Condensing and Extracting Against Online Adversaries

Eshan Chattopadhyay
Cornell University

Mohit Gurumukhani
Cornell University

Noam Ringach
Cornell University

Rocco Servedio
Columbia University

Part 0: Introduction

Randomness in computation

Randomness in computation

- Useful for randomized algorithms, cryptography, distributed computing protocols, machine learning, etc.

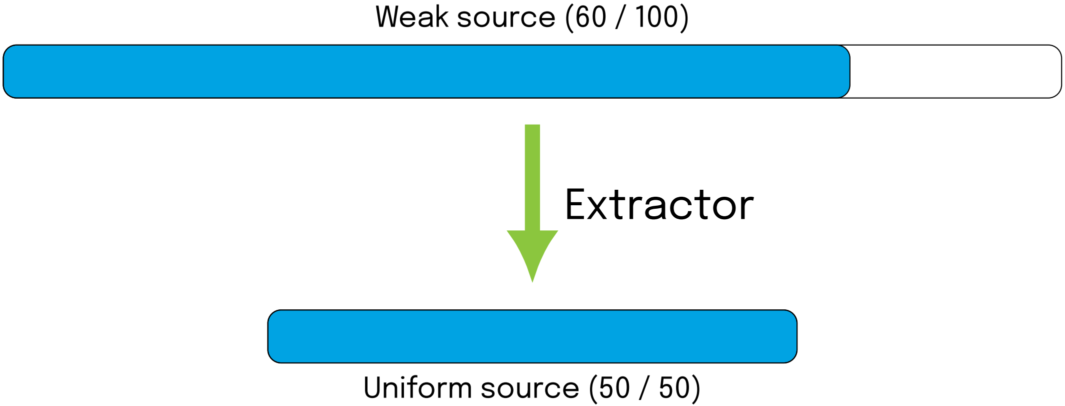
Randomness in computation

- Useful for randomized algorithms, cryptography, distributed computing protocols, machine learning, etc.
- Most applications need high quality randomness.

Randomness in computation

- Useful for randomized algorithms, cryptography, distributed computing protocols, machine learning, etc.
- Most applications need high quality randomness.
- In practice, randomness is derived from nature and is of low quality.

Extractor



Extractor

Definition (Extractor)

Ext : $\{0,1\}^n \to \{0,1\}^m$ is ε-extractor for class $\mathcal{X}$ if for all $\mathbf{X} \in \mathcal{X}$,

$$\left|\mathrm{Ext}(\mathbf{X}) - \textbf{Uniform}_m\right| \leq \varepsilon,$$

$|\cdot|$ denotes statistical distance / total variation distance:

$$|\mathbf{A} - \mathbf{B}| = \max_{S \subset \Omega} \left|\Pr\left(\mathbf{A} \in S\right) - \Pr\left(\mathbf{B} \in S\right)\right| = \frac{1}{2}\left\|\mathbf{A} - \mathbf{B}\right\|_1$$

Single extractor for every distribution?

Single extractor for every distribution?

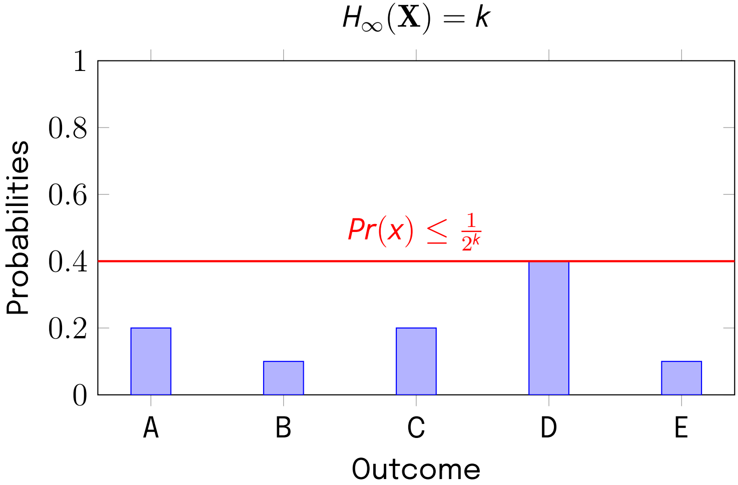
NO!

Single extractor for every distribution?

NO!

$\rightarrow$ **Distributions must have entropy**

Min-entropy


$H_\infty(\mathbf{X}) = k$
1
0.8
0.6
0.4
0.2
0
Probabilities
$Pr(x) \leq \frac{1}{2^k}$
A
B
C
D
E
Outcome

Min-entropy

Definition (Min-entropy)

Min-entropy of source $\mathbf{X}$:

$$H_\infty(\mathbf{X}) = -\log\left(\max_{x \in \mathsf{support}(\mathbf{X})} \Pr(\mathbf{X} = x)\right)$$

Min-entropy

Definition (Min-entropy)

Min-entropy of source $\mathbf{X}$:

$$H_\infty(\mathbf{X}) = -\log\left(\max_{x \in \mathsf{support}(\mathbf{X})} \Pr(\mathbf{X} = x)\right)$$

Definition (Smooth Min-entropy)

Smooth min-entropy of source $\mathbf{X}$ with parameter ε:

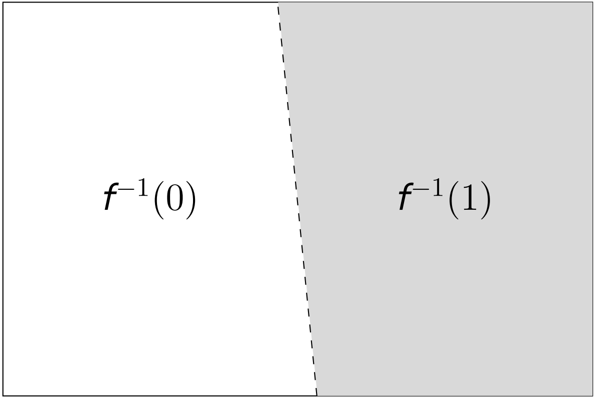
$$H_\infty^\varepsilon(\mathbf{X}) = \max_{\mathbf{Y}:|\mathbf{X}-\mathbf{Y}|\leq\varepsilon} H_\infty(\mathbf{Y})$$

Single extractor for every high min-entropy distribution?

Single extractor for every high min-entropy distribution?

NO!

Single extractor for every high min-entropy distribution?



Single extractor for every high min-entropy distribution?

NO!

Solution: Distributions are structured.

Seedless extractors: a brief history

Seedless extractors: a brief history

- Two independent sources [Chor – Goldreich'88, ..., Li'23].
- Sources generated by circuits / low complexity classes (applications to circuit lower bounds) [Trevisan – Vadhan'00, ..., Viola'14, ...].
- Sources sampled by polynomials over large fields [Dvir – Gabizon – Wigderson'09, ...].
- Sources sampled by polynomials over $\mathbb{F}_2$ [Chattopadhyay – Goodman – Gurumukhani (CGG)'24].

Sometimes extractors don’t exist

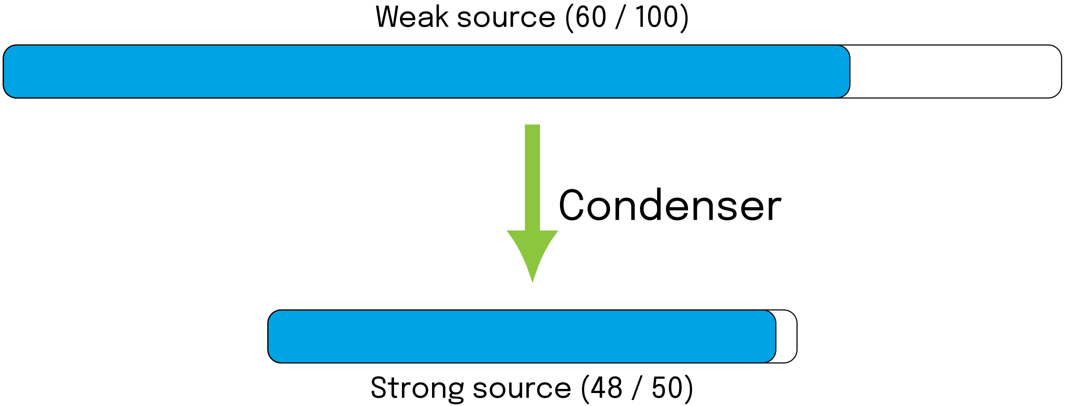
Sometimes extractors don’t exist

- Extractors guarantee closeness to uniform distribution.

Sometimes extractors don't exist

- Extractors guarantee closeness to uniform distribution.
- Relax this: guarantee closeness to high entropy distribution.

Condenser



Condenser

Condenser

Cond : $\{0,1\}^n \to \{0,1\}^m$ is a *$(k_{in}, k_{out}, \varepsilon)$-condenser* for class of distributions $\mathcal{X}$ with entropy at least k_{in} if for all $\mathbf{X} \in \mathcal{X}$,

$$H_\infty^\varepsilon(\text{Cond}(\mathbf{X})) \geq k_{out}$$

Condenser

Condenser

Cond : $\{0,1\}^n \to \{0,1\}^m$ is a *$(k_{in}, k_{out}, \varepsilon)$-condenser* for class of distributions $\mathcal{X}$ with entropy at least k_{in} if for all $\mathbf{X} \in \mathcal{X}$,

$$H_\infty^\varepsilon(\mathrm{Cond}(\mathbf{X})) \geq k_{out}$$

- Care about increasing **entropy rate**:

$$\frac{k_{in}}{n} \text{ vs } \frac{k_{out}}{m}$$

Condenser

Condenser

Cond : $\{0,1\}^n \to \{0,1\}^m$ is a $(k_{in}, k_{out}, \varepsilon)$-*condenser* for class of distributions $\mathcal{X}$ with entropy at least k_{in} if for all $\mathbf{X} \in \mathcal{X}$,

$$H_\infty^\varepsilon(\text{Cond}(\mathbf{X})) \geq k_{out}$$

- Care about increasing **entropy rate**:

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

Condenser

Condenser

Cond : $\{0,1\}^n \to \{0,1\}^m$ is a $(k_{in}, k_{out}, \varepsilon)$-*condenser* for class of distributions $\mathcal{X}$ with entropy at least k_{in} if for all $\mathbf{X} \in \mathcal{X}$,

$$H_\infty^\varepsilon(\text{Cond}(\mathbf{X})) \geq k_{out}$$

- Care about increasing **entropy rate**:

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

- Care about minimizing **entropy gap**:

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

Condensing is useful

Condensing is useful

Simulating using only weak random source:

Condensing is useful

Simulating using only weak random source:

- Randomized algorithms with $\mathrm{poly}(\Delta_{out})$ overhead [Zuckerman'95].

Condensing is useful

Simulating using only weak random source:

- Randomized algorithms with $\mathrm{poly}(\Delta_{out})$ overhead [Zuckerman'95].
- "One-shot simulations" for randomized protocols, cryptography, interactive proofs etc.

Condensing is useful

Simulating using only weak random source:

- Randomized algorithms with $\mathrm{poly}(\Delta_{out})$ overhead [Zuckerman'95].
- "One-shot simulations" for randomized protocols, cryptography, interactive proofs etc.

Condensers **can exist** where extractors (provably) **can't**

Single condenser for every high min-entropy distribution?

Single condenser for every high min-entropy distribution?

NO!

Single condenser for every high min-entropy distribution?

NO!

→ **Same solution: Distributions should be structured.**

Seedless condensers: prior work

Seedless condensers: prior work

- Condensers for Chor-Goldreich (CG) sources and adversarial Chor-Coldreich (CG) sources [Doron – Moshkovitz – Oh – Zuckerman'23].
- Improved Condensers for Chor-Goldreich Sources [Goodman – Li – Zuckerman'24]

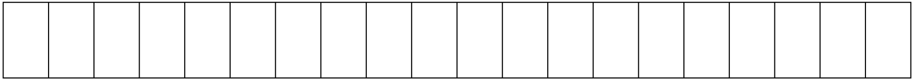
Part 1: Models and Results

OBFs

OBFs

Oblivious Bit Fixing Sources (OBFs)

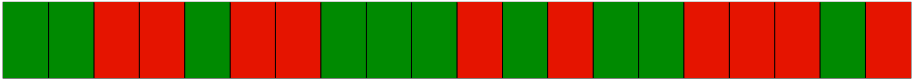
- ℓ bit input.



OBFs

Oblivious Bit Fixing Sources (OBFs)

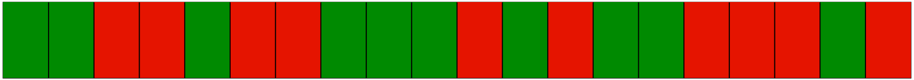
- ℓ bit input.
- g good bits: uniform, $\ell - g$ bad bits: constants.



OBFs

Oblivious Bit Fixing Sources (OBFs)

- ℓ bit input.
- g good bits: uniform, $\ell - g$ bad bits: constants.



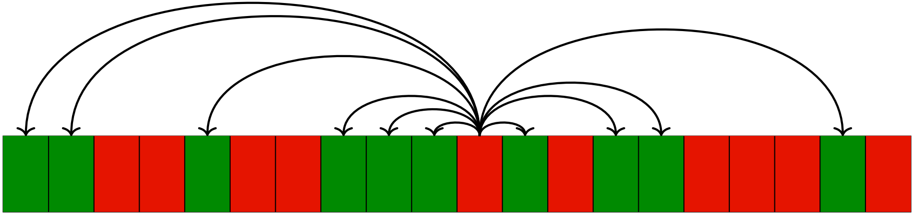
PARITY extracts from $(1, \ell)$-OBFs.

NOBFs

NOBFs

Non-Oblivious Bit Fixing Sources (NOBFs)

- g good bits: uniform, $\ell - g$ bad bits: arbitrary functions of good bits.



Extracting / Condensing from NOBFs

Extracting / Condensing from NOBFs

Kahn – Kalai – Linial'88, Ben-Or – Linial'89, Ajtai – Linial'93

- **Can't** extract from $\left(\ell - \frac{\ell}{\log(\ell)}, \ell\right)$-NOBFs.

Extracting / Condensing from NOBFs

Kahn – Kalai – Linial'88, Ben-Or – Linial'89, Ajtai – Linial'93

- **Can't** extract from $\left(\ell - \frac{\ell}{\log(\ell)}, \ell\right)$-NOBFs.
- **Can** extract from $\left(\ell - \frac{\ell}{\log^2(\ell)}, \ell\right)$-NOBFs.

Extracting / Condensing from NOBFs

Kahn – Kalai – Linial'88, Ben-Or – Linial'89, Ajtai – Linial'93

- **Can't** extract from $\left(\ell - \frac{\ell}{\log(\ell)}, \ell\right)$-NOBFs.
- **Can** extract from $\left(\ell - \frac{\ell}{\log^2(\ell)}, \ell\right)$-NOBFs.

Question

Can you condense from (g, ℓ)-NOBFs when $g < \ell - \frac{\ell}{\log \ell}$?

Extracting / Condensing from NOBFs

Kahn – Kalai – Linial'88, Ben-Or – Linial'89, Ajtai – Linial'93

- **Can't** extract from $\left(\ell - \frac{\ell}{\log(\ell)}, \ell\right)$-NOBFs.
- **Can** extract from $\left(\ell - \frac{\ell}{\log^2(\ell)}, \ell\right)$-NOBFs.

Theorem (Chattopadhyay – Gurumukhani – R (CGR)'24)

*For constant α, **can't** condense $((1-\alpha)\cdot\ell, \ell)$-NOBFs beyond **rate** $1-\alpha$.*

NOSFs

NOSFs

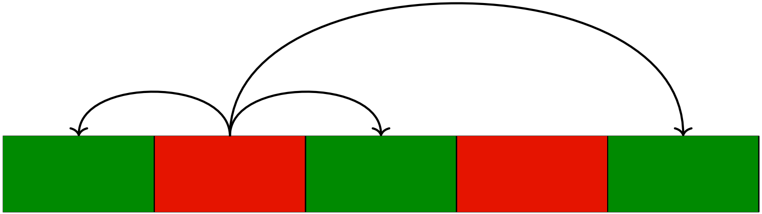
Non-Oblivious Symbol Fixing Sources (NOSFs)

- ℓ blocks of length n each.

NOSFs

Non-Oblivious Symbol Fixing Sources (NOSFs)

- ℓ blocks of length n each.
- g good blocks: uniform, $\ell - g$ bad blocks: arbitrary functions of good blocks.



Extracting / Condensing from NOSFs

Extracting / Condensing from NOSFs

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

Can’t extract from $(0.99\ell, \ell)$-NOSFs.

Extracting / Condensing from NOSFs

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

Can't extract from $(0.99\ell, \ell)$-NOSFs.

Question

Can you condense from (g, ℓ)-NOSFs?

Extracting / Condensing from NOSFs

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

Can't extract from $(0.99\ell, \ell)$-NOSFs.

Theorem (CGR'24)

Can't *condense* (g, ℓ)*-NOSFs beyond* ***rate*** $\boldsymbol{g/\ell}$**.**

oNOSFs

oNOSFs

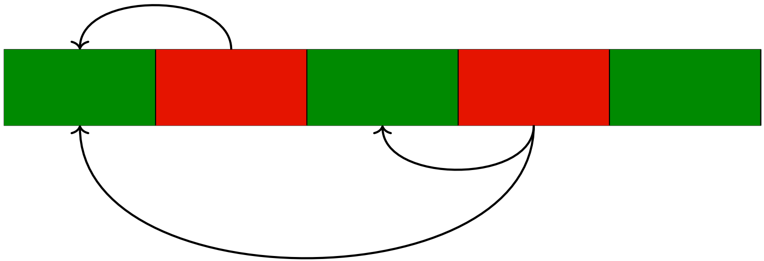
Online Non-Oblivious Symbol Fixing Sources (oNOSFs)

- g good blocks: uniform, $\ell - g$ bad blocks: arbitrary functions of good blocks **that appear before it**.

oNOSFs

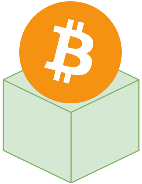
Online Non-Oblivious Symbol Fixing Sources (oNOSFs)

- g good blocks: uniform, $\ell - g$ bad blocks: arbitrary functions of good blocks **that appear before it**.

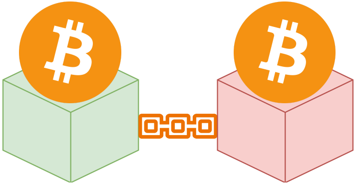


oNOSFs = Blockchain

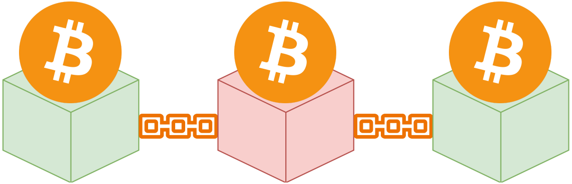
oNOSFs = Blockchain



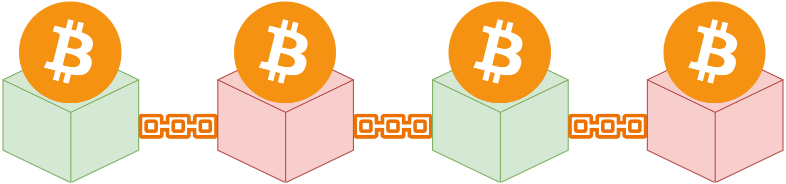
oNOSFs = Blockchain



oNOSFs = Blockchain

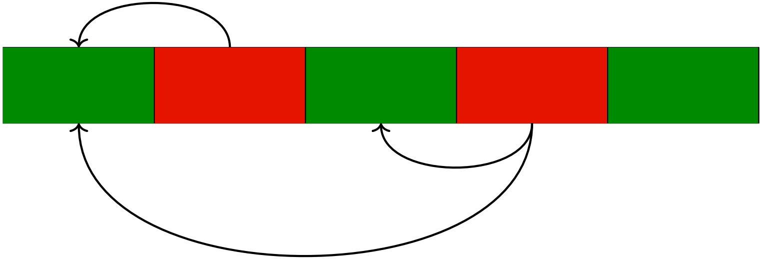


oNOSFs = Blockchain



oNOSFs = Blockchain

oNOSFs = Blockchain



Extracting / Condensing from oNOSFs

Extracting / Condensing from oNOSFs

[AORSV'20]

Can't extract from $(0.99\ell, \ell)$-oNOSFs.

Extracting / Condensing from oNOSFs

[AORSV'20]

Can't extract from $(0.99\ell, \ell)$-oNOSFs.

Question

Can you condense from (g, ℓ)-oNOSFs?

Extracting / Condensing from oNOSFs

[AORSV'20]

Can't extract from $(0.99\ell, \ell)$-oNOSFs.

Theorem (CGR'24, CGRS'25)

Can't *condense* (g, ℓ)*-oNOSFs beyond* ***rate*** $\boldsymbol{\frac{1}{\lfloor \ell / g \rfloor}}$**.**

Extracting / Condensing from oNOSFs

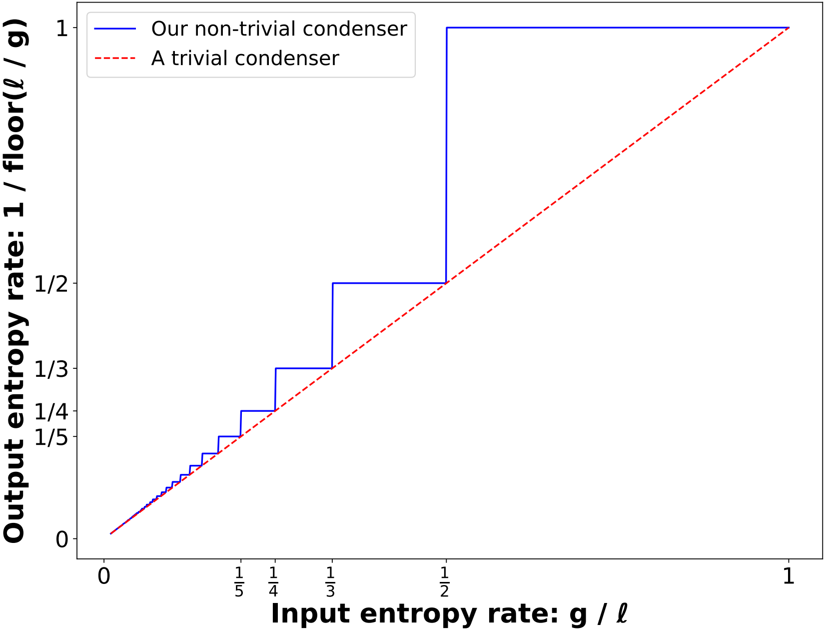
[AORSV'20]

Can't extract from $(0.99\ell, \ell)$-oNOSFs.

Theorem (CGR'24, CGRS'25)

Can't *condense* (g, ℓ)*-oNOSFs beyond* ***rate*** $\boldsymbol{\frac{1}{\lfloor \ell/g \rfloor}}$.

Can *condense* (g, ℓ)*-oNOSFs to* ***rate*** $\boldsymbol{\frac{1}{\lfloor \ell/g \rfloor}}$.


Our non-trivial condenser
A trivial condenser
Output entropy rate: 1 / floor(ℓ / g)
Input entropy rate: g / ℓ
1
1/2
1/3
1/4
1/5
0
0
$\frac{1}{5}$
$\frac{1}{4}$
$\frac{1}{3}$
$\frac{1}{2}$
1

Extracting / Condensing from oNOSFs

Corollary (Sharp threshold at $\boldsymbol{g} = \boldsymbol{\ell/2}$)

Can't *condense* $(0.5\ell, \ell)$*-oNOSFs beyond* ***rate*** $\mathbf{1/2}$ *- Impossibility.*
Can *condense* $(0.51\ell, \ell)$*-oNOSFs to* ***rate*** $\mathbf{0.99}$ *- Possibility.*

Part 2: Possibility

Condensers for (g, ℓ)-oNOSF sources

Theorem (Condensing uniform oNOSF sources)

For $g \geq 0.51\ell$, large constant block length n, and ℓ increasing, we can condense any oNOSF source to entropy rate 0.99.

Condensers for (g, ℓ)-oNOSF sources

Theorem (Condensing uniform oNOSF sources)

For $g \geq 0.51\ell$, $\ell = \Omega(\log(1/\varepsilon))$, *and* $n = 10^4$, *exists* $\mathsf{Cond} : \{0,1\}^{\ell n} \to \{0,1\}^m$ *s.t. for any* (g, ℓ)*-oNOSF* $\mathbf{X}$, $H_\infty^\varepsilon(\mathsf{Cond}(\mathbf{X})) \geq \mathbf{0.99}m$ *where* $m = \Omega(\ell + \log(1/\varepsilon))$.

Condensers for (g, ℓ)-oNOSF sources

Theorem (Condensing uniform oNOSF sources)

For $g \geq 0.51\ell$, $\ell = \Omega(\log(1/\varepsilon))$, and $n = 10^4$, exists Cond $: \{0,1\}^{\ell n} \to \{0,1\}^m$ *s.t. for any (g, ℓ)-oNOSF $\mathbf{X}$, $H_\infty^\varepsilon(\mathbf{Cond}(\mathbf{X})) \geq \mathbf{0.99}\boldsymbol{m}$ where $m = \Omega(\ell + \log(1/\varepsilon))$.*

Theorem (Condensing low-entropy oNOSF sources)

For $g \geq 0.51\ell$, we can similarly condense oNOSF sources with logarithmic min-entropy.

Condensers for (g, ℓ)-oNOSF sources

Theorem (Condensing uniform oNOSF sources)

For $g \geq 0.51\ell$, $\ell = \Omega(\log(1/\varepsilon))$, *and* $n = 10^4$, *exists* Cond : $\{0,1\}^{\ell n} \to \{0,1\}^m$ *s.t. for any* (g, ℓ)*-oNOSF* $\mathbf{X}$, $\boldsymbol{H_\infty^\varepsilon}(\textbf{Cond}(\mathbf{X})) \geq \boldsymbol{0.99m}$ *where* $m = \Omega(\ell + \log(1/\varepsilon))$.

Theorem (Condensing low-entropy oNOSF sources)

For $g \geq 0.51\ell$, $n = \mathrm{polylog}(\ell/\varepsilon)$ *exists* Cond : $(\{0,1\}^n)^\ell \to \{0,1\}^m$ *s.t. for any* ***low-entropy*** (g, ℓ)*-oNOSF* $\mathbf{X}$ *with* $k = \Omega(\log(\ell/\varepsilon))$, $\boldsymbol{H_\infty^\varepsilon}(\textbf{Cond}(\mathbf{X})) \geq \boldsymbol{m - O(m/\log m) - O(\log(1/\varepsilon))}$ *where* $m = \Omega(k)$.

Condensers for (g,ℓ)-oNOSF sources

Theorem (Condensing uniform oNOSF sources)

For $g \geq 0.51\ell$, $\ell = \Omega(\log(1/\varepsilon))$, *and* $n = 10^4$, *exists* Cond : $\{0,1\}^{\ell n} \to \{0,1\}^m$ *s.t. for any* (g,ℓ)*-oNOSF* $\mathbf{X}$, $H_\infty^\varepsilon(\mathbf{Cond}(\mathbf{X})) \geq \mathbf{0.99}m$ *where* $m = \Omega(\ell + \log(1/\varepsilon))$.

Theorem (Condensing low-entropy oNOSF sources)

For $g \geq 0.51\ell$, $n = \mathrm{polylog}(\ell/\varepsilon)$ *exists* Cond : $(\{0,1\}^n)^\ell \to \{0,1\}^m$ *s.t. for any* ***low-entropy*** (g,ℓ)*-oNOSF* $\mathbf{X}$ *with* $k = \Omega(\log(\ell/\varepsilon))$, $H_\infty^\varepsilon(\mathbf{Cond}(\mathbf{X})) \geq m - O(m/\log m) - O(\log(1/\varepsilon))$ *where* $m = \Omega(k)$.

Theorem (Extend AORSV'20 result)

Transform low-entropy (g,ℓ)*-oNOSFs* $\to$ *uniform* $(0.99g,\ell)$*-oNOSFs.*

Condensers for (g, ℓ)-oNOSF sources

Theorem (Condensing uniform oNOSF sources)

For $g \geq 0.51\ell$, $\ell = \Omega(\log(1/\varepsilon))$, *and* $n = 10^4$, *exists* $\mathsf{Cond} : \{0,1\}^{\ell n} \to \{0,1\}^m$ *s.t. for any* (g, ℓ)*-oNOSF* $\mathbf{X}$, $\boldsymbol{H}_\infty^{\varepsilon}(\mathbf{Cond}(\mathbf{X})) \geq \mathbf{0.99}\boldsymbol{m}$ *where* $m = \Omega(\ell + \log(1/\varepsilon))$.

Does a random function work?

Condensers for (g, ℓ)-oNOSF sources

Theorem (Condensing uniform oNOSF sources)

For $g \geq 0.51\ell$, $\ell = \Omega(\log(1/\varepsilon))$, and $n = 10^4$, exists Cond : $\{0,1\}^{\ell n} \to \{0,1\}^m$ *s.t. for any (g, ℓ)-oNOSF $\mathbf{X}$, $H_\infty^\varepsilon(\mathbf{Cond}(\mathbf{X})) \geq \mathbf{0.99}\boldsymbol{m}$ where $m = \Omega(\ell + \log(1/\varepsilon))$.*

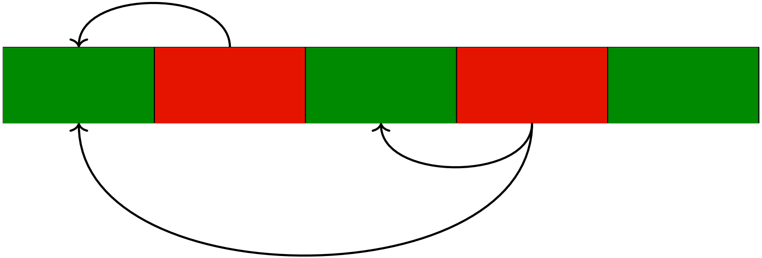
Does a random function work?

No!

Condensers for (g, ℓ)-oNOSF sources

Theorem (Condensing uniform oNOSF sources)

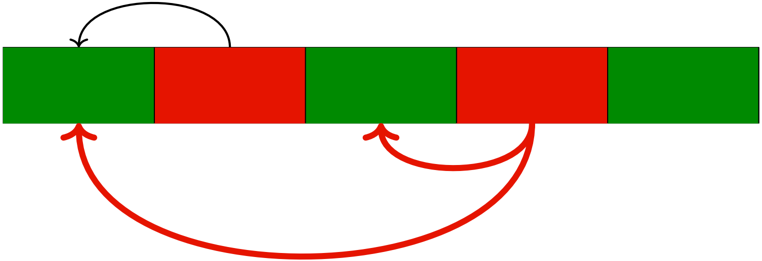
For $g \geq 0.51\ell$*,* $\ell = \Omega(\log(1/\varepsilon))$*, and* $n = 10^4$*, exists* Cond : $\{0,1\}^{\ell n} \to \{0,1\}^m$ *s.t. for any* (g, ℓ)*-oNOSF* $\mathbf{X}$*,* $\boldsymbol{H_\infty^\varepsilon}(\mathbf{Cond}(\mathbf{X})) \geq \mathbf{0.99}\boldsymbol{m}$ *where* $m = \Omega(\ell + \log(1/\varepsilon))$.



Condensers for (g, ℓ)-oNOSF sources

Theorem (Condensing uniform oNOSF sources)

For $g \geq 0.51\ell$, $\ell = \Omega(\log(1/\varepsilon))$, *and* $n = 10^4$, *exists* Cond : $\{0,1\}^{\ell n} \to \{0,1\}^m$ *s.t. for any* (g, ℓ)*-oNOSF* $\mathbf{X}$, $H_\infty^\varepsilon(\mathbf{Cond}(\mathbf{X})) \geq \mathbf{0.99}m$ *where* $m = \Omega(\ell + \log(1/\varepsilon))$.



Constructing the condenser

Problem

A random function doesn't condense because the adversary has too much power in latter blocks.

$$\boxed{\mathbf{X}_1 \mid \quad \cdots \quad \mid \mathbf{X}_{\ell/2}} \qquad \boxed{\mathbf{X}_{\ell/2+1} \mid \quad \cdots \quad \mid \mathbf{X}_{\ell}}$$

Constructing the condenser

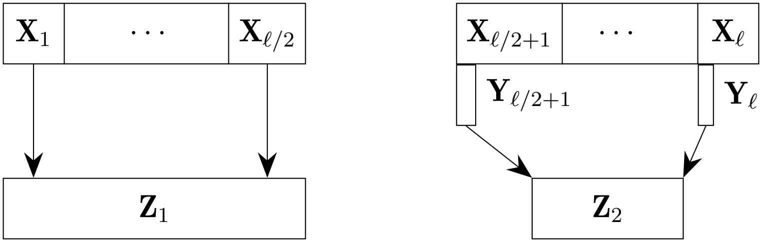
Solution

Take only first bit of latter half of blocks to weaken the adversary.

Constructing the condenser

Solution

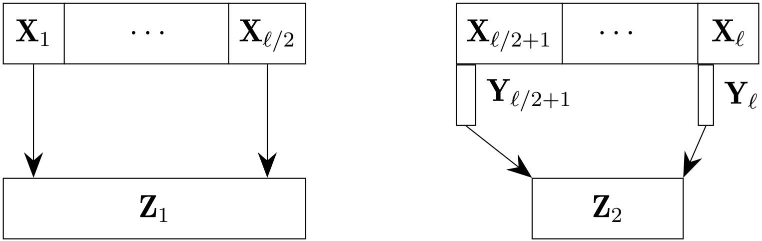
Take only first bit of latter half of blocks to weaken the adversary.



Constructing the condenser

Solution

Take only first bit of latter half of blocks to weaken the adversary.

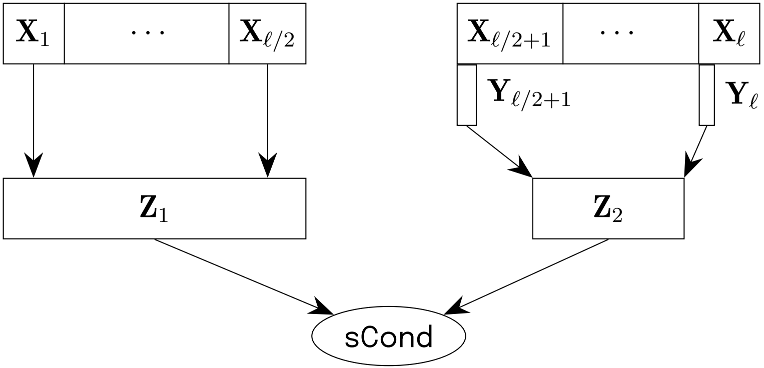


Now a random function works!

Constructing the condenser

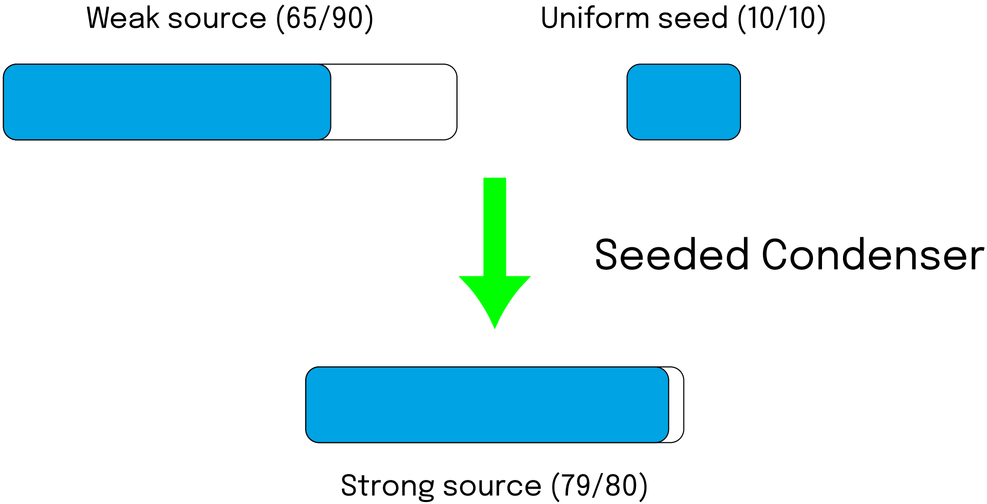
Solution

Take only first bit of latter half of blocks to weaken the adversary.



Seeded Condensers

Seeded Condensers



Seeded Condensers

Formal definition

A function sCond : $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a *(k, ε)-seeded condenser* for a class of sources $\mathcal{X}$ if for all $\mathbf{X} \in \mathcal{X}$,

$$H_\infty^\varepsilon(\mathrm{sCond}(\mathbf{X}, \mathbf{U}_d)) \geq k$$

Seeded Condensers

Formal definition

A function sCond : $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a *(k,ε)-seeded condenser* for a class of sources $\mathcal{X}$ if for all $\mathbf{X} \in \mathcal{X}$,

$$H_\infty^\varepsilon(\mathsf{sCond}(\mathbf{X}, \mathbf{U}_d)) \geq k$$

Theorem (Good seeded condensers exist)

Seeded condensers with logarithmic seed length and linear output length exist.

Seeded Condensers

Formal definition

A function $\mathsf{sCond} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a *(k, ε)-seeded condenser* for a class of sources $\mathcal{X}$ if for all $\mathbf{X} \in \mathcal{X}$,

$$H_\infty^\varepsilon(\mathsf{sCond}(\mathbf{X}, \mathbf{U}_d)) \geq k$$

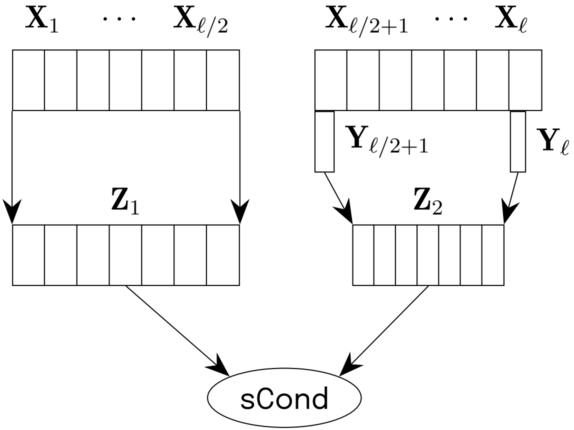
Theorem (Good seeded condensers exist)

For all d, ε s.t. $d \geq \log(\ell n/\varepsilon) + O(1)$ and $m = 0.01\ell n + d + \log(1/\varepsilon) + O(1)$, exists $\mathsf{sCond} : \{0,1\}^{\ell n/2} \times \{0,1\}^d \to \{0,1\}^m$ s.t. for all $\mathbf{X} \sim \{0,1\}^{\ell n/2}$ with $H_\infty(\mathbf{X}) \geq 0.01\ell n$, we have

$$H_\infty^\varepsilon(\mathsf{sCond}(\mathbf{X}, \mathbf{U}_d)) \geq 0.01\ell n + d$$

Correctness of the Condenser

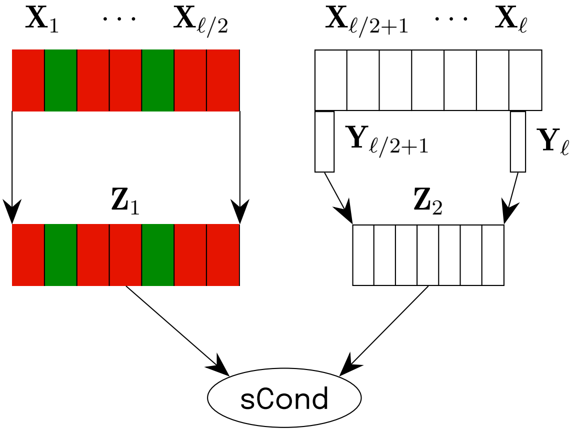
Proof.



Correctness of the Condenser

Proof.

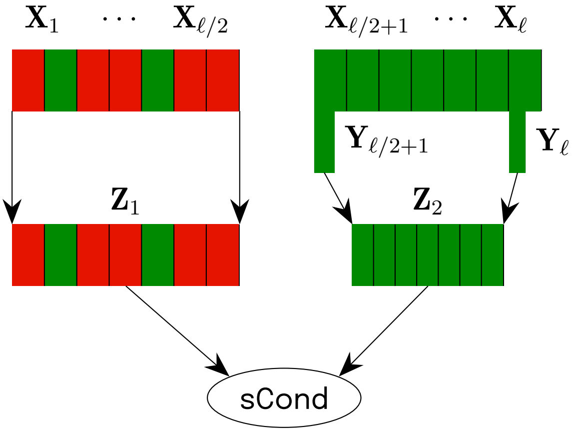
- $g \geq 0.51\ell \implies$ at least 0.01ℓ blocks in $\mathbf{Z}_1 \sim \{0,1\}^{\ell n/2}$ are good.



Correctness of the Condenser

Proof.

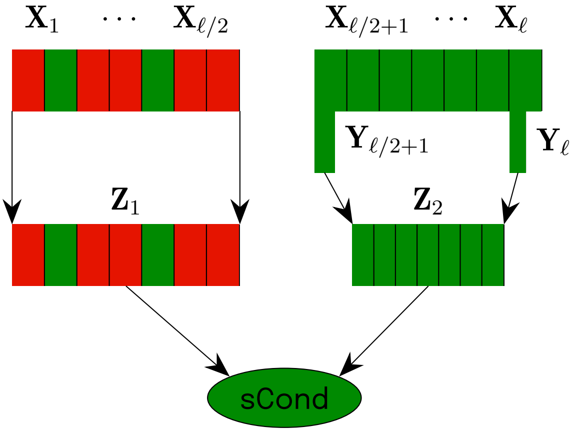
- $g \geq 0.51\ell \implies$ at least 0.01ℓ blocks in $\mathbf{Z}_1 \sim \{0,1\}^{\ell n/2}$ are good.
- Pretend $\mathbf{Z}_2 \sim \{0,1\}^{\ell/2}$ is uniform.



Correctness of the Condenser

Proof.

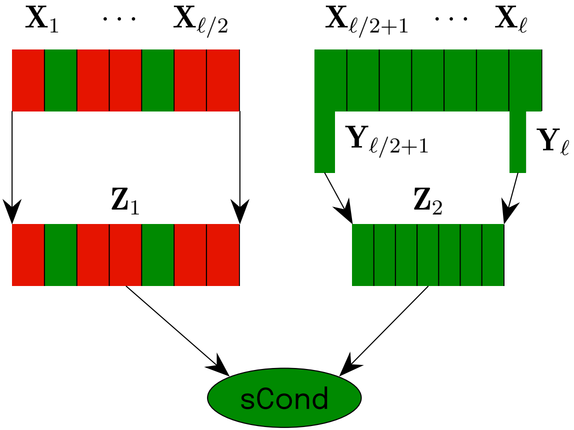
- $g \geq 0.51\ell \implies$ at least 0.01ℓ blocks in $\mathbf{Z}_1 \sim \{0,1\}^{\ell n/2}$ are good.
- Pretend $\mathbf{Z}_2 \sim \{0,1\}^{\ell/2}$ is uniform.
- sCond requirements satisfied!



Correctness of the Condenser

Proof.

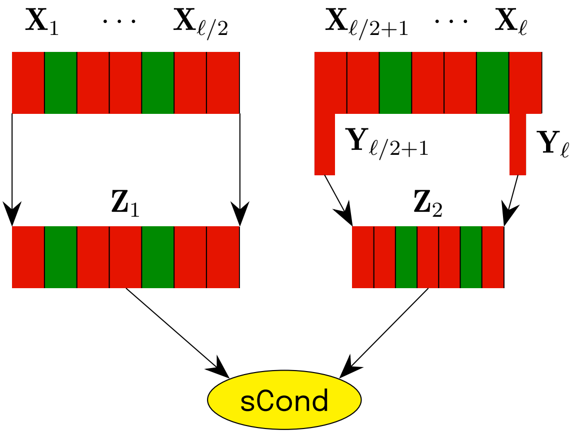
- $g \geq 0.51\ell \implies$ at least 0.01ℓ blocks in $\mathbf{Z}_1 \sim \{0,1\}^{\ell n/2}$ are good.
- Pretend $\mathbf{Z}_2 \sim \{0,1\}^{\ell/2}$ is uniform.
- sCond requirements satisfied!
- $H_\infty^{\varepsilon_{\mathsf{sCond}}}(\mathsf{sCond}(\mathbf{Z}_1, \mathbf{U}_{\ell/2})) \geq k_{\mathsf{sCond}}$.



Correctness of the Condenser

Proof.

- $g \geq 0.51\ell \implies$ at least 0.01ℓ blocks in $\mathbf{Z}_1 \sim \{0,1\}^{\ell n/2}$ are good.
- Pretend $\mathbf{Z}_2 \sim \{0,1\}^{\ell/2}$ is uniform.
- sCond requirements satisfied!
- $H_\infty^{\varepsilon_{\mathsf{sCond}}}(\mathsf{sCond}(\mathbf{Z}_1, \mathbf{U}_{\ell/2})) \geq k_{\mathsf{sCond}}$.
- BUT $\mathbf{Z}_2$ might have 0.49ℓ bad bits!



Adversary can’t make things too bad

Adversary can't make things too bad

Lemma

Let $\mathbf{X} \sim \{0,1\}^n$ *and* sCond *be s.t.* $H_\infty^{\varepsilon_{\mathsf{sCond}}}(\mathsf{sCond}(\mathbf{X}, \mathbf{U}_d)) \geq k_{\mathsf{sCond}}$.
Let $\mathbf{U}'_d$ *be* $\mathbf{U}_d$ *except an adversary controls some b bits. Then,*

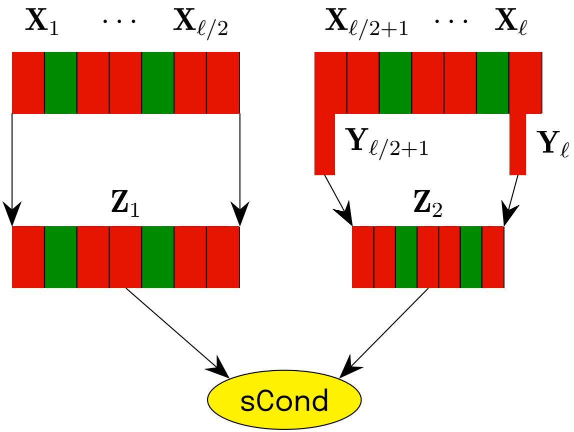
$$H_\infty^{\varepsilon'}(\mathsf{sCond}(\mathbf{X}, \mathbf{U}'_d)) \geq k_{\mathsf{sCond}} - b$$

where $\varepsilon' = \varepsilon_{\mathsf{sCond}} \cdot 2^b$.

Correctness of the Condenser

Proof.

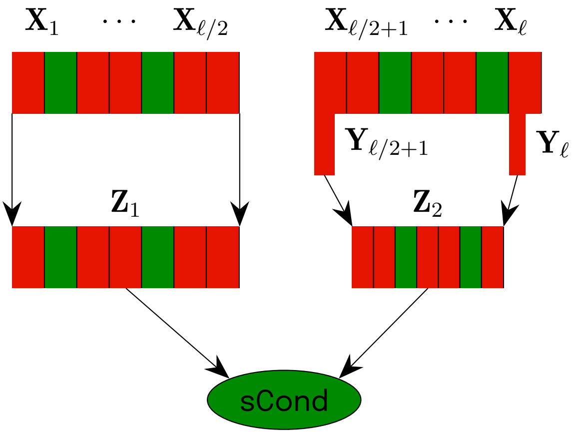
- $g \geq 0.51\ell \implies$ at least 0.01ℓ blocks in $\mathbf{Z}_1 \sim \{0,1\}^{\ell n/2}$ are good.
- Pretend $\mathbf{Z}_2 \sim \{0,1\}^{\ell/2}$ is uniform.
- sCond requirements satisfied!
- $H_\infty^{\varepsilon_{\mathsf{sCond}}}(\mathsf{sCond}(\mathbf{Z}_1, \mathbf{U}_{\ell/2})) \geq k_{\mathsf{sCond}}$.
- BUT $\mathbf{Z}_2$ might have 0.49ℓ bad bits!



Correctness of the Condenser

Proof.

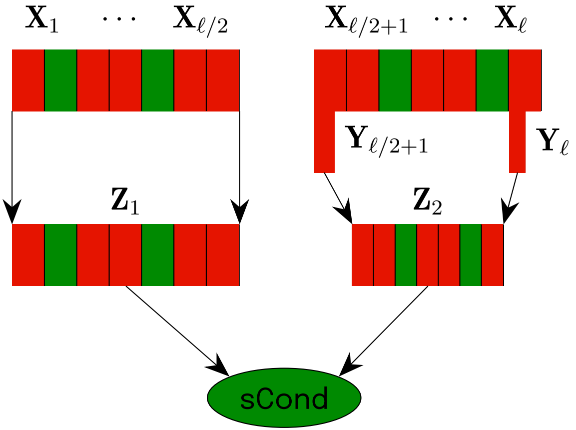
- $g \geq 0.51\ell \implies$ at least 0.01ℓ blocks in $\mathbf{Z}_1 \sim \{0,1\}^{\ell n/2}$ are good.
- Pretend $\mathbf{Z}_2 \sim \{0,1\}^{\ell/2}$ is uniform.
- sCond requirements satisfied!
- $H_\infty^{\varepsilon_{\mathsf{sCond}}}(\mathsf{sCond}(\mathbf{Z}_1, \mathbf{U}_{\ell/2})) \geq k_{\mathsf{sCond}}$.
- BUT $\mathbf{Z}_2$ might have 0.49ℓ bad bits!
- Save sCond using lemma that adversary can't be too bad.



Correctness of the Condenser

Proof.

- $g \geq 0.51\ell \implies$ at least 0.01ℓ blocks in $\mathbf{Z}_1 \sim \{0,1\}^{\ell n/2}$ are good.
- Pretend $\mathbf{Z}_2 \sim \{0,1\}^{\ell/2}$ is uniform.
- sCond requirements satisfied!
- $H_\infty^{\varepsilon_{\mathsf{sCond}}}(\mathsf{sCond}(\mathbf{Z}_1, \mathbf{U}_{\ell/2})) \geq k_{\mathsf{sCond}}$.
- BUT $\mathbf{Z}_2$ might have 0.49ℓ bad bits!
- Save sCond using lemma that adversary can't be too bad.
- $H_\infty^{\varepsilon'}(\mathsf{sCond}(\mathbf{Z}_1, \mathbf{Z}_2)) \geq k_{\mathsf{sCond}} - 0.49\ell$ with $\varepsilon' = \varepsilon_{\mathsf{sCond}} \cdot 2^{0.49\ell}$.



Correctness of the Condenser

Proof.

- $g \geq 0.51\ell \implies$ at least 0.01ℓ blocks in $\mathbf{Z}_1 \sim \{0,1\}^{\ell n/2}$ are good.
- Pretend $\mathbf{Z}_2 \sim \{0,1\}^{\ell/2}$ is uniform.
- sCond requirements satisfied!
- $H_\infty^{\varepsilon_{\mathsf{sCond}}}(\mathsf{sCond}(\mathbf{Z}_1, \mathbf{U}_{\ell/2})) \geq k_{\mathsf{sCond}}$.
- BUT $\mathbf{Z}_2$ might have 0.49ℓ bad bits!
- Save sCond using lemma that adversary can't be too bad.
- $H_\infty^{\varepsilon'}(\mathsf{sCond}(\mathbf{Z}_1, \mathbf{Z}_2) \geq k_{\mathsf{sCond}} - 0.49\ell$ with $\varepsilon' = \varepsilon_{\mathsf{sCond}} \cdot 2^{0.49\ell}$.

Proof.

- To get error ε, need $\varepsilon_{\mathsf{sCond}} = \varepsilon \cdot 2^{-0.49\ell}$.

Correctness of the Condenser

Proof.

- $g \geq 0.51\ell \implies$ at least 0.01ℓ blocks in $\mathbf{Z}_1 \sim \{0,1\}^{\ell n/2}$ are good.
- Pretend $\mathbf{Z}_2 \sim \{0,1\}^{\ell/2}$ is uniform.
- sCond requirements satisfied!
- $H_\infty^{\varepsilon_{\mathsf{sCond}}}(\mathsf{sCond}(\mathbf{Z}_1, \mathbf{U}_{\ell/2})) \geq k_{\mathsf{sCond}}$.
- BUT $\mathbf{Z}_2$ might have 0.49ℓ bad bits!
- Save sCond using lemma that adversary can't be too bad.
- $H_\infty^{\varepsilon'}(\mathsf{sCond}(\mathbf{Z}_1, \mathbf{Z}_2)) \geq k_{\mathsf{sCond}} - 0.49\ell$ with $\varepsilon' = \varepsilon_{\mathsf{sCond}} \cdot 2^{0.49\ell}$.

Proof.

- To get error ε, need $\varepsilon_{\mathsf{sCond}} = \varepsilon \cdot 2^{-0.49\ell}$.
- For sCond to exist, need $0.5\ell \geq \log(\ell n/\varepsilon_{\mathsf{sCond}}) + O(1)$

Correctness of the Condenser

Proof.

- $g \geq 0.51\ell \implies$ at least 0.01ℓ blocks in $\mathbf{Z}_1 \sim \{0,1\}^{\ell n/2}$ are good.
- Pretend $\mathbf{Z}_2 \sim \{0,1\}^{\ell/2}$ is uniform.
- sCond requirements satisfied!
- $H_\infty^{\varepsilon_{\mathsf{sCond}}}(\mathsf{sCond}(\mathbf{Z}_1, \mathbf{U}_{\ell/2})) \geq k_{\mathsf{sCond}}$.
- BUT $\mathbf{Z}_2$ might have 0.49ℓ bad bits!
- Save sCond using lemma that adversary can't be too bad.
- $H_\infty^{\varepsilon'}(\mathsf{sCond}(\mathbf{Z}_1, \mathbf{Z}_2)) \geq k_{\mathsf{sCond}} - 0.49\ell$ with $\varepsilon' = \varepsilon_{\mathsf{sCond}} \cdot 2^{0.49\ell}$.

Proof.

- To get error ε, need $\varepsilon_{\mathsf{sCond}} = \varepsilon \cdot 2^{-0.49\ell}$.
- For sCond to exist, need $0.5\ell \geq \log(\ell n/\varepsilon_{\mathsf{sCond}}) + O(1)$
- So require $\varepsilon \geq 2^{-0.01\ell}$.

Correctness of the Condenser

Proof.

- $g \geq 0.51\ell \implies$ at least 0.01ℓ blocks in $\mathbf{Z}_1 \sim \{0,1\}^{\ell n/2}$ are good.
- Pretend $\mathbf{Z}_2 \sim \{0,1\}^{\ell/2}$ is uniform.
- sCond requirements satisfied!
- $H_\infty^{\varepsilon_{\text{sCond}}}(\text{sCond}(\mathbf{Z}_1, \mathbf{U}_{\ell/2})) \geq k_{\text{sCond}}$.
- BUT $\mathbf{Z}_2$ might have 0.49ℓ bad bits!
- Save sCond using lemma that adversary can't be too bad.
- $H_\infty^{\varepsilon'}(\text{sCond}(\mathbf{Z}_1, \mathbf{Z}_2)) \geq k_{\text{sCond}} - 0.49\ell$ with $\varepsilon' = \varepsilon_{\text{sCond}} \cdot 2^{0.49\ell}$.

Proof.

- To get error ε, need $\varepsilon_{\text{sCond}} = \varepsilon \cdot 2^{-0.49\ell}$.
- For sCond to exist, need $0.5\ell \geq \log(\ell n/\varepsilon_{\text{sCond}}) + O(1)$
- So require $\varepsilon \geq 2^{-0.01\ell}$.
- sCond outputs $m = 0.01\ell n + O(1)$ bits with entropy $m - O(\ell)$.

Correctness of the Condenser

Proof.

- $g \geq 0.51\ell \implies$ at least 0.01ℓ blocks in $\mathbf{Z}_1 \sim \{0,1\}^{\ell n/2}$ are good.
- Pretend $\mathbf{Z}_2 \sim \{0,1\}^{\ell/2}$ is uniform.
- sCond requirements satisfied!
- $H_\infty^{\varepsilon_{\text{sCond}}}(\text{sCond}(\mathbf{Z}_1, \mathbf{U}_{\ell/2})) \geq k_{\text{sCond}}$.
- BUT $\mathbf{Z}_2$ might have 0.49ℓ bad bits!
- Save sCond using lemma that adversary can't be too bad.
- $H_\infty^{\varepsilon'}(\text{sCond}(\mathbf{Z}_1, \mathbf{Z}_2)) \geq k_{\text{sCond}} - 0.49\ell$ with $\varepsilon' = \varepsilon_{\text{sCond}} \cdot 2^{0.49\ell}$.

Proof.

- To get error ε, need $\varepsilon_{\text{sCond}} = \varepsilon \cdot 2^{-0.49\ell}$.
- For sCond to exist, need $0.5\ell \geq \log(\ell n/\varepsilon_{\text{sCond}}) + O(1)$
- So require $\varepsilon \geq 2^{-0.01\ell}$.
- sCond outputs $m = 0.01\ell n + O(1)$ bits with entropy $m - O(\ell)$.
- So for large const n, get entropy rate $\frac{m-O(\ell)}{m} \geq 0.99$.

Condensing from oNOSFs

Corollary (Sharp threshold at $\boldsymbol{g} = \boldsymbol{\ell/2}$)

Can't *condense* $(\ell/2, \ell)$*-oNOSFs beyond* ***rate*** $\mathbf{1/2}$ *- Impossibility.*
Can *condense* $(0.51\ell, \ell)$*-oNOSFs to* ***rate*** $\mathbf{0.99}$ *- Possibility.* $\checkmark$

Part 3: Future Directions

Open questions

Open questions

Open questions

- Explicit condensers for oNOSFs with constant block length?

Open questions

- Explicit condensers for oNOSFs with constant block length?
- Our condensers (explicit and existential) have super-constant output entropy gap . Is constant possible (for any values of ℓ and n)?

Open questions

- Explicit condensers for oNOSFs with constant block length?
- Our condensers (explicit and existential) have super-constant output entropy gap . Is constant possible (for any values of ℓ and n)?
- Construct condensers for oNOBFs (online NOBFs).

Open questions

- Explicit condensers for oNOSFs with constant block length?
- Our condensers (explicit and existential) have super-constant output entropy gap . Is constant possible (for any values of ℓ and n)?
- Construct condensers for oNOBFs (online NOBFs).