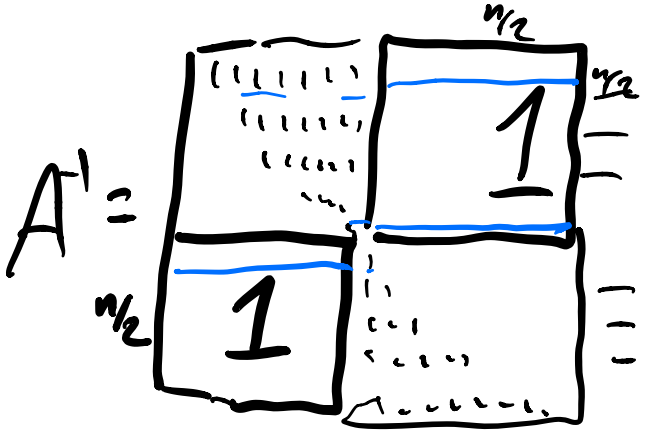


I only need $\approx n$ gates to compute.

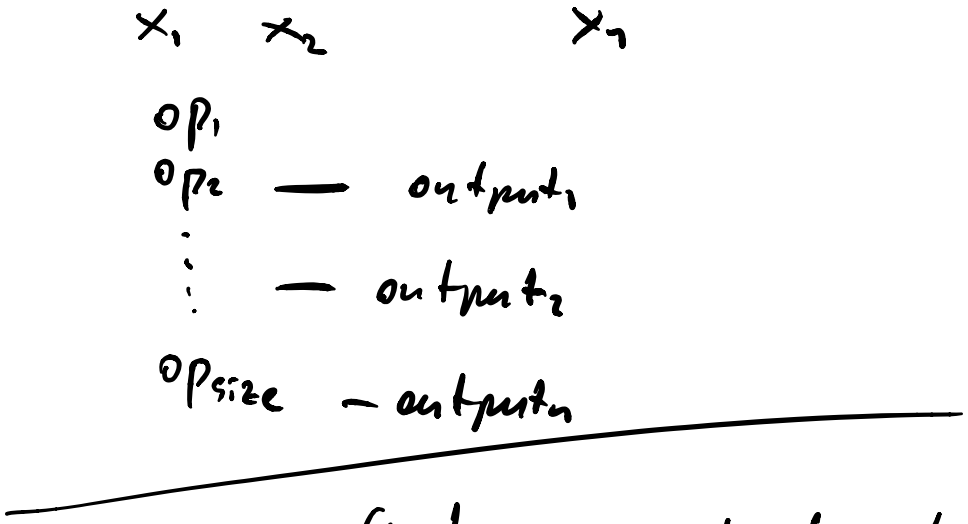
$f(x) \rightarrow x \qquad A^{-1}$

Circuit C:

$x \rightarrow A^{-1}x$



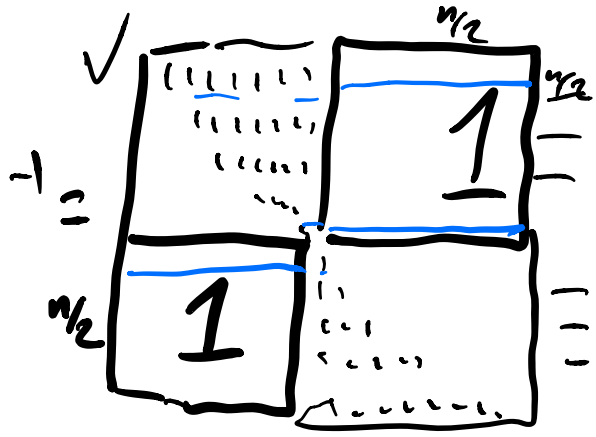
$size(C) \geq \frac{3n}{2}$



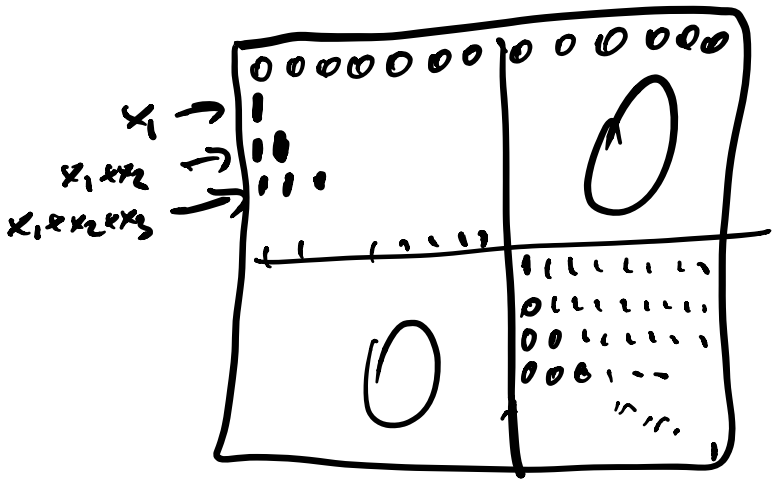
operation that corresponds to output$_1$

even outputs can only be computed in $op_{\frac{n}{2}-1}$, but after output$_1$ I still have $\geq n-1$ operations.

$\Rightarrow$ circuit size $\geq \frac{3}{2}n$.



Inputs $x_1 + x_2 + \cdots + x_n = 0 \pmod 2$



invert in
line n

1. We read the known constructions ✓

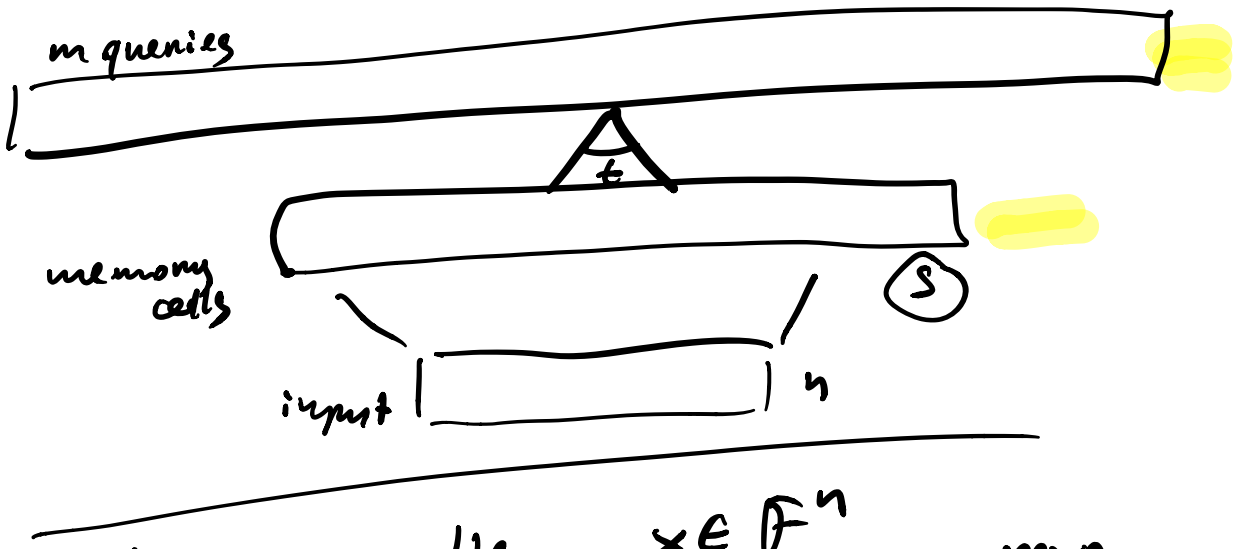
2. We show they are easy to invent on $\frac{1}{2}$ inputs ○

3. [Optional] Develop a function which is hard to invent on average. (⇒ A version of matrix rigidity!)

○

II Data Structures & Rigidity.

Linear DS



Linear problem $x \in \mathbb{F}^n$

Mx for some $M \in \mathbb{F}^{m \times n}$

Memory cells computes:

$A \cdot x$ for some $A \in \mathbb{F}^{s \times n}$

Queries $\boxed{B \cdot (Ax)}$ $B \in \mathbb{F}^{m \times s}$

in every row of B $\leq t$ non-zeros

B is sparse

$\exists$ Efficient linear DS for M

$\Longleftrightarrow$ $M = B \cdot A$

B is sparse

A is small

$M \in \mathbb{F}^{m \times n}$ $\quad m = n^{100}$

$B \in \mathbb{F}^{m \times s}$ $\quad s = 100n$

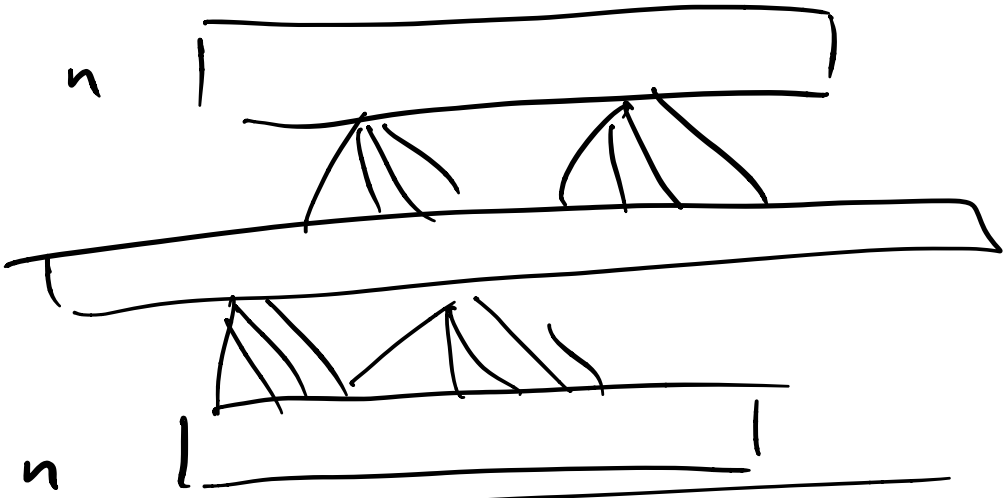
t-sparse, $t = \log n$

$A \in \mathbb{F}^{s \times n}$ – small

DS LB $\Leftrightarrow$ matrix $M \neq$

$\neq$ sparse · small

Depth-2 circuits, linear



size circuit = # edges

$M = D \cdot C$,

size of circuit = # non-zeros in C and D.

Circuit lower bound $\Leftrightarrow$

$M \neq C \cdot D$ for sparse C & D.

↗ we know how to prove some circuit lower bounds.

---

1. Systematic DS $\Leftrightarrow$ Matrix Rigidity ✓

2. Several nice circuits lower bounds (some are proven via matrix rigidity). ✓

3. [Optional]. Let's see which of these techniques can be used for DS. ○

III Random Algebraic Method.

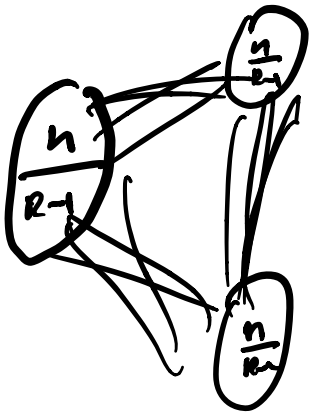
The probabilistic Method.
+ Algebraic techniques

||

Random Alg Method.

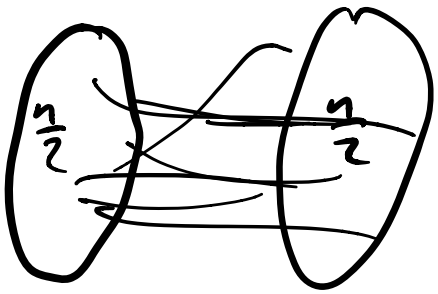
1. It proves results that cannot w prob method
2. It works well for related problems

Turan Thm - how many edges can a graph without K_R have?



R-1 parts

Δ-Free



$\frac{n^2}{4}$

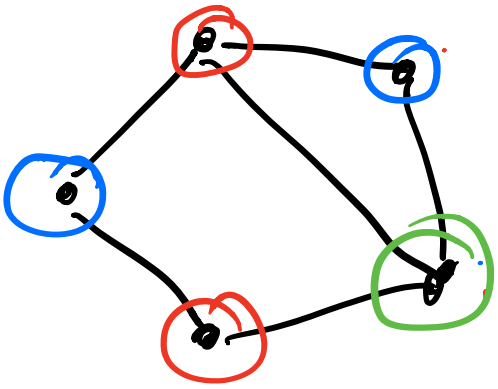
$$ex(n, K_R) = \left(\frac{n}{R-1}\right)^2 \cdot \binom{R-1}{2}$$

What instead of K_R I have some other graph H.

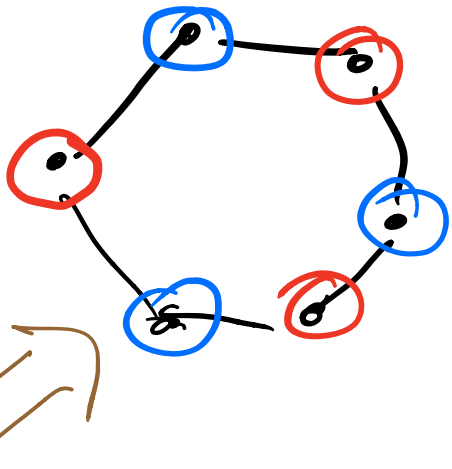
Erdős-Stone-Simonovits Thm:

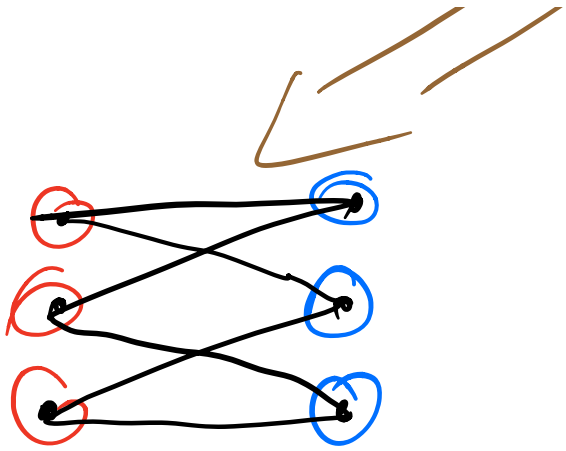
$$ex(n, H) = \binom{n}{2} \cdot \left(1 - \frac{1}{\chi(H)-1}\right) + o(n^2)$$

$\chi(H)$ = min # of colors in a coloring H: neighboring vertices have diff colors.



2-colorable.





2-colorable $\equiv$ bipartite

$\chi(H) = 2$

$$ex(n, H) = \left(\frac{n}{2}\right) \cdot \left(1 - \frac{1}{\chi(H)-1}\right) + o(n^2)$$

what $\chi(H) = 2$ $\rightarrow$ 0

$$ex(n, H) = o(n^2)$$

Zarankiewicz problem

$$ex(n, K_{s,t}) \leq n^{2-\frac{1}{s}}$$
$$\leq n^{2-\frac{1}{t}}$$

60 years

Tight for $s=t=2$
$s=t=3$.

$s=t=4$???

Prob. method provably cannot construct such graphs

Bukh constructed such graphs with a simple ext. of the method: random alg method.

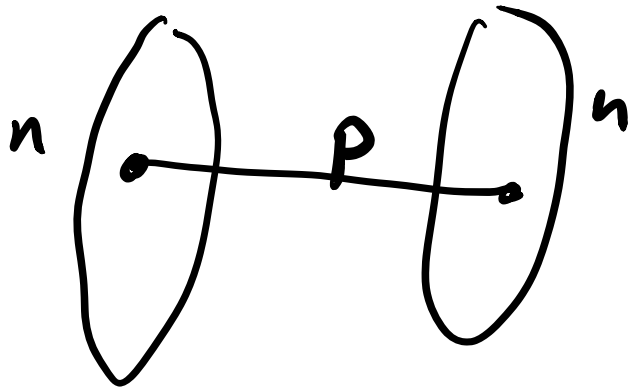
We want to construct graphs with

$$n^{2-1/s}$$ edges

that do not have

$$K_{s,t}$$

Prob. method.



$$\#\text{edges} = n^{2-1/s} = n^2 \cdot p \Rightarrow p = n^{-1/s}$$

$$t \geq s \cdot \frac{\log n}{\log q \log n}$$

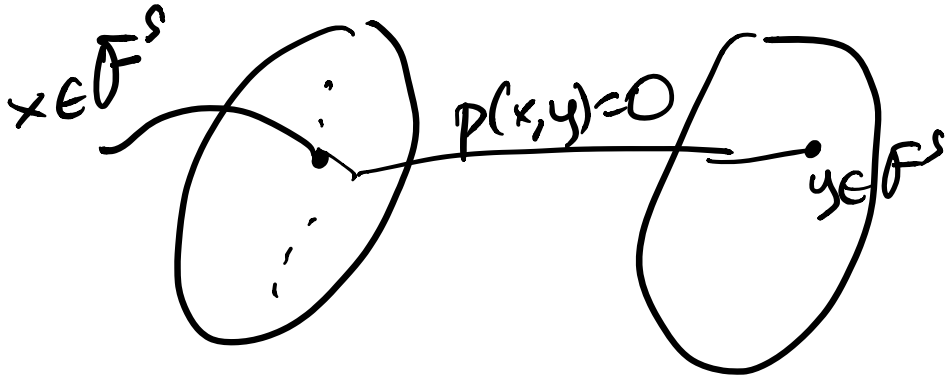
A random graph with

$$t = \frac{s \cdot \log n}{\log q \log n} \cdot \frac{1}{\omega} \cdots$$

DOES have $K_{s,t}$.

Ideal: $s = t$

Random Alg.



random poly P with 2^s inputs

1. We look at a few Random algebraic method papers.
2. [Optional] Extend to matrix rigidity.

Prob. method:

$n \log n$ bits of randomness to construct a rigid matrix

$\mathrm{DTime}[2^{n \log n}]$

We want $\mathrm{DTime}[2^{100n}]$