Condensing and Extracting Against Online Adversaries




Eshan Chattopadhyay
Cornell University

Mohit Gurumukhani
Cornell University

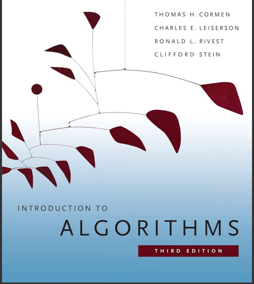
Noam Ringach
Cornell University

Rocco Servedio
Columbia University

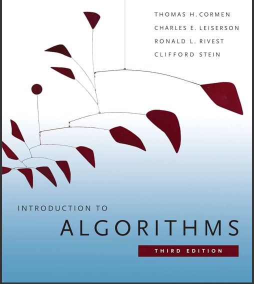
Background

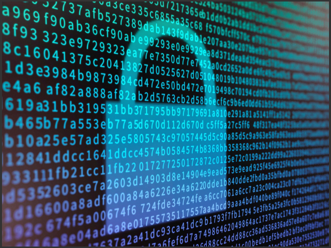
Randomness is Useful

Randomness is Useful

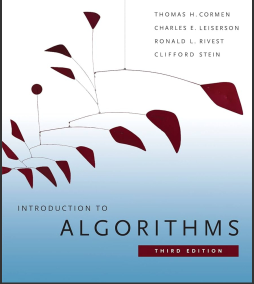


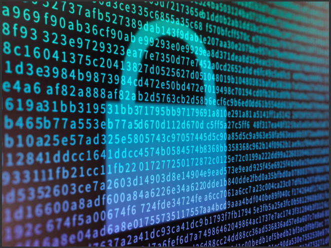
Randomness is Useful



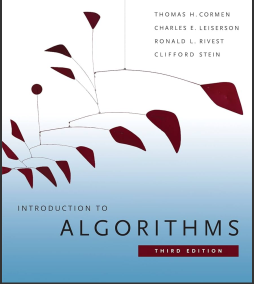


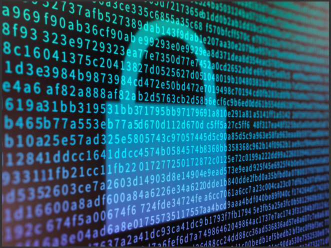
Randomness is Useful





Randomness is Useful





How to get High Quality Randomness?

How to get High Quality Randomness?

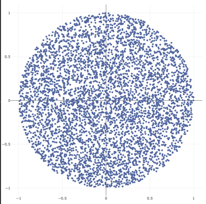
- Find 'natural' source of entropic randomness **X**

How to get High Quality Randomness?

- Find 'natural' source of entropic randomness $\mathbf{X}$
- Construct 'randomness purifier' f

How to get High Quality Randomness?

- Find ‘natural’ source of entropic randomness $\mathbf{X}$
- Construct ‘randomness purifier’ f
- Output $f(\mathbf{X})$ - high quality randomness



Measuring randomness

Measuring randomness

Statistical Distance from Uniform

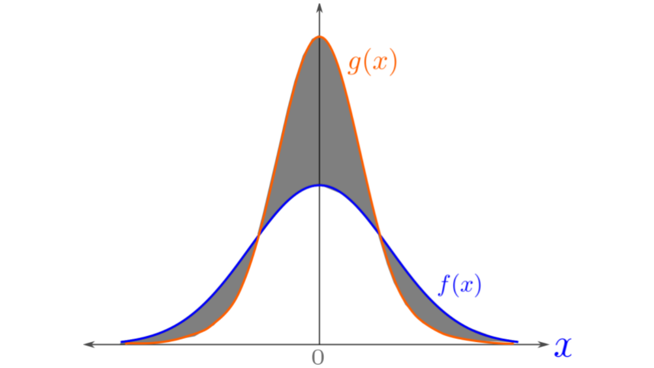
For $\mathbf{X} \sim \{0,1\}^r$, measure is $|\mathbf{X} - \mathbf{U}_r|$

Measuring randomness

Statistical Distance from Uniform

For $\mathbf{X} \sim \{0,1\}^r$, measure is $|\mathbf{X} - \mathbf{U}_r|$

$$|\mathbf{A} - \mathbf{B}| = \max_{H \subset \{0,1\}^r} |\Pr[\mathbf{A} \in H] - \Pr[\mathbf{B} \in H]| = \frac{1}{2} \cdot |\mathbf{A} - \mathbf{B}|_1$$



Measuring randomness again

Measuring randomness again

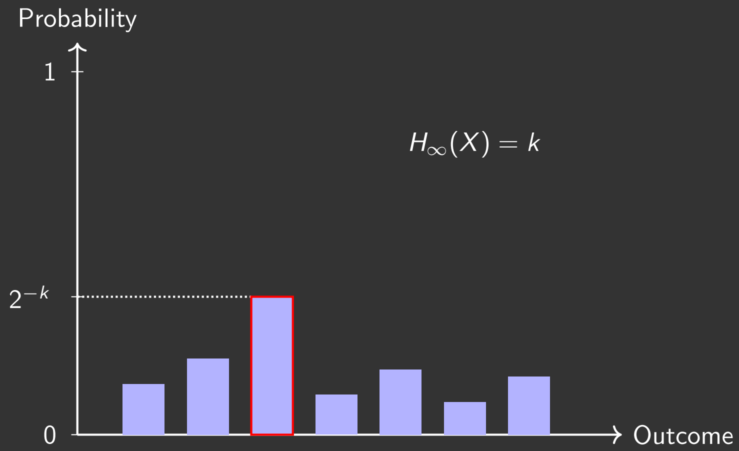
Min-Entropy

$H_\infty(\mathbf{X}) = \min_x \log(1/\Pr[\mathbf{X} = x])$

Measuring randomness again

Min-Entropy

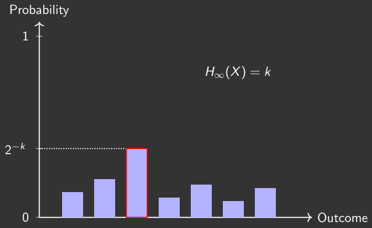
$H_\infty(\mathbf{X}) = \min_x \log(1/\Pr[\mathbf{X} = x])$



Measuring randomness again

Min-Entropy

$H_\infty(\mathbf{X}) = \min_x \log(1/\Pr[\mathbf{X} = x])$

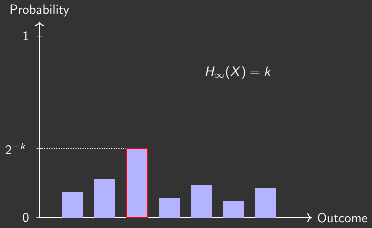


Observe

Measuring randomness again

Min-Entropy

$H_\infty(\mathbf{X}) = \min_x \log(1/\Pr[\mathbf{X} = x])$



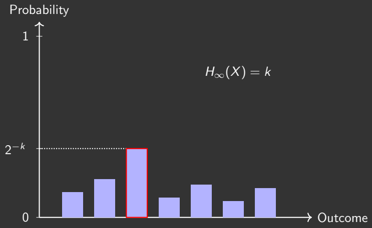
Observe

- For $\mathbf{X} \sim \{0,1\}^r$, $0 \leq H_\infty(\mathbf{X}) \leq r$

Measuring randomness again

Min-Entropy

$H_\infty(\mathbf{X}) = \min_x \log(1/\Pr[\mathbf{X} = x])$



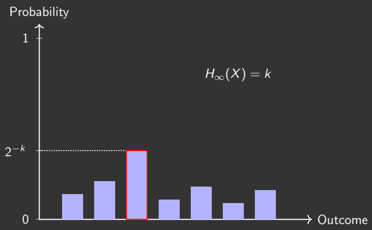
Observe

- For $\mathbf{X} \sim \{0,1\}^r$, $0 \leq H_\infty(\mathbf{X}) \leq r$
- If $H_\infty(\mathbf{X}) = r$, then $\mathbf{X} \equiv \mathbf{U}_r$

Measuring randomness again

Min-Entropy

$H_\infty(\mathbf{X}) = \min_x \log(1/\Pr[\mathbf{X} = x])$



Observe

- For $\mathbf{X} \sim \{0,1\}^r$, $0 \leq H_\infty(\mathbf{X}) \leq r$
- If $H_\infty(\mathbf{X}) = r$, then $\mathbf{X} \equiv \mathbf{U}_r$

Smooth Min-Entropy

For $\varepsilon \geq 0$, $H^\varepsilon_\infty(\mathbf{X}) = \max_{|\mathbf{X}-\mathbf{Y}| \leq \varepsilon} H_\infty(\mathbf{Y})$

Randomness Purification - Condensing and Extracting

Randomness Purification - Condensing and Extracting

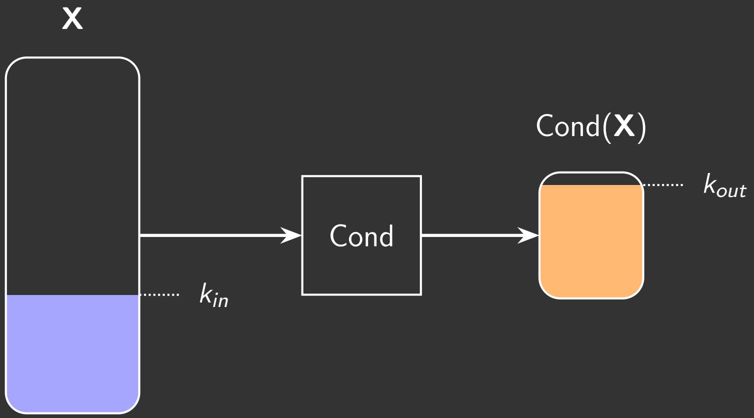
Condenser

Cond : $\{0,1\}^r \to \{0,1\}^m$ is $\boldsymbol{(k_{in}, k_{out}, \varepsilon)}$-condenser for $\mathcal{X}$ if for all $\mathbf{X} \in \mathcal{X}$ with $H_\infty(\mathbf{X}) \geq k_{in}$, $\boldsymbol{H^{\varepsilon}_{\infty}(\mathrm{Cond}(\mathbf{X})) \geq k_{out}}$

Randomness Purification - Condensing and Extracting

Condenser

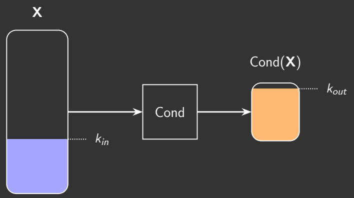
$\mathsf{Cond} : \{0,1\}^r \to \{0,1\}^m$ is $(k_{in}, k_{out}, \varepsilon)$-condenser for $\mathcal{X}$ if for all $\mathbf{X} \in \mathcal{X}$ with $H_\infty(\mathbf{X}) \geq k_{in}$, $H_\infty^\varepsilon(\mathsf{Cond}(\mathbf{X})) \geq k_{out}$



Randomness Purification - Condensing and Extracting

Condenser

$\mathrm{Cond} : \{0,1\}^r \to \{0,1\}^m$ is $(k_{in}, k_{out}, \varepsilon)$-condenser for $\mathcal{X}$ if for all $\mathbf{X} \in \mathcal{X}$ with $H_\infty(\mathbf{X}) \geq k_{in}$, $H_\infty^\varepsilon(\mathrm{Cond}(\mathbf{X})) \geq k_{out}$



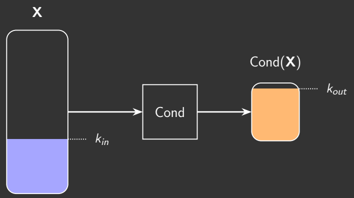
- Care about increasing **entropy rate**:

$$\frac{k_{in}}{r} \lll \frac{k_{out}}{m}$$

Randomness Purification - Condensing and Extracting

Condenser

Cond : $\{0,1\}^r \to \{0,1\}^m$ is $(k_{in}, k_{out}, \varepsilon)$-condenser for $\mathcal{X}$ if for all $\mathbf{X} \in \mathcal{X}$ with $H_\infty(\mathbf{X}) \geq k_{in}$, $H_\infty^\varepsilon(\text{Cond}(\mathbf{X})) \geq k_{out}$



- Care about increasing **entropy rate**:

$$\frac{k_{in}}{r} \lll \frac{k_{out}}{m}$$

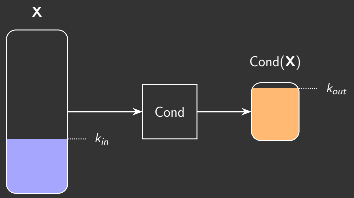
- Care about minimizing **entropy gap**:

$$\Delta_{out} = m - k_{out}$$

Randomness Purification - Condensing and Extracting

Condenser

Cond : $\{0,1\}^r \to \{0,1\}^m$ is $(k_{in}, k_{out}, \varepsilon)$-condenser for $\mathcal{X}$ if for all $\mathbf{X} \in \mathcal{X}$ with $H_\infty(\mathbf{X}) \geq k_{in}$, $H_\infty^\varepsilon(\mathrm{Cond}(\mathbf{X})) \geq k_{out}$



- Care about increasing **entropy rate**:

$$\frac{k_{in}}{r} \lll \frac{k_{out}}{m}$$

- Care about minimizing **entropy gap**:

$$\Delta_{out} = m - k_{out}$$

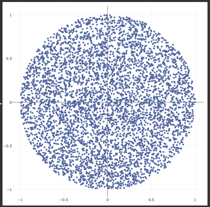
Extractor

Extractor is condenser with $\Delta_{out} = 0$, $\frac{k_{out}}{m} = 1$

Obtaining High Quality Randomness

Obtaining High Quality Randomness

- Find ‘natural’ source of entropic randomness $\mathbf{X}$
- Construct ‘randomness purifier’ f
- Output $f(\mathbf{X})$ - high quality randomness



Concretely Obtaining High Quality Randomness

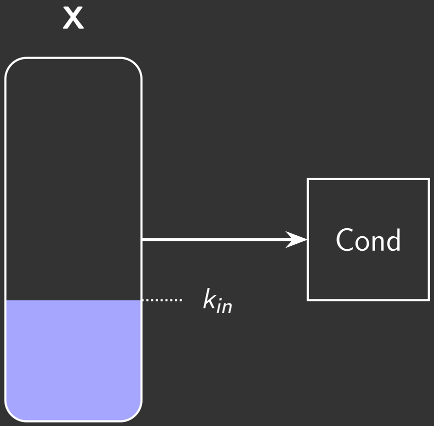
Concretely Obtaining High Quality Randomness

- Construct randomness condenser Cond for class of sources $\mathcal{X}$

$$\boxed{\text{Cond}}$$

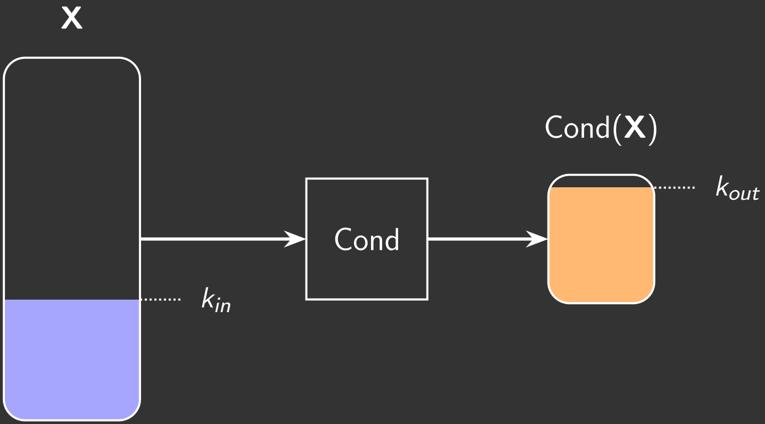
Concretely Obtaining High Quality Randomness

- Construct randomness condenser Cond for class of sources $\mathcal{X}$
- Find natural source of entropic randomness **X** from $\mathcal{X}$



Concretely Obtaining High Quality Randomness

- Construct randomness condenser Cond for class of sources $\mathcal{X}$
- Find natural source of entropic randomness $\mathbf{X}$ from $\mathcal{X}$
- Output Cond($\mathbf{X}$) - high quality randomness



Utility of Condensing

Utility of Condensing

- For many natural distribution classes, **provably impossible** to **extract**

Utility of Condensing

- For many natural distribution classes, **provably impossible** to **extract**
- Can condense and get **rate $1 - o(1)$** distributions

Utility of Condensing

- For many natural distribution classes, **provably impossible** to **extract**
- Can condense and get **rate $1 - o(1)$** distributions
- Can simulate Randomized algorithms with **poly(Δ_{out})** overhead [Zuckerman'95].

Utility of Condensing

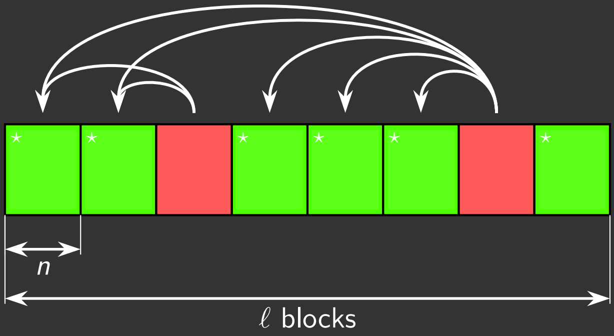
- For many natural distribution classes, **provably impossible** to **extract**
- Can condense and get **rate $1 - o(1)$** distributions
- Can simulate Randomized algorithms with **poly(Δ_{out})** overhead [Zuckerman'95].
- "One-shot simulations" for randomized protocols, cryptography, interactive proofs etc.

oNOSF sources

Online Non Oblivious Symbol Fixing (oNOSF) Sources

Online Non Oblivious Symbol Fixing (oNOSF) Sources

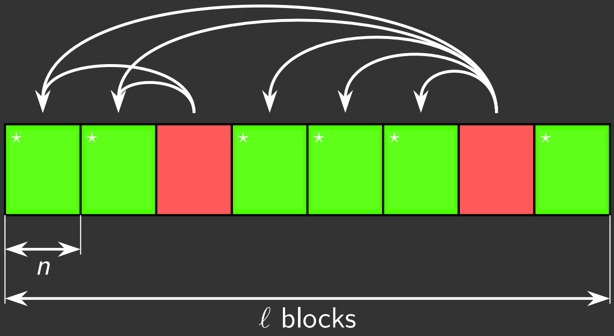
(g, ℓ, n) **oNOSF source X**



Online Non Oblivious Symbol Fixing (oNOSF) Sources

(g, ℓ, n) **oNOSF source X**

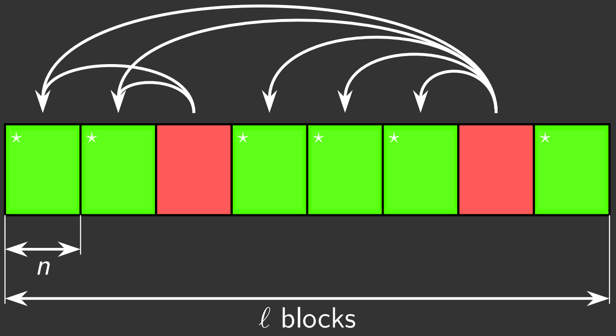
- $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$ with $\mathbf{X}_i \sim \{0,1\}^n$



Online Non Oblivious Symbol Fixing (oNOSF) Sources

(g, ℓ, n) oNOSF source X

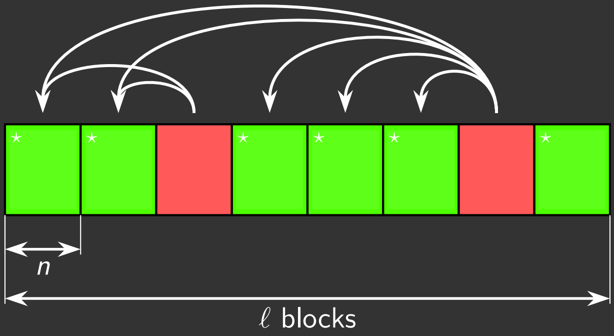
- $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$ with $\mathbf{X}_i \sim \{0,1\}^n$
- g good blocks, $\ell - g$ bad blocks



Online Non Oblivious Symbol Fixing (oNOSF) Sources

(g, ℓ, n) oNOSF source X

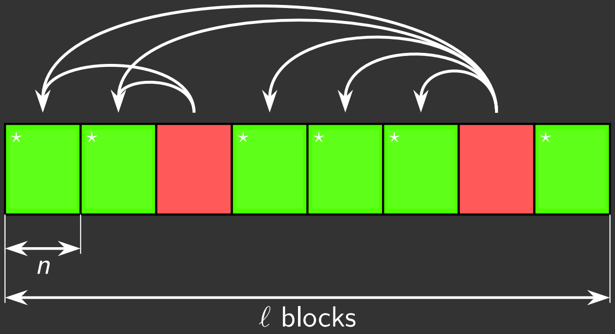
- $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$ with $\mathbf{X}_i \sim \{0,1\}^n$
- g good blocks, $\ell - g$ bad blocks
- Good blocks: **Independent** and **Uniform**



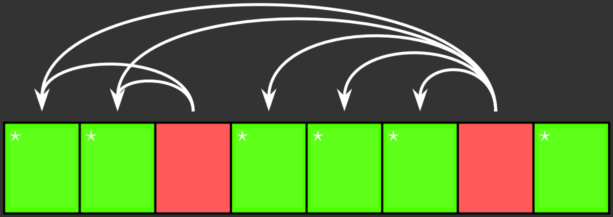
Online Non Oblivious Symbol Fixing (oNOSF) Sources

(g, ℓ, n) oNOSF source $\mathbf{X}$

- $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$ with $\mathbf{X}_i \sim \{0,1\}^n$
- g good blocks, $\ell - g$ bad blocks
- Good blocks: **Independent** and **Uniform**
- Bad blocks: Deterministic function of **previous blocks**

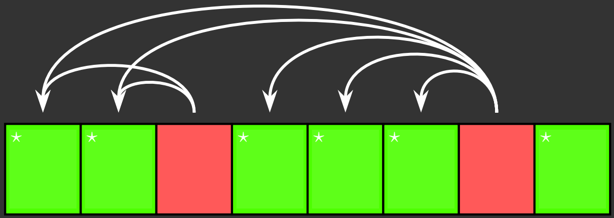


Motivation



Motivation

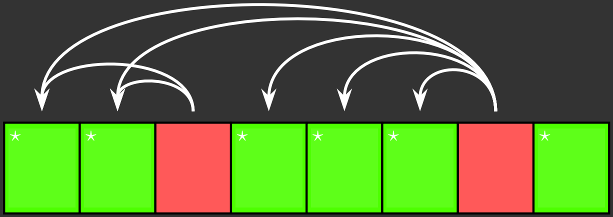
Blockchains as randomness beacon - CRS model



Motivation

Blockchains as randomness beacon - CRS model

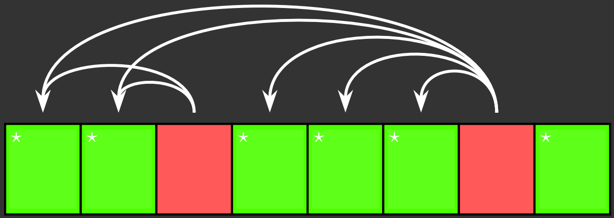
- Each good block has independent entropy



Motivation

Blockchains as randomness beacon - CRS model

- Each good block has independent entropy
- Real time generation - bad blocks depend on previous blocks

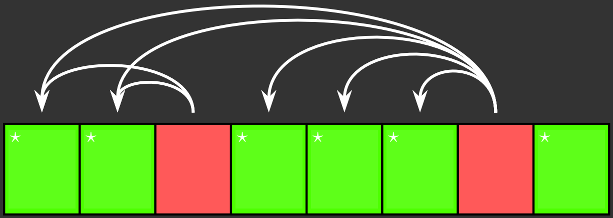


Motivation

Blockchains as randomness beacon - CRS model

- Each good block has independent entropy
- Real time generation - bad blocks depend on previous blocks

We show, can transform these to oNOSF sources — each good block **uniform**



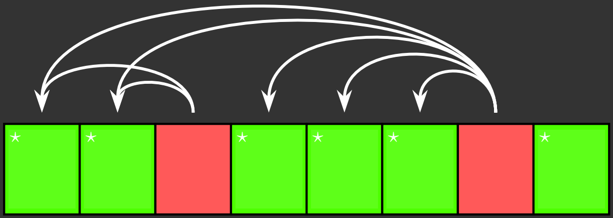
Motivation

Blockchains as randomness beacon - CRS model

- Each good block has independent entropy
- Real time generation - bad blocks depend on previous blocks

We show, can transform these to oNOSF sources — each good block **uniform**

Single turn coin flipping protocols **Ben-Or, Linial'85**



Motivation

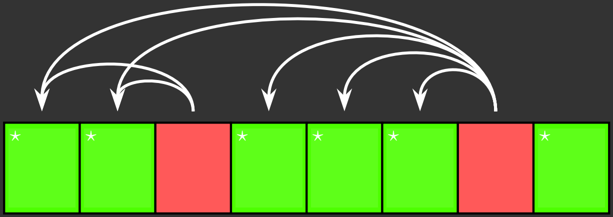
Blockchains as randomness beacon - CRS model

- Each good block has independent entropy
- Real time generation - bad blocks depend on previous blocks

We show, can transform these to oNOSF sources — each good block **uniform**

Single turn coin flipping protocols Ben-Or, Linial'85

- ℓ players, g good, access to independent n uniform bits



Motivation

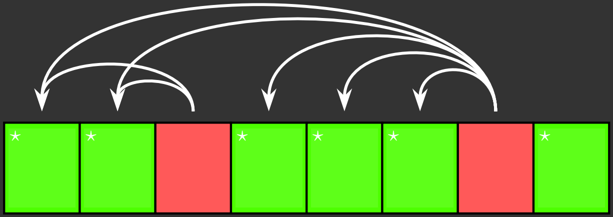
Blockchains as randomness beacon - CRS model

- Each good block has independent entropy
- Real time generation - bad blocks depend on previous blocks

We show, can transform these to oNOSF sources — each good block **uniform**

Single turn coin flipping protocols **Ben-Or, Linial'85**

- ℓ players, g good, access to independent n uniform bits
- Take turns broadcasting their sources



Brief History

Brief History

Aggarwal – Obremski – Ribeiro – Siniscalchi – Visconti (AORSV)'20

- Convert low entropy oNOSF sources to NOSF sources
- Extracting from oNOSF sources

Brief History

Aggarwal – Obremski – Ribeiro – Siniscalchi – Visconti (AORSV)'20

- Convert low entropy oNOSF sources to NOSF sources
- Extracting from oNOSF sources

Chattopadhyay – G – Ringach (CGR)'24

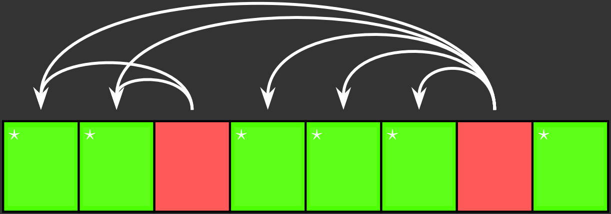
- Convert low entropy oNOSF sources to oNOSF sources
- Condensing from oNOSF sources

Condensing against Online Adversaries

Condensing from oNOSF sources

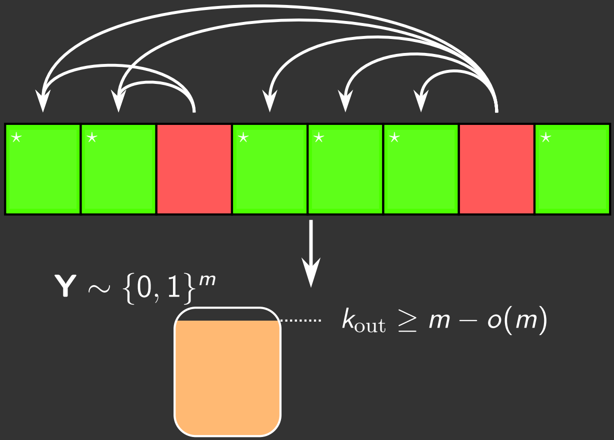
Condensing from oNOSF sources

Input: (g, ℓ, n) oNOSF source with $\boldsymbol{g \geq 0.51\ell}$



Condensing from oNOSF sources

Input: (g, ℓ, n) oNOSF source with $\boldsymbol{g \geq 0.51\ell}$
Output: $\mathbf{Y} \sim \{0,1\}^m$ with $\boldsymbol{H_\infty^\varepsilon(\mathbf{Y}) = k_{out} \geq m - o(m)}$



Condensing from oNOSF Sources

Input: (g, ℓ, n) oNOSF source with $\boldsymbol{g \geq 0.51\ell}$
Output: $\mathbf{Y} \sim \{0,1\}^m$ with $\boldsymbol{H_\infty^\varepsilon(\mathbf{Y}) = k_{out} \geq m - o(m)}$

Why not $g \leq 0.5\ell$

Condensing from oNOSF Sources

Input: (g, ℓ, n) oNOSF source with $\boldsymbol{g \geq 0.51\ell}$
Output: $\mathbf{Y} \sim \{0,1\}^m$ with $\boldsymbol{H_\infty^\varepsilon(\mathbf{Y}) = k_{out} \geq m - o(m)}$

Why not $g \leq 0.5\ell$

CGR'24 : For any $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, exists $(\boldsymbol{g = 0.5\ell}, \ell, n)$ oNOSF source $\mathbf{X}$ s.t. $\boldsymbol{H_\infty^\varepsilon(f(\mathbf{X})) \leq 0.5m}$, $\varepsilon = 0.1$

Condensing from oNOSF Sources

Input: (g, ℓ, n) oNOSF source with $\boldsymbol{g \geq 0.51\ell}$
Output: $\mathbf{Y} \sim \{0,1\}^m$ with $\boldsymbol{H_\infty^\varepsilon(\mathbf{Y}) = k_{out} \geq m - o(m)}$

Why not $g \leq 0.5\ell$

CGR'24 : For any $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, exists $(\boldsymbol{g = 0.5\ell}, \ell, n)$ oNOSF source $\mathbf{X}$ s.t. $\boldsymbol{H_\infty^\varepsilon(f(\mathbf{X})) \leq 0.5m}$, $\varepsilon = 0.1$

Why not non-online

Condensing from oNOSF Sources

Input: (g, ℓ, n) oNOSF source with $\boldsymbol{g \geq 0.51\ell}$
Output: $\mathbf{Y} \sim \{0,1\}^m$ with $\boldsymbol{H_\infty^\varepsilon(\mathbf{Y}) = k_{out} \geq m - o(m)}$

Why not $g \leq 0.5\ell$

CGR'24 : For any $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, exists $(\boldsymbol{g = 0.5\ell}, \ell, n)$ oNOSF source $\mathbf{X}$ s.t. $\boldsymbol{H_\infty^\varepsilon(f(\mathbf{X})) \leq 0.5m}$, $\varepsilon = 0.1$

Why not non-online

CGR'24 : For non-online sources, can't condense when $\boldsymbol{g = 0.8\ell}$, beyond **rate 0.8**

Condensing from oNOSF Sources

Input: (g, ℓ, n) oNOSF source with $\boldsymbol{g \geq 0.51\ell}$
Output: $\mathbf{Y} \sim \{0,1\}^m$ with $\boldsymbol{H_\infty^\varepsilon(\mathbf{Y}) = k_{out} \geq m - o(m)}$

Why not $g \leq 0.5\ell$

CGR'24 : For any $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, exists $(\boldsymbol{g = 0.5\ell}, \ell, n)$ oNOSF source $\mathbf{X}$ s.t. $\boldsymbol{H_\infty^\varepsilon(f(\mathbf{X})) \leq 0.5m}$, $\varepsilon = 0.1$

Why not non-online

CGR'24 : For non-online sources, can't condense when $\boldsymbol{g = (1-\delta)\ell}$, beyond **rate $\boldsymbol{1-\delta}$**

Condensing from oNOSF Sources

Input: (g, ℓ, n) oNOSF source with $\boldsymbol{g \geq 0.51\ell}$
Output: $\mathbf{Y} \sim \{0,1\}^m$ with $\boldsymbol{H_\infty^\varepsilon(\mathbf{Y}) = k_{out} \geq m - o(m)}$

Why not $g \leq 0.5\ell$

CGR'24 : For any $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, exists $(\boldsymbol{g = 0.5\ell}, \ell, n)$ oNOSF source $\mathbf{X}$ s.t. $\boldsymbol{H_\infty^\varepsilon(f(\mathbf{X})) \leq 0.5m}$, $\varepsilon = 0.1$

Why not non-online

CGR'24 : For non-online sources, can't condense when $\boldsymbol{g = (1-\delta)\ell}$, beyond **rate** $\boldsymbol{1 - \delta}$

Why not extract uniform randomness?

Condensing from oNOSF Sources

Input: (g, ℓ, n) oNOSF source with $\boldsymbol{g \geq 0.51\ell}$
Output: $\mathbf{Y} \sim \{0,1\}^m$ with $\boldsymbol{H_\infty^\varepsilon(\mathbf{Y}) = k_{out} \geq m - o(m)}$

Why not $g \leq 0.5\ell$

CGR'24 : For any $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, exists $(\boldsymbol{g = 0.5\ell}, \ell, n)$ oNOSF source $\mathbf{X}$ s.t. $\boldsymbol{H_\infty^\varepsilon(f(\mathbf{X})) \leq 0.5m}$, $\varepsilon = 0.1$

Why not non-online

CGR'24 : For non-online sources, can't condense when $\boldsymbol{g = (1-\delta)\ell}$, beyond **rate $\boldsymbol{1-\delta}$**

Why not extract uniform randomness?

AORSV'20 : Can't extract even if $g = 0.99\ell$

Condensing from oNOSF Sources - Constructions

Input: (g, ℓ, n) oNOSF source $\mathbf{X}$ with $\boldsymbol{g \geq 0.51\ell}$
Output: $\mathbf{Y} \sim \{0,1\}^m$ with $\boldsymbol{H_\infty^\varepsilon(\mathbf{Y}) \geq m - o(m)}$

Condensing from oNOSF Sources - Constructions

Input: (g, ℓ, n) oNOSF source $\mathbf{X}$ with $\boldsymbol{g \geq 0.51\ell}$
Output: $\mathbf{Y} \sim \{0,1\}^m$ with $\boldsymbol{H_\infty^\varepsilon(\mathbf{Y}) \geq m - o(m)}$
Parameters: $\boldsymbol{m = O(\ell n), \varepsilon = 1/\mathrm{poly}(n)}$

Condensing from oNOSF Sources - Constructions

Input: (g, ℓ, n) oNOSF source $\mathbf{X}$ with $\boldsymbol{g \geq 0.51\ell}$
Output: $\mathbf{Y} \sim \{0,1\}^m$ with $\boldsymbol{H_\infty^\varepsilon(\mathbf{Y}) \geq m - o(m)}$
Parameters: $\boldsymbol{m = O(\ell n), \varepsilon = 1/\mathrm{poly}(n)}$

Problem gets **harder** as $\boldsymbol{n}$ gets **smaller**

Work	Existential / Explicit	n

Condensing from oNOSF Sources - Constructions

Input: (g, ℓ, n) oNOSF source $\mathbf{X}$ with $\boldsymbol{g \geq 0.51\ell}$
Output: $\mathbf{Y} \sim \{0,1\}^m$ with $\boldsymbol{H_\infty^\varepsilon(\mathbf{Y}) \geq m - o(m)}$
Parameters: $\boldsymbol{m = O(\ell n), \varepsilon = 1/\mathrm{poly}(n)}$

Problem gets **harder** as $\boldsymbol{n}$ gets **smaller**

Work	Existential / Explicit	n
CGR'24	Existential	$\geq 2^{\Omega(\ell)}$

Condensing from oNOSF Sources - Constructions

Input: (g, ℓ, n) oNOSF source $\mathbf{X}$ with $\boldsymbol{g \geq 0.51\ell}$
Output: $\mathbf{Y} \sim \{0,1\}^m$ with $\boldsymbol{H_\infty^\varepsilon(\mathbf{Y}) \geq m - o(m)}$
Parameters: $\boldsymbol{m = O(\ell n), \varepsilon = 1/\mathrm{poly}(n)}$

Problem gets **harder** as $\boldsymbol{n}$ gets **smaller**

Work	Existential / Explicit	n
CGR'24	Existential	$\geq 2^{\Omega(\ell)}$
Our Result	Existential	$\geq \omega(1)$

Condensing from oNOSF Sources - Constructions

Input: (g, ℓ, n) oNOSF source $\mathbf{X}$ with $g \geq 0.51\ell$
Output: $\mathbf{Y} \sim \{0,1\}^m$ with $H_\infty^\varepsilon(\mathbf{Y}) \geq m - o(m)$
Parameters: $m = O(\ell n), \varepsilon = 1/\text{poly}(n)$

Problem gets **harder** as n gets **smaller**

Work	Existential / Explicit	n
CGR'24	Existential	$\geq 2^{\Omega(\ell)}$
Our Result	Existential	$\geq \omega(1)$
Our Result	Explicit	$\geq \text{polylog}(\ell)$

Condensing from entropic and $g = 1$ oNOSF source

Condensing from entropic and $g = 1$ oNOSF source

Statement

Condensing from entropic and $g = 1$ oNOSF source

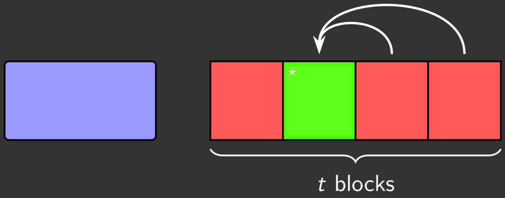
Statement

- $\mathbf{A} \sim \{0,1\}^r$ s.t. $H_\infty(\mathbf{A}) \geq 0.01r$

Condensing from entropic and $g = 1$ oNOSF source

Statement

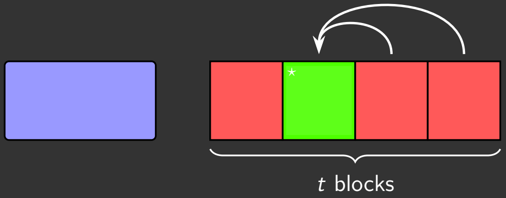
- $\mathbf{A} \sim \{0,1\}^r$ s.t. $H_\infty(\mathbf{A}) \geq 0.01r$
- $\mathbf{B}$: $(1, t, n)$ oNOSF source with $n \geq 2^{\Omega(t)} \cdot \log(r/\varepsilon)$



Condensing from entropic and $g = 1$ oNOSF source

Statement

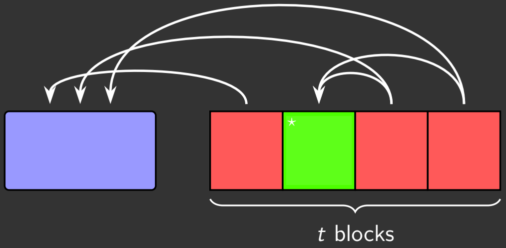
- $\mathbf{A} \sim \{0,1\}^r$ s.t. $H_\infty(\mathbf{A}) \geq 0.01r$
- **B**: $(1, t, n)$ oNOSF source with $n \geq 2^{\Omega(t)} \cdot \log(r/\varepsilon)$
- Good block in **B** **independent** of **A**



Condensing from entropic and $g = 1$ oNOSF source

Statement

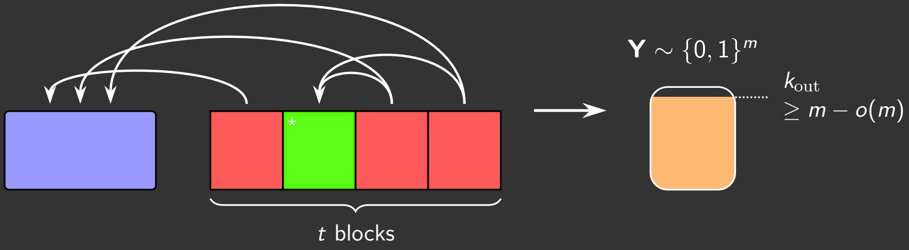
- $\mathbf{A} \sim \{0,1\}^r$ s.t. $H_\infty(\mathbf{A}) \geq 0.01r$
- **B**: $(1, t, n)$ oNOSF source with $n \geq 2^{\Omega(t)} \cdot \log(r/\varepsilon)$
- Good block in **B** **independent** of **A**
- Bad blocks in **B** **depend arbitrarily** on **A**



Condensing from entropic and $g = 1$ oNOSF source

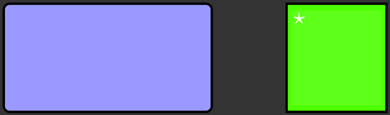
Statement

- $\mathbf{A} \sim \{0,1\}^r$ s.t. $H_\infty(\mathbf{A}) \geq 0.01r$
- $\mathbf{B}$: $(1, t, n)$ oNOSF source with $n \geq 2^{\Omega(t)} \cdot \log(r/\varepsilon)$
- Good block in **B** **independent** of **A**
- Bad blocks in **B** **depend arbitrarily** on **A**
- Can **explicitly** construct Cond s.t.
  $H^{\varepsilon}_{\infty}(\mathrm{Cond}(\mathbf{A}, \mathbf{B})) \geq m - o(m)$ with $m = \Omega(r)$



Condensing from entropic and $g = 1$ oNOSF source

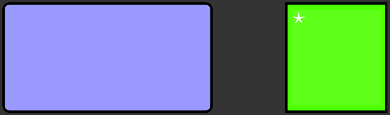
What if $g = t = 1$



Condensing from entropic and $g = 1$ oNOSF source

What if $g = t = 1$

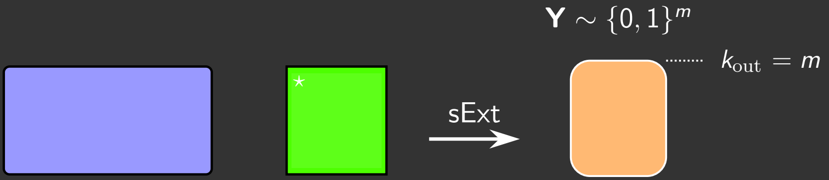
- **A**: **Entropic**, **B**: **independent** and **uniform**



Condensing from entropic and $g = 1$ oNOSF source

What if $g = t = 1$

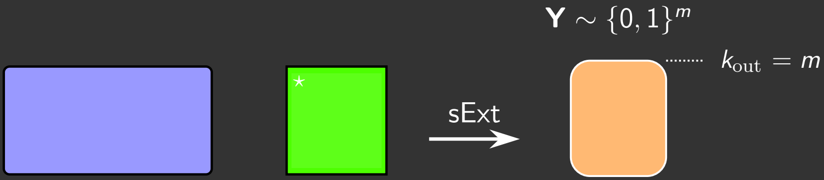
- **A**: **Entropic**, **B**: **independent** and **uniform**
- Exactly need **seeded extractors** Nisan-Zuckerman'96



Condensing from entropic and $g = 1$ oNOSF source

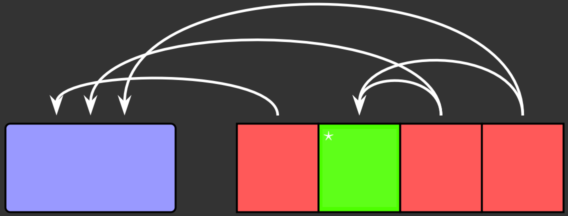
What if $g = t = 1$

- **A**: **Entropic**, **B**: **independent** and **uniform**
- Exactly need **seeded extractors** Nisan-Zuckerman'96
- Output **sExt(A, B)**



Condensing from entropic and $g = 1$ oNOSF source

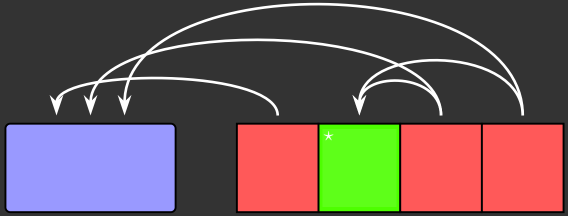
For $g = 1, t > 1$



Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$

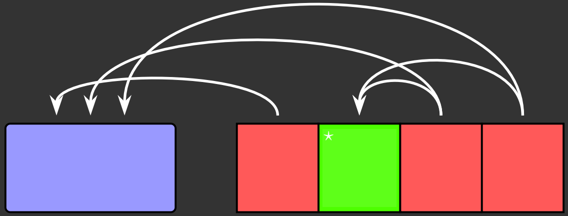
- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index j



Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$

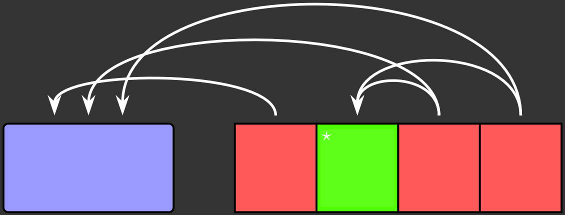
- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index j
- Construction Attempt: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$



Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$

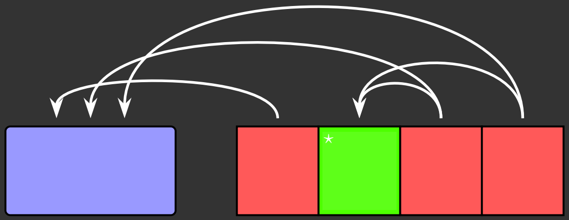
- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index j
- Construction Attempt: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$
- $\mathsf{sExt}(\mathsf{A}, \mathsf{B}_j)$ is uniform



Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$

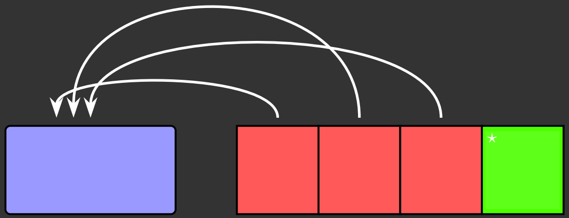
- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index j
- Construction Attempt: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$
- $\mathsf{sExt}(\mathsf{A}, \mathsf{B}_j)$ is uniform
- So what?



Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and Last block good

- **A**: **Entropic**, **B**: $(1, t, n)$ **oNOSF** source, good index $j = t$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$

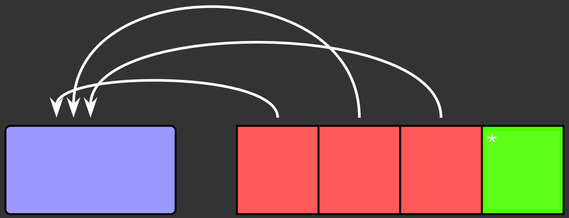


Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and Last block good

- **A**: **Entropic**, **B**: $(1, t, n)$ **oNOSF** source, good index $j = t$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$

Proof of Uniform output



Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and Last block good

- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index $j = t$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathbf{A}, \mathbf{B}_i)$

Proof of Uniform output

1. Condition on fixing bad blocks - $\mathbf{B}_1 = b_1, \ldots, \mathbf{B}_{t-1} = b_{t-1}$

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and Last block good

- **A**: **Entropic**, **B**: $(1, t, n)$ **oNOSF** source, good index $j = t$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathbf{A}, \mathbf{B}_i)$

Proof of Uniform output

1. Condition on fixing bad blocks - $\mathbf{B}_1 = b_1, \ldots, \mathbf{B}_{t-1} = b_{t-1}$
   - **A**: **Entropic**, $\mathbf{B}_t$: **Uniform and Independent**

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and Last block good

- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index $j = t$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$

Proof of Uniform output

1. Condition on fixing bad blocks - $\mathbf{B}_1 = b_1, \ldots, \mathbf{B}_{t-1} = b_{t-1}$
   - **A**: **Entropic**, $\mathbf{B}_t$: **Uniform and Independent**
   - Output — $\left(\bigoplus_{i=1}^{t-1} \mathsf{sExt}(\mathsf{A}, b_i)\right) \oplus \mathsf{sExt}(\mathsf{A}, \mathsf{B}_t)$

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and Last block good

- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index $\boldsymbol{j = t}$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathbf{A}, \mathbf{B}_i)$

Proof of Uniform output

1. Condition on fixing bad blocks - $\mathbf{B}_1 = b_1, \ldots, \mathbf{B}_{t-1} = b_{t-1}$
   - **A**: **Entropic**, $\mathbf{B}_t$: **Uniform and Independent**
   - Output — $f(\mathbf{A}) \oplus \mathsf{sExt}(\mathbf{A}, \mathbf{B}_t)$

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and Last block good

- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index $j = t$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$

Proof of Uniform output

1. Condition on fixing bad blocks - $\mathbf{B}_1 = b_1, \ldots, \mathbf{B}_{t-1} = b_{t-1}$
   - **A**: **Entropic**, $\mathbf{B}_t$: **Uniform and Independent**
   - Output — $f(\mathsf{A}) \oplus \mathsf{sExt}(\mathsf{A}, \mathsf{B}_t)$
2. Condition on fixing $f(\mathsf{A})$

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and Last block good

- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index $\boldsymbol{j = t}$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$

Proof of Uniform output

1. Condition on fixing bad blocks - $\mathbf{B}_1 = b_1, \ldots, \mathbf{B}_{t-1} = b_{t-1}$
   - **A**: **Entropic**, $\mathbf{B}_t$: **Uniform and Independent**
   - Output — $f(\mathsf{A}) \oplus \mathsf{sExt}(\mathsf{A}, \mathsf{B}_t)$
2. Condition on fixing $f(\mathsf{A})$
   - **A**: **Entropic**, $\mathbf{B}_t$: **Uniform and Independent**

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and Last block good

- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index $j = t$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathbf{A}, \mathbf{B}_i)$

Proof of Uniform output

1. Condition on fixing bad blocks - $\mathbf{B}_1 = b_1, \ldots, \mathbf{B}_{t-1} = b_{t-1}$
   - **A**: **Entropic**, $\mathbf{B}_t$: **Uniform and Independent**
   - Output — $f(\mathbf{A}) \oplus \mathsf{sExt}(\mathbf{A}, \mathbf{B}_t)$
2. Condition on fixing $f(\mathbf{A})$
   - **A**: **Entropic**, $\mathbf{B}_t$: **Uniform and Independent**
   - Output — $y_0 \oplus \mathsf{sExt}(\mathbf{A}, \mathbf{U})$

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and Last block good

- **A**: **Entropic**, **B**: $\mathbf{(1, t, n)}$ **oNOSF** source, good index $\boldsymbol{j = t}$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$

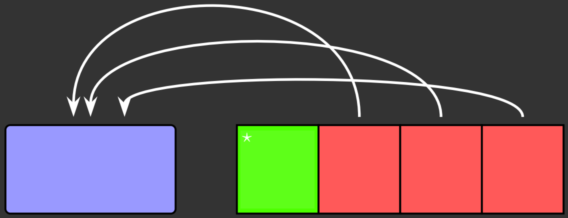
Proof of Uniform output

1. Condition on fixing bad blocks - $\mathbf{B}_1 = b_1, \ldots, \mathbf{B}_{t-1} = b_{t-1}$
   - **A**: **Entropic**, $\mathbf{B}_t$: **Uniform and Independent**
   - Output — $f(\mathsf{A}) \oplus \mathsf{sExt}(\mathsf{A}, \mathsf{B}_t)$
2. Condition on fixing $f(\mathsf{A})$
   - **A**: **Entropic**, $\mathbf{B}_t$: **Uniform and Independent**
   - Output — $y_0 \oplus \mathsf{sExt}(\mathsf{A}, \mathsf{U})$
3. By property of **sExt**, Output — **Uniform**

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(A, B_i)$

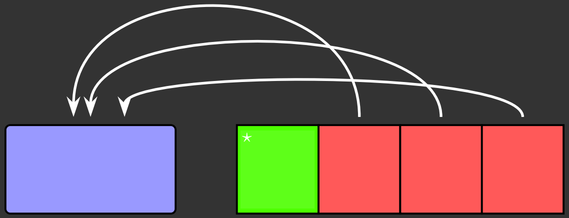


Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$

Adversary can't make things too bad lemma CGR'24



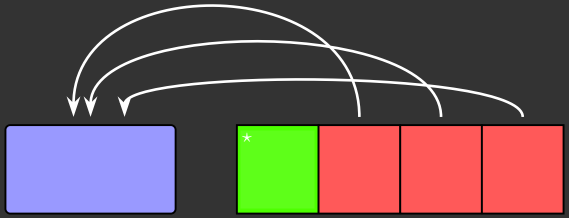
Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: $(1, t, n)$ **oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathbf{A}, \mathbf{B}_i)$

Adversary can't make things too bad lemma CGR'24

Say $\mathbf{Y} = f(\mathbf{X})$ and b bits in **X** **controlled by adversary**



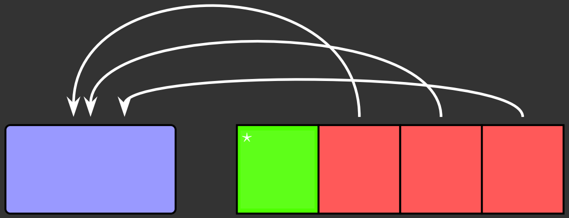
Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathbf{A}, \mathbf{B}_i)$

Adversary can't make things too bad lemma CGR'24

Say $\mathbf{Y} = f(\mathbf{X})$ and b bits in $\mathbf{X}$ **controlled by adversary**
If those b bits **uniform**, $\mathbf{Y}_{\text{uniform}}$ s.t. $H_\infty^\varepsilon(\mathbf{Y}_{\text{uniform}}) \geq k_{out}$



Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

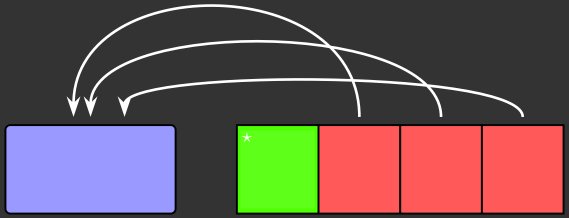
- **A**: **Entropic**, **B**: $\mathbf{(1, t, n)}$ **oNOSF** source, good index $\boldsymbol{j = 1}$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$

Adversary can't make things too bad lemma CGR'24

Say $\mathbf{Y} = f(\mathbf{X})$ and b bits in $\mathbf{X}$ **controlled by adversary**

If those b bits **uniform**, $\mathbf{Y}_{\text{uniform}}$ s.t. $H_\infty^{\varepsilon}(\mathbf{Y}_{\text{uniform}}) \geq k_{out}$

Then, $\mathbf{Y}$ s.t. $H_\infty^{\varepsilon \cdot 2^b}(\mathbf{Y}) \geq k_{out} - b$



Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: $(1, t, n)$ **oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathbf{A}, \mathbf{B}_i)$

Adversary can't make things too bad lemma CGR'24

Say $\mathbf{Y} = f(\mathbf{X})$ and b bits in $\mathbf{X}$ **controlled by adversary**

If those b bits **uniform**, $\mathbf{Y}_{\text{uniform}}$ s.t. $H_\infty^\varepsilon(\mathbf{Y}_{\text{uniform}}) \geq k_{out}$

Then, $\mathbf{Y}$ s.t. $H_\infty^{\varepsilon \cdot 2^b}(\mathbf{Y}) \geq k_{out} - b$

Applying above

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: $(1, t, n)$ **oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathbf{A}, \mathbf{B}_i)$

Adversary can't make things too bad lemma CGR'24

Say $\mathbf{Y} = f(\mathbf{X})$ and b bits in $\mathbf{X}$ **controlled by adversary**
If those b bits **uniform**, $\mathbf{Y}_{\text{uniform}}$ s.t. $H_\infty^{\varepsilon}(\mathbf{Y}_{\text{uniform}}) \geq k_{out}$
Then, $\mathbf{Y}$ s.t. $H_\infty^{\varepsilon \cdot 2^b}(\mathbf{Y}) \geq k_{out} - b$

Applying above

- Adversary controls $b = n \cdot (t - 1)$ bits

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: $(1, t, n)$ **oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathbf{A}, \mathbf{B}_i)$

Adversary can't make things too bad lemma CGR'24

Say $\mathbf{Y} = f(\mathbf{X})$ and b bits in $\mathbf{X}$ **controlled by adversary**
If those b bits **uniform**, $\mathbf{Y}_{\text{uniform}}$ s.t. $H_\infty^\varepsilon(\mathbf{Y}_{\text{uniform}}) \geq k_{out}$
Then, $\mathbf{Y}$ s.t. $H_\infty^{\varepsilon \cdot 2^b}(\mathbf{Y}) \geq k_{out} - b$

Applying above

- Adversary controls $b = n \cdot (t - 1)$ bits
- If all blocks uniform, $k_{out} = m$

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: $(1, t, n)$ **oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathbf{A}, \mathbf{B}_i)$

Adversary can't make things too bad lemma CGR'24

Say $\mathbf{Y} = f(\mathbf{X})$ and b bits in $\mathbf{X}$ **controlled by adversary**
If those b bits **uniform**, $\mathbf{Y}_{\text{uniform}}$ s.t. $H_\infty^{\varepsilon}(\mathbf{Y}_{\text{uniform}}) \geq k_{out}$
Then, $\mathbf{Y}$ s.t. $H_\infty^{\varepsilon \cdot 2^b}(\mathbf{Y}) \geq k_{out} - b$

Applying above

- Adversary controls $b = n \cdot (t - 1)$ bits
- If all blocks uniform, $k_{out} = m$
- Can ensure $k_{out} - b \geq m - o(m)$

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$

Adversary can't make things too bad lemma CGR'24

Say $\mathsf{Y} = f(\mathsf{X})$ and b bits in **X** **controlled by adversary**
If those b bits **uniform**, $\mathsf{Y}_{\text{uniform}}$ s.t. $H_\infty^\varepsilon(\mathsf{Y}_{\text{uniform}}) \geq k_{out}$
Then, **Y** s.t. $H_\infty^{\varepsilon \cdot 2^b}(\mathsf{Y}) \geq k_{out} - b$

Applying above

- Adversary controls $b = n \cdot (t-1)$ bits
- If all blocks uniform, $k_{out} = m$
- Can ensure $k_{out} - b \geq m - o(m)$
- Need $\varepsilon < 2^{-b}$

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

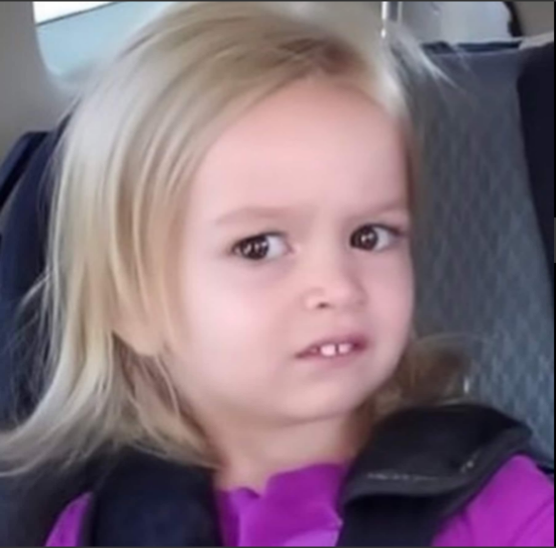
- **A**: **Entropic**, **B**: $(1, t, n)$ **oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$

Adversary can't make things too bad lemma CGR'24

Say $\mathbf{Y} = f(\mathbf{X})$ and b bits in $\mathbf{X}$ **controlled by adversary**
If those b bits **uniform**, $\mathbf{Y}_{\text{uniform}}$ s.t. $H_\infty^{\varepsilon}(\mathbf{Y}_{\text{uniform}}) \geq k_{out}$
Then, $\mathbf{Y}$ s.t. $H_\infty^{\varepsilon \cdot 2^b}(\mathbf{Y}) \geq k_{out} - b$

Applying above

- Adversary controls $b = n \cdot (t - 1)$ bits
- If all blocks uniform, $k_{out} = m$
- Can ensure $k_{out} - b \geq m - o(m)$
- Need $\varepsilon < 2^{-b}$
  By sExt requirements, $n \geq 2\log(1/\varepsilon) \geq 2b = 2n \cdot (t - 1)$



$$n \geq 2\log(1/\varepsilon) \geq 2b = 2n \cdot (t-1)$$

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: $(1, t, n)$ **oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$

Applying Adversary can't make things too bad lemma

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: $(1, t, n)$ **oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$

Applying Adversary can't make things too bad lemma

- Need $\varepsilon < 2^{-b}$, and by sExt requirements,

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$

Applying Adversary can't make things too bad lemma

- Need $\varepsilon < 2^{-b}$, and by sExt requirements,
  $n = |\mathsf{B}_1| \geq 2\log(1/\varepsilon) = 2b = 2\sum_{i=2}^{t} |\mathsf{B}_t| = 2n(t-1)$

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: $(1, t, n)$ **oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathsf{A}, \mathsf{B}_i)$

Applying Adversary can't make things too bad lemma

- Need $\varepsilon < 2^{-b}$, and by sExt requirements, $n = |\mathsf{B}_1| \geq 2\log(1/\varepsilon) = 2b = 2\sum_{i=2}^{t} |\mathsf{B}_t| = 2n(t-1)$
- Key observation: This works if $|\mathsf{B}_1| > 2\sum_{i=2}^{t} |\mathsf{B}_t|$

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: $(1, t, n)$ **oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathbf{A}, \mathbf{B}_i)$

Applying Adversary can't make things too bad lemma

- Need $\varepsilon < 2^{-b}$, and by sExt requirements,
  $n = |\mathbf{B_1}| \geq 2\log(1/\varepsilon) = 2b = 2\sum_{i=2}^{t} |\mathbf{B}_t| = 2n(t-1)$
- Key observation: This works if $|\mathbf{B_1}| > 2\sum_{i=2}^{t} |\mathbf{B}_t|$

For $g = 1, t > 1$ and position j good

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: $(\mathbf{1}, \boldsymbol{t}, \boldsymbol{n})$ **oNOSF** source, good index $\boldsymbol{j} = \mathbf{1}$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathbf{A}, \mathbf{B}_i)$

Applying Adversary can't make things too bad lemma

- Need $\varepsilon < 2^{-b}$, and by sExt requirements,
  $n = |\mathbf{B}_1| \geq 2\log(1/\varepsilon) = 2b = 2\sum_{i=2}^{t} |\mathbf{B}_t| = 2n(t-1)$
- Key observation: This works if $|\mathbf{B}_1| > 2\sum_{i=2}^{t} |\mathbf{B}_t|$

For $g = 1, t > 1$ and position j good

- Require $|\mathbf{B}_j| > 2\sum_{i=j+1}^{t} |\mathbf{B}_t|$

Condensing from entropic and $g = 1$ oNOSF source

For $g = 1, t > 1$ and First block good

- **A**: **Entropic**, **B**: $(1, t, n)$ **oNOSF** source, good index $j = 1$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(\mathbf{A}, \mathbf{B}_i)$

Applying Adversary can't make things too bad lemma

- Need $\varepsilon < 2^{-b}$, and by sExt requirements,
  $n = |\mathbf{B}_1| \geq 2\log(1/\varepsilon) = 2b = 2\sum_{i=2}^{t} |\mathbf{B}_t| = 2n(t-1)$
- Key observation: This works if $|\mathbf{B}_1| > 2\sum_{i=2}^{t} |\mathbf{B}_t|$

For $g = 1, t > 1$ and position j good

- Require $|\mathbf{B}_j| > 2\sum_{i=j+1}^{t} |\mathbf{B}_t|$
- Works if $|\mathbf{B}_i| = 2^{\Omega(t-i)}$

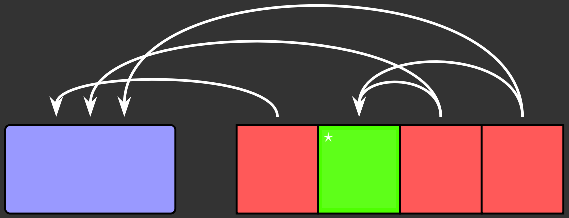
Condensing from entropic and $g = 1$ oNOSF source

Actual Construction

Condensing from entropic and $g = 1$ oNOSF source

Actual Construction

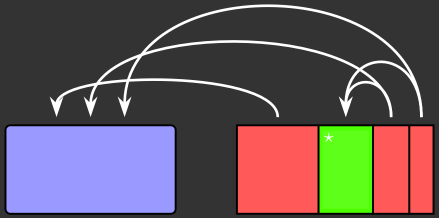
- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source



Condensing from entropic and $g = 1$ oNOSF source

Actual Construction

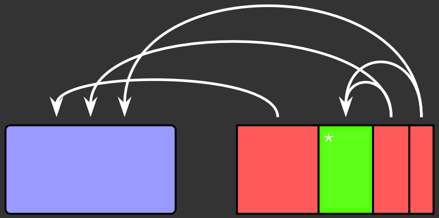
- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source
- Let $\mathbf{B}'_i$ be **first $2^{\Omega(t-i)}$** bits of $\mathbf{B}_i$



Condensing from entropic and $g = 1$ oNOSF source

Actual Construction

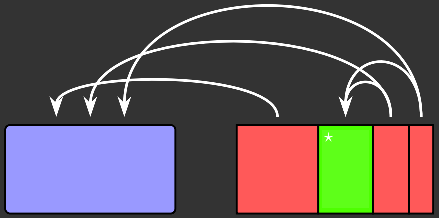
- **A**: **Entropic**, **B**: **$(1, t, n)$ oNOSF** source
- Let **B'_i** be **first $2^{\Omega(t-i)}$** bits of **B**$_i$
- Construction: $\bigoplus_{i=1}^{t} \mathsf{sExt}(A, B'_i)$



Condensing from entropic and $g = 1$ oNOSF source

Actual Construction

- **A**: **Entropic**, **B**: $\boldsymbol{(1, t, n)}$ **oNOSF** source
- Let $\mathbf{B}'_i$ be **first** $\mathbf{2^{\Omega(t-i)}}$ bits of $\mathbf{B}_i$
- Construction: $\bigoplus_{i=1}^{t} \mathbf{sExt}(\mathbf{A}, \mathbf{B}'_i)$
- Output entropy $\boldsymbol{m - o(m)}$



Condensing from oNOSF Sources

Condensing from entropic and $g = 1$ oNOSF source

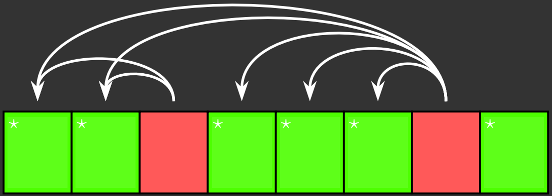
A: entropic, **B**: $(g = 1, t, n = 2^{\Omega(t)})$ oNOSF

Condensing from oNOSF Sources

Condensing from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(g = 1, t, n = 2^{\Omega(t)})$ oNOSF

Condensing from $g = 0.51\ell$, $n = 2^{\Omega(\ell)}$ oNOSF source



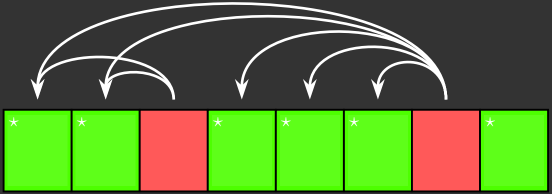
Condensing from oNOSF Sources

Condensing from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(\boldsymbol{g = 1, t, n = 2^{\Omega(t)}})$ oNOSF

Condensing from $g = 0.51\ell$, $\boldsymbol{n = 2^{\Omega(\ell)}}$ oNOSF source

- Given $\boldsymbol{g = 0.51\ell}$ oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$



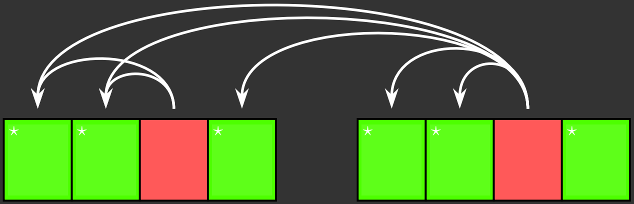
Condensing from oNOSF Sources

Condensing from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(g = 1, t, n = 2^{\Omega(t)})$ oNOSF

Condensing from $g = 0.51\ell$, $n = 2^{\Omega(\ell)}$ oNOSF source

- Given $g = 0.51\ell$ oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$
- Let $\mathbf{A} = (\mathbf{X}_1, \ldots, \mathbf{X}_{\ell/2})$ and $\mathbf{B} = (\mathbf{X}_{\ell/2+1}, \ldots, \mathbf{X}_\ell)$



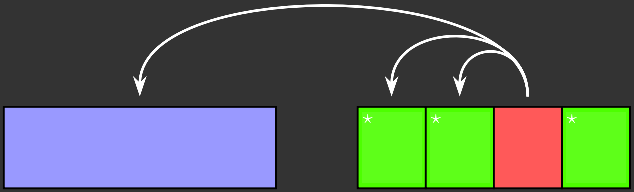
Condensing from oNOSF Sources

Condensing from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(g = 1, t, n = 2^{\Omega(t)})$ oNOSF

Condensing from $g = 0.51\ell$, $n = 2^{\Omega(\ell)}$ oNOSF source

- Given $g = 0.51\ell$ oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$
- Let $\mathbf{A} = (\mathbf{X}_1, \ldots, \mathbf{X}_{\ell/2})$ and $\mathbf{B} = (\mathbf{X}_{\ell/2+1}, \ldots, \mathbf{X}_\ell)$
- $|\mathbf{A}| = 0.5\ell n$, $H_\infty(\mathbf{A}) \geq 0.01\ell n$



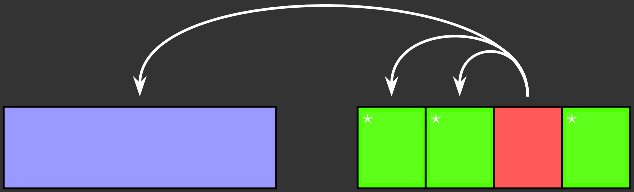
Condensing from oNOSF Sources

Condensing from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(g = 1, t, n = 2^{\Omega(t)})$ oNOSF

Condensing from $g = 0.51\ell$, $n = 2^{\Omega(\ell)}$ oNOSF source

- Given $g = 0.51\ell$ oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$
- Let $\mathbf{A} = (\mathbf{X}_1, \ldots, \mathbf{X}_{\ell/2})$ and $\mathbf{B} = (\mathbf{X}_{\ell/2+1}, \ldots, \mathbf{X}_\ell)$
- $|\mathbf{A}| = 0.5\ell n$, $H_\infty(\mathbf{A}) \geq 0.01\ell n$
- **B** has $\geq 0.01\ell$ **good players**, and is oNOSF source



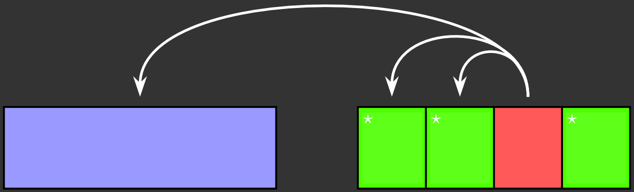
Condensing from oNOSF Sources

Condensing from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(g = 1, t, n = 2^{\Omega(t)})$ oNOSF

Condensing from $g = 0.51\ell$, $n = 2^{\Omega(\ell)}$ oNOSF source

- Given $g = 0.51\ell$ oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$
- Let $\mathbf{A} = (\mathbf{X}_1, \ldots, X_{\ell/2})$ and $\mathbf{B} = (\mathbf{X}_{\ell/2+1}, \ldots, X_\ell)$
- $|\mathbf{A}| = 0.5\ell n$, $H_\infty(\mathbf{A}) \geq 0.01\ell n$
- **B** has $\geq 0.01\ell$ **good players**, and is oNOSF source
- **Cond(A, B)** from above condenses



Condensing from oNOSF Sources

Can Condense from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(\boldsymbol{g = 1, t, n \geq 2^{\Omega(t)}})$ oNOSF

Condensing from $g = 0.51\ell, \boldsymbol{n = \text{polylog}(\ell)}$ oNOSF source

Condensing from oNOSF Sources

Can Condense from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(\boldsymbol{g = 1, t, n \geq 2^{\Omega(t)}})$ oNOSF

Condensing from $g = 0.68\ell$, $\boldsymbol{n} = \textbf{poly}(\boldsymbol{\ell})$ oNOSF source

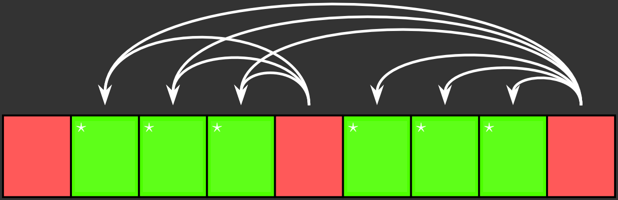
Condensing from oNOSF Sources

Can Condense from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(\boldsymbol{g = 1, t, n \geq 2^{\Omega(t)}})$ oNOSF

Condensing from $g = 0.68\ell$, $\boldsymbol{n = \mathrm{poly}(\ell)}$ oNOSF source

- Given $\boldsymbol{g = 0.68\ell}$ oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$



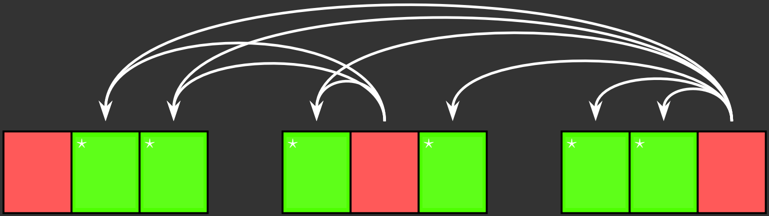
Condensing from oNOSF Sources

Can Condense from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(\boldsymbol{g = 1, t, n \geq 2^{\Omega(t)}})$ oNOSF

Condensing from $g = 0.68\ell$, $\boldsymbol{n = \mathrm{poly}(\ell)}$ oNOSF source

- Given $\boldsymbol{g = 0.68\ell}$ oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$
- Divide players in $\mathbf{X}$ into three equal parts - **S, A, B**



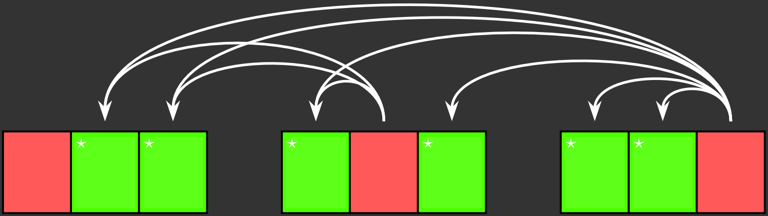
Condensing from oNOSF Sources

Can Condense from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(\boldsymbol{g = 1, t, n \geq 2^{\Omega(t)}})$ oNOSF

Condensing from $g = 0.68\ell$, $\boldsymbol{n = \mathrm{poly}(\ell)}$ oNOSF source

- Given $\boldsymbol{g = 0.68\ell}$ oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$
- Divide players in **X** into three equal parts - **S, A, B**
- Each has $\boldsymbol{\geq 0.01\ell}$ good players



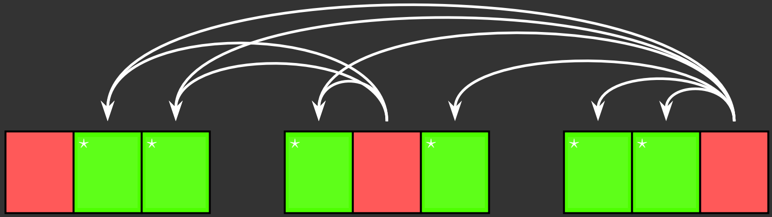
Condensing from oNOSF Sources

Can Condense from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(\boldsymbol{g = 1, t, n \geq 2^{\Omega(t)}})$ oNOSF

Condensing from $g = 0.68\ell$, $\boldsymbol{n = \mathrm{poly}(\ell)}$ oNOSF source

- Given $\boldsymbol{g = 0.68\ell}$ oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$
- Divide players in **X** into three equal parts - **S, A, B**
- Each has $\geq \boldsymbol{0.01\ell}$ good players
- Committee selection Russell-Zuckerman'97, Feige'98 over **S** to select $\boldsymbol{t = \log(\ell)}$ players from **B** with ≥ 1 good player whp



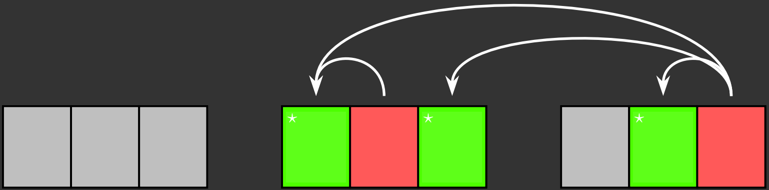
Condensing from oNOSF Sources

Can Condense from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(\boldsymbol{g = 1, t, n \geq 2^{\Omega(t)}})$ oNOSF

Condensing from $g = 0.68\ell$, $\boldsymbol{n = \text{poly}(\ell)}$ oNOSF source

- Given $\boldsymbol{g = 0.68\ell}$ oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$
- Divide players in **X** into three equal parts - **S, A, B**
- Each has $\geq \boldsymbol{0.01\ell}$ good players
- Committee selection Russell-Zuckerman'97, Feige'98 over **S** to select $\boldsymbol{t = \log(\ell)}$ players from **B** with ≥ 1 good player whp



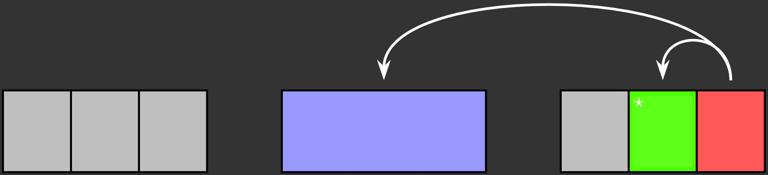
Condensing from oNOSF Sources

Can Condense from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(\boldsymbol{g = 1, t, n \geq 2^{\Omega(t)}})$ oNOSF

Condensing from $g = 0.68\ell$, $\boldsymbol{n = \mathrm{poly}(\ell)}$ oNOSF source

- Given $\boldsymbol{g = 0.68\ell}$ oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$
- Divide players in $\mathbf{X}$ into three equal parts - **S, A, B**
- Each has $\geq \boldsymbol{0.01\ell}$ good players
- Committee selection Russell-Zuckerman'97, Feige'98 over **S** to select $\boldsymbol{t = \log(\ell)}$ players from **B** with ≥ 1 good player whp
- Output $\mathbf{Cond(A, B|_{t=\log(\ell)})}$



Condensing from oNOSF Sources

Can Condense from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(g = 1, t, n = 2^{\Omega(t)})$ oNOSF

Condensing from $g = 0.68\ell, n = \text{poly}(\ell)$ oNOSF source

- Given $g = 0.68\ell$ oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$
- Divide players in **X** into three equal parts - **S, A, B**
- Each has $\geq 0.01\ell$ good players
- Committee selection Russell-Zuckerman'97, Feige'98 over **S** to select $t = \log(\ell)$ players from **B** with ≥ 1 good player whp
- Output $\text{Cond}(\mathbf{A}, \mathbf{B}|_{t=\log(\ell)})$
- Requires $n = 2^{O(t)} = \text{poly}(\ell)$

Condensing from oNOSF Sources

Can Condense from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(\boldsymbol{g = 1, t, n = 2^{\Omega(t)}})$ oNOSF

Condensing from $g = 0.68\ell$, $\boldsymbol{n = \text{poly}(\ell)}$ oNOSF source

- Given $\boldsymbol{g = 0.68\ell}$ oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$
- Divide players in $\mathbf{X}$ into three equal parts - **S, A, B**
- Each has $\geq \boldsymbol{0.01\ell}$ good players
- Committee selection Russell-Zuckerman'97, Feige'98 over **S** to select $\boldsymbol{t = \log(\ell)}$ players from **B** with ≥ 1 good player whp
- Output $\mathbf{Cond(A, B|_{t=\log(\ell)})}$
- Requires $\boldsymbol{n = 2^{O(t)} = \text{poly}(\ell)}$

For $\boldsymbol{n = \text{polylog}(\ell)}$, select $\boldsymbol{t = \log(\log(\ell))}$ sized committee

Condensing from oNOSF Sources

Can Condense from entropic and $g = 1$ oNOSF source

A: entropic, **B**: $(\boldsymbol{g = 1, t, n = 2^{\Omega(t)}})$ oNOSF

Condensing from $g = 0.68\ell, \boldsymbol{n} = \textbf{poly}(\ell)$ oNOSF source

- Given $\boldsymbol{g = 0.68\ell}$ oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$
- Divide players in $\mathbf{X}$ into three equal parts - **S, A, B**
- Each has $\geq \boldsymbol{0.01\ell}$ good players
- Committee selection Russell-Zuckerman'97, Feige'98 over **S** to select $\boldsymbol{t} = \textbf{log}(\ell)$ players from **B** with ≥ 1 good player whp
- Output $\textbf{Cond}(\mathbf{A}, \mathbf{B}|_{t=\log(\ell)})$
- Requires $\boldsymbol{n = 2^{O(t)}} = \textbf{poly}(\ell)$

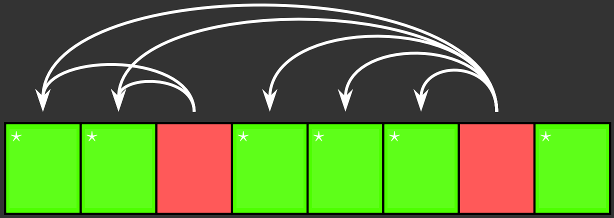
For $\boldsymbol{n} = \textbf{polylog}(\ell)$, select $\boldsymbol{t} = \textbf{log}(\textbf{log}(\ell))$ sized committee
With care, can handle $\boldsymbol{g = 0.51\ell}$

Extracting against Online Adversaries

Extracting from oNOSF sources

Extracting from oNOSF sources

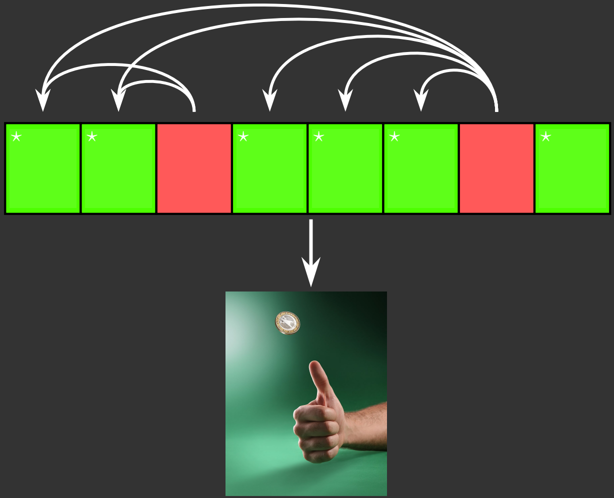
Input: (g, ℓ, n) oNOSF source



Extracting from oNOSF sources

Input: (g, ℓ, n) oNOSF source

Output: ε-close to $\mathbf{U}_1$



Extracting from oNOSF sources: Constructions

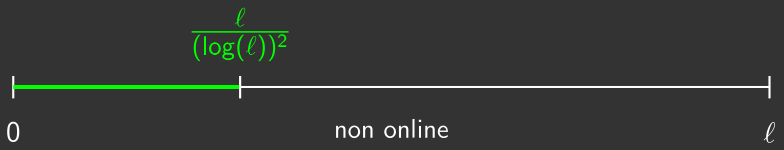
Extracting from oNOSF sources: Constructions

Extracting against non online adversaries

Extracting from oNOSF sources: Constructions

Extracting against non online adversaries

Ajtai-Linial'93 : Extract from $b = \frac{\ell}{(\log(\ell))^2}$ bad players with $n = 1$

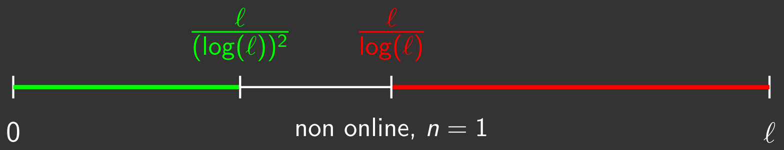


Extracting from oNOSF sources: Constructions

Extracting against non online adversaries

Ajtai-Linial'93 : Extract from $\boldsymbol{b = \frac{\ell}{(\log(\ell))^2}}$ bad players with $\boldsymbol{n = 1}$

Kahn-Kalai-Linial'88 : Can't Extract $\boldsymbol{b = \frac{\ell}{\log(\ell)}}$ with $\boldsymbol{n = 1}$



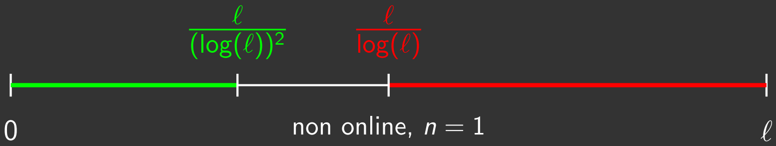
Extracting from oNOSF sources: Constructions

Extracting against non online adversaries

Ajtai-Linial'93 : Extract from $\boldsymbol{b = \frac{\ell}{(\log(\ell))^2}}$ bad players with $\boldsymbol{n = 1}$

Kahn-Kalai-Linial'88 : Can't Extract $\boldsymbol{b = \frac{\ell}{\log(\ell)}}$ with $\boldsymbol{n = 1}$

Our Results — against Online adversaries



Extracting from oNOSF sources: Constructions

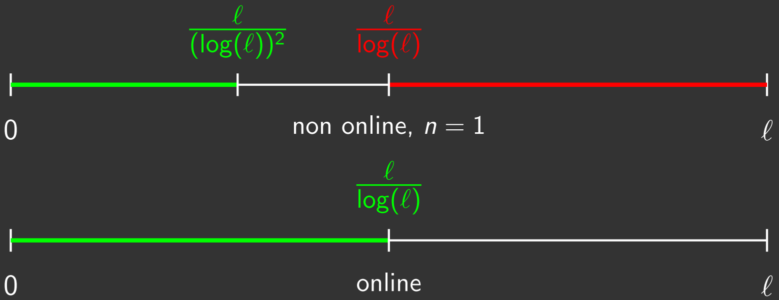
Extracting against non online adversaries

Ajtai-Linial'93 : Extract from $\boldsymbol{b = \frac{\ell}{(\log(\ell))^2}}$ bad players with $\boldsymbol{n = 1}$

Kahn-Kalai-Linial'88 : Can't Extract $\boldsymbol{b = \frac{\ell}{\log(\ell)}}$ with $\boldsymbol{n = 1}$

Our Results — against Online adversaries

- Extract from $\boldsymbol{b = \frac{\ell}{\log(\ell)}}$ bad players, with $\boldsymbol{n = 1}$



Extracting from oNOSF sources: Constructions

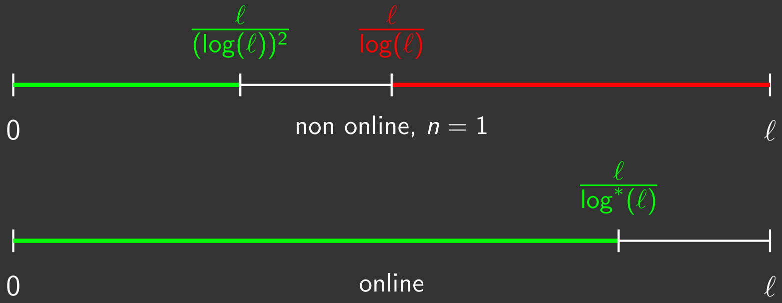
Extracting against non online adversaries

Ajtai-Linial'93 : Extract from $b = \frac{\ell}{(\log(\ell))^2}$ bad players with $n = 1$

Kahn-Kalai-Linial'88 : Can't Extract $b = \frac{\ell}{\log(\ell)}$ with $n = 1$

Our Results — against Online adversaries

- Extract from $b = \frac{\ell}{\log(\ell)}$ bad players, with $n = 1$
- Extract from $b = \frac{\ell}{\log^*(\ell)}$ bad players with $n = \log(\ell)$



Open Problems

Open Problems

Extraction

- How many bad players can one tolerate and still extract?
- For $n = 1$, answer between $\frac{\ell}{\log(\ell)}$ and 0.01ℓ
- For $n = \log(\ell)$, answer between $\frac{\ell}{\log^*(\ell)}$ and 0.01ℓ

Open Problems

Extraction

- How many bad players can one tolerate and still extract?
- For $n = 1$, answer between $\frac{\ell}{\log(\ell)}$ and 0.01ℓ
- For $n = \log(\ell)$, answer between $\frac{\ell}{\log^*(\ell)}$ and 0.01ℓ

Simple Explicit Optimal Condenser

- Explicitly construct seeded condenser with seed length dependence $1 \cdot \log(1/\varepsilon)$
- For our existential construction, rely on this object
- Will improve error dependence on n

Open Problems

Extraction

- How many bad players can one tolerate and still extract?
- For $\boldsymbol{n = 1}$, answer between $\frac{\ell}{\log(\ell)}$ and $\mathbf{0.01}\ell$
- For $\boldsymbol{n = \log(\ell)}$, answer between $\frac{\ell}{\log^*(\ell)}$ and $\mathbf{0.01}\ell$

Simple Explicit Optimal Condenser

- Explicitly construct seeded condenser with seed length dependence $\mathbf{1 \cdot \log(1/\varepsilon)}$
- For our existential construction, rely on this object
- Will improve error dependence on n

Condensing for $n = 1$

Show one **can condense** from $\boldsymbol{(g = 0.51\ell, \ell, n = 1)}$ oNOSF sources, or that this is **impossible**

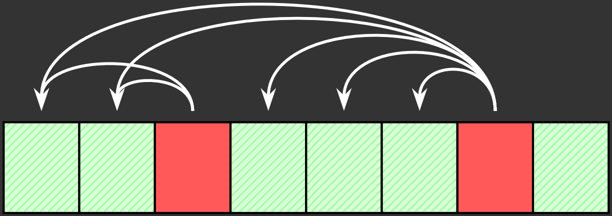
Thank You

Bonus: Converting oNOSF sources to uniform oNOSF sources

Desired transformation

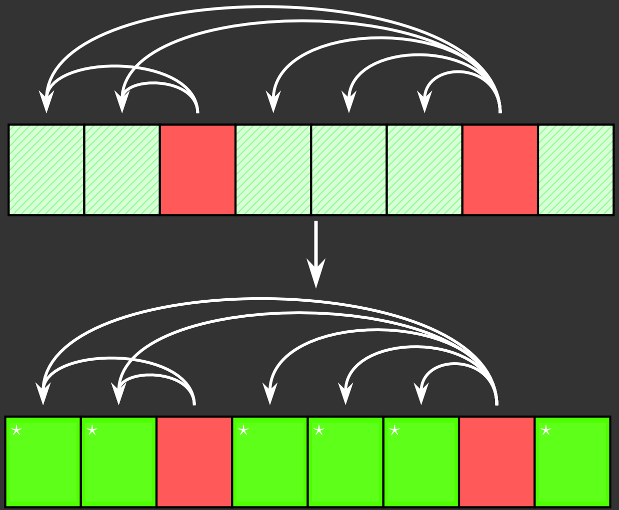
Desired transformation

Input: (g, ℓ, n, k)-oNOSF source



Desired transformation

Input: (g, ℓ, n, k)-oNOSF source
Output: ε-close to (g', ℓ', n') uniform oNOSF source



Previous Works and Our Results

Previous Works and Our Results

Input: (g, ℓ, n, k) oNOSF source Output: (g', ℓ', n') uniform oNOSF source

Previous Works and Our Results

Input: (g, ℓ, n, k) oNOSF source Output: (g', ℓ', n') uniform oNOSF source

Work	**In** k	**In** n	**Out** g	**Out** ℓ	**Out online?**

Previous Works and Our Results

Input: (g, ℓ, n, k) oNOSF source Output: (g', ℓ', n') uniform oNOSF source

Work	**In** k	**In** n	**Out** g	**Out** ℓ	**Out online?**
AORSV'20	$\geq 0.99n$	$\geq \ell^{0.01}$	$g - 1$	$\ell - 1$	No

Previous Works and Our Results

Input: (g, ℓ, n, k) oNOSF source Output: (g', ℓ', n') uniform oNOSF source

Work	**In** k	**In** n	**Out** g	**Out** ℓ	**Out online?**
AORSV'20	$\geq 0.99n$	$\geq \ell^{0.01}$	$g-1$	$\ell-1$	No
AORSV'20	$\geq 0.01n$	$\geq \ell^{0.01}$	$g-1$	100ℓ	No

Previous Works and Our Results

Input: (g, ℓ, n, k) oNOSF source Output: (g', ℓ', n') uniform oNOSF source

Work	**In** k	**In** n	**Out** g	**Out** ℓ	**Out online?**
AORSV'20	$\geq 0.99n$	$\geq \ell^{0.01}$	$g-1$	$\ell-1$	No
AORSV'20	$\geq 0.01n$	$\geq \ell^{0.01}$	$g-1$	100ℓ	No
CGR'24	$\geq \text{polylog}(n)$	$\geq \ell \cdot \text{polylog}(\ell)$	$g-1$	$\ell-1$	Yes

Previous Works and Our Results

Input: (g, ℓ, n, k) oNOSF source Output: (g', ℓ', n') uniform oNOSF source

Work	In k	In n	Out g	Out ℓ	Out online?
AORSV'20	$\geq 0.99n$	$\geq \ell^{0.01}$	$g-1$	$\ell-1$	No
AORSV'20	$\geq 0.01n$	$\geq \ell^{0.01}$	$g-1$	100ℓ	No
CGR'24	$\geq \mathrm{polylog}(n)$	$\geq \ell \cdot \mathrm{polylog}(\ell)$	$g-1$	$\ell-1$	Yes
Our Results	$\geq \mathrm{polylog}(n) + \log(\ell)$	$\geq \mathrm{polylog}(\ell)$	$g-o(\ell)$	$\ell-1$	Yes

Bonus: Extracting from oNOSF sources: Negative Results

Extracting from oNOSF sources: Negative Results

Extracting from oNOSF sources: Negative Results

AORSV'20

For $\boldsymbol{b = 0.01\ell}$ and $\boldsymbol{\varepsilon = 0.0002}$, impossible to extract from $(\ell - b, \ell, \boldsymbol{n})$-uniform oNOSF source with error $< \varepsilon$

Extracting from oNOSF sources: Negative Results

AORSV'20

For $\boldsymbol{b = 0.01\ell}$ and $\boldsymbol{\varepsilon = 0.0002}$, impossible to extract from $(\ell - b, \ell, \boldsymbol{n})$-uniform oNOSF source with error $< \varepsilon$

Our Results

For $\boldsymbol{b = 0.01\ell}$ and $\boldsymbol{\varepsilon = 0.0098}$ impossible to extract from $(\ell - b, \ell, \mathbf{1})$-uniform oNOSF source with error $< \varepsilon$

Extracting from oNOSF sources: Negative Techniques

Extracting from oNOSF sources: Negative Techniques

Goal: Given $f : \{0,1\}^\ell \to \{0,1\}$, corrupt $\mathbf{0.01\ell}$ variables to bias f with distance $\mathbf{0.0098}$

Extracting from oNOSF sources: Negative Techniques

Goal: Given $f : \{0,1\}^\ell \to \{0,1\}$, corrupt $\mathbf{0.01\ell}$ variables to bias f with distance $\mathbf{0.0098}$

For non-online setting

Extracting from oNOSF sources: Negative Techniques

Goal: Given $f : \{0,1\}^\ell \to \{0,1\}$, corrupt $\mathbf{0.01\ell}$ variables to bias f with distance $\mathbf{0.0098}$

For non-online setting

- Use notion of **influence** of variable for boolean function

Extracting from oNOSF sources: Negative Techniques

Goal: Given $f : \{0,1\}^\ell \rightarrow \{0,1\}$, corrupt $\mathbf{0.01\ell}$ variables to bias f with distance $\mathbf{0.0098}$

For non-online setting

- Use notion of **influence** of variable for boolean function
- Prove f has **highly influential** variable Kahn-Kalai-Linial'88

Extracting from oNOSF sources: Negative Techniques

Goal: Given $f : \{0,1\}^\ell \to \{0,1\}$, corrupt $\mathbf{0.01\ell}$ variables to bias f with distance $\mathbf{0.0098}$

For non-online setting

- Use notion of **influence** of variable for boolean function
- Prove f has **highly influential** variable Kahn-Kalai-Linial'88
- **Inductively** collect influential variables and make them 'bad'

Extracting from oNOSF sources: Negative Techniques

Goal: Given $f : \{0,1\}^\ell \to \{0,1\}$, corrupt $\mathbf{0.01\ell}$ variables to bias f with distance **0.0098**

For non-online setting

- Use notion of **influence** of variable for boolean function
- Prove f has **highly influential** variable Kahn-Kalai-Linial'88
- **Inductively** collect influential variables and make them 'bad'

Our Techniques for Online Setting

Extracting from oNOSF sources: Negative Techniques

Goal: Given $f : \{0,1\}^\ell \to \{0,1\}$, corrupt $\mathbf{0.01\ell}$ variables to bias f with distance **0.0098**

For non-online setting

- Use notion of **influence** of variable for boolean function
- Prove f has **highly influential** variable Kahn-Kalai-Linial'88
- **Inductively** collect influential variables and make them 'bad'

Our Techniques for Online Setting

- Introduce notion of **online influence** of variable for boolean function

Extracting from oNOSF sources: Negative Techniques

Goal: Given $f : \{0,1\}^{\ell} \to \{0,1\}$, corrupt $\mathbf{0.01\ell}$ variables to bias f with distance **0.0098**

For non-online setting

- Use notion of **influence** of variable for boolean function
- Prove f has **highly influential** variable Kahn-Kalai-Linial'88
- **Inductively** collect influential variables and make them 'bad'

Our Techniques for Online Setting

- Introduce notion of **online influence** of variable for boolean function
- Prove f has **highly influential** variable - Poincaré inequality

Extracting from oNOSF sources: Negative Techniques

Goal: Given $f : \{0,1\}^\ell \to \{0,1\}$, corrupt $\mathbf{0.01\ell}$ variables to bias f with distance **0.0098**

For non-online setting

- Use notion of **influence** of variable for boolean function
- Prove f has **highly influential** variable Kahn-Kalai-Linial'88
- **Inductively** collect influential variables and make them 'bad'

Our Techniques for Online Setting

- Introduce notion of **online influence** of variable for boolean function
- Prove f has **highly influential** variable - Poincaré inequality
- **Inductively** collect influential variables and make them 'bad'

Extracting from oNOSF sources: Negative Techniques

Goal: Given $f : \{0,1\}^{\ell} \to \{0,1\}$, corrupt $\mathbf{0.01\ell}$ variables to bias f with distance **0.0098**

For non-online setting

- Use notion of **influence** of variable for boolean function
- Prove f has **highly influential** variable Kahn-Kalai-Linial'88
- **Inductively** collect influential variables and make them 'bad'

Our Techniques for Online Setting

- Introduce notion of **online influence** of variable for boolean function
- Prove f has **highly influential** variable - Poincaré inequality
- **Inductively** collect influential variables and make them 'bad'

Construct tight example for online influence