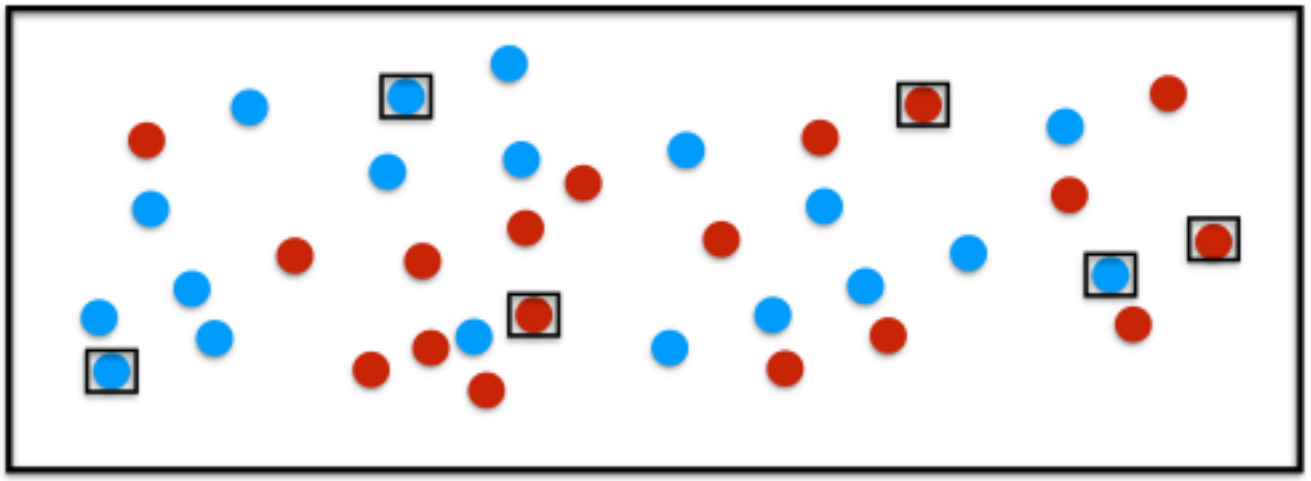
Towards Optimal Ramsey Graphs and Extractors

Eshan Chattopadyay
IAS

Random Sampling

300 million voters in an election



With 95% certainty, a random sample of 400 people can estimate the results up to 5% accuracy!

Randomized Algorithms

Polynomial Identity Testing: many natural problems can be reduced.

Randomized strategy: evaluate at random point.

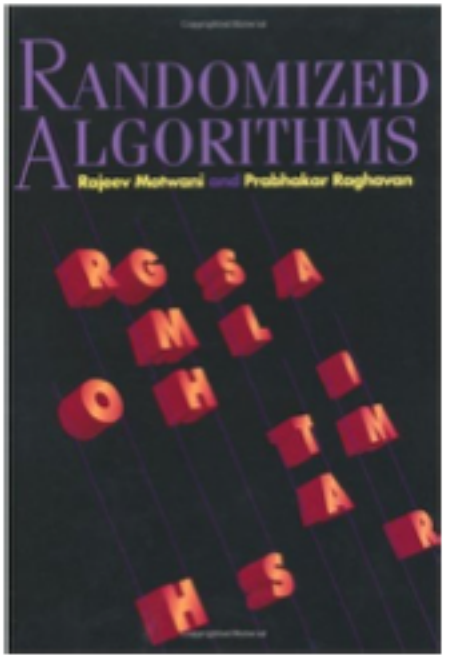
Theorem [Schwartz-Zippel]: Low degree polynomials have few roots.

Major Open Question: Efficient Deterministic Algorithm

More Generally,

Does every efficient randomized algorithm have a deterministic counterpart?

BPP=P?

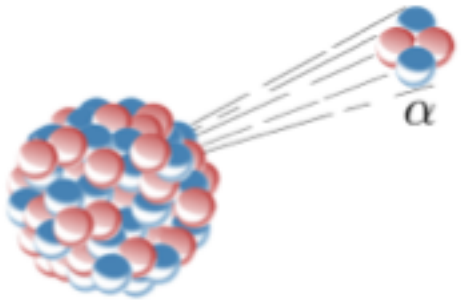


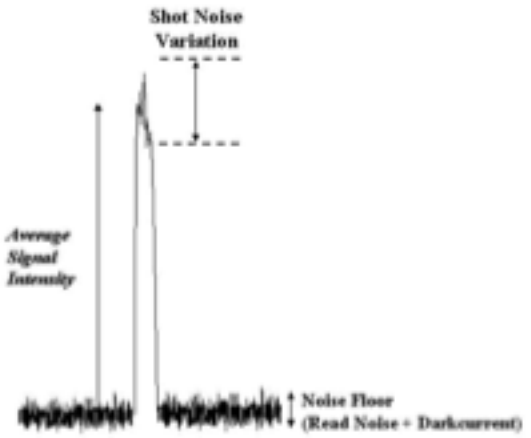
Randomness in Cryptography

Secret keys in Encryption systems: Many easy attacks on leakage of information.

Digital Signatures

How to generate random bits?

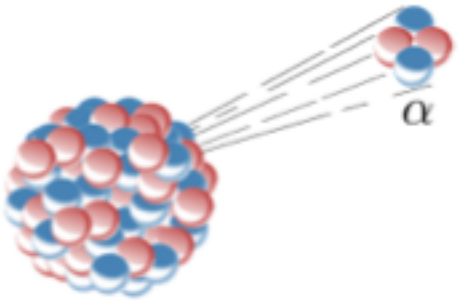


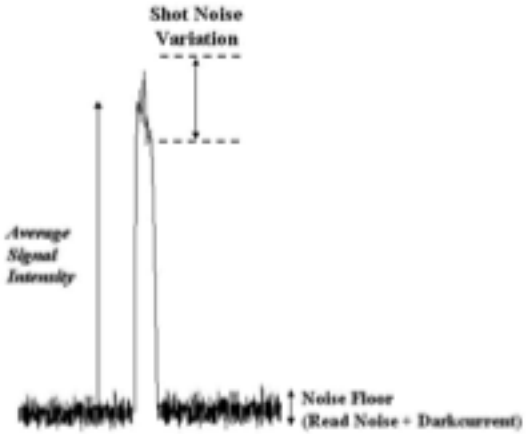


Thunderstorms generate atmospheric noise

Entropy Collectors

Typically, a stream of correlated bits are produced





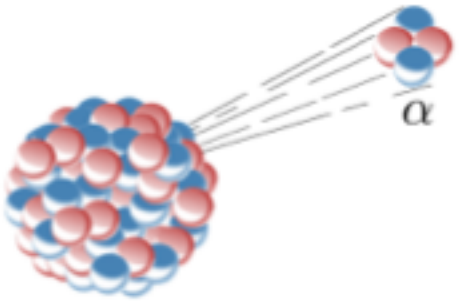
Thunderstorms generate atmospheric noise

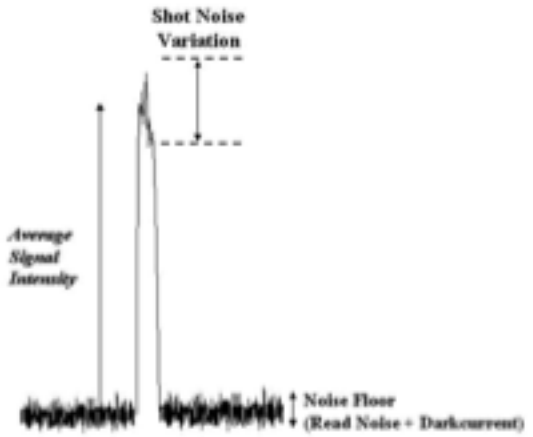
Randomness Extractor

Uniform Bits

Extractor

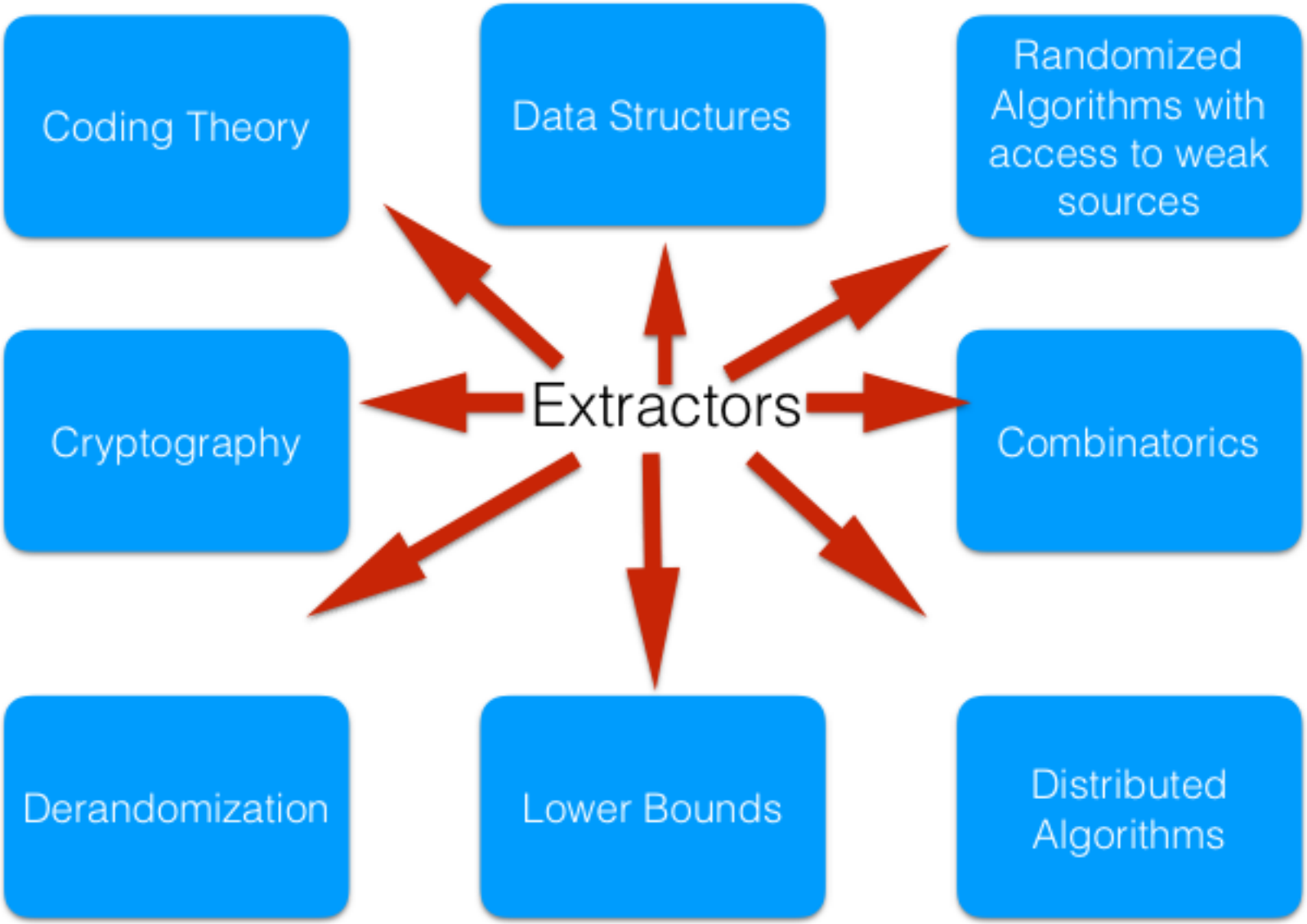
Entropy sources





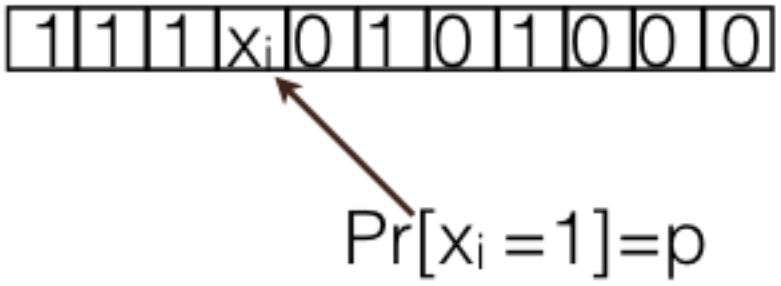
Thunderstorms generate atmospheric noise

Applications of Extractors



Modelling Weak Sources

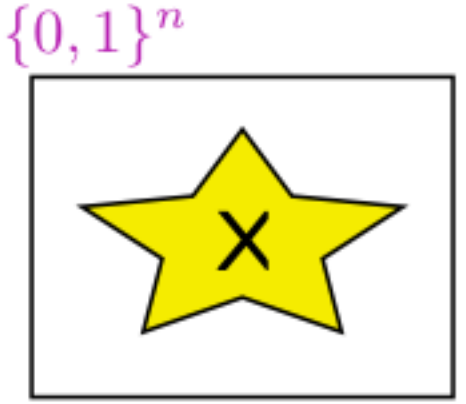
Stream of independent p-biased bits



- Studied by von Neumann in 1951
- von Neumann Extractor:
  - Pair bits. If 01, output 0; If 10, output 1. Else REPEAT.

General Weak Sources

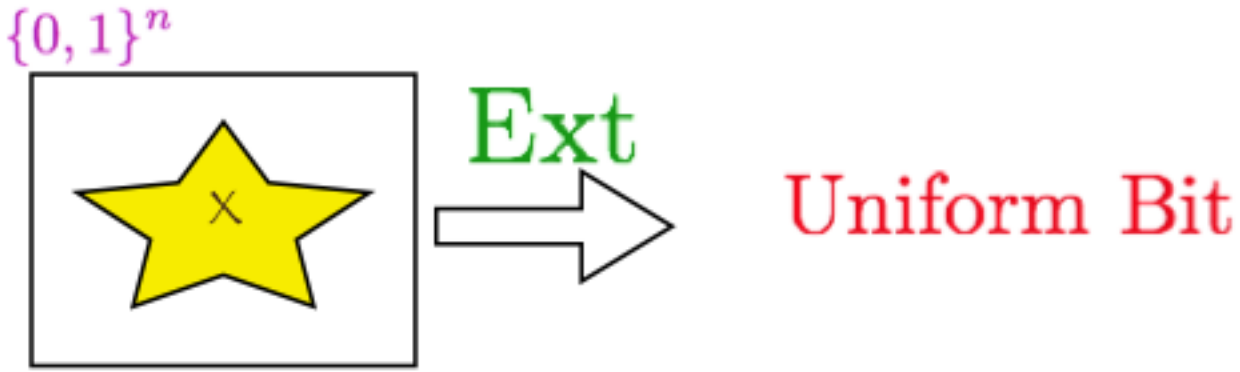
- Min-Entropy: X has min-entropy k if the maximum probability to an element is 2^{-k}.



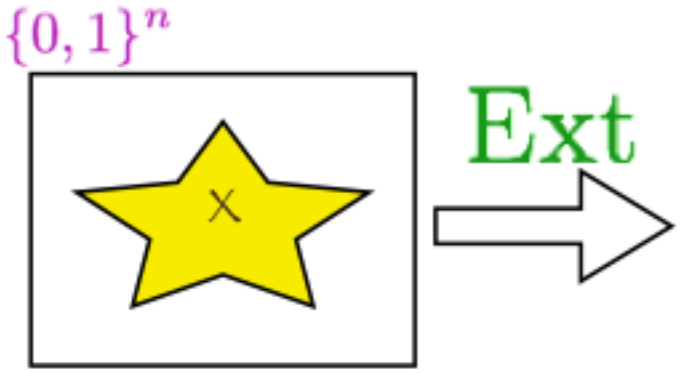
- (n,k)-Source
  - Source on n bits, Min-Entropy at least k.
  - Special Case: X uniform on set of size 2^k.

Randomness Extractor

- Extractor: deterministic procedure to extract uniform bits from ANY (n,k)-source.



One Source Extractor ?

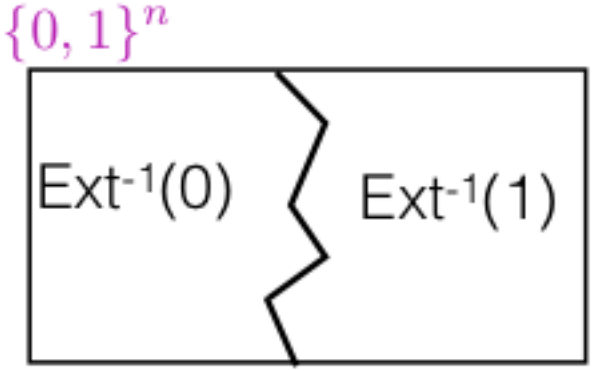


Lemma: There CANNOT exist an extractor for (n,n-1) sources.

Proof Idea:

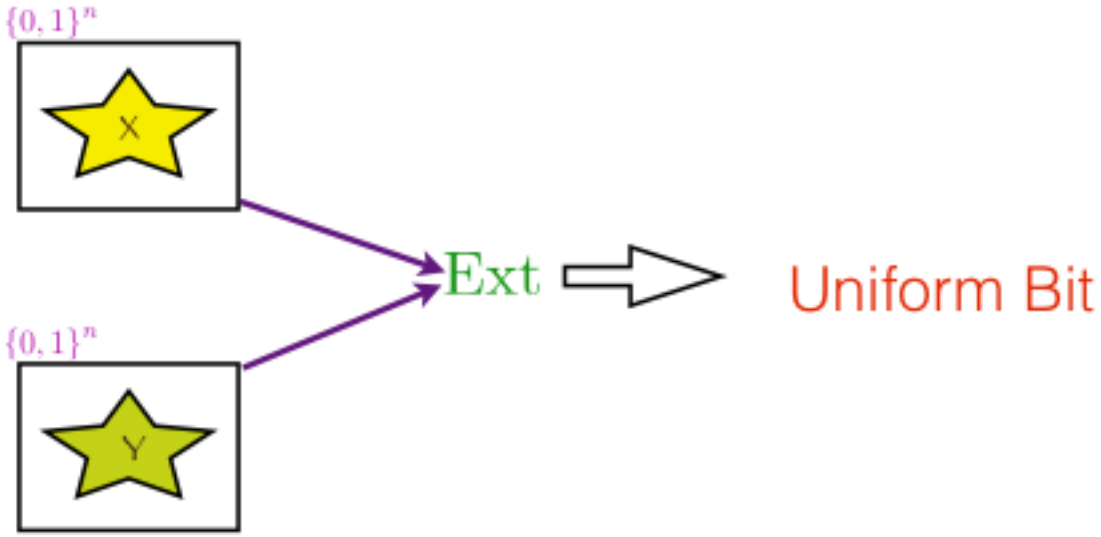
Assume Ext.

$\max\{|Ext^{-1}(0)|, |Ext^{-1}(1)|\} \geq 2^{n-1}$.



2-Source Extractor

X, Y are independent (n,k)-sources



More formally,

$$\left|\Pr[\mathrm{Ext}(X,Y)=1]-\frac{1}{2}\right|\leq\epsilon$$

Random functions are good 2-Source Extractors!

Thm.(Probabilistic method)$\exists$ 2-source extractor for min-entropy $k = \log n + O(1)$.

Naive Derandomization: More than Exponential time.

Santha-Vazirani 84, Chor-Goldreich 85:

Explicitly construct 2-source extractors.

Implications to Combinatorics

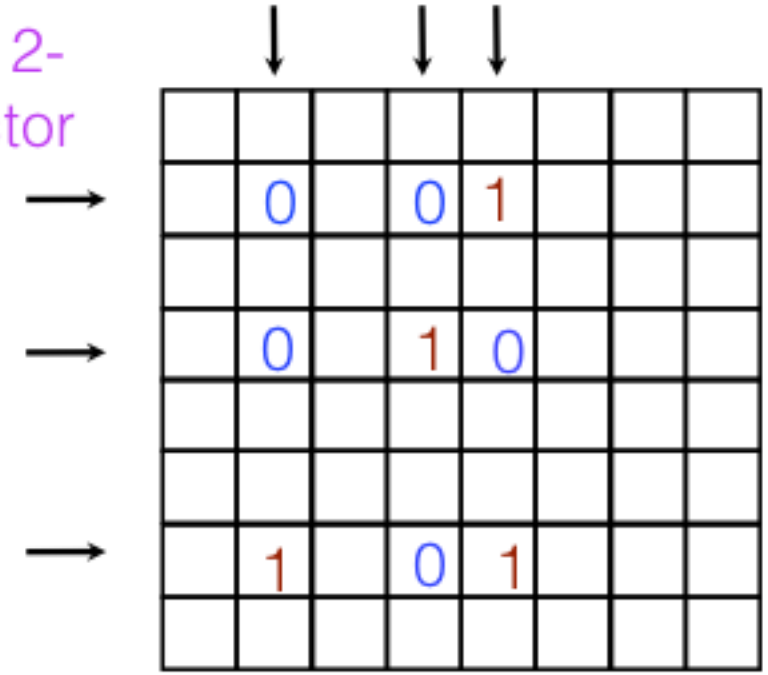
Matrix View

$N=2^n$, $K=2^k$

Construct a low discrepancy Boolean N×N matrix: i.e,

Every K×K submatrix contains 'almost equal' number of 0's and 1's.

Truth table of 2-source extractor



Ramsey Graphs

K-Ramsey graph: No independent set or clique of size K.

Ramsey (1928): Does not exist K-Ramsey graphs on N vertices for $K = (\log N)/2$.

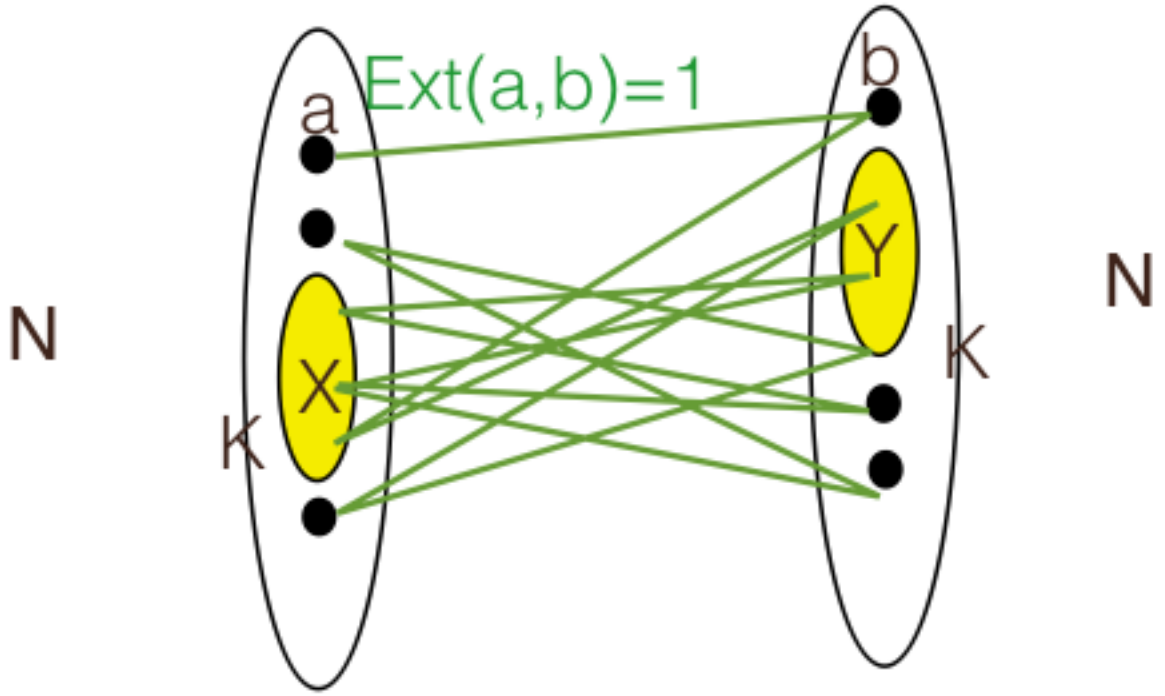
Erdos (1947): Existence of K-Ramsey graphs on N vertices for

$K=2 \log N$.

Explicit Constructions?

Graph View

$N=2^n$, $K=2^k$



Ext: 2-source extractor for min-entropy k

Known Explicit Constructions

Known Constructions: X, Y are independent (n,k)-sources

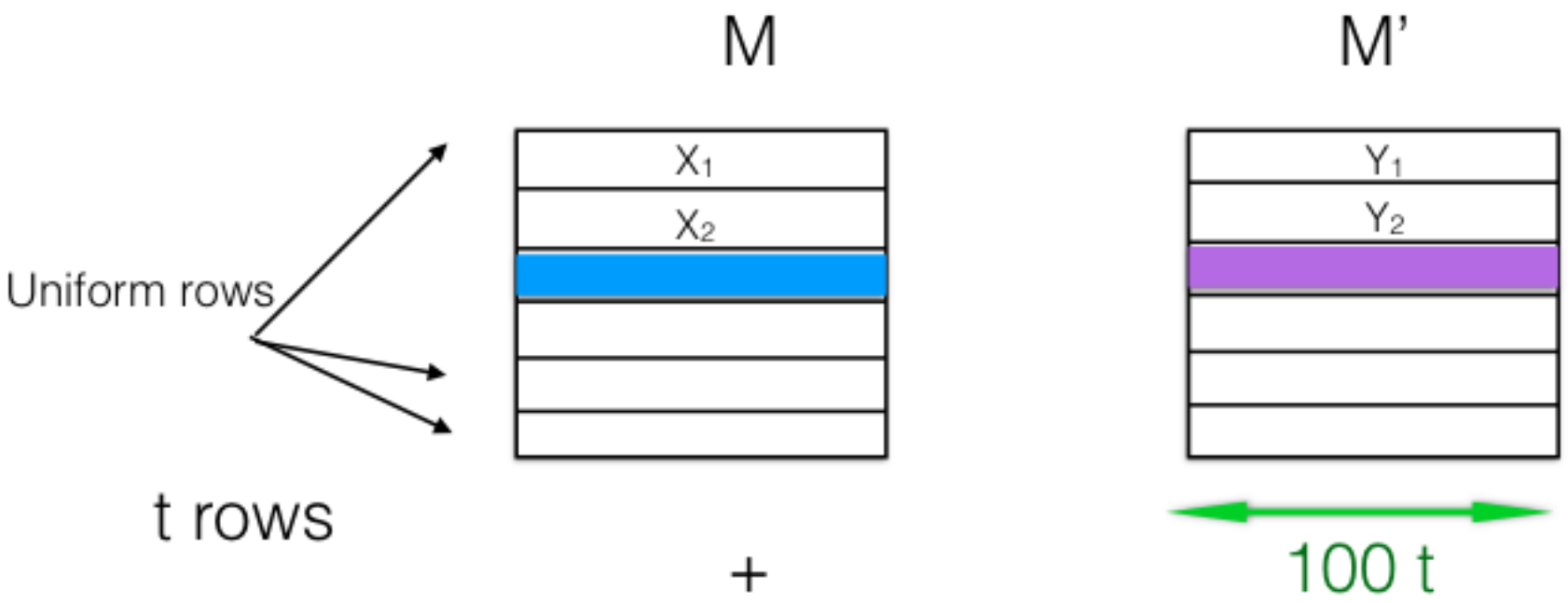
Reference	k
Chor-Goldreich 1985	$>n/2$
Bourgain 2005	$\geq 0.49n$
C-Zuckerman 16	$(\log n)^{75}$
Meka 17	$(\log n)^{10}$
Ben-Aroya-Doron-Ta-Shma 17, C-Li 17, Cohen 17	$(\log n)^{1+o(1)}$
Li 17	$\log n \log \log n$

Explicit Ramsey Graphs: 70 years of history!

Reference	K
Erdös 47 (existential)	$\geq 2 \log N$
Frankl-Wilson81, Naor92, Alon98, Grolmusz00, Ba, Gopalan06, Barak-Rao-Shaltiel-Wigderson 12	$2^{2\sqrt{\log(\log N)}}$
From 2-source Extractors	$(\log N)^{(\log \log N)}$

Obtaining 2-Source Extractors for

Obtaining 2-Source Extractors for entropy O(log n)



+

Indep. seed Y

↓

Merger(M,Y) | {Merger(M',Y), Y} has entropy Ω(t).

Thanks!

Questions?