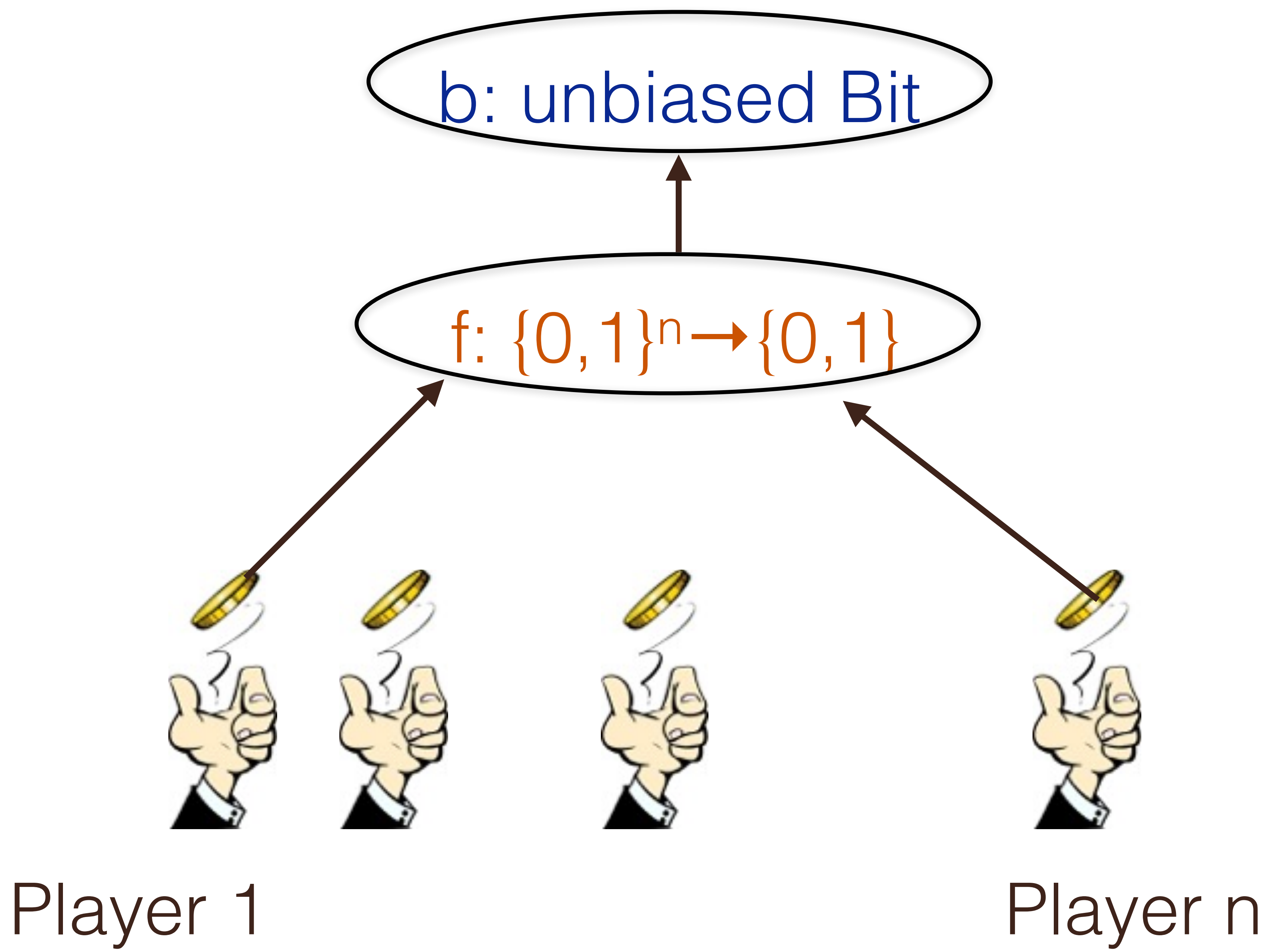
Resilient Functions

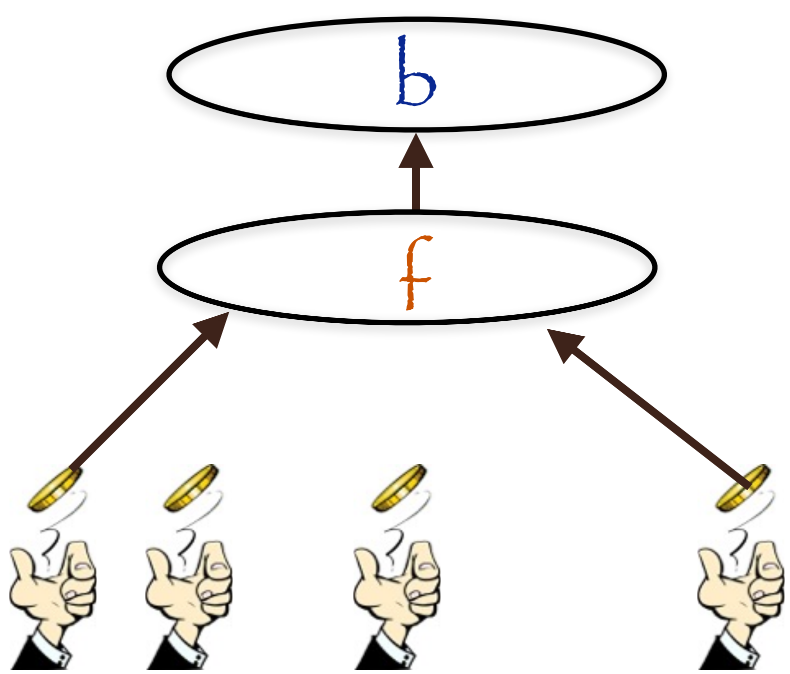
Eshan Chattopadhyay
IAS

Area of Research: Theoretical Computer Science, Combinatorics

Collective Coin-Flipping



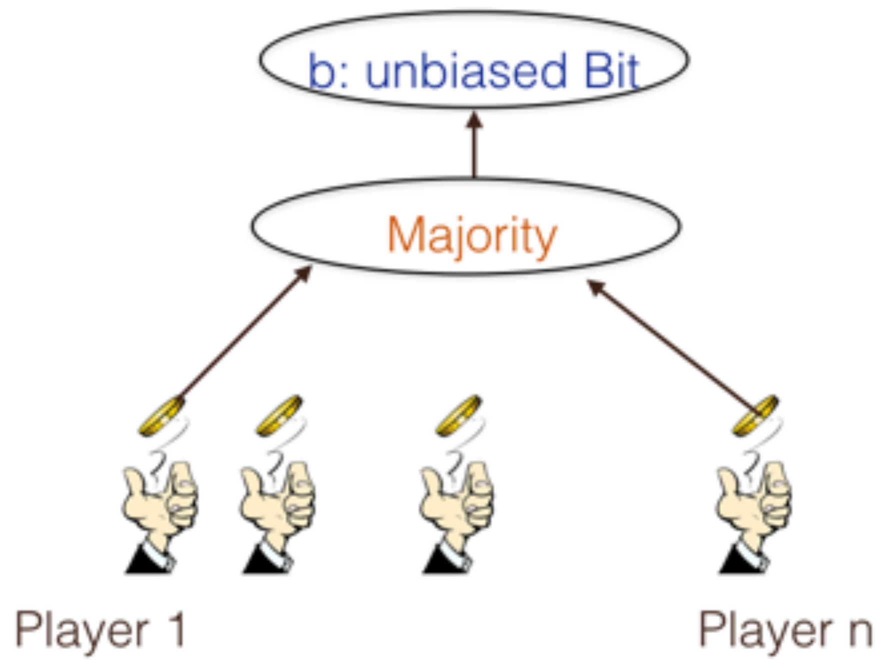
An Adversarial Model



Malicious Coalition of players $Q \subset [n]$:

- Adaptively sends bits AFTER seeing coin flips of other players.
- PARITY FAILS!

Majority works better…

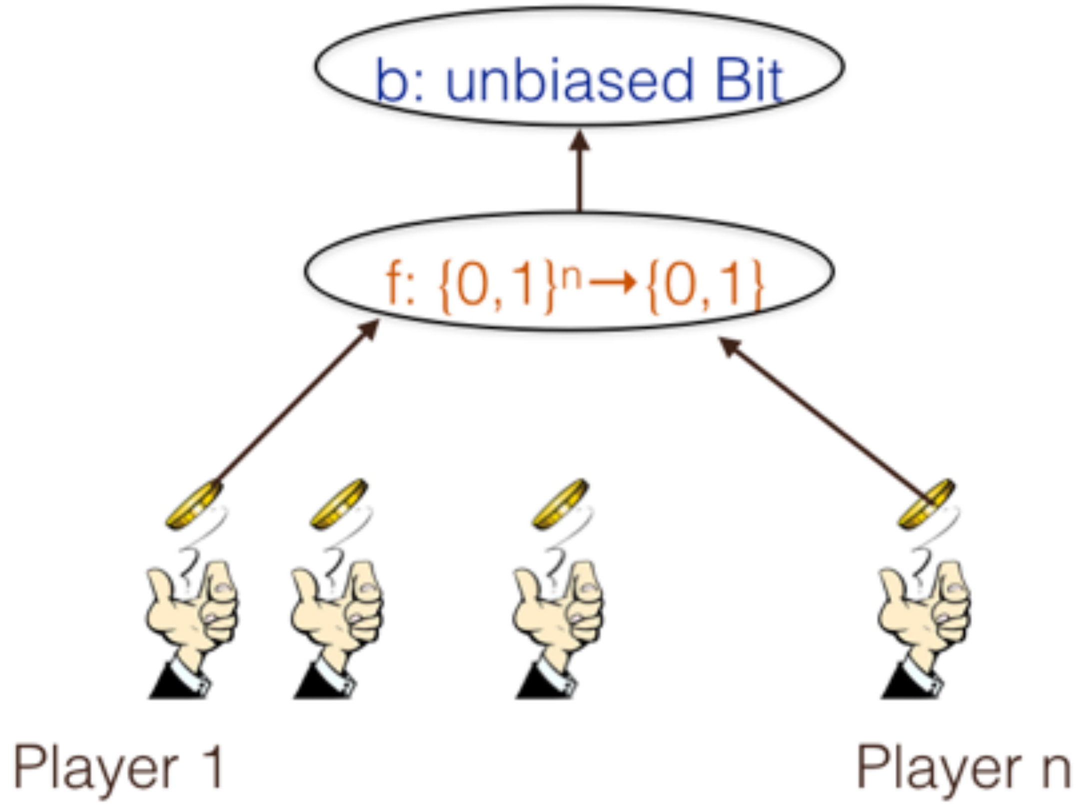


q malicious players

X: # of heads in (n-q) random coin flips

$\Pr[X \in [n/2 - q, n/2 + q]] = O(q/\sqrt{n})$

Influence of Sets



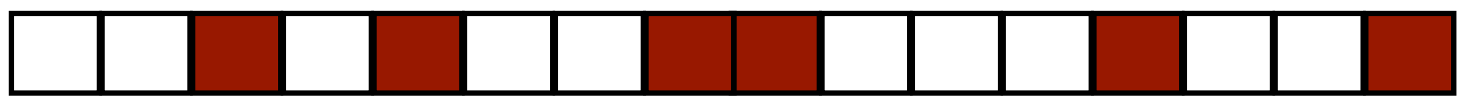
- Influence of Q: Probability output of f can be changed by Q after the 'good players' flip their coins

More formally…

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

$Q \subset [n]$

X:



Bits in Q: unfixed

Bits sampled uniformly

Pr[f(X) is NOT constant] = Influence of Q on f

Resilient Functions

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

(q,ε)-resilient function: $\forall\, Q \subset [n]$, $|Q| = q$,
Influence of Q on f is at most ε.

Assume $\mathbf{E}[f] = 1/2$.

Example: MAJORITY is $(n^{0.49}, \varepsilon)$-resilient.

PARITY is NOT $(1, \varepsilon)$-resilient, any $\varepsilon < 1$.

Limits on resilience

$t(n,\varepsilon) = \max\{q : \exists$ a (q,ε)-resilient function $f: \{0,1\}^n \to \{0,1\}$, $\mathbf{E}[f] = 1/2\}$

Rest of the talk: Upper and Lower Bounds on $t(n,\varepsilon)$

- Key to understanding limits of coin-flipping games
- Basic Question about Boolean functions

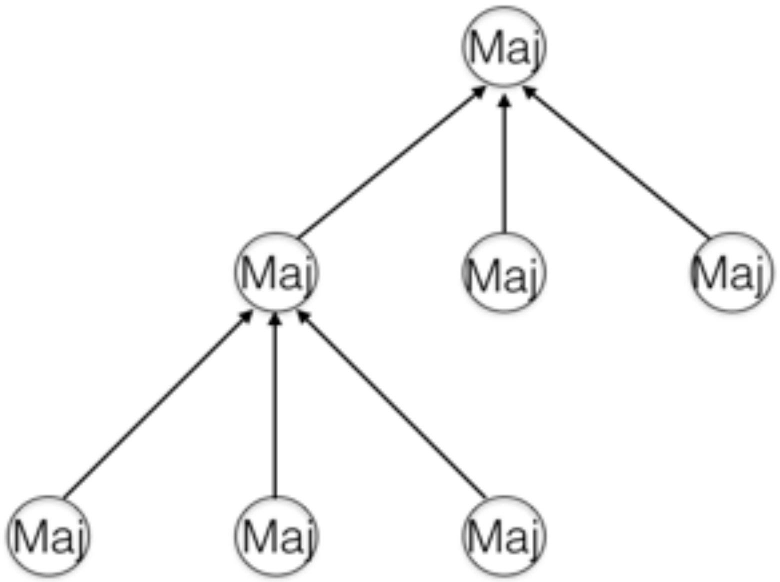
Upper Bound on $t(n,\varepsilon)$

- Kahn-Kalai-Linial '88: $\exists$ a coordinate with influence $(\log n)/n$.
    - Edge Isoperimetry→ $\exists$ coordinate with influence $1/n$
- Induction gives $O(n/\log n)$ coordinates with influence $\Omega(1)$.

$$t(n,0.1) \leq n / \log n$$

Lower Bound on t(n,ε)

- $t(n,0.1) = \Omega(\sqrt{n})$ Majority
- $t(n,0.1) = \Omega(n^{0.63})$ Recursive Majority [Ben-Or Linial 88]



Lower Bound on $t(n,\varepsilon)$

- Ajtai-Linial 1990: There exists a $(n/\log^2 n)$-resilient function that is almost balanced.
  - Probabilistic construction

$$t(n, 0.1) \geq n / \log^2 n$$

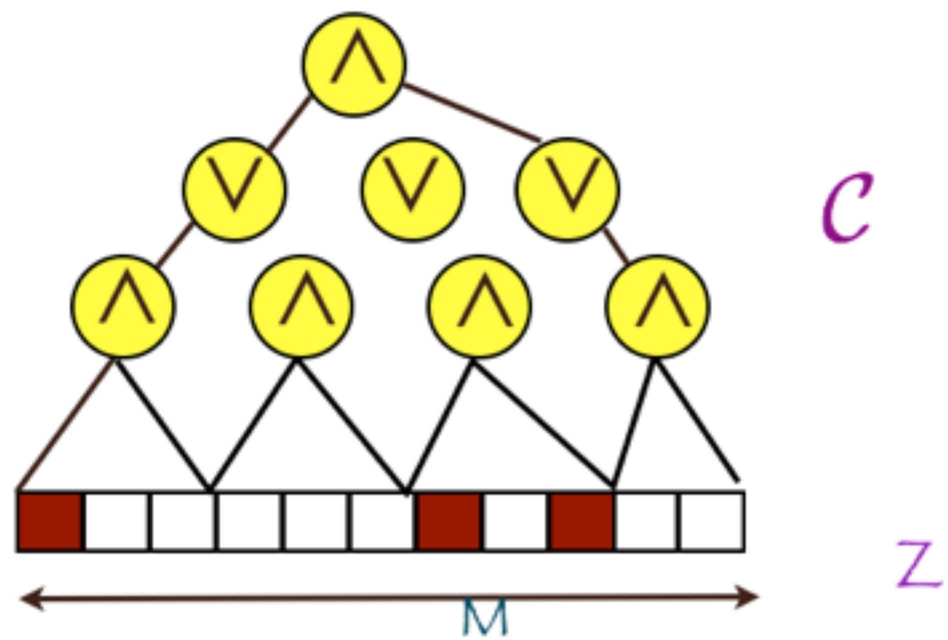
Explicit resilient functions

- Recall: Resilient functions imply coin flipping protocols.

Reference	Resilience
Majority	$\sqrt{n}$
Recursive Majority [BenOr-Linial 85]	$n^{0.63}$
[Meka, C-Zuckerman 16]	$n^{0.99}$
[Meka 16]	$n/\log^2 n$

[C-Zuckerman 16], [Meka 16] : Based on derandomizing Ajtai-Linial

A bit more about the construction in [C-Zuckerman 16]

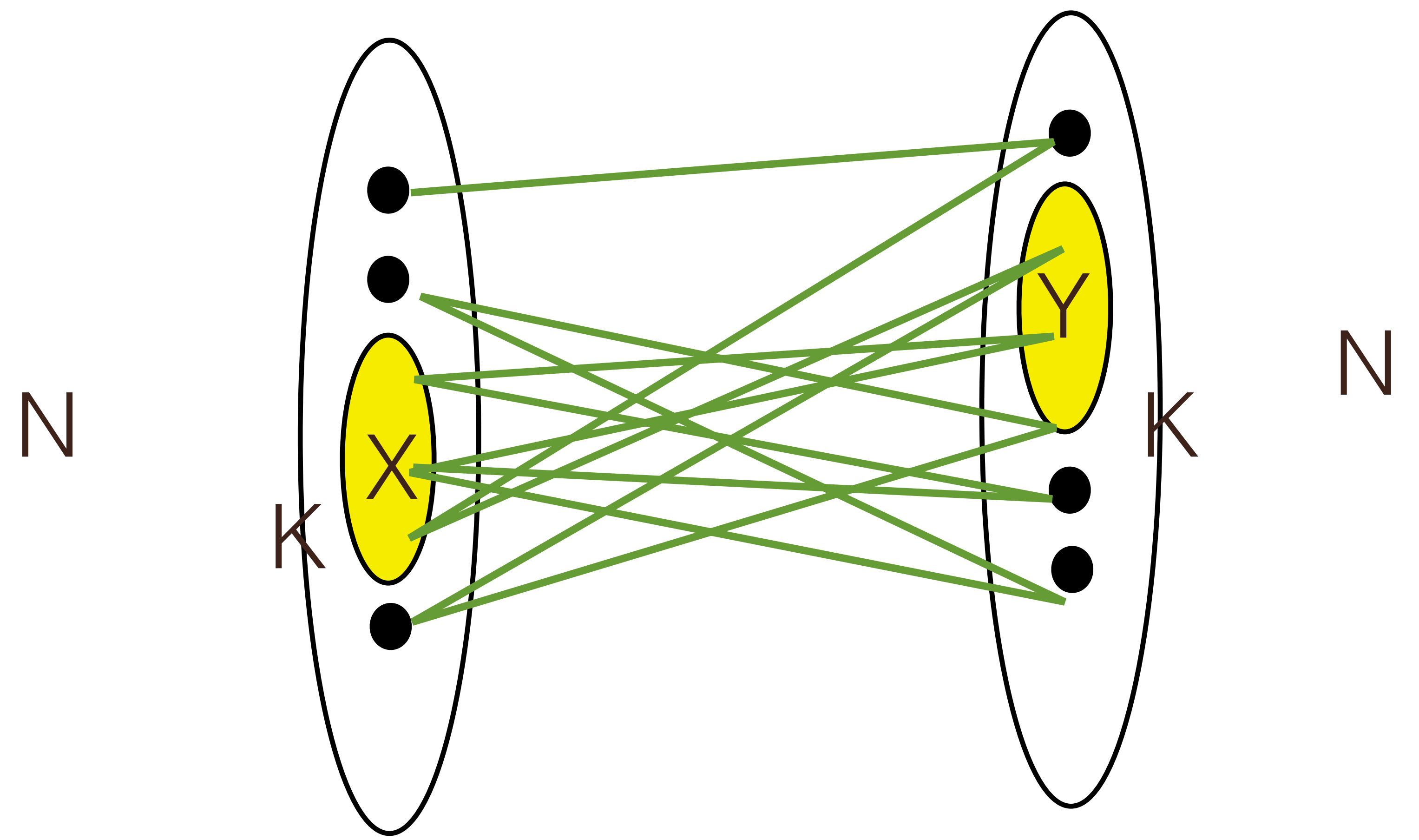


□ Bits are sampled from t-wise independent distribution

■ Bits arbitrarily depend on □ bits

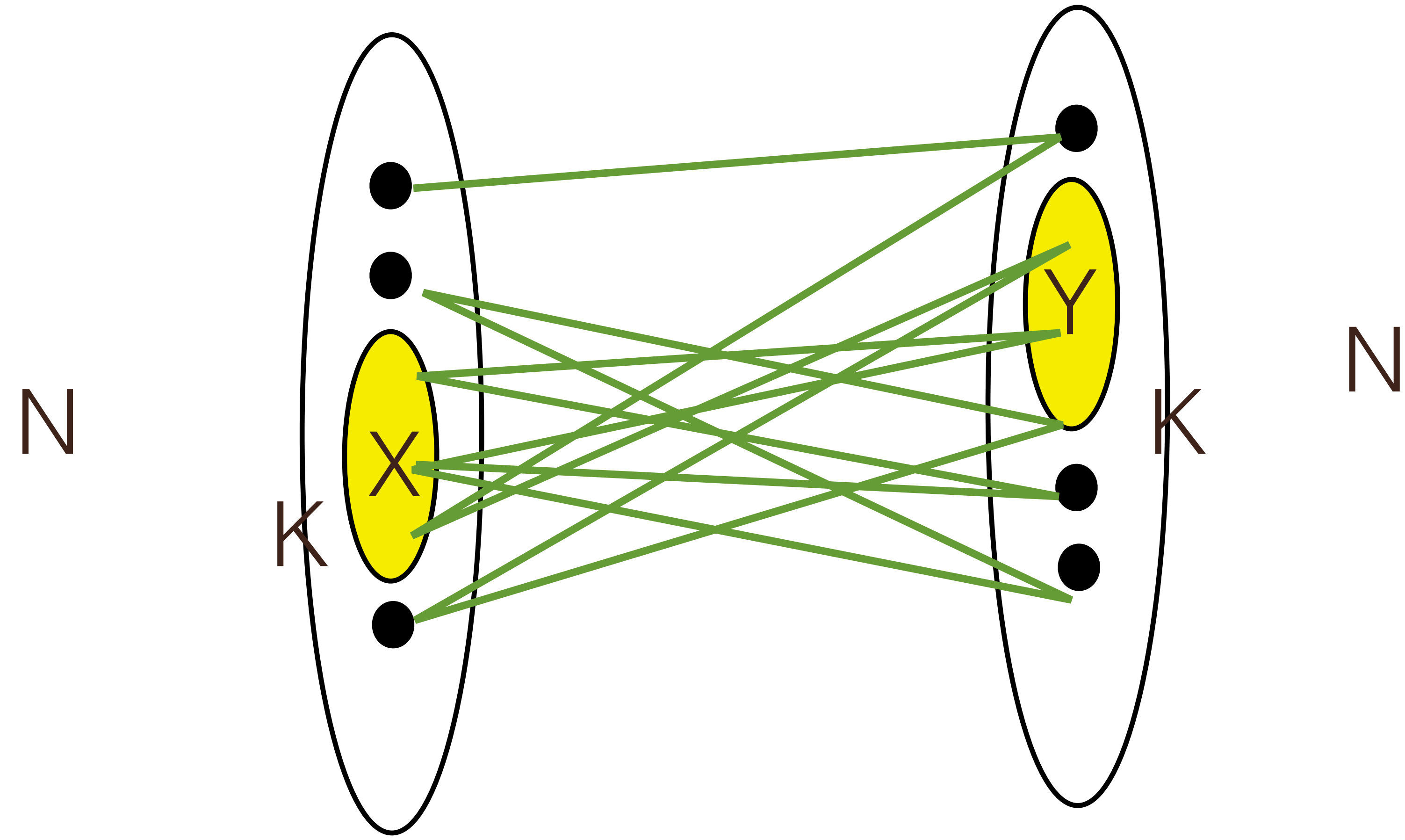
C is monotone and can be computed fast in parallel.

An Application: Explicit Ramsey graphs [C-Zuckerman 16]



Bipartite K-Ramsey graph: Bipartite graph with NO complete or empty $K \times K$ sub-graph.

Explicit Ramsey graphs



Ramsey (1928): Does not exist (log N)/2-Ramsey graphs

Erdos (1947): ∃ 2log N-Ramsey graphs

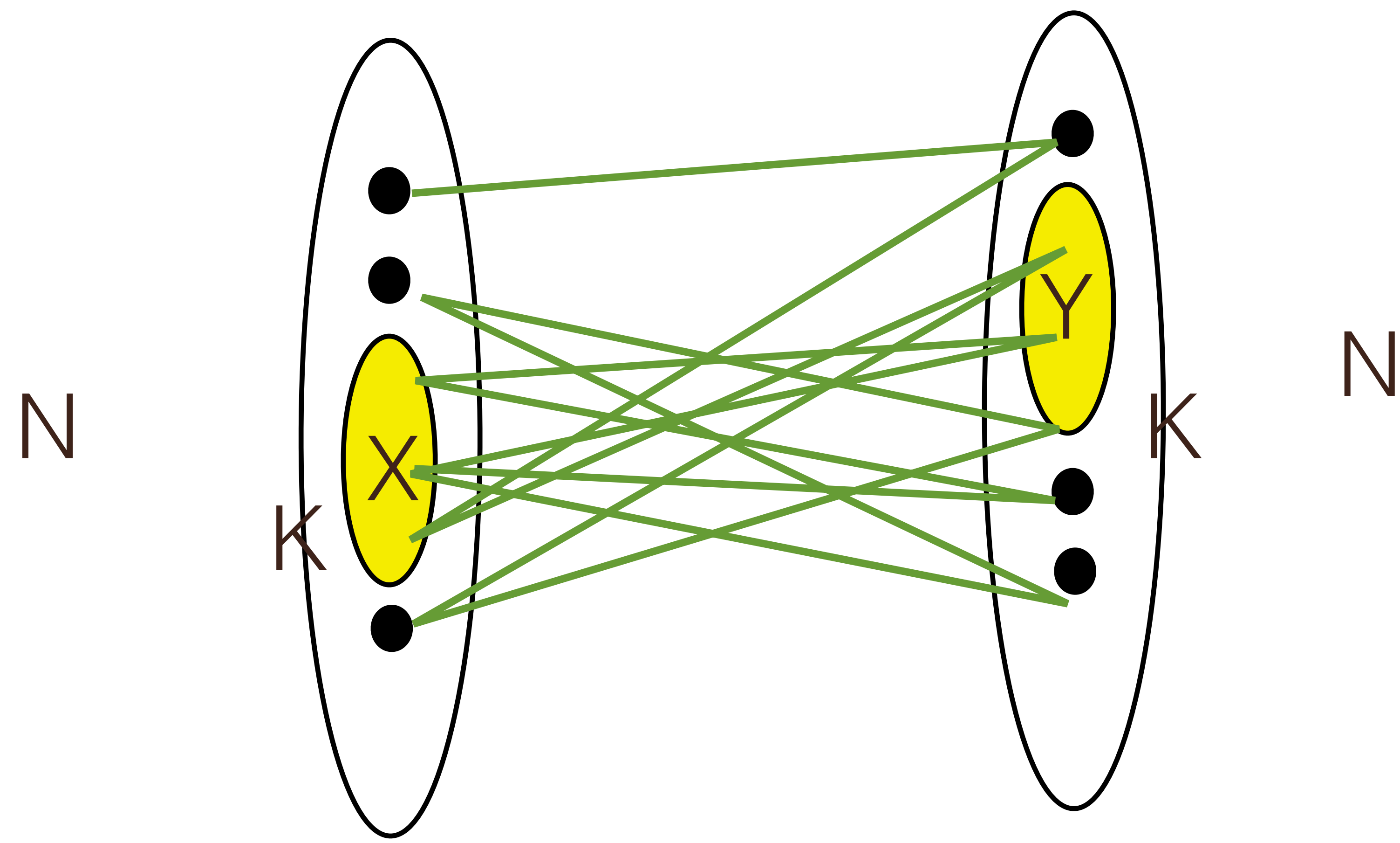
Erdos: Explicit Constructions?

$(N=2^n, \quad K=2^k)$

Explicit Ramsey Graphs

Reference	K	Bipartite
Erdös 47 (existential)	$\geq 2 \log N$	Yes
Hadamard Matrix	$\sqrt{N}$	Yes
Frankl-Wilson81, Naor92, Alon98, Grolmusz00, Ba Gopalan06	$2^{\Omega(\sqrt{(\log N \log\log N)})}$	No
Pudlak-Rödl 04	$\sqrt{N}/2^{\sqrt{\log N}}$	Yes
Barak-Kindler-Shaltiel-Sudakov-Wigderson 10	N^{δ}	Yes
Barak-Rao-Shaltiel -Wigderson 12	$(\log N)^{2^{\sqrt{\log\log N}}}$	Yes

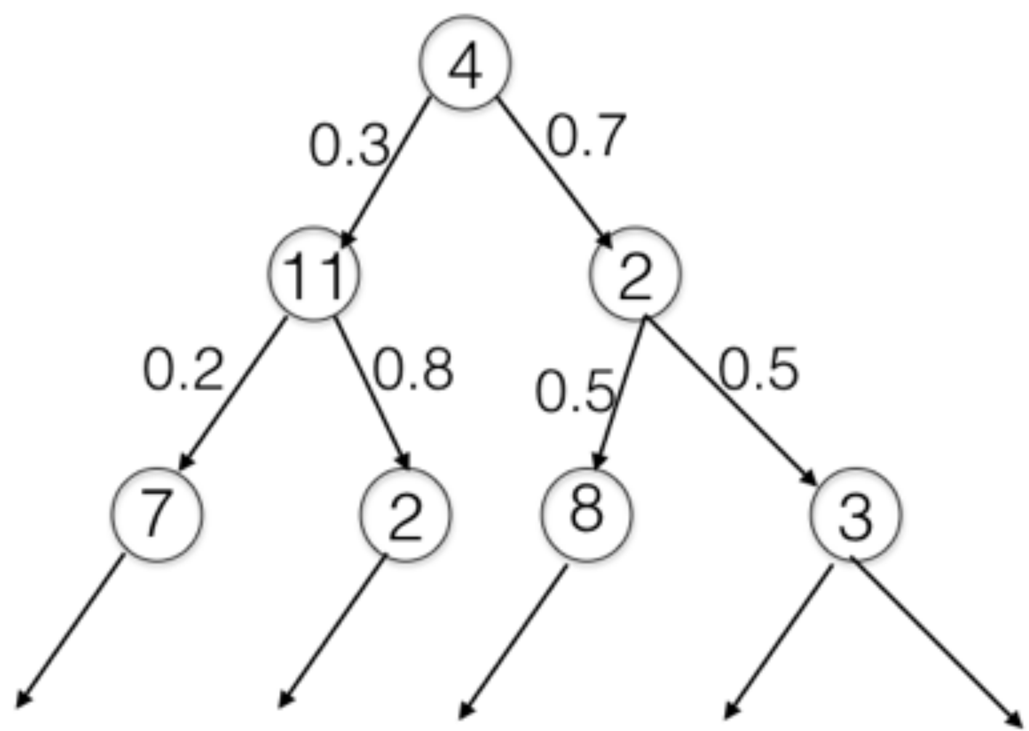
Explicit Ramsey graphs



Corollary of [C-Zuckerman 16]: Explicit $(\log N)^{\mathrm{poly}(\log \log N)}$-Ramsey graph

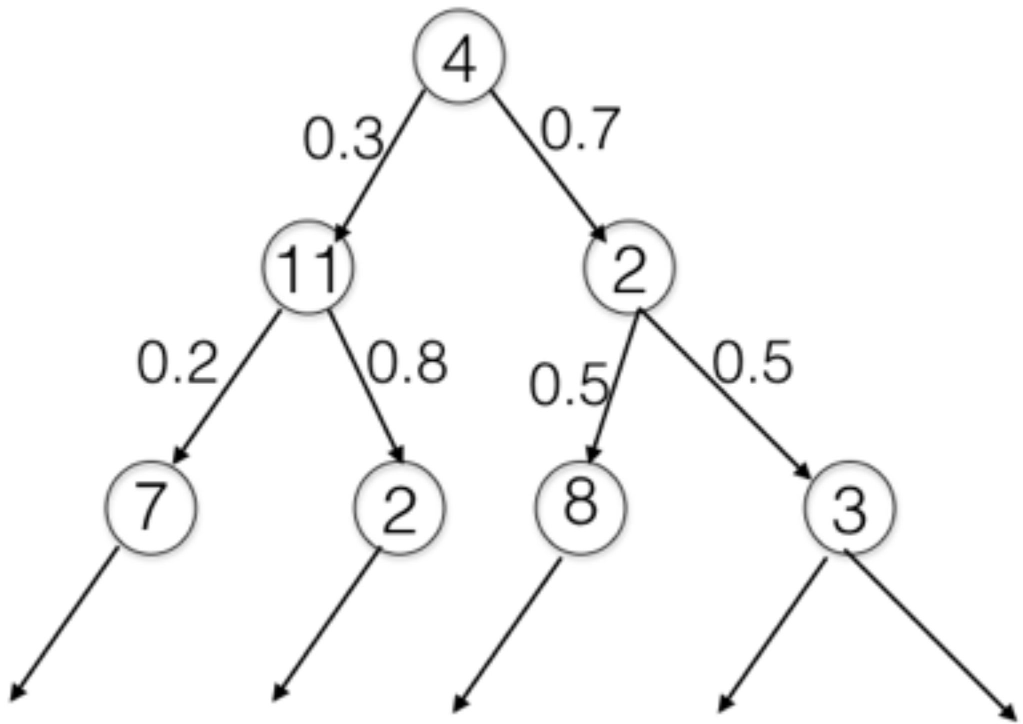
- Independent work [Cohen 16] achieves similar parameters.

General Coin-Flipping Games



- Internal Nodes: Labeled by players
- Leaves: Labeled by 0 or 1 (output of the protocol)

General Coin-Flipping Games



- Well studied Model [BN 85, Saks 89, AN 90, BopN93, RZ98, RSZ99,F99]

- Protocols can handle (1/2- ε)n sized adversaries.

Open Directions

- Close the gap: $n / \log^2 n \leq t(n, 0.1) \leq n / \log n$
- Resilience of functions on larger domains.
  - $f: [0,1]^n \rightarrow \{0,1\}$
  - Known: $n/\log^2 n \leq t(n, 0.1) < n / 2$
- More applications.

Thanks!

Questions?