On the Existence of Seedless Condensers: Exploring the Terrain

Eshan Chattopadhyay
Cornell University
Ithaca, USA
eshan@cs.cornell.edu

Mohit Gurumukhani
Cornell University
Ithaca, USA
mgurumuk@cs.cornell.edu

Noam Ringach
Cornell University
Ithaca, USA
nomir@cs.cornell.edu

***Abstract*—While the existence of randomness extractors, both seeded and seedless, has been studied for many sources of randomness, currently, not much is known regarding the existence of seedless condensers in many settings. Here, we prove several new results for seedless condensers in the context of three related classes of sources: Non-Oblivious Symbol Fixing (NOSF) sources, online NOSF (oNOSF) sources (originally defined as SHELA sources in [1]), and almost Chor-Goldreich (CG) sources as defined in [2]. We will think of these sources as a sequence of random variables $\mathbf{X} = \mathbf{X}_1, \ldots, \mathbf{X}_\ell$ on ℓ symbols where at least g out of these ℓ symbols are "good" (i.e., have some min-entropy requirement), denoted as a (g, ℓ)-source, and the remaining "bad" $\ell - g$ symbols may adversarially depend on these g good blocks. The difference between each of these sources is realized by restrictions on the power of the adversary, with the adversary in NOSF sources having no restrictions.**

Prior to our work, the only known seedless condenser upper or lower bound in these settings is due to [2], where they explicitly construct a seedless condenser for a restricted subset of (g, ℓ)-adversarial CG sources.

The following are our main results concerning seedless condensers for each of these sources.

1) **oNOSF sources**
   a) **When $g \leq \ell/2$, we prove that condensing with error 0.99 above rate $\frac{1}{\lfloor \ell/g \rfloor}$ is impossible. In fact, we show that this is tight.**
   b) **Quite surprisingly, for $g > \ell/2$, we show the existence of excellent condensers for uniform oNOSF sources. In addition, we show the existence of similar condensers for oNOSF sources with only logarithmic min-entropy. Our results are based on a new type of two-source extractors, called *output-light two-source extractors*, that we introduce and prove the existence of.**
2) **Adversarial CG sources**
   a) **We observe that uniform adversarial CG sources are equivalent to uniform oNOSF sources and consequently inherit the same results.**
   b) **We show that one cannot condense beyond the min-entropy gap of each block or condense low min-entropy CG sources above rate $1/2$.**
3) **NOSF sources**
   a) **We show that condensing with constant error above rate $\frac{g}{\ell}$ is impossible for uniform NOSF sources for any g and ℓ, thus ruling out the possibility of any non-trivial condensing. This shows an interesting distinction between NOSF and oNOSF sources.**

E.C. and M.G. supported by an NSF CAREER Award 2045576 and a Sloan Research Fellowship. N.R. supported by NSF GRFP grant DGE – 2139899, NSF CAREER Award 2045576 and a Sloan Research Fellowship.

***Index Terms*—pseudorandomness, condensers, adversarial sources, non-oblivious symbol fixing sources, Chor-Goldreich sources**

I. Introduction

One of the most fruitful lines of research in computer science has been that of randomness. From the traditionally more applied areas of algorithm design (e.g., Monte Carlo simulations), error-correcting codes and cryptography to the more theoretical areas of property testing, combinatorics, and circuit lower bounds, randomness has played a key role in seminal discoveries. In many of these works, the use of high-quality random bits, or alternatively, a way to convert low-quality randomness into high-quality randomness, is essential. In cryptography, the authors of [3] showed that high-quality randomness is essential for tasks such as bit commitment schemes and secure two-party computation. On the other hand, being able to extract uniform bits from low-quality randomness allows us to simulate randomized algorithms [4].

In most use-cases, randomness takes the form of uniformly random bits. These motivated the construction of randomness extractors,[1] functions that take low-quality randomness (which we often like to think of as natural processes) and convert it into uniformly random bits. It is impossible to extract from the class of all sources and so extractors are constructed with respect to a restricted class of sources.

A number of works [4]–[7] have shown that deterministic extraction is impossible for many natural classes of randomness sources. The question that arises for such sources then is whether any improvement to their randomness can be made. That is, while it may not be possible to convert a source into uniform bits, maybe it is possible to condense a source into another source with a higher density of randomness. The central focus of our paper is in understanding the possibility of condensing for various natural models of weak sources where it is known that extraction is impossible.

We first introduce the way that we measure randomness and the notions of extractors and condensers. The notion of randomness that is standard in this line of work is that of min-entropy. For a source $\mathbf{X}$ on n bits, we define its *min-entropy* as $H_\infty(\mathbf{X}) = \min_{x \in \{0,1\}^n} \{-\log(\Pr[\mathbf{X} =$

[1] In this paper, when we mention extractors/condensers, we usually mean seedless extractors/condensers.

2575-8454/24/$31.00 ©2024 IEEE
DOI 10.1109/FOCS61266.2024.00093

$x])\}$. A source $\mathbf{X}$ over n bits with min-entropy at least k is called an (n,k)-*source*. Given any two distributions $\mathbf{X}$ and $\mathbf{Y}$ on $\{0,1\}^n$, we define their statistical distance or total-variation (TV) distance as $|\mathbf{X}-\mathbf{Y}| = \max_{Z\subseteq\{0,1\}^n} |\Pr_{x\sim\mathbf{X}}[x\in Z] - \Pr_{y\sim\mathbf{Y}}[y\in Z]|$. We also need the notion of *smooth min-entropy*: for a source $\mathbf{X}$ on $\{0,1\}^n$, it=s smooth min-entropy with smoothness parameter ε is $H^{\varepsilon}_{\infty}(\mathbf{X}) = \max_{\mathbf{Y}:|\mathbf{X}-\mathbf{Y}|\leq\varepsilon} H_{\infty}(\mathbf{Y})$. Conceptually, smooth min-entropy asks that the source we are looking at be ε-close in TV-distance to some other source with the desired amount of min-entropy. We are now in a position to define randomness extraction and condensing.

Definition I.1. *Let $\mathcal{X}$ be a family of distributions over $\{0,1\}^n$. A function $\mathsf{Ext}:\{0,1\}^n\to\{0,1\}^m$ is an* extractor *for $\mathcal{X}$ with error $\varepsilon>0$ if for all $\mathbf{X}\in\mathcal{X}$ we have $|\mathsf{Ext}(\mathbf{X})-\mathbf{U}_m|\leq\varepsilon$.*

For extractors to exist, we require all sources in $\mathcal{X}$ to have entropy. When each source in $\mathcal{X}$ is an (n,k)-source, we say that Ext is a (k,ε)-extractor for $\mathcal{X}$. For some classes, an extractor may not exist (such as for the class of all $(n,n-1)$-sources). Consequently, we turn to the looser requirements of condensing.

Definition I.2. *For a family of distributions $\mathcal{X}$ over $\{0,1\}^n$, a function $\mathsf{Cond}:\{0,1\}^n\to\{0,1\}^m$ is a* condenser *with error $\varepsilon\geq 0$ if for all $\mathbf{X}\in\mathcal{X}$ we have that $H^{\varepsilon}_{\infty}(\mathsf{Cond}(\mathbf{X}))/m \geq H_{\infty}(\mathbf{X})/n$. We say that* Cond *has* entropy gap Δ *if $H^{\varepsilon}_{\infty}(\mathsf{Cond}(\mathbf{X}))\geq m-\Delta$. When $\mathcal{X}$ is the class of (n,k)-sources and $k'=m-\Delta$, we say that* Cond *is a (k,k',ε)-condenser.*

Unfortunately, even this notion is too strong as we cannot condense with error ε from the class of all (n,k)-sources so that the output entropy rate is larger than k/n. [2] We thus study condensing from classes of sources which have some additional structure along with a min-entropy requirement. In this paper, we explore the possibility of condensing from three related models of weak sources. These models, some of which have been studied since the 1980s, are very general and well-motivated by practical considerations.

The rest of the introduction is organized as follows: In section I-A, we present the case that condensers have many applications and are hence a natural direction of study, in particular when extraction is not feasible. In section I-B, we discuss the models of weak sources that we study, present relevant prior work on these models, and discuss our results for each of them.

A. The utility of condensing

We present two viewpoints in motivating our study of condensers. We compare what is possible via condensing in contrast to extracting and consider the utility of condensing for simulating BPP algorithms.

[2] Assuming $m\leq n$, the output entropy can be shown to be most $k+m-n+\log(1/(1-\varepsilon))$. See lemma V.20 for a proof of this fact.

1) Condensing vs. extracting: Condensers exist in many scenarios when it can be provably shown that deterministic extraction is not possible. Thus, they allow us to obtain randomness that is more useful than what we began with in cases where extracting uniform bits is impossible. One significant example is that of Santha-Vazirani (SV) sources [5] and their generalization, Chor-Goldreich (CG) sources [6].

Informally, an SV source is a string of random bits such that the conditional distribution of each bit on the bits that come before it is guaranteed to have some minimum amount of min-entropy; a CG source generalizes this to allow each bit to instead be a symbol in $\{0,1\}^n$. It is well known that deterministic extraction is impossible for both SV and CG sources [5]–[7]. The recent result of [2] with regards to condensing from CG sources stands in contrast to these impossibility results for extraction. Other examples of sources for which deterministic extraction is not possible while deterministic condensing are the *somewhat dependent* sources of [8] and block sources [9].

We briefly mention that seeded condensers are known to achieve parameters unattainable by seeded extractors [10]. Further, seeded condensers have been extremely useful in excellent constructions of seeded extractors [11]–[14].

2) Condensing for simulating BPP algorithms: Condensers with small entropy gap are useful in simulating randomized algorithms with low overhead [2]. There are two ways one can go about this. First, there exists an explicit seeded extractor Ext with seed length $d=O(\log(\Delta))$ that can extract from any (n,k)-source $\mathbf{X}$ with entropy gap $\Delta=n-k$ [15]. Then, to simulate a randomized algorithm $\mathcal{A}$ in BPP, we instead sample $x\sim\mathbf{X}$ and take the majority of the output of $\mathcal{A}$ on $\{\mathsf{Ext}(x,s)\}$ where we cycle over all seeds s [16].

For some applications in randomized protocols, cryptography and interactive proofs, one cannot afford to compute Ext all 2^d times by cycling through every seed [17]–[20]. Alternatively, we can simulate $\mathcal{A}$ using a "one-shot" method in which we do not iterate over all seeds. A result from [20] allows us to simulate $\mathcal{A}$ on the condensed source $\mathbf{X}$ (with entropy gap Δ) by reducing the error of $\mathcal{A}$ to $2^{-\Delta-1}\cdot\varepsilon$ and then using $\mathbf{X}$ directly to simulate random bits in $\mathcal{A}$. Such a simulation will have error ε.

B. Models of weak sources and our results

We consider three adversarial classes of sources motivated by weak sources that appear in practice as well as in various cryptographic settings. These sources are natural generalizations of the well-studied independent sources wherein we allow for an adversarial dependence between sources. Changing the scope and power of the adversary in natural ways gives rise to the three different classes of sources that we will consider.

The three randomness sources that we focus on in this work are all composed of blocks of bits, known as symbols, which vary in how they are permitted to relate to other symbols in the source. In these definitions, we will consider sources $\mathbf{X}=\mathbf{X}_1,\ldots,\mathbf{X}_\ell$ of length ℓ where each $\mathbf{X}_i\in\{0,1\}^n$ is called a block. Generally, we will term blocks that have some minimum

amount of randomness "good" and blocks that are chosen by an adversary as "bad". Next, we discuss these three models of weak sources, presenting what was known from prior work and our new results for each of these models.

1) Online non-oblivious symbol fixing sources: The first class of adversarial sources that we will define is that of *online non-oblivious symbol fixing (oNOSF) sources*. While these are a restriction of general NOSF sources, which we will define later, we introduce them first since they have the weakest adversary and, consequently, the strongest positive results. Formally, we define oNOSF sources as follows.

Definition I.3 (oNOSF sources, [1])**.** *A (g, ℓ, n, k)-oNOSF source $\mathbf{X} = \mathbf{X}_1, \ldots, \mathbf{X}_\ell$ on $(\{0,1\}^n)^\ell$ is such that g out of the ℓ blocks are independently sampled (n, k)-sources (i.e., good), and the remaining $\ell - g$ bad blocks only depend on blocks with smaller indices (i.e., to their left).*

If $k = n$, we call $\mathbf{X}$ a *uniform (g, ℓ)-oNOSF source*. oNOSF sources form a natural class of sources to study when an adversary is working in real time and cannot predict the future. One such real-world example is that of blockchains. From [21], [22], we know that in a sequence of blocks, there will be some fraction of blocks that are chosen by honest players. Moreover, since these honest players are not working together, their chosen blocks may be considered as independent, fulfilling the requirement for good blocks for oNOSF sources. The adversarial players, on the other hand, can only see blocks added to the blockchain thus far and do not know which values of blocks will be added in the future, fulfilling the requirements for bad blocks for oNOSF sources. For more uses of oNOSF sources, see [1].

Previous work: Prior to our work, the only results for condensing or extracting from oNOSF sources are due to [1]. In [1], the authors study Somewhere Honest Entropic Look Ahead (SHELA) sources, which are exactly convex combinations of oNOSF sources (see proposition IV.15). They (1) transform (not uniform) oNOSF sources into uniform NOSF sources and (2) show that for any $\gamma \in (0, 1)$, there exists an ℓ such that extraction is not possible for $(\lfloor \gamma \ell \rfloor, \ell)$-oNOSF sources.

Our results: We prove the existence of condensers with excellent parameters when the majority of the blocks of a uniform oNOSF source are good.

Theorem I.4 (Informal version of theorem VI.13)**.** *For all constant g, ℓ and all ε such that $g > \ell/2$, there exists a condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any uniform (g, ℓ)-oNOSF source $\mathbf{X}$, we have $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq m - O(\log(m/\varepsilon))$ where $m = n$.*

For our construction, we introduce a new type of two-source extractor[3] that we call a *R-output-light* two-source extractor. Such a two-source extractor $\mathsf{2Ext} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ satisfies the additional guarantee that each output $z \in \{0,1\}^m$ can only be produced by R inputs $x \in \{0,1\}^{n_1}$ in the first source (see definition VI.10 for the formal definition). The existence of such extractors is not obvious, and we show that output-light two-source extractors exist with strong parameters in lemma VI.11. Our proof uses the observation that R-output-lightness is implied by the notion of R-invertibility, which simply bounds $\|\mathsf{Cond}(\mathbf{X})\|_\infty$ by R (see definition VI.18 for a formal definition). Incidentally, this latter notion has been recently used in a different context, to construct explicit random access linear codes with constant rate and distance [23]. While we are unable to explicitly construct such output-light two-source extractors, we do construct an explicit output-light *seeded* extractor, which we use to condense from uniform $(2, 3)$-oNOSF sources and more.

In fact, we can achieve a stronger result and show existence of condensers for oNOSF sources with only logarithmic min-entropy guarantee in the good blocks.

Theorem I.5 (Informal version of corollary VI.14)**.** *For any constant g, ℓ and all ε such that $g > \ell/2 + 1$, there exists a condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any (g, ℓ, n, k)-oNOSF source $\mathbf{X}$ with $k \geq 2\log(n/\varepsilon)$ we have $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq m - O(\log(m/\varepsilon))$ where $m = \Omega(k)$.*

To accomplish this, we transform logarithmic min-entropy oNOSF sources to uniform oNOSF sources and then apply the condenser for uniform oNOSF sources. We transform logarithmic min-entropy oNOSF sources to uniform oNOSF sources by modifying the construction of a somewhere-extractor for high min-entropy SHELA sources by [1]. These results imply that oNOSF sources can be useful for low overhead simulation of BPP algorithms. Furthermore, taken in tandem with the result that for all $\gamma > 0$ there exists a large enough ℓ such that one cannot extract from uniform $(\lfloor \gamma \ell \rfloor, \ell)$-oNOSF sources from [1], we have shown that oNOSF sources are one of the natural classes of sources that admit seedless condensing but not seedless extraction. This adds oNOSF sources to the short list of such natural sources mentioned in section I-A1.

In contrast, condensing in the regime of $g \leq \ell/2$ is more nuanced: some non-trivial condensing beyond rate $\frac{g}{\ell}$ is possible provided g does not divide ℓ, but condensing to a significantly higher rate is not possible.

Theorem 1 (theorem V.1, restated)**.** *For any function $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$ and $\varepsilon > 0$, there exists a constant δ and uniform (g, ℓ)-oNOSF source $\mathbf{X}$ with $g \leq \ell/2$ such that $H^\varepsilon_\infty(f(\mathbf{X})) \leq \frac{1}{\lfloor \ell/g \rfloor} \cdot m + \delta$.*

This partially resolves[4] a conjecture of [1]: they conjectured that (g, ℓ)-oNOSF sources cannot be transformed into uniform (g', ℓ')-NOSF sources with $\frac{g'}{\ell'} > \frac{g}{\ell}$. Our condensing impossibility implies $\frac{g'}{\ell'} \leq \frac{1}{\lfloor \ell/g \rfloor}$ for any such transformation. This negative result is tight and we are able to condense uniform (g, ℓ)-oNOSF sources up to rate $\frac{1}{\lfloor \ell/g \rfloor}$.

[3]See definition IV.9 for a definition of two-source extractors

[4]Our result on the existence of condensers falls short of completely resolving their conjecture as it does not transform uniform oNOSF sources into uniform NOSF sources.

Theorem 2. *(Informal version of theorem VI.3) For any constant g, ℓ and ε such that $\lfloor \ell/g \rfloor = r$ and $\ell/g \neq r$, there exists a condenser* $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ *such that for any uniform (g,ℓ)-oNOSF source $\mathbf{X}$ we have $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq \frac{1}{r} \cdot m - O(\log(m/\varepsilon))$ where $m = \Omega(n)$.*

As before in theorem 2, we can convert a logarithmic min-entropy oNOSF source to a uniform oNOSF source and then apply theorem 2. This yields:

Theorem 3. *(Informal version of theorem VI.1) For all constant g, ℓ and ε such that $\left\lfloor \frac{\ell-1}{g-1} \right\rfloor = r$ and $\frac{\ell-1}{g-1} \neq r$, there exists a condenser* $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ *such that for any (g,ℓ,n,k)-oNOSF source $\mathbf{X}$ with $k \geq 2\log(n/\varepsilon)$, we have that $H^\varepsilon_\infty(\mathbf{X}) \geq \frac{1}{r} \cdot m - O(\log(m/\varepsilon))$ with $m = \Omega(k)$.*

We note that theorem I.4 and theorem I.5 are special cases of theorem 2 and theorem 3 in the case that $\lfloor \ell/g \rfloor = r = 1$, allowing us to state all of our condensing possibility results succinctly.

Put together, our results demonstrate a sharp threshold at $g = \ell/2$ for condensing from oNOSF sources with a small entropy gap. To our knowledge, there is no other set of sources that exhibits such behavior, making oNOSF sources unique among both adversarial sources and general randomness sources.

2) Adversarial Chor-Goldreich sources: Next, we consider a generalization of oNOSF sources, termed *adversarial Chor-Goldreich (CG) sources*, that we obtain by strengthening the adversary's power. Adversarial CG sources share the motivation from oNOSF sources that the adversary cannot predict the future. Rather than forcing the adversary to have its blocks only depend on blocks in the past (those with smaller indices), aCG sources require that good blocks have some entropy conditioned on all blocks that came before them. In other words, bad blocks cannot expose all of the entropy of future good blocks.

Definition I.6 (Adversarial CG (aCG) sources, [2], [6])**.** *We define a (g,ℓ,n,k)-*aCG source $\mathbf{X} = \mathbf{X}_1, \ldots, \mathbf{X}_\ell$ *to be a distribution on $(\{0,1\}^n)^\ell$ such that there exists a set of good indices $\mathcal{G} \subseteq [\ell]$ of size at least g for which $H_\infty(\mathbf{X}_i \mid \mathbf{X}_1 = x_1, \ldots, \mathbf{X}_{i-1} = x_{i-1}) \geq k$ for all $i \in \mathcal{G}$ and all prefixes $x_1, \ldots, x_{i-1}$.*

As before, if $k = n$, then we say that $\mathbf{X}$ is a uniform (g,ℓ)-aCG source. Observe that because the good blocks of a oNOSF source are independent of all blocks before it, oNOSF sources are trivially aCG sources as well. As a consequence, our condensing impossibility results from theorem 1 immediately apply to aCG sources as well. Moreover, a convenient fact that we later show in proposition IV.17 and will rely on is that uniform (g,ℓ)-aCG sources and uniform (g,ℓ)-oNOSF sources are equivalent.

CG sources are a well-studied class of sources introduced by [6] as a generalization of Santha-Vazirani sources [5]. Hence, the majority of the work done on CG sources has been in the non-adversarial setting in which $g = \ell$. Adversarial CG sources that contain bad blocks were only recently introduced in [2] (although they use the terminology "almost" CG sources), in which the authors show several condensing results for CG and adversarial CG sources. Our work can then be seen as a meaningful addition to this long line of research on CG sources and their generalizations.

Previous work: The impossibility of extraction from both oNOSF sources and aCG sources due to [1], [6] naturally raises the question of whether there is a distinction between these two sources with regards to randomness condensing.

For CG sources, [24] showed that errorless condensing is impossible. In contrast, [2] proved several possibility results regarding condensing with error for CG sources. Their results assume that the size of each block is very small (almost constant) compared to the number of blocks.

We also note that the authors of [2] considered various other relaxations of the definition of aCG sources that we do not consider here. These include good blocks having only smooth min-entropy conditioned on previous blocks instead of the stronger condition of min-entropy, having smooth min-entropy conditioned on a constant fraction of prefixes of previous blocks instead of all prefixes, and having a Shannon entropy requirement instead of min-entropy requirement.

Our results: In [2], the authors pose the question of whether it is possible to condense from aCG sources with a constant entropy gap.[5] We give a partially positive answer to this by showing that we can condense from uniform (g,ℓ)-aCG sources with $g > \ell/2$ with logarithmic entropy gap since uniform (g,ℓ)-aCG sources are equivalent to uniform (g,ℓ)-oNOSF sources and we can defer to theorem 2. Of course, all of theorem 2 applies to uniform aCG sources, so we can condense any uniform (g,ℓ)-aCG source to rate $\frac{1}{\lfloor \ell/g \rfloor}$. The generalization of these results in theorem I.5 do not hold for non-uniform aCG sources since non-uniform aCG sources need not be oNOSF sources. Before our work, no non-trivial condensing was known for uniform (g,ℓ,n)-aCG sources even in the case of $g = \ell - 1$. It is important to note that our results hold for comparatively large block sizes $n = 2^{\omega(\ell)}$, in contrast to the results of [2] that hold for constant block sizes and increasing ℓ.

As previously mentioned, since oNOSF sources are a subclass of aCG sources, our condensing impossibility results from theorem 1 transfer over. Thus, in the $g \leq \ell/2$ regime, we give a negative answer to the question of [2] by showing that good condensers do not exist for uniform (g,ℓ)-aCG sources, let alone condensers with a constant entropy gap. Note that unlike our condensing possibility results that only apply to uniform aCG sources, our impossibility result applies to non-uniform aCG sources as well.

In addition, we prove various condensing impossibility results that work even when there are no bad blocks (i.e., for non-adversarial, or just regular, CG sources): the first result of theorem 4 is based on a reduction from general (n,k)-sources

[5] In their paper, they phrase it as removing the requirement of suffix-friendliness.

to CG sources and the second result uses a reduction from uniform oNOSF sources to low min-entropy CG sources.

Theorem 4 (Informal version of theorem V.21 and theorem V.22)**.** *For all $\Delta > 0$ and for every function $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, there exists an (ℓ,ℓ)-aCG source $\mathbf{X}$ satisfying either of the following with $\varepsilon = 0.99$:*

- *The good blocks have min-entropy at least $n - \Delta - \log(\ell) - O(1)$ conditioned on all fixings of previous blocks and $H^\varepsilon_\infty(f(\mathbf{X})) \leq m - \Delta - \max(m - \ell n, 0) + O(1)$.*
- *The good blocks have min-entropy at least $n/\ell - \log(\ell) - O(1)$ conditioned on all fixings of previous blocks and $H^\varepsilon_\infty(f(\mathbf{X})) \leq \frac{1}{2} \cdot m + O(1)$.*

It is important to note that the first bullet above does not subsume the second. In particular, the second bullet point from above gives a stronger result than the first in the setting when m is much larger than n.

We note that these results do not contradict the condensing result from [2] as in the parameter regimes for which theorem 4 works, the condenser of [2] does not result in an entropy increase. This also shows a separation between aCG sources and oNOSF sources since theorem 3 can condense from oNOSF sources in this parameter regime.

3) Non-oblivious symbol fixing sources: Finally, we strengthen the adversary one last time by letting the bad blocks depend arbitrarily on all the good blocks. This gives rise to NOSF sources which themselves generalize the setting of non-oblivious bit-fixing (NOBF) sources [25] where each block is a bit (i.e., $n = 1$).

Definition I.7 (NOSF sources)**.** *A (g,ℓ,n,k)-NOSF source $\mathbf{X} = \mathbf{X}_1, \ldots, \mathbf{X}_\ell$ on $(\{0,1\}^n)^\ell$ is such that g out of the ℓ blocks are independently sampled (n,k)-sources (i.e., "good") while the other $\ell - g$ bad blocks may depend arbitrarily on the good blocks.*

When $k = n$ and n is clear from context, we simply call $\mathbf{X}$ a uniform (g,ℓ)-NOSF source. The adversary in NOSF sources clearly has a significant amount of power; every single good block is sampled before the adversary gets to decide what to place in the bad blocks. As NOSF sources are in the setting in which the adversary is the strongest, they are also the sources for which we are most motivated to be able to extract or condense as they are the most general. We note that much of the progress on explicit constructions of two-source extractors and condensers [9], [26], a major problem in the area of randomness extraction, is based on constructing extractors and condensers for NOSF sources (in a parameter regime where it was existentially known that extraction is possible). This further motivates our exploration of condensing from NOSF sources in a more general parameter setting.

Previous work: We can trace back study of extracting from NOBF sources to the seminal work of Ben-Or and Linial in [27].[6] They made the connection between NOBF extractors and the influence of sets of variables on Boolean functions. Together with the work of Kahn, Kalai, and Linial in [28], in which they demonstrated lower bounds on the influence of variables on Boolean functions, these works show that it is not possible to extract from uniform (g,ℓ)-NOBF sources when the number of bad bits is $b = \ell - g = \Omega(\ell/\log\ell)$. While no analogous result is known for NOSF sources,[7] the extraction impossibility result from [1] for oNOSF sources also applies for NOSF sources: for any $\gamma > 0$ there exists a large constant ℓ such that it is impossible to extract even one bit from uniform $(\gamma\ell,\ell)$-NOSF sources.

To attempt to match these lower bounds on extraction, resilient functions, introduced by [31], have yielded the current best results. The resilient function of Ajtai and Linial in [32] and its explicit versions constructed by [26], [33] achieve extractors for uniform (g,ℓ)-NOBF sources when $b = O(\ell/\log^2\ell)$, leaving a $1/\log\ell$ gap between the lower and upper bounds.

Noting that a uniform (g,ℓ,n)-NOSF source is a uniform $(ng, n\ell)$-NOBF source, these results imply extractors when $g > \ell(1 - 1/C\log^2(n\ell))$, for some large enough constant C. This still leaves open whether condensing is possible for most settings of parameters.

Related to this, the work of [34] explores what they call extracting multimergers, which we may consider as extractors for uniform NOSF sources. For seedless extracting multimergers, their result implies that extracting from uniform $(2,3)$-NOSF sources is impossible.

Our results: As oNOSF sources are also NOSF sources, our condensing impossibility result in theorem 1 also applies to (g,ℓ)-NOSF sources when $g \leq \ell/2$. However, we are able to show an even stronger result for any setting of g and ℓ and thus extend existing lower bounds of extraction to condensing.

Theorem 5 (corollary V.10 restated)**.** *For all constant $g,\ell \in \mathbb{N}$, there exist constant $\varepsilon,\delta > 0$ so the following holds: for all $a,m,n \in \mathbb{N}$ and all functions $f : (\{0,1\}^n)^{a\ell} \to \{0,1\}^m$, there exists a uniform $(ag,a\ell)$-NOSF source $\mathbf{X}$ such that $H^\varepsilon_\infty(f(\mathbf{X})) \leq \frac{g}{\ell} \cdot m + \delta$.*

By varying a above, we extend our result for any g and ℓ to any rate g/ℓ uniform NOSF source. These results together put NOSF sources in stark contrast with adversarial CG and oNOSF sources since they can both be condensed in a useful manner for simulating BPP algorithms, while we have shown that NOSF sources cannot be condensed in such a manner.

II. Proof Overview

We present the main ideas and techniques for proving our main condensing impossibility results in section II-A and possibility results in section II-B. In this version of our paper, we do not provide full proofs and instead refer the reader to the full version of our paper at https://arxiv.org/abs/2312.15087.

[6] They used the terminology "collective coin flipping protocol" instead of "NOBF extractor".

[7] Although one is conjectured in [29] that attempts to recover what was initially proposed in [30].

A. Impossibility results

In this subsection, we will go over the main techniques used in proving the condensing impossibility result for the case that $g \leq \ell/2$ in section II-A1, the condensing impossibility result for uniform NOSF sources when $g > \ell/2$ in section II-A2, and the condensing impossibility result for low min-entropy CG sources in section II-A3.

1) Impossibility of condensing from uniform (g, ℓ)-oNOSF sources for $g \leq \ell/2$: We prove that when the number of good blocks g is not more than half of the total number of blocks ℓ, then condensing beyond rate $\frac{1}{\lfloor \ell/g \rfloor}$ is impossible. Formally, we will prove the following statement.

Theorem II.1 (theorem V.1, restated)**.** *For all ε, there exists a δ such that for all $g, \ell \in \mathbb{N}$ with $g \leq \ell/2$ and for all $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, there exists a uniform (g, ℓ)-oNOSF source $\mathbf{X}$ such that $H^\varepsilon_\infty(f(\mathbf{X})) \leq \frac{1}{\lfloor \ell/g \rfloor} \cdot m + \delta$.*

The steps we take to achieve the result of theorem II.1 are, broadly, as follows:

1) We first reduce proving the theorem to only proving it for the special case of $g = 1$. We show that if it is possible to condense uniform (g, ℓ)-oNOSF sources to entropy-rate more than $\frac{1}{\lfloor \ell/g \rfloor}$, then it is possible to condense uniform $(1, \ell')$-oNOSF sources to rate beyond $\frac{1}{\lfloor \ell'/1 \rfloor} = \frac{1}{\ell'}$ where $\ell' = \lfloor \ell/g \rfloor$. We do this by transforming any uniform $(1, \ell')$-oNOSF source to a uniform (g, ℓ)-oNOSF source.
2) We prove the theorem for the special case of $g = 1$ and arbitrary ℓ. We do this by using an "induct or win" argument. We show either condensing from uniform $(1, \ell)$-oNOSF sources is impossible (win) or we reduce to the case of condensing from uniform $(1, \ell - 1)$-oNOSF sources (induct). Either we will win at some point in our reduction or we will reach the base case of $g = \ell = 1$ where the claim trivially holds. Let f be a candidate condenser and take cases on whether there exists a fixing of the first block in f such that the partial function obtained by fixing f to that values will have small support. If such a fixing exists, then we reduce the problem to condensing from uniform $(1, \ell - 1)$-oNOSF sources. If not, then we directly construct a uniform $(1, \ell)$-oNOSF source where f fails to condense from by reducing to a graph problem.
3) The graph problem we reduce to in the "win" case is the following: Let $G = (U, V)$ be a bipartite graph with $U = [N], V = [M]$ and such that $\deg(u) \geq c_0 M^\delta$ for all $u \in U$ where $\delta > 0$ is some constant. Then, show there exists $D \subset V$ such that $|\text{Nbr}(D)| \geq c_1 N$ and $|D| \leq c_2 \cdot M^{1-\delta}$ where c_0, c_1, c_2 are some universal constants.

We expand on these three steps and prove them.

Step 1: In this step, we transform any uniform $(1, \ell')$-oNOSF source $\mathbf{X}$ to a uniform (g, ℓ)-oNOSF source $\mathbf{Y}$ where $\ell' = \lfloor \ell/g \rfloor$. Divide ℓ by ℓ' so that $\ell = a\ell' + r$ where $0 \leq r < \ell'$. We compute that $a \geq g$. We split the blocks of $\mathbf{X}$ as evenly as possible: split up the first r blocks of $\mathbf{X}$ into $a+1$ blocks and the remaining $\ell' - r$ blocks into a blocks. These $a\ell' + r = \ell$ blocks that we obtained by splitting $\mathbf{X}$ will form $\mathbf{Y}$. If a block in $\mathbf{X}$ is uniform, then all the split up blocks will also be uniform. Similarly, if a block in $\mathbf{X}$ is bad and only depended on blocks appearing before it, so will all the blocks formed after splitting it. Also, as at least one block in $\mathbf{X}$ is good, $\mathbf{Y}$ must have at least $a \geq g$ good blocks in it. Hence, $\mathbf{Y}$ is indeed a uniform (g, ℓ)-oNOSF source.

Step 2: In this step, we execute our induct or win argument. Fix a candidate condenser function $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$. We proceed by contradiction and assume f can condense from uniform $(1, \ell)$-oNOSF sources beyond rate $1/\ell$. We either directly construct a uniform $(1, \ell)$-oNOSF source $\mathbf{X}$ where f will fail to condense from or we show how using f, we can obtain a condenser for uniform $(1, \ell - 1)$-oNOSF sources, which is a contradiction.

Case 1. There exists a fixing of the first block x_1 such that $\left|f(x_1, y_1, \ldots, y_{\ell-1}) | (y_1, \ldots, y_{\ell-1}) \in \{0,1\}^{n(\ell-1)}\right| \leq 2^{m(1-1/\ell)}$. Then, by appropriately relabeling outputs, we can define $h : (\{0,1\}^n)^{\ell-1} \to \{0,1\}^{m(1-1/\ell)}$ as $h(y_1, \ldots, y_{\ell-1}) = f(x_1, y_1, \ldots, y_{\ell-1})$. We now show that h will be a condenser for uniform $(1, \ell - 1)$-oNOSF sources. Let $\mathbf{Y}$ be arbitrary uniform $(1, \ell - 1)$-oNOSF source. We transform $\mathbf{Y}$ into a uniform $(1, \ell)$-oNOSF source$\mathbf{Y}'$ by letting the first block of $\mathbf{Y}'$ be fixed to x_1 and the remaining $\ell - 1$ blocks behave as $\mathbf{Y}$. By assumption, f can condense $\mathbf{Y}'$ so that output entropy is more than $\frac{1}{\ell} \cdot m$. However this implies h can condense $\mathbf{Y}$ to have entropy more than $\frac{1}{\ell} \cdot m = \frac{1}{\ell-1} \cdot m(1 - 1/\ell)$. As h outputs $m(1 - 1/\ell)$ bits, this is a contradiction.

Case 2. For every fixing of the first block $x_1 : |f(x_1, y_1, \ldots, y_{\ell-1})| > 2^{m(1-1/\ell)}$. To show f fails to condense from $\mathbf{X}$, it suffices to show that with constant probability, $f(\mathbf{X})$ will lie in a small set $D \subset \{0,1\}^m$ where $|D| = O\left(2^{m(1/\ell)}\right)$ (see claim IV.3 for a formal version of this). Consider the bipartite graph $H = (U = (\{0,1\}^n), V = \{0,1\}^m)$ where edge (u, v) is included if there exist $y_1, \ldots, y_{\ell-1}$ such that $f(x_1, y_1, \ldots, y_{\ell-1}) = v$. By assumption, for all $u \in U : \deg(u) > 2^{m(1-1/\ell)}$. Our graph theoretic dominating set lemma from Item 3. guarantees that there exists $D \subset \{0,1\}^m$ such that $|D| \leq c_0 2^{m(1/\ell)}$ and $|\text{Nbr}(D)| \geq c_1 2^n$ where c_0, c_1 are universal constants. Now, let $\mathbf{X}$ be uniform $(1, \ell)$-oNOSF source where the first block is uniform and the remaining $\ell - 1$ blocks are adversarial where the value of those $\ell - 1$ blocks (depending on the value of the first block) is set so that f outputs an element from D if possible. By the construction of the bipartite graph and the construction of $\mathbf{X}$, with probability c_1, $f(\mathbf{X})$ will output an element in D. Hence, as f outputs an element from a small set, D, with high probability, it fails to condense from $\mathbf{X}$.

Step 3: We prove the dominating set lemma for bipartite graph in this step to conclude the proof of the "win" argument. We construct D by repeatedly adding the vertex from V that has the highest degree, removing vertices incident to that vertex, and stopping until at least $c_1 N$ many vertices from

U are incident to some vertex from D. Whenever we attempt to add a vertex to D, the graph will have at least $(1-c_1)N$ many vertices and so at least $(1-c_1)N \cdot c_0 \cdot M^{1-\delta}$ many edges. This implies there will always be a vertex $v \in V$ such that $\deg(v) \geq c_0(1-c_1) \cdot \frac{N}{M^\delta}$. This is true at each stage and we repeat this until at least $c_1 N$ many vertices are covered. Hence, $|D| \leq c_2 \cdot M^{1-\delta}$ for some universal constant c_2 as desired.

2) Impossibility of condensing from uniform NOSF sources: We prove much stronger condensing impossibility result for uniform NOSF sources: we prove that no non-trivial condensing is possible. We are able to do so since the bad blocks have no restrictions and can arbitrarily depend on any good block. Formally, we show the following:

Theorem II.2 (corollary V.10 restated)**.** *For all fixed $g, \ell \in \mathbb{N}$, there exist fixed $\varepsilon, \delta > 0$ so that the following holds: for all $a, m, n \in \mathbb{N}$ and all functions $f : (\{0,1\}^n)^{a\ell} \to \{0,1\}^m$, there exists a uniform $(ag, a\ell)$-NOSF source $\mathbf{X}$ such that $H^\varepsilon_\infty(f(\mathbf{X})) \leq \frac{g}{\ell} \cdot m + \delta$.*

We prove theorem II.2 using the following strategy:

1) We reduce the general case to the special case of $a = 1$ and $g > \ell/2$.
2) Our high level strategy for this step is same as in item 2 from section II-A1. We perform an "induct or win" argument to show it is impossible to condense from uniform (g, ℓ)-NOSF sources where $g > \ell/2$ beyond rate g/ℓ. As earlier, we show either condensing from uniform (g, ℓ)-NOSF sources is impossible (win) or we reduce to the case of condensing from uniform $(g, \ell-1)$-NOSF sources (induct). So, we recursively apply this argument and either win at some point or reach a base case of $g = \ell$ where the claim trivially holds. Let f be a candidate condenser and take cases on whether there exists a block position p such that for constant fraction of fixings of all other blocks, the partial function obtained by fixing f to those values will have large support. If this holds, then we use the almost-dominating set argument from item 3 (from section II-A1) to reduce to the case of condensing from uniform $(g, \ell-1)$-NOSF sources. If such a position p with these fixings do not exist, then we directly construct a uniform (g, ℓ)-oNOSF source where f fails to condense from by reducing to a hypergraph problem.
3) The hypergraph problem we reduce to in the "win" case is the following: Let $H = (V_1, \ldots, V_t, E)$ be a t-uniform t-partite hypergraph with $V_1 = \cdots = V_t = [N], |E| = c_0 N^t$. Let the edges of H be colored in M colors in a 'locally light' way: such that for every position $p \in [T]$, and every $(t-1)$ tuples: $(v_1, \ldots, v_{p-1}, v_{p+1}, \ldots, v_t) \in [N]^{t-1}$, the number of distinct colored edges as entries in position p vary is $\leq c_1 M^\delta$. Formally, $|\chi(v_1, \ldots, v_{p-1}, y, v_{p+1}, \ldots, v_t) : y \in [N]| \leq c_1 M^\delta$. Then, there exists $D \subseteq [M]$ such that $|D| \leq c_2 \cdot M^{t\delta}$ and at least $c_3 N^t$ edges in H are colored in one of the colors from D. Here, c_0, c_1, c_2, c_3 are some constants.

We expand on these three steps and prove them.

Step 1: We show how to reduce to the case of $a = 1$. We do this using the same argument as in item 1 from section II-A1: we transform uniform (g, ℓ)-NOSF sources into uniform $(ag, a\ell)$-NOSF sources by splitting up blocks; this way, a condenser for uniform $(ag, a\ell)$-NOSF sources will also condense from uniform (g, ℓ)-NOSF sources.

We next carefully examine the argument made in item 2 and see that the induct or win argument made there can be generalized to show the following: either condensing from uniform (g, ℓ)-NOSF source is impossible or we reduce to the case of condensing from uniform $(g, \ell - g)$-NOSF source. Applying this recursively to arbitrary g, ℓ, we either win and show impossibility at some step or we end up reducing to showing impossibility for condensing from uniform (g, ℓ)-NOSF sources where $g > \ell/2$.

Combining these two steps, we reduce the general case to the special case of $a = 1$ and $g > \ell/2$.

Step 2: In this step, we execute our induct or win argument. We fix a candidate condenser function $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$. Proceed by contradiction and assume f can condense from uniform (g, ℓ)-NOSF sources beyond rate g/ℓ. We either directly construct a uniform (g, ℓ)-NOSF source $\mathbf{X}$ where f will fail to condense from or we show how using f, we can obtain a condenser for uniform $(g, \ell-1)$-NOSF sources, which is a contradiction. For $p \in [\ell]$, let S_p be the set of $\ell - 1$ tuples $(x_1, \ldots, x_{p-1}, x_{p+1}, \ldots, x_\ell)$ such that

$$|\{f(x_1, \ldots, x_{p-1}, y, x_{p+1}, \ldots, x_\ell) : y \in \{0,1\}^n\}| \geq c_0 2^{m/\ell}$$

Case 1. There exists $p \in [\ell]$ such that $|S_p| \geq c_1 2^{n(\ell-1)}$ where $c_1 > 0$ is a small constant. Without loss of generality let $p = 1$. Construct a bipartite graph $G = (U, V)$ where $U = S_1, V = \{0,1\}^m$ and edge (u, v) if there exists a fixing y of block p such that $f(u, y) = v$. Then, we see that G satisfies the requirement for item 3 and hence, there exists $D \subset \{0,1\}^m$ such that $|D| \leq 2^{m(1-1/\ell)}$ which neighbors at least $c_3 2^{n(\ell-1)}$ vertices from U. For the sake of presentation, assume $c_1 = c_3 = 1$. In the full proof, $c_1, c_3 > 0$ are small constants and we need to induct using a stronger inductive hypothesis. Now, define $h : \{0,1\}^{n(\ell-1)} \to \{0,1\}^{m(1-1/\ell)}$ as $h(y_1, \ldots, y_{\ell-1}) = f(x_1, y_1, \ldots, y_{\ell-1})$ where x_1 is such that $f(x_1, y_1, \ldots, y_{\ell-1}) \in D$ (as $c_1 = c_3 = 1$, such x_1 always exists). The output domain of h can be made $\{0,1\}^{m(1-1/\ell)}$ instead of D by appropriately relabeling the output. We then show, similar to proof of case 1 of item 2, h will be a condenser for uniform $(g, \ell-1)$-NOSF sources and get a contradiction.

Case 2. For all $p \in [\ell]$, $|S_p| \leq c_1 2^{n(\ell-1)}$. We say $x = (x_1, \ldots, x_\ell) \in \{0,1\}^{n\ell}$ is bad if for some $p \in [\ell]$, removing position p from x makes it an element of S_p. Let B be set of such bad strings. Then, $|B| \leq c_1 \ell \cdot 2^{n\ell}$. Let $H = (V_1, \ldots, V_\ell)$ where $V_i = \{0,1\}^n$ be ℓ-uniform ℓ-partite hypergraph where edge $v = (v_1, \ldots, v_\ell)$ is in H if $v \notin B$. Then, H has at least $(1 - c_1\ell)2^{n\ell}$ edges. By an averaging argument, there exists $x = (x_1, \ldots, x_{\ell-g}) \in \{0,1\}^{n(\ell-g)}$ such that the number of

edges in H containing that x is at least $(1-c_1\ell)2^{ng}$. Consider uniform (g,ℓ)-oNOSF source $\mathbf{Y}$ where the first $\ell-g$ blocks always output x and the remaining g blocks are uniform. To show f fails to condense from $\mathbf{X}$, it suffices to show: constant probability, $f(\mathbf{X})$ will lie in a small set $D \subset \{0,1\}^m$ where $|D| = O\left(2^{m(g/\ell)}\right)$ (see claim IV.3 for a formal version of this).

Let $H' = (U_1, \ldots, U_g)$ where $U_i = \{0,1\}^n$ be g-uniform g-partite hypergraph where edge $u = (u_1, \ldots, u_g)$ is in H' if $(x_1, \ldots, x_{\ell-g}, u_1, \ldots, u_g)$ is in H. Then, H' has at least $(1-c_1\ell)2^{ng}$ edges. Now, color H' into 2^m colors by coloring edge $(u_1, \ldots, u_g)$ as $f(x_1, \ldots, x_{\ell-g}, u_1, \ldots, u_g)$. By definition of S_p and construction of H', we see that for every $\ell-1$ tuples u in $\{0,1\}^{n(\ell-1)}$, the number of distinct colors in H' is at most $c_0 \cdot 2^{m/\ell}$. We apply the hypergraph lemma to H' and infer that there exists $D \subset \{0,1\}^m$ such that $|D| \leq c_2 \cdot 2^{m(g/\ell)}$ at least $c_3 \cdot 2^{ng}$ edges in in H' are colored in one of the colors from D. Hence, we found a small set D such that with constant probability, $f(\mathbf{X})$ lies in D as desired.

Step 3: We finally solve the hypergraph problem to conclude the proof of the "win" argument. We repeatedly pick the color which covers the most edges to D until the number of edges covered is at least $c_3 \cdot N^t$. At the last step of the process, H must have at least $(c_0 - c_3) \cdot N^t$ edges. We show that at that stage, the chosen a color will cover at least $c_4 N^t / M^{t\delta}$ edges. This implies at each step before this, the chosen color must cover at least that many edges and hence, $|D| \leq \frac{1}{c_4} M^{t\delta}$ as desired.

So, our goal is to show that in a t-uniform t-partite hypergraph $H = (V_1, \ldots, V_t)$ having at least $c_5 N^t$ edges and colored in M colors in a 'locally light' manner - on fixing any $t-1$ tuple, the number of colors adjacent to it as last entry varies is at most $c_1 \cdot M^\delta$, there exists a color γ covering at least $\Omega(N^t/M^{t\delta})$ edges. We induct on t and show this. We sketch the idea below for bipartite graphs.

For every $v_2 \in V_2$, let $C_{v_2} \subset [M]$ be the set of colors that have at most $c_6 \cdot (N/M^\delta)$ where c_6 is a very small constant. We remove edge (v_1, v_2) from H if $(v_1, v_2) \in C_{v_2}$. For each v_2, we remove at most $c_1 c_6 \cdot N$ edges incident to it. Overall, we end up removing at most $c_1 c_6 \cdot N^2$ edges from H and it still has $(c_5 - c_1 c_6)N^2$ edges. Doing this ensures that every color incident to every vertex v_2 in V_2 has at least $c_6 \cdot (N/M^\delta)$ edges incident to it. We finally find such a popular color by doing the following: By averaging argument, let $v_1^* \in V_1$ and $\gamma^* \in [M]$ be such that the number of edges incident to v_1^* with color γ is at least $\frac{c_5 - c_1 c_6}{c_1} \cdot (N/M^\delta)$. Let $\text{Nbr}_\gamma(v_1^*) = \{v_2 \in V_2 : (v_1^*, v_2) \text{ is colored with color } \gamma\}$. Moreover, for every $v_2 \in \text{Nbr}_\gamma(v_1^*)$, the number of edges incident to them with color γ is at least $c_6 \cdot N/M^\delta$. We are done as at least $c_6 \cdot \frac{c_5 - c_1 c_6}{c_1} \cdot N^2/M^{2\delta} = \Omega(N^2/M^{2\delta})$ edges in H colored with color γ.

3) Impossibility of condensing from low min-entropy aCG sources: We provide two impossibility result for (ℓ,ℓ)-aCG source, we only sketch proof for one of them as they both share many ideas. Our impossibility result theorem V.21 is based on reduction from general (n,k)-sources and the fact that it is impossible to condense from such sources.

Here, we sketch a proof of the second impossibility result where we show that it is impossible to condense from non-adversarial CG sources when each block's min-entropy, conditioned on previous blocks, is roughly bounded by $n/(\ell+1)$.

Theorem II.3 (theorem V.22 restated)**.** *For all $0 < \varepsilon < 1$ there exists a $\delta > 0$ such that the following holds: for every function $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, there exists a (ℓ,ℓ)-aCG source $\mathbf{X}$ where the good blocks have min-entropy at least $\frac{n - \ell\log(2\ell/\varepsilon)}{\ell+1}$ conditioned on all fixings of previous blocks and $H_\infty^\varepsilon(f(\mathbf{X})) \leq \frac{1}{2} \cdot m + \delta$.*

The bulk of the proof is based on a transformation from a uniform $(1,2)$-oNOSF source $\mathbf{X} = \mathbf{X}_1, \mathbf{X}_2$ to a source $\mathbf{Y} = \mathbf{Y}_1, \ldots, \mathbf{Y}_\ell$ that is $\varepsilon/2$-close to an (ℓ,ℓ)-aCG source. With this transformation, applying theorem II.1 with $\ell = 2$ and $\varepsilon/2$ to $\mathbf{X}$ then allows us to infer that we also cannot condense from $\mathbf{Y}$ with error ε. Thus, we focus on how to construct $\mathbf{Y}$ next.

Briefly, to construct $\mathbf{Y}$, we will take substrings of $\mathbf{X}_1$ and $\mathbf{X}_2$ to place into each block of $\mathbf{Y}$. From $\mathbf{X}_2$, we will take constant sized chunks of size $t_2 = \frac{n - \ell\log(2\ell/\gamma)}{\ell+1}$ where $\gamma = \frac{\varepsilon}{2\ell}$ to place into each $\mathbf{Y}_i$, and from $\mathbf{X}_1$ we will take blocks of increasing size $i \cdot t_1 - 1$ to place into each $\mathbf{Y}_i$ where $t_1 = t_2 + \log(1/\gamma)$. Our proof then finishes with an inductive argument to claim that $\mathbf{Y}$ is indeed $\varepsilon/2$-close to an (ℓ,ℓ)-aCG source source, as required.

B. Possibility results

In this subsection, we will present our existential construction of condensers for oNOSF sources and uniform aCG sources. We begin by describing the construction of our condenser for uniform (g,ℓ)-oNOSF sources and uniform (g,ℓ)-aCG source in the setting of $g > \ell/2$ in section II-B1. Then we generalize this result to any setting of g and ℓ in section II-B2. Finally, we deal with logarithmic min-entropy oNOSF sources in section II-B3.

1) Condensing from uniform (g,ℓ)-oNOSF sources for $g > \ell/2$: Before we dive into the actual proof, it is instructive to see why a random function fails to be a condenser for uniform (g,ℓ)-oNOSF sources. In particular, let us consider uniform $(2,3)$-oNOSF sources. For a random function $f : \{0,1\}^{3n} \to \{0,1\}^m$, with high probability over $x_1, x_2 \in \{0,1\}^n$, we have $|f(x_1, x_2, \cdot)| = 2^m$. Hence, if the adversary is in position 3, then it can depend on x_1 and x_2 to ensure the output of f always lies in a small set. To overcome this, one can consider restricting the number of choices adversary has when it is in position 3. This intuition indeed works out and we give further details.

Theorem II.4 (theorem VI.13 restated)**.** *For all g, ℓ such that $g > \ell/2$ and ε, there exists a condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any uniform (g,ℓ)-oNOSF source $\mathbf{X}$, $H_\infty^\varepsilon(\mathsf{Cond}(\mathbf{X})) \geq m - (5^{\ell-g} - 3)\log(gn/\varepsilon)$ where $m = n - 2(5^{\ell-g} - 1)\log(gn)$.*

Our construction relies on a (k_1, k_2, ε)-two-source extractor $\mathsf{Ext} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ with a property that we term *output-lightness*, the definition and importance of which we will see soon, and a clever choice of a partition and prefixes of our input source $\mathbf{X}$. We do not currently know of a construction of a two-source extractor with our desired min-entropy and error parameters that is also output-light, so our construction is currently based on an existential output-light two-source extractor that we show in lemma VI.11. In particular, if we write $\mathbf{X} = \mathbf{X}_1, \ldots, \mathbf{X}_\ell$ and we take $\mathbf{Y}_i$ to be the prefix of $\mathbf{X}_i$ containing the first $5^{\ell-i} \cdot 4\log(gn/\varepsilon)$ bits, then we define our two inputs to Ext as $\mathbf{Z}_1 = \mathbf{X}_1, \ldots, \mathbf{X}_g$ and $\mathbf{Z}_2 = \mathbf{Y}_{g+1}, \ldots, \mathbf{Y}_\ell$. Thus, our condenser becomes $\mathsf{Cond}(\mathbf{X}) := \mathsf{Ext}(\mathbf{Z}_1, \mathbf{Z}_2)$.

There are only two cases we must consider: when the adversary places at least one good block in $\mathbf{X}_{g+1}, \ldots, \mathbf{X}_\ell$ and when all of $\mathbf{X}_{g+1}, \ldots, \mathbf{X}_\ell$ are adversarial (so $\mathbf{X}_1, \ldots, \mathbf{X}_g$ is uniform). In the latter case, we have that $\mathbf{Z}_1$ is just the uniform distribution on gn bits and $\mathbf{Z}_2$ is fully controlled by the adversary. For $\mathsf{Ext}(\mathbf{Z}_1, \mathbf{Z}_2)$ to condense then, we would require that no element $h \in \{0,1\}^m$ have too much weight placed on it by the adversary. Recalling that $\mathbf{Z}_1$ is uniform in this case, this statement is equivalent to asking that the sum over all settings z_1 of $\mathbf{Z}_1$ of the number of z_2 such that $\mathsf{Ext}(z_1, z_2) = h$ is not larger than $R = 2^{n_1+n_2-m+O(1)}$. This is precisely our definition of R-output-lightness (see definition VI.10 for a formal definition). With this property, we use claim IV.5 to get that $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq n_1 = \log(R/\varepsilon)$.

In the case that there is at least one good block among $\mathbf{X}_{g+1}, \ldots, \mathbf{X}_\ell$, then we notice that there must be one good block among $\mathbf{X}_1, \ldots, \mathbf{X}_g$ because $g > \ell/2$, so $H_\infty(\mathbf{Z}_1) \geq n$. Without loss of generality, we also assume that we only have one good block $\mathbf{X}_j$ for $j \in \{g+1, \ldots, \ell\}$. Consequently, we can define $\mathbf{A} = \mathbf{Y}_{g+1}, \ldots, \mathbf{Y}_{j-1}$ and $\mathbf{B} = \mathbf{Y}_{j+1}, \ldots \mathbf{Y}_\ell$ so that $\mathbf{Z}_2 = \mathbf{A} \circ \mathbf{Y}_j \circ \mathbf{B}$ where the adversary controls both $\mathbf{A}$ and $\mathbf{B}$ but not $\mathbf{Y}_j$. Since $\mathbf{X}$ is a oNOSF source, $\mathbf{Y}_j$ remains uniform regardless of any fixing of $\mathbf{A}$, so $H_\infty(\mathbf{Y}_j \mid A) = H_\infty(\mathbf{Y}_j) = 5^{\ell-j} \cdot 4\log(gn/\varepsilon)$. In addition, since we chose $\mathbf{A}$ to be logarithmically small in n, the min-entropy chain rule (lemma IV.4) gives us that, with high probability over the fixings of $\mathbf{A}$, the min-entropy of $\mathbf{Z}_1$ is not decreased by too much more than the length of $\mathbf{A}$ which is at most n_2. In particular, for any of these good fixings $a \in \mathsf{Supp}(\mathbf{A})$, we chose k_1 to be such that $H_\infty(\mathbf{Z}_1 \mid \mathbf{A} = a) \geq k_1$. Then if we temporarily make the assumption that $\mathbf{B}$ is uniform, we have that $H_\infty(\mathbf{Z}_2 \mid \mathbf{A} = a) = H_\infty(a, \mathbf{Y}_j, \mathbf{B} \mid \mathbf{A} = a) = \sum_{i=j}^{\ell} 5^{\ell-j} \cdot 4\log(gn/\varepsilon) = (5^{\ell-i+1} - 1)\log(gn/\varepsilon)$. Since we can choose k_2 to be smaller than $H_\infty(\mathbf{Z}_2 \mid \mathbf{A} = a)$, we get that $\mathsf{Ext}(\mathbf{Z})$ is ε-close to $\mathbf{U}_m$. Of course, $\mathbf{B}$ may be adversarially chosen. To take this into account, we use lemma VI.16, which says that if only a few bits of a source are adversarially controlled then we can still condense, to reduce our output entropy by the length of $\mathbf{B}$ and multiplicatively increase our error by $2^{\mathrm{length}(\mathbf{B})}$. Finally, because we constructed $\mathbf{B}$ to have $\sum_{i=j+1}^{\ell} 5^{\ell-j} \cdot 4\log(gn/\varepsilon) = (5^{\ell-i} - 1)\log(gn/\varepsilon)$ bits, it is still short enough in comparison $\mathbf{Y}_j$ to allow us to condense with our desired error.

2) Condensing from uniform (g, ℓ)-oNOSF sources for any g and ℓ: While we can condense from uniform (g, ℓ)-oNOSF sources for $g > \ell/2$ as we saw above (theorem II.4), we know from theorem II.1 that when $g \leq \ell/2$ we cannot condense from uniform (g, ℓ)-oNOSF sources above rate $\frac{1}{\lfloor \ell/g \rfloor}$. Here, we sketch the argument for a matching bound showing that this is indeed tight by generalizing theorem II.4.

Theorem II.5 (theorem VI.3 restated)**.** *For any g, ℓ, ε such that $\lfloor \ell/g \rfloor = r$ and $r < \ell/g$, there exists a condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any uniform (g, ℓ)-oNOSF source $\mathbf{X}$ we have $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq \frac{1}{r} \cdot m - 2(5^{\ell-g} - 1)\log(gn/\varepsilon)$ where $m = r(n - 2(5^{\ell-g} - 1)\log(gn))$.*

Satisfyingly, we need no new tools to construct this condenser. Instead, we use r instances of the condenser from theorem II.4. We will prove this inductively on r, so let us consider the base case of $r = 1$. Notice that $r = 1$ implies that $g > \ell/2$, so we are exactly in a position to use the condenser $\mathsf{Cond}_1 : (\{0,1\}^n)^\ell \to \{0,1\}^{m_1}$ from theorem II.4 without modification. Thus, we define our output block as $\mathbf{O} = \mathbf{O}_1 = \mathsf{Cond}_1(\mathbf{X})$.

To generalize to larger values of r, we perform induction on r and take the inductive hypothesis of $r - 1$ to be true. We consider two cases. Beginning with the case that all of $\mathbf{X}_1, \ldots, \mathbf{X}_g$ are bad, we notice that $\mathbf{X}_{g+1}, \ldots, \mathbf{X}_\ell$ is a uniform $(g, \ell - g)$-oNOSF source with $\left\lfloor \frac{\ell-g}{g} \right\rfloor = r-1$ and $\frac{\ell-g}{g} \neq r-1$. Our inductive hypothesis then gives us $r - 1$ output blocks $\mathbf{O}_2, \ldots, \mathbf{O}_r$ on $(\{0,1\}^{m_r})^{r-1}$ where at least one is condensed. On the other hand, consider when at least one of $\mathbf{X}_1, \ldots, \mathbf{X}_g$ is good and take Cond_1 to be an instance of the condenser from theorem II.4 for $\mathbf{X}$, and define $\mathbf{O}_1$ to be $\mathsf{Cond}_1(\mathbf{X})$ truncated to its first m_r bits. Observe that if $\mathsf{Cond}_1(\mathbf{X})$ succeeds and condenses $\mathbf{X}$ to some min-entropy k source, then $H_\infty(\mathbf{O}_1) \geq k - (m_1 - m_r)$, so we only lose as many bits of entropy in $\mathbf{O}_1$ as we truncate from $\mathsf{Cond}_1(\mathbf{X})$, which we show in lemma VI.17, and $m_1 - m_r$ is still constant in g and ℓ. Then in this case we again get that $\mathbf{O}_1$ must be properly condensed by $2\mathsf{Ext}_1$ being output-light when all of $\mathbf{X}_1, \ldots, \mathbf{X}_g$ are good or by $2\mathsf{Ext}_1$ being a two-source extractor when at least one of $\mathbf{X}_1, \ldots, \mathbf{X}_g$ is good. Thus, if we let our output be $\mathbf{O} = \mathbf{O}_1, \ldots, \mathbf{O}_r$, then at least one block is always condensed in any case.

3) Condensing from logarithmic min-entropy (g, ℓ)-oNOSF sources: We can extend theorem II.4 and theorem II.5 to logarithmic min-entropy oNOSF source by converting a logarithmic min-entropy oNOSF source into a uniform oNOSF source via the following theorem.

Theorem II.6 (theorem VI.2 restated)**.** *For any g, ℓ, ε, there exists a function $f : (\{0,1\}^n)^\ell \to (\{0,1\}^m)^{\ell-1}$ with $m = \frac{k}{8\ell}$ such that for any (g, ℓ, k)-oNOSF source $\mathbf{X}$ with $k \geq 2\log(n/\varepsilon)$ there exists a uniform $(g-1, \ell-1)$-oNOSF source $\mathbf{Y}$ such that $|f(\mathbf{X}) - \mathbf{Y}| \leq \varepsilon$.*

Thus, if we take a (g, ℓ, n, k)-oNOSF source $\mathbf{X}$ such that $g > \ell/2+1$ so $g-1 > (\ell-1)/2$, we can simply apply f from

theorem II.6 to $\mathbf{X}$ and then pass the result to our condenser from theorem II.5 to condense from logarithmic min-entropy oNOSF source.

Theorem II.7 (theorem VI.1 restated)**.** *For all $g, \ell, r \in \mathbb{N}$ and ε such that $\left\lfloor \frac{\ell-1}{g-1} \right\rfloor = r$ and $r < \frac{\ell-1}{g-1}$, there exists a condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any (g, ℓ, n, k)-oNOSF source $\mathbf{X}$ with $k \geq 2\log(n/\varepsilon)$, we have that $H^\varepsilon_\infty(\mathbf{X}) \geq \frac{1}{r} \cdot m - 2(5^{\ell-g} - 1)\log\left(\frac{(g-1)k}{8\ell\varepsilon}\right)$ with $m = r\left(\frac{k}{8\ell} - 2(5^{\ell-g} - 1)\log\left(\frac{(g-1)k}{8\ell}\right)\right)$.*

All that is left then is to show how we convert a low min-entropy oNOSF source to a uniform oNOSF source in theorem II.6. Our method here is based on the somewhere extractor for low-entropy oNOSF source from [1] with two important modifications. First, we use a two-source extractor instead of a seeded extractor which enables us to handle logarithmic min-entropy in the good blocks of a oNOSF source instead of just linear. Second, we require that the output of our function is not just somewhere random, but instead a uniform oNOSF source. To achieve this, we decrease the output length of our two-source extractor (which decreases the block length of our resulting uniform oNOSF source) to show that the good blocks in our resulting source are independent from all adversarial blocks before them.

The construction of f from theorem II.6 is quite straightforward. For every $i \in \{2, \ldots, \ell\}$, we use the same existential two-source extractor from lemma VI.11 that we used in the proof of theorem II.4 to define $2\mathsf{Ext}_i : (\{0,1\}^n)^{i-1} \times \{0,1\}^n \to \{0,1\}^m$ where $m = \frac{k}{8\ell}$ and $k \geq 2\log(n/\varepsilon)$ is the min-entropy requirement of each good block in our (g, ℓ, n, k)-oNOSF source $\mathbf{X} = \mathbf{X}_1, \ldots, \mathbf{X}_\ell$. We then define our $\ell - 1$ output blocks as $\mathbf{O}_i = 2\mathsf{Ext}_i((\mathbf{X}_1, \ldots, \mathbf{X}_{i-1}), \mathbf{X}_i)$, so $f(\mathbf{X}) = \mathbf{O}_2, \ldots, \mathbf{O}_\ell$. Because there are g good blocks in $\mathbf{X}$ at indices $G_1, \ldots, G_g$, we are guaranteed that $\mathbf{O}_{G_2}, \ldots, \mathbf{O}_{G_g}$ are the outputs of a two-source extractor with a good block in each source. The crux of our argument then is to show that $\mathbf{O}_{G_2}, \ldots, \mathbf{O}_{G_g}$ are close to uniform and independent of the adversarial blocks before them. This part of our argument follows that of [1] closely, so we do not expand on it here except to note that shortening the length of our output blocks from $m = O(k)$, not depending on ℓ, in [1] to $m = k/8\ell$ is what allows us to show that good output blocks are uniform and independent of output blocks before them.

III. Open Questions

There are several natural questions that are raised by our work. A few immediate open questions are:

1) Explicitly construct output-light two-source extractor. This would immediately imply explicit condensers for oNOSF sources and uniform aCG sources by lemma VI.12.
2) In our condensing possibility results for uniform oNOSF sources and uniform aCG sources in theorem II.4 and theorem II.5, and our possibility results for logarithmic min-entropy oNOSF sources in theorem II.7, we require $\ell = o(\log(n))$, that our block size to be much smaller than the total number of blocks. It would be interesting to extend these results to smaller block sizes, such as the regime achieved for almost CG sources in [2].
3) Is it possible to improve our condenser for uniform aCG sources in theorem II.4 to have constant entropy gap?
4) Can our condensing impossibility result for CG sources in theorem V.22 be strengthened to close the gap with the results in [2]?

IV. Preliminaries

We will generally denote distributions or sources in a bold font, such as $\mathbf{X}$, and reserve $\mathbf{U}_m$ to be the uniform distribution on m bits. When these sources are actually a sequence of sources, we use subscripts to denote blocks of that source as $\mathbf{X} = \mathbf{X}_1, \ldots, \mathbf{X}_\ell$. In addition, since we often consider binary strings of length n and m, we let $N = 2^n$ and $M = 2^m$. Often it is convenient to consider strings as labels, in which case we use the notation $[N] = \{1, 2, \ldots, N\}$.

A. Basic probability lemmas

Here, we first state a few basic probability facts that will be useful to us throughout. Our first one is a direct reverse Markov style inequality.

Claim IV.1 (Reverse Markov)**.** *Let $\mathbf{X}$ be a random variable taking values in $[0,1]$. Then, for $0 \leq d < \mathbb{E}[X]$, it holds that*

$$\Pr[\mathbf{X} > d] \geq \frac{\mathbb{E}[\mathbf{X}] - d}{1 - d}$$

We will use the following version of the Chernoff bound:

Claim IV.2 (Chernoff Bound)**.** *Let $\mathbf{X}_1, \ldots, \mathbf{X}_n$ be independent random variables taking values in $\{0,1\}$. Let $\mathbf{X} = \sum_i \mathbf{X}_i$. Let $\mu = \mathbb{E}[\mathbf{X}]$. Then, for all $\delta \geq 0$, the following holds:*

$$\Pr[\mathbf{X} \geq (1+\delta)\mu] \leq \exp(-\delta^2\mu/(2+\delta))$$

Several of our impossibility results rely on a simple TV distance bound.

Claim IV.3 (TV distance lower bound)**.** *Let $\mathbf{X} \sim \{0,1\}^n$ and $S \subset \{0,1\}^n$ be such that $\Pr_{x \sim \mathbf{X}}[x \in S] \geq p$. Then, for $0 < \varepsilon < p$, it holds that $H^\varepsilon_\infty(\mathbf{X}) \leq \log\left(\frac{|S|}{p-\varepsilon}\right)$.*

We will utilize the very useful min entropy chain rule in our constructions.

Lemma IV.4 (Min-entropy chain rule)**.** *For any random variables $\mathbf{X} \sim X$ and $\mathbf{Y} \sim Y$ and $\varepsilon > 0$,*

$$\Pr_{y \sim \mathbf{Y}}[H_\infty(\mathbf{X} \mid \mathbf{Y} = y) \geq H_\infty(\mathbf{X}) - \log|\mathsf{Supp}(\mathbf{Y})| - \log(1/\varepsilon)] \geq 1 - \varepsilon.$$

Lastly, we will later utilize a consequence of upper bounds on smooth min-entropy.

Claim IV.5 (Lemma 8.8 from [12])**.** *Let $\mathbf{X} \sim \{0,1\}^n$ be such that $H^\varepsilon_\infty(\mathbf{X}) < k$. Then, there exists $D \subset \mathsf{Supp}(\mathbf{X})$ such that $|D| < 2^k$ and $\Pr[\mathbf{X} \in D] \geq \varepsilon$.*

B. Extractors

Let $\mathbf{A} \approx_\varepsilon \mathbf{B}$ mean that $\mathbf{A}$ and $\mathbf{B}$ are ε close in statistical distance. Recall the definition of a seeded extractor.

Definition IV.6. *A (k,ε)-seeded extractor* $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *satisfies the following: for every (n,k)-source $\mathbf{X}$, and every $\mathbf{Y} = \mathbf{U}_d$,*

$$\mathsf{Ext}(\mathbf{X},\mathbf{Y}) \approx_\varepsilon \mathbf{U}_m.$$

d is called the seed length *of* Ext. Ext *is called strong if*

$$\mathsf{Ext}(\mathbf{X},\mathbf{Y}),\mathbf{Y} \approx_\varepsilon \mathbf{U}_m,\mathbf{Y}.$$

A useful fact about strong seeded extractors that they work even when the seed is not fully uniform. (See for example Lemma 6.4 from [35] for a proof.)

Lemma IV.7. *Let $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ be a strong (k,ε)-seeded extractor. Let $\mathbf{X}$ be a (n,k)-source and let $\mathbf{Y}$ be a $(d, d-\lambda)$-source. Then,*

$$|\mathsf{Ext}(\mathbf{X},\mathbf{Y}),\mathbf{Y} - \mathbf{U}_m,\mathbf{Y}| \le 2^\lambda \varepsilon.$$

We will use the following construction of seeded extractors:

Theorem IV.8 (Theorem 1.5 in [14])**.** *For all constant $\alpha > 0$ and all n,k,ε, there exists an explicit (k,ε)-seeded extractor $\mathsf{sExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ with $d = O(\log(n/\varepsilon))$ and $m \ge (1-\alpha)k$.*

In addition, we will use a generalization of seeded extractors, two-source extractors, that only require the second source to be independent from the first and not necessarily be uniform.

Definition IV.9. *A function $2\mathsf{Ext} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ is a (k_1,k_2,ε)-*two-source extractor *if for every (n_1,k_1)-source $\mathbf{X}_1$ and (n_2,k_2)-source $\mathbf{X}_2$ where $\mathbf{X}_1$ and $\mathbf{X}_2$ are independent of each other, we have*

$$2\mathsf{Ext}(\mathbf{X}_1,\mathbf{X}_2) \approx_\varepsilon \mathbf{U}_m.$$

It is said to be strong in the first argument *if*

$$2\mathsf{Ext}(\mathbf{X}_1,\mathbf{X}_2),\mathbf{X}_1 \approx_\varepsilon \mathbf{U}_m,\mathbf{X}_1.$$

Similarly, one can define $2\mathsf{Ext}$ that is strong in the second argument. If $2\mathsf{Ext}$ is strong in both arguments, we simply say that it is *strong*. We use the fact that inner product function is a good two source extractor:

Theorem IV.10. *[6], [36], [37] Let $\mathbf{X},\mathbf{Y} \sim \{0,1\}^n$ with $H_\infty(\mathbf{X}) = k_1, H_\infty(\mathbf{Y}) = k_2$. Let $m = \frac{n}{r}$ for some $r \in \mathbb{N}$. Let $\mathsf{IP}(x,y) : \{0,1\}^{2n} \to \{0,1\}^m$ be the function that interprets x,y as elements of $\mathbb{F}_{2^m}^r$ and outputs the m bit string corresponding to $x \cdot y$. Then, $|\mathsf{IP}(\mathbf{X},\mathbf{Y}) - \mathbf{U}_m| \le 2^{(n+m-k_1-k_2)/2}$.*

For a proof of the above theorem, see Theorem 2.5.3 in [38].

C. Randomness sources relevant to our work

We now formally introduce the randomness sources that are relevant to our work. We begin with NOSF sources, which have no restrictions on the adversary producing the bad blocks.

Definition IV.11 (NOSF source)**.** *A (g,ℓ,n,k)-*NOSF source $\mathbf{X}$ *with symbols in $\Sigma = \{0,1\}^n$ and length ℓ is over Σ^ℓ, written as $\mathbf{X} = \mathbf{X_1},\ldots,\mathbf{X}_\ell$, and has the following property: There exists a set of good blocks $\mathcal{G} \subseteq [\ell]$ such that $|\mathcal{G}| \ge g$ and the random variables in $\{\mathbf{X}_i\}_{i\in\mathcal{G}}$ are each independently sampled (n,k)-sources. We say that a block $\mathbf{X}_i$ is* good *if $i \in \mathcal{G}$ and* bad *otherwise.*

Note that we have no restrictions on how bad blocks may depend on the good blocks. If $k = n$, we say that $\mathbf{X}$ is a *uniform (g,ℓ,n)-NOSF* source. When n is implicit or not relevant, we simply call $\mathbf{X}$ a uniform (g,ℓ)-NOSF source. Next, we introduce oNOSF sources by restricting the NOSF adversary.

Definition IV.12 (Online NOSF source)**.** *A (g,ℓ,n,k)-*oNOSF source $\mathbf{X}$ *with symbols in $\Sigma = \{0,1\}^n$ and length ℓ is over Σ^ℓ, written as $\mathbf{X} = \mathbf{X_1},\ldots,\mathbf{X}_\ell$, and has the following property: There exists a set of good blocks $\mathcal{G} \subseteq [\ell]$ such that $|\mathcal{G}| \ge g$ and the random variables in $\{\mathbf{X}_i\}_{i\in\mathcal{G}}$ are each independently sampled (n,k)-sources such that $\mathbf{X}_i$ is independent of $\mathbf{X}_1,\ldots,\mathbf{X}_{i-1}$. We say that a block $\mathbf{X}_i$ is* good *if $i \in \mathcal{G}$ and* bad *otherwise.*

Remark IV.13. *Online NOSF sources are also NOSF sources because the adversary in oNOSF sources is strictly weaker than that of NOSF sources.*

These oNOSF sources are special cases of the SHELA sources from [1]. We now introduce SHELA sources in their full generality.

Definition IV.14 (SHELA source [1])**.** *A distribution $\mathbf{X}$ over $(\{0,1\}^n)^\ell$ is a (g,ℓ,n,k)-*Somewhere Honest Entropic Look Ahead (SHELA) source *if there exists a (possibly randomized) adversary $\mathcal{A}$ such that $\mathbf{X}$ is produced by sampling g out of ℓ indices to place independently sampled (n,k)-sources and then placing adversarial blocks in the other $\ell - g$ indices that may depend arbitrarily on any block that comes before it.*

Concretely, there must exist random variables $1 \le \mathbf{I}_1 < \mathbf{I}_2 < \cdots < \mathbf{I}_g \le \ell$ with arbitrary joint distribution, denoting the indices of the independent (n,k)-sources, and g independent (n,k)-sources $\mathbf{Z}_1,\mathbf{Z}_2,\ldots,\mathbf{Z}_g$ such that $\mathbf{X}$ is generated in the following manner:

1) *Sample $(i_1,i_2,\ldots,i_g) \sim (\mathbf{I}_1,\mathbf{I}_2,\ldots,\mathbf{I}_g)$.*
2) *For all $j \in [g]$ set $\mathbf{B}_{i_j} = \mathbf{Z}_j$.*
3) *For all $i \in [\ell] \setminus \{i_1,i_2,\ldots,i_g\}$, the adversary sets $\mathbf{B}_i = \mathcal{A}(\mathbf{B}_1,\ldots,\mathbf{B}_{i-1},i_1,\ldots,i_g\}$.*
4) *Finally, let $\mathbf{X} = (\mathbf{B}_1,\ldots,\mathbf{B}_\ell)$.*

We will generally call the blocks $\mathbf{Z}_1,\ldots,\mathbf{Z}_g$ the "good" blocks and the remaining blocks "bad" blocks.

Similar to NOSF sources, when $k = n$ we will simply say $\mathbf{X}$ is a (g,ℓ,n)-*uniform SHELA* source, and when n is implicit we will simplify further to a uniform (g,ℓ)-SHELA source.

While working over oNOSF sources is easier than working over general SHELA sources, all of our results still apply

to general SHELA sources since SHELA sources are convex combinations of oNOSF sources.

Proposition IV.15. *Every (g, ℓ, n, k)-SHELA source $\mathbf{X}$ is a convex combination of (g, ℓ, n, k)-oNOSF sources.*

Lastly, we define adversarial Chor-Goldreich (CG) sources, which have an adversary like that of oNOSF sources that can depend arbitrarily on past blocks, but the adversary of adversarial CG sources can have some effect on future blocks, unlike that of oNOSF sources.

Definition IV.16 (Adversarial CG source)**.** *A (g, ℓ, n, k)-*aCG source $\mathbf{X}$ *with symbols in $\Sigma = \{0,1\}^n$ and length ℓ is over Σ^ℓ, written as $\mathbf{X} = \mathbf{X_1}, \ldots, \mathbf{X}_\ell$, and has the following property: There exists a set of good blocks $\mathcal{G} \subseteq [\ell]$ such that $|\mathcal{G}| \geq g$ and the random variables in $\{\mathbf{X}_i\}_{i \in \mathcal{G}}$ have the property that for all prefixes $(a_1, \ldots, a_{i-1}) \in (\{0,1\}^n)^{i-1}$,*

$$H_\infty(\mathbf{X}_i \mid \mathbf{X}_1, \ldots, \mathbf{X}_{i-1} = a_1, \ldots, a_{i-1}) \geq k.$$

As before, if $k = n$ then we simply call $\mathbf{X}$ a uniform (g, ℓ, n)-aCG source, and we omit n when it is implicit.

We have introduced all of these definitions since our results resolve open questions for each. The relationship between all these definitions is necessary to clearly see how our lower and upper bounds apply. In line with this, we show an equivalence between uniform oNOSF sources and uniform aCG sources.

Proposition IV.17. *A source $\mathbf{X}$ is a uniform oNOSF source if and only if it is a uniform aCG source.*

Therefore, when we prove a condensing impossibility result by constructing a oNOSF source, that same result applies to NOSF sources and aCG sources sources as well. On the other hand, our condensing possibility results for uniform oNOSF sources also apply to uniform aCG sources, but our results for non-uniform oNOSF sources may not apply to non-uniform aCG sources.

V. Impossibility Results

In this section, we prove condensing impossibility results for uniform NOSF sources and uniform oNOSF sources. First, in section V-A we demonstrate condensing impossibility results for all three classes of sources when $g \leq \ell/2$. Then, in section V-B we show a condensing impossibility result for uniform (g, ℓ)-NOSF sources for arbitrary settings of g and ℓ. Finally, we use a result from section V-A to show the impossibility of condensing from low min-entropy CG sources in section V-C.

A. Impossibility of condensing when $g \leq \ell/2$

We will prove that for $g \leq \ell/2$, it is impossible to condense from uniform (g, ℓ)-oNOSF sources to rate more than $\frac{1}{\lfloor \ell/g \rfloor}$. As we noted in remark IV.13 and proposition IV.17, these results apply to uniform NOSF sources and uniform aCG sources as well.

Theorem V.1. *For all $\varepsilon > 0$, there exists a $\delta > 0$ such that for all $g, \ell \in \mathbb{N}$ with $g \leq \ell/2$ and for all $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, there exists a uniform (g, ℓ)-oNOSF source $\mathbf{X}$ so that $H^\varepsilon_\infty(f(\mathbf{X})) \leq \frac{1}{\lfloor \ell/g \rfloor} \cdot m + \delta$.*

This implies that for the special case when g divides ℓ, any non-trivial condensing is impossible.

Corollary V.2. *For all $\varepsilon > 0, g, \ell \in \mathbb{N}$ with $g \mid \ell$, there exists a $\delta > 0$ such that: for all functions $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, there exists a uniform (g, ℓ)-oNOSF source $\mathbf{X}$ such that $H^\varepsilon_\infty(f(\mathbf{X})) < \frac{g}{\ell} \cdot m + \delta$.*

The proof of theorem V.1 involves two ingredients. First, we show that for the special case of $g = 1$, condensing above rate $\frac{1}{\ell}$ is impossible for uniform $(1, \ell)$-oNOSF sources. Second, we extend these results to uniform (g, ℓ)-oNOSF sources with $g \leq \ell/2$ by showing that if it is impossible to condense from uniform $(1, \ell')$-oNOSF sources, then it is impossible to condense above rate $\frac{1}{\ell'}$ from uniform (g, ℓ)-oNOSF sources when $\frac{g}{\ell} \leq \frac{1}{\ell'}$.

Formally, these two lemmas are as follows:

Lemma V.3. *For all $\varepsilon > 0$, there exists a $\delta > 0$ such that for all functions $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, there exists a uniform $(1, \ell)$-oNOSF source $\mathbf{X}$ so that $H^\varepsilon_\infty(f(\mathbf{X})) < \frac{1}{\ell} \cdot m + \delta$.*

Lemma V.4. *Let $g, \ell, \ell', n', n, m \in \mathbb{N}$ be such that $\ell' \leq \ell$, $\frac{g}{\ell} \leq \frac{1}{\ell'}$, $\lceil \ell/\ell' \rceil \, n < n'$. Let $0 < \varepsilon < 1, \delta > 0$ be such that: for any function $f : (\{0,1\}^{n'})^{\ell'} \to \{0,1\}^m$, there exists a uniform $(1, \ell')$-oNOSF source $\mathbf{Y}$ so that $H^\varepsilon_\infty(f(\mathbf{Y})) < \frac{1}{\ell'} \cdot m + \delta$. Then, for any function $h : (\{0,1\}^n)^\ell \to \{0,1\}^m$, there exists a uniform (g, ℓ)-oNOSF source $\mathbf{X}$ such that $H^\varepsilon_\infty(h(\mathbf{X})) \leq \frac{1}{\ell'} \cdot m + \delta$.*

Our main theorem follows by combining these two lemmas. We defer the proof of lemma V.4 until section V-D. In the next subsubsection, we will focus on proving lemma V.3.

1) Proving main theorem for the case of $g = 1$: We prove this lemma by showing that if one cannot condense from uniform (g, ℓ)-oNOSF sources, then one cannot condense from uniform $(g, \ell + g)$-oNOSF sources.

Lemma V.5. *Let $c_0, c_1, \varepsilon, \delta \in \mathbb{R}$ and $g, n, \ell \in \mathbb{N}$ be such that $g \leq \ell, 0 < c_0 < 1, \varepsilon < c_1 < 1$. Assume that for all $A \in \mathbb{N}$ and function $f : (\{0,1\}^n)^\ell \to [A]$, there exists a uniform (g, ℓ)-oNOSF source (uniform (g, ℓ)-NOSF source, respectively) $\mathbf{X}$ such that $H^\varepsilon_\infty(f(\mathbf{X})) \leq \frac{g}{\ell} \cdot \log(A) + \delta$. Then, for all $M \in \mathbb{N}$ and every function $h : (\{0,1\}^n)^{\ell+g} \to [M]$, there exists a uniform $(g, \ell + g)$-oNOSF source (uniform (g, ℓ)-NOSF source, respectively) $\mathbf{Y}$ such that $H^\varepsilon_\infty(h(\mathbf{Y})) \leq \frac{g}{\ell+g} \cdot m + \delta'$ where $\delta' = \max\left(\log\left(\frac{c_1}{(1-c_1)c_0(c_1-\varepsilon)}\right), \delta + \frac{\log(c_0)g}{\ell}\right)$ and $m = \log(M)$.*

We remark that lemma V.5 paves the way for an inductive argument and we instantiate it to prove lemma V.3.

2) Recursive impossibility lemma: To prove lemma V.5, we find a dominating set in dense bipartite graphs with left degree lower bound. We will use it to construct a uniform oNOSF source that will serve as a counterexample for a candidate condenser.

Lemma V.6 (Small Dominating Set in Bipartite Graph)**.** *Let $c_0 > 0, 0 < c_1 < 1, \delta > 0 \in \mathbb{R}, N, M \in \mathbb{N}$ be arbitrary. Let $G = (U, V, E)$ be a bipartite graph with $|U| = N$, $|V| = M$, such that for all $u \in U : \deg(u) \geq c_0 \cdot M^{\delta}$. Then, there exists $D \subseteq V$ with $|D| \leq \frac{c_1}{(1-c_1)c_0} \cdot M^{1-\delta}$ such that $|Nbr(D)| \geq c_1 N$.*

Using this dominating set lemma, we are able to prove lemma V.5.

B. Impossibility of condensing from uniform (g, ℓ)-NOSF sources

Our main theorem in this subsection is that it is impossible to condense from uniform (g, ℓ)-NOSF sources where $g \geq \frac{\ell}{2} + 1$. Using it and previous results, we obtain impossibility results for all g, ℓ.

Theorem V.7. *There exists a universal constant $c > 0$ such that for all $g, \ell, m, n \in \mathbb{N}$ with $\ell/2 < g < \ell$, there exist $\varepsilon = \left(\frac{1}{c\ell}\right)^{\ell - g}, \delta = c \cdot \ell^2 \log(\ell)$ so that the following holds: for any function $f : (\{0,1\}^n)^{\ell} \to \{0,1\}^m$, there exists a uniform (g, ℓ)-NOSF source $\mathbf{X}$ such that $H^{\varepsilon}_{\infty}(f(\mathbf{X})) \leq \frac{g}{\ell} \cdot m + \delta$.*

We also infer the following useful corollary that shows that uniform (g, ℓ)-NOSF sources cannot be condensed beyond rate $1 - 1/\ell'$ with error $O(1/\ell')$ where ℓ' is the smallest integer such that $g/\ell \leq 1 - 1/\ell'$.

Corollary V.8. *There exists a universal constant c such that the following holds: For all $g, \ell, \ell', m, n \in \mathbb{N}$ where ℓ' is the smallest integer such that $\frac{g}{\ell} \leq \frac{\ell'-1}{\ell'}$, there exist $\varepsilon = \frac{1}{c\ell'}, \delta = c \cdot (\ell')^2 \log(\ell')$ so that the following holds: for all functions $f : (\{0,1\}^n)^{\ell} \to \{0,1\}^m$, there exists a uniform (g, ℓ)-NOSF source $\mathbf{X}$ such that $H^{\varepsilon}_{\infty}(f(\mathbf{X})) \leq \frac{1}{\ell'} \cdot m + \delta$.*

We also get a stronger impossibility result for uniform (g, ℓ)-NOSF sources (compared to condensing impossibility for uniform (g, ℓ)-oNOSF sources proved in theorem V.1) for the regime $g \leq \ell/2$.

Corollary V.9. *There exists a universal constant c such that for all $\ell, g, r, m, n \in \mathbb{N}$ with $\ell \mod g = r$, there exist $\varepsilon = \left(\frac{1}{c(g+r)}\right)^{r}, \delta = c \cdot (r+g)^2 \log(g+r)$ so that the following holds: for all functions $f : (\{0,1\}^n)^{\ell} \to \{0,1\}^m$, there exists a uniform (g, ℓ)-NOSF source $\mathbf{X}$ such that $H^{\varepsilon}_{\infty}(f(\mathbf{X})) \leq \frac{g}{\ell} \cdot m + \delta$.*

We obtain impossibility result for all uniform $(ag, a\ell)$-NOSF sources where g and ℓ are constants and $a \in \mathbb{N}$ is arbitrarily large.

Corollary V.10. *For all fixed $g, \ell \in \mathbb{N}$, there exist constants $\varepsilon, \delta > 0$ so that the following holds: for all $a, m, n \in \mathbb{N}$ and for all functions $f : (\{0,1\}^n)^{a\ell} \to \{0,1\}^m$, there exists a uniform $(ag, a\ell)$-NOSF source $\mathbf{X}$ such that $H^{\varepsilon}_{\infty}(f(\mathbf{X})) \leq \frac{g}{\ell} \cdot m + \delta$.*

We also record the special case of when the total number of blocks ℓ is a constant.

Corollary V.11. *For all fixed $g, \ell \in \mathbb{N}$, there exist constants $\varepsilon, \delta > 0$ so that the following holds: For all $m, n \in \mathbb{N}$ and for all functions $f : (\{0,1\}^n)^{\ell} \to \{0,1\}^m$, there exists a uniform (g, ℓ)-NOSF source $\mathbf{X}$ such that $H^{\varepsilon}_{\infty}(f(\mathbf{X})) \leq \frac{g}{\ell} \cdot m + \delta$.*

We prove our main theorem using the following general version of the theorem which we denote as our main lemma:

Lemma V.12. *There exists universal constants c such that for all $c_0 > 0, g, \ell, M, n \in \mathbb{N}$ with $\ell/2 < g < \ell$, and for all $A \subset (\{0,1\}^n)^{\ell}$ with $|A| = c_0(2^n)^{\ell}$, the following holds: for any function $f : (\{0,1\}^n)^{\ell} \to [M]$, there exists a uniform (g, ℓ)-NOSF source $\mathbf{X}$, $A' \subset A \cap \mathrm{Supp}(\mathbf{X})$ and $D \subset [M]$ such that $f(A') \subset D$ where $|A'| \geq c_0 \cdot \left(\frac{1}{c\ell}\right)^{\ell - g} \cdot N^g$, and $|D| \leq (c\ell)^{\ell^2} \cdot \left(\frac{2}{c_0}\right)^{g} \cdot M^{g/\ell}$.*

Using this main lemma, the theorem follows.

To prove our corollary regarding condensing uniform (g, ℓ)-NOSF sources where $\frac{g}{\ell}$ is a large constant, we will use the following lemma:

Lemma V.13. *Let $g, \ell, \ell', n', n, m \in \mathbb{N}$ be such that $\frac{g}{\ell} \leq \frac{\ell'-1}{\ell'}, \lceil \ell/\ell' \rceil n < n'$. Let $0 < \varepsilon < 1, \delta > 0$ be such that: for any function $f : (\{0,1\}^{n'})^{\ell'} \to \{0,1\}^m$, there exists a uniform $(\ell' - 1, \ell')$-NOSF source $\mathbf{Y}$ so that $H^{\varepsilon}_{\infty}(f(\mathbf{Y})) \leq \frac{\ell'-1}{\ell'} \cdot m + \delta$. Then, for any function $h : (\{0,1\}^n)^{\ell} \to \{0,1\}^m$, there exists a uniform (g, ℓ)-NOSF source $\mathbf{X}$ such that $H^{\varepsilon}_{\infty}(h(\mathbf{X})) \leq \frac{\ell'-1}{\ell'} \cdot m + \delta$.*

We will prove this lemma in a later in section V-D. Using it, the corollary immediately follows.

To prove our corollary regarding condensing uniform $(ag, a\ell)$-NOSF sources where g and ℓ are constants and a is arbitrary, we will use the following lemma that allows us to generalize the impossibility result:

Lemma V.14. *Let $g, \ell \in \mathbb{N}$ and $0 < \varepsilon < 1, \delta > 0$ be such that for all $n, m \in \mathbb{N}$ and all functions $f : (\{0,1\}^n)^{\ell} \to \{0,1\}^m$, there exists an uniform (g, ℓ)-NOSF source $\mathbf{X}$ such that $H^{\varepsilon}_{\infty}(f(\mathbf{X})) \leq \frac{g}{\ell} \cdot m + \delta$. Then, for all $a, n, m \in \mathbb{N}$ and all functions $f : (\{0,1\}^n)^{a\ell} \to \{0,1\}^m$, there exists an uniform $(ag, a\ell)$-NOSF source $\mathbf{X}$ such that $H^{\varepsilon}_{\infty}(f(\mathbf{X})) \leq \frac{g}{\ell} \cdot m + \delta$.*

We will also prove this lemma in section V-D. Using it, the corollary immediately follows.

1) Proving the main lemma: Here, we will prove lemma V.12. We first introduce some helpful notation for this part. For an edge $e \in E$, let $\chi(e)$ denote the color of e in H. For a vertex $x \in H$, let

$$\mathrm{Nbr}_H(x) = \{y \in H : (x, y) \in E\}.$$

Similarly, for a vertex $x \in H$, and color $\gamma \in [M]$, let

$$\mathrm{Nbr}_H(x, \gamma) = \{y \in H : (x, y) \in E \text{ and } \chi(x, y) = \gamma\}.$$

To prove the main lemma, we will utilize the following special case of the main lemma, corresponding to the case of $g = \ell - 1$, that we prove later:

Lemma V.15. *There exists a universal constant $c > 0$ such that for all $M, n, \ell \geq 3 \in \mathbb{N}$, and $A \subset (\{0,1\}^n)^\ell$ with $|A| = c_0(2^n)^\ell$, the following holds: for any function $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, there exists a uniform $(\ell-1,\ell)$-NOSF source $\mathbf{X}$, $A' \subset A \cap \mathrm{Supp}(\mathbf{X})$ with $|A'| \geq \frac{1}{c} \cdot \frac{c_0}{\ell} \cdot N^{\ell-1}$, and $D \subset [M]$ with $|D| \leq c \cdot \frac{1}{\ell^2} \cdot \left(\frac{2}{c_0}\right)^{\ell-2} \cdot M^{(\ell-1)/\ell}$ such that $f(A') \subset D$.*

The main lemma follows by an inductive argument where the special case above is the base case.

Remark V.16. *In proof of lemma V.12, one can use $g = \ell$ as the base case as well. However, for clarity's sake we use $g = \ell - 1$ as the base case. For first time readers, it will be helpful to first read the direct non-inductive proof of lemma V.15 presented in section V-B2 before reading the proof of lemma V.12 as both these proofs share a lot of ideas.*

2) Proving the main lemma for $g = \ell-1$: We will prove our main lemma for the case of $g = \ell - 1$ using a color covering lemma for dense t-partite t-uniform hypergraphs colored in some special way:

Lemma V.17 (Small Color Covering for Hypergraphs)**.** *Let $0 < c_0 \leq 1, 0 < c_1, 0 < \varepsilon < c_0$ be arbitrary. Let $H = (V_1, \ldots, V_t, E)$ be a t-uniform t-partite hypergraph with $V_1 = \cdots = V_t = [N], |E| = c_0 N^t$. Let the edges of H be colored in one of M colors so that for every position $p \in [T]$, and every $(t-1)$ tuples: $(v_1, \ldots, v_{p_1}, v_{p+1}, \ldots, v_t) \in [N]^{t-1}$, the number of distinct colored edges as entries position p vary is $\leq c_1 M^\delta$. Formally, $|\chi(v_1, \ldots, v_{p-1}, y, v_{p+1}, \ldots, v_t) : y \in [N]| \leq c_1 M^\delta$. Then, there exists $D \subseteq [M]$ such that $|D| \leq \frac{\varepsilon c_1 (c_1+1)^{t(t+1)/2-1}}{(c_0-\varepsilon)^t} \cdot M^{t\delta}$ and at least εN^t edges in H are colored in one of the colors from D.*

We prove this color covering lemma later. Using it, we are able to prove our main lemma for the case of $g = \ell - 1$.

3) Finding a small color covering in locally-light hypergraphs: We consider dense t-uniform t-partite hypergraphs where all edges are colored and the hypergraph satisfies a "locally-light" condition: all $t-1$-tuples are adjacent to a small number of colors. The covering lemma finds small set of colors that covers constant fraction of edges in the hypergraph. We do this by finding a popular color in such a hypergraph.

Lemma V.18 (Popular Color in Locally-Light Hypergraphs)**.** *Let $0 < c_0 \leq 1, 0 < c_1$ be arbitrary. Let $t \geq 2 \in \mathbb{N}$. Let $H = (V_1, \ldots, V_t, E)$ be a t-uniform t-partite hypergraph with $|V_1| = \cdots = |V_t| = N, |E| = c_0 N^t$. Let the edges of H be colored in one of M colors so that for every position $p \in [T]$, and every $(t-1)$ tuples: $(v_1, \ldots, v_{p_1}, v_{p+1}, \ldots, v_t) \in [N]^{t-1}$, the number of distinct colored edges as entries position p vary is $\leq c_1 M^\delta$. Formally, $|\chi(v_1, \ldots, v_{p-1}, y, v_{p+1}, \ldots, v_t) : y \in [N]| \leq c_1 M^\delta$. Then, there exists a color $\gamma \in [M]$ such that at least $\frac{c_0^t}{c_1 (c_1+1)^{t(t+1)/2-1}} \cdot N^t / M^{t\delta}$ edges in H are colored with color γ.*

Using this lemma, our color covering lemma for hypergraph follows by repeatedly finding such popular colors.

4) Finding a popular color in locally-light hypergraphs: For the base case, we find such a popular color in graphs:

Lemma V.19 (Popular Color in Locally-Light Graphs)**.** *Let $0 < c_0 \leq 1, 0 < c_1$ be arbitrary. Let $H = (U, V, E)$ be a bipartite graph with $|U| = |V| = N, |E| = c_0 N^2$. Let the edges of H be colored in one of M colors so that for every vertex $x \in H$, the number of distinct colored edges incident on x is $\leq c_1 M^\delta$. Then, there exists a color $\gamma \in [M]$ such that at least $\frac{c_0^2}{(c_1+1)^2 c_1} \cdot N^2 / M^{2\delta}$ edges in H are colored with color γ.*

Using this, we inductively find a popular color in locally-light hypergraphs.

Finally, we directly argue a popular color exists in dense locally-light bipartite graphs.

C. Impossibility of condensing from CG sources

We prove two impossibility results regarding impossibility of condensing from (ℓ,ℓ)-aCG sources. Our first result theorem V.21 states that any candidate condenser cannot decrease the entropy gap present in the blocks of CG sources. Our second result in contrast, states that when blocks have linear entropy, then condenser cannot condense beyond rate $1/2$. The latter result is much stronger than the former in regimes where m is comparatively larger than n (say $m = O(n\ell)$ and $\ell = \omega(1)$).

1) Impossibility of non-trivial condensing beyond min-entropy gap: We will use the fact that it is impossible to condense from general (n,k)-sources.

Lemma V.20. *For all $n, k, m \in \mathbb{N}$ and $\varepsilon > 0$ the following holds: For all functions $f : \{0,1\}^n \to \{0,1\}^m$, there exists an (n,k) source $\mathbf{X}$ such that $H_\infty^\varepsilon(f(\mathbf{X})) \leq m - (n-k) + \log(1/(1-\varepsilon)) - \max(m-n, 0)$.*

We believe a result of this form is well-known but we were unable to find a good reference. Thus, for the sake of completeness, we prove this lemma at the end of this subsection. Using this, we prove our impossibility result for (ℓ,ℓ)-aCG sources.

Theorem V.21. *For all $0 < \varepsilon < 1, \Delta$ and $\ell, m, n \in \mathbb{N}$, the following holds: for every function $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, there exists a (ℓ,ℓ)-aCG source $\mathbf{X}$ where the good blocks have min-entropy at least $n - \Delta - \log(\ell/\varepsilon) - O(1)$ conditioned on all fixings of previous blocks and $H_\infty^\varepsilon(f(\mathbf{X})) \leq m - \Delta + \log(2/(2-\varepsilon)) - \max(m - \ell n, 0)$.*

Lastly, we proved that no non-trivial condensers exist for arbitrary (n,k)-sources.

2) Impossibility of condensing beyond rate $1/2$: Using condensing impossibility result for uniform $(1,2)$-oNOSF sources, we prove a condensing impossibility result for (ℓ,ℓ)-aCG source (which are just CG sources, with no adversarial blocks) where the good blocks have min-entropy at least $O(n/\ell)$ conditioned on every fixing of previous blocks.

Theorem V.22. *For all $0 < \varepsilon < 1$ there exists a $\delta > 0$ such that the following holds: for every function $f : (\{0,1\}^n)^\ell \to \{0,1\}^m$, there exists a (ℓ, ℓ)-aCG source $\mathbf{X}$ where the good blocks have min-entropy at least $\frac{n - \ell \log(2\ell/\varepsilon)}{\ell+1}$ conditioned on all fixings of previous blocks and $H^\varepsilon_\infty(f(\mathbf{X})) \leq \frac{1}{2} \cdot m + \delta$.*

Lastly we prove our claim that most fixings of previous blocks preserve min-entropy in the later block.

D. Deferred proofs of helpful lemmas

The remaining deferred proofs of lemmas follow from the following results, proofs of which we include in the full version of our paper.

Lemma V.23. *Let $g, \ell, n, g', \ell', n', m \in \mathbb{N}$ be such that $g \leq a \cdot g' + \max(b - (\ell' - g'), 0), (a+1)n \leq n'$ where $a, b \in \mathbb{N}$ are unique integers such that $\ell = a \cdot \ell' + b$ where $0 \leq b < \ell'$. Let $0 < \varepsilon < 1, \delta > 0$ be such that: for any function $f : (\{0,1\}^{n'})^{\ell'} \to \{0,1\}^m$, there exists a uniform (g', ℓ')-oNOSF source (uniform (g', ℓ')-NOSF source, respectively) $\mathbf{Y}$ so that $H^\varepsilon_\infty(f(\mathbf{Y})) \leq \frac{g'}{\ell'} \cdot m + \delta$. Then, for any function $h : (\{0,1\}^n)^\ell \to \{0,1\}^m$, there exists a uniform (g, ℓ)-oNOSF source (uniform (g, ℓ)-NOSF source, respectively) $\mathbf{X}$ such that $H^\varepsilon_\infty(h(\mathbf{X})) \leq \frac{g'}{\ell'} \cdot m + \delta$.*

The deferred proofs of several lemmas follow from this result.

VI. Condensers for oNOSF Sources

We will prove the following main theorem regarding condensing from oNOSF sources in this section:

Theorem VI.1. *For all $g, \ell, r \in \mathbb{N}, \varepsilon > 0$ such that $\left\lfloor \frac{\ell-1}{g-1} \right\rfloor = r$ and $r < \frac{\ell-1}{g-1}$, there exists a condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any (g, ℓ, n, k)-oNOSF source $\mathbf{X}$ with $k \geq 2\log(gn/\varepsilon)$, we have that $H^\varepsilon_\infty(\mathbf{X}) \geq \frac{1}{r} \cdot m - 2(5^{\ell-g} - 1)\log\left(\frac{(g-1)k}{8\ell\varepsilon}\right)$ with $m = r\left(\frac{k}{8\ell} - 2(5^{\ell-g} - 1)\log\left(\frac{(g-1)k}{8\ell}\right)\right)$.*

This result is tight up to lower order terms as it asymptotically matches the impossibility results of theorem V.1.

We prove this theorem in two steps. First, we show how to transform oNOSF sources to uniform oNOSF sources:

Theorem VI.2. *For any g, ℓ, ε, there exists a function $f : (\{0,1\}^n)^\ell \to (\{0,1\}^m)^{\ell-1}$ with $m = \frac{k}{8\ell}$ such that for any (g, ℓ, k)-oNOSF source $\mathbf{X}$ with $k \geq 2\log(gn/\varepsilon)$ there exists a uniform $(g-1, \ell-1)$-oNOSF source $\mathbf{Y}$ such that $|f(\mathbf{X}) - \mathbf{Y}| \leq \varepsilon$.*

Second, we show how to condense from uniform oNOSF sources.

Theorem VI.3. *For any g, ℓ, ε such that $\lfloor \ell/g \rfloor = r$ and $r < \ell/g$, there exists a condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any uniform (g, ℓ)-oNOSF source $\mathbf{X}$ we have $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq \frac{1}{r} \cdot m - 2(5^{\ell-g} - 1)\log(gn/\varepsilon)$ where $m = r(n - 2(5^{\ell-g} - 1)\log(gn))$.*

Using these two ingredients, our main theorem follows.

A. Transforming low entropy oNOSF sources to uniform oNOSF sources

We will prove theorem VI.2 in this subsection. We will use the fact that a random function is a very good two source extractor.

Lemma VI.4. *Let $n_1, n_2, k_1, k_2, m, \varepsilon$ be such that $k_1 \leq n_1, k_2 \leq n_2, m = k_1 + k_2 - 2\log(1/\varepsilon) - O(1)$, $k_2 \geq \log(n_1 - k_1) + 2\log(1/\varepsilon) + O(1)$, and $k_1 \geq \log(n_2 - k_2) + 2\log(1/\varepsilon) + O(1)$. Then, a random function $\mathsf{Ext} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ is a (k_1, k_2, ε)-two source extractor with probability $1 - o(1)$.*

We defer proof of this to section VI-C. Using this, we will prove our main lemma:

Lemma VI.5. *Let $g, \ell, m, n \in \mathbb{N}$ and $k, k_1, k_2, \varepsilon > 0$ be such that $k \geq k_1 + \ell m + \log(1/\varepsilon), k \geq k_2$. Suppose there exists a (k_1, k_2, ε)-two-source extractor $2\mathsf{Ext} : \{0,1\}^{(\ell-1)\cdot n} \times \{0,1\}^n \to \{0,1\}^m$. Then we can construct a function $f : (\{0,1\}^n)^\ell \to (\{0,1\}^m)^{\ell-1}$ such that for any (g, ℓ, n, k)-oNOSF source $\mathbf{X}$, there exists a uniform $(g-1, \ell-1)$-oNOSF source $\mathbf{Y}$ such that $|f(\mathbf{X}) - \mathbf{Y}| \leq 2(g-1)\varepsilon$.*

Using this main lemma, theorem VI.2 follows.

One can get an explicit version of this transformation, with polynomial error by using an explicit two-source extractor, such as the one from [26].

We now focus on proving lemma VI.5. We extend an argument for a somewhere extractor for low entropy oNOSF sources from [1]. We do this by using a two source extractor instead of a seeded extractor in their construction.

To achieve this result, we use the notion of *average conditional min-entropy* and use some known results about two-source extractors.

Definition VI.6. *For any two distributions $\mathbf{X}$ and $\mathbf{W}$, define the* average conditional min-entropy *of $\mathbf{X}$ given $\mathbf{W}$ as*

$$\widetilde{H}_\infty(\mathbf{X} \mid \mathbf{W}) = -\log\left(\mathop{\mathbb{E}}_{w \sim \mathbf{W}}\left[\max_{x \in \mathsf{Supp}(\mathbf{X})} \Pr[\mathbf{X} = x \mid \mathbf{W} = w]\right]\right).$$

We use this notion of average conditional min-entropy to define notions of average-case strongness in two-source extractors:

Definition VI.7. *We say that $2\mathsf{Ext}$ is* average-case *strong if*

$$2\mathsf{Ext}(\mathbf{X}_1, \mathbf{X}_2), \mathbf{W} \approx_\varepsilon \mathbf{U}_m, \mathbf{W}$$

for every $\mathbf{X}_1$ and $\mathbf{W}$ such that $\widetilde{H}_\infty(\mathbf{X}_1 \mid \mathbf{W}) \geq k_1$ with $\mathbf{X}_2$ independent of $\mathbf{X}_1$ and $\mathbf{W}$.

One benefit of the average conditional min-entropy in comparison to conditional min-entropy is that the chain rule is simpler:

Lemma VI.8. *[39] Let $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ be distributions such that $\mathsf{Supp}(\mathbf{B}) \leq 2^\lambda$. Then $\widetilde{H}_\infty(\mathbf{A} \mid \mathbf{B}, \mathbf{C}) \geq \widetilde{H}_\infty(\mathbf{A}, \mathbf{B} \mid \mathbf{C}) - \lambda \geq \widetilde{H}_\infty(\mathbf{A} \mid \mathbf{C}) - \lambda$.*

In addition, Lemma 2.3 of [39] shows that two-source extractors are average-case-two-source extractors with similar parameters.

Lemma VI.9. *[39] For any $\eta > 0$, if $2\mathsf{Ext}$ is a (k_1, k_2, ε)-two-source extractor, then $2\mathsf{Ext}$ is a $(k_1 + \log(1/\eta), k_2, \varepsilon + \eta))$-average-case-two-source extractor.*

We will use it to prove our main theorem in which we provide a general transformation of low min-entropy oNOSF sources to uniform oNOSF sources given a two-source extractor. This transformation is based on a similar transformation in [1].

B. Condensing from oNOSF sources using output-light two source extractors

In this subsection, we will prove theorem VI.3. To obtain the condenser, we will utilize two-source extractors which have an additional property that we call output-light.

Formally, we define output-light two source extractors as follows:

Definition VI.10 (Output-light Two Source Extractor)**.** *Let $\mathsf{Ext} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ be a (k_1, k_2, ε)-two source extractor. Then, Ext is R-output-light if for every $z \in \{0,1\}^m$, it holds that $|\{x \in \{0,1\}^{n_1} : \exists y \in \{0,1\}^{n_2} (\mathsf{Ext}(x, y) = z)\}| \leq R$.*

We will show a random function is a output-light two source extractor with strong parameters and we will use it with the following parameters:

Lemma VI.11. *Let $0 < \delta < 1, C \geq 4$ be arbitrary constants. Let n_1, k_1, n_2, k_2, m, $\varepsilon_{\mathsf{Ext}}, \varepsilon$ be such that n_1 is arbitrary, $n_2 = C(\log(n_1) + \log(1/\varepsilon)), k_1 = \delta n_1 - 2n_2, k_2 = 4(\log(n_1) + \log(1/\varepsilon)), m = k_1 - 2n_2, \varepsilon_{\mathsf{Ext}} = 2^{-k_2/4}$ (note that if k_2 is larger than the minimum requirement, then $\varepsilon_{\mathsf{Ext}}$ gets proportionally smaller). Then, a random function $\mathsf{Ext} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ is an R-output-light $(k_1, k_2, \varepsilon_{\mathsf{Ext}})$ two-source-extractor where $R = 2^{n_1+n_2-m+O(1)}$.*

We defer proof of their existence in section VI-C. Using such an extractor, we will prove the following general condensing result:

Lemma VI.12. *Let $g, \ell, r, n, \varepsilon$ be such that $r = \lfloor \ell/g \rfloor$ and $r < \ell/g$. Assume that for $c \in \{1, \ldots, r\}$, there exists an R_c-output-light $(k_{1,c}, k_{2,c}, \varepsilon_{\mathsf{Ext}_c})$-two-source extractor $2\mathsf{Ext}_c : \{0,1\}^{n_{1,c}} \times \{0,1\}^{n_{2,c}} \to \{0,1\}^{m_c}$ where $n_{1,c} = gn$, $n_{2,c} = \frac{5^{\ell-cg}-1}{4} \cdot 4\log(gn/\varepsilon)$, $k_{1,c} = n - 2n_{2,c}$, $k_{2,c} = 4(\log(gn) + \log(1/\varepsilon))$, $m_c = n - 2n_{2,c}, \varepsilon_{\mathsf{Ext}_c} = 2^{-k_{2,c}/4}$ and $\log(R_c/\varepsilon) \leq n_{1,c} + 2n_{2,c} - m_c$. Then there exists a condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any uniform (g, ℓ)-oNOSF source $\mathbf{X}$, we have $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq \frac{1}{r} \cdot m - 2n_{2,1}$ here $m = r \cdot m_r$.*

Using this main lemma, the theorem follows. Before we prove this main lemma, we prove theorem VI.3 for the special case when $g > \ell/2$.

Theorem VI.13. *For all g, ℓ, ε such that $g > \ell/2$, there exists a condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any uniform (g, ℓ)-oNOSF source $\mathbf{X}$, $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq m - (5^{\ell-g} - 3)(\log(gn) + \log(1/\varepsilon))$ where $m = n - 2(5^{\ell-g} - 1)\log(gn)$.*

As an application of this theorem, we construct a condenser from a low min-entropy (g, ℓ)-oNOSF source with $g > \ell/2 + 1$. We do this by composing our transformation from theorem VI.2 with the condenser from theorem VI.13.

Corollary VI.14. *For all g, ℓ, ε such that $g > \ell/2 + 1$, there exists a condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any (g, ℓ, n, k)-oNOSF source $\mathbf{X}$ with $k \geq 2\log(n)$, we have $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq m - (5^{\ell-g} - 3)\log\left(\frac{(g-1)k}{8\ell\varepsilon}\right)$ where $m = \frac{k}{8\ell} - 2(5^{\ell-g} - 1)\log\left(\frac{(g-1)k}{8\ell}\right)$.*

1) Condensing from (g, ℓ)-oNOSF sources with $g > \ell/2$: We will prove theorem VI.13 that allows us to condense from uniform (g, ℓ)-oNOSF sources when $g > \ell/2$. This theorem allows us to condense to almost full entropy.

We will prove this theorem using the following general lemma:

Lemma VI.15. *Assume that for some g, n, ε there exists an R-output-light $(k_1, k_2, \varepsilon_{\mathsf{Ext}})$-two-source-extractor $\mathsf{Ext} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ where $n_1 = gn, n_2 = \frac{5^{\ell-g}-1}{4} \cdot 4\log(gn/\varepsilon), k_1 = n - 2n_2, k_2 = 4\log(gn/\varepsilon), m = n - 2n_2, \varepsilon_{\mathsf{Ext}} = 2^{-k_2/4}$ (notice that we require that if k_2 supplied is larger, then $\varepsilon_{\mathsf{Ext}}$ gets proportionally smaller). Then, there exists a condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any uniform (g, ℓ)-oNOSF source $\mathbf{X}$ with $g > \ell/2$, $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) = \min(m - n_2, n_1 - \log(R/\varepsilon))$.*

Using this, our theorem directly follows.

Towards proving our general lemma, we show that for any flat distribution $\mathbf{X}$ over n bits, if a function f condenses from $\mathbf{X}$, then f also condenses (with a slight loss in parameters) from a distribution $\mathbf{X}'$ which is the same as the distribution $\mathbf{X}$ on most output bits but some output bits are arbitrarily controlled by an adversary. We note that a lemma similar in spirit to this one was shown as Lemma 28 in [9].

Lemma VI.16. *Let $\mathbf{X} \sim \{0,1\}^n$ be an arbitrary flat distribution and let $\mathsf{Cond} : \{0,1\}^n \to \{0,1\}^m$ be such that $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) = k$. Let $G \subset [n]$ with $|G| = n - b$. Let $\mathbf{X}_G \sim \{0,1\}^{n-b}$ be the projection of $\mathbf{X}$ onto G. Let $\mathbf{X}' \sim \{0,1\}^n$ be the distribution where the output bits defined by G equal $\mathbf{X}_G$ and remaining b bits are deterministic functions of the $n - b$ bits defined by G under the restriction that $\mathrm{Supp}(\mathbf{X}') \subset \mathrm{Supp}(\mathbf{X})$. Then, $H^{\varepsilon'}_\infty(f(\mathbf{X}')) \geq k - b$ where $\varepsilon' = \varepsilon \cdot 2^b$.*

We will prove this result later. Using this result, we use output-light two-source-extractor to prove our general lemma.

We finally prove our useful lemma that states a condenser for a distribution $\mathbf{X}$ still condenses from a tampered version of $\mathbf{X}$ where some output bits are controlled by an adversary.

2) Condensing from uniform oNOSF sources in all regimes: We finally prove our main lemma of the section - lemma VI.12. We will use the following simple claim that guarantees projections of high-entropy distributions have high-entropy.

Lemma VI.17. *Let $\mathbf{X}$ be an arbitrary (n,k)-source and $\pi : \{0,1\}^n \to \{0,1\}^{n-d}$ be a projection onto $n-d$ bits of $\mathbf{X}$ (i.e., removes d bits of $\mathbf{X}$). Then $\pi(\mathbf{X})$ is a $(n-d, k-d)$-source.*

We are finally ready to prove the main lemma. The proof of this main lemma uses a similar strategy as in lemma VI.15.

C. Existence of output-light two-source extractors

In this subsection, we show a random function is an output-light two-source extractor. Towards showing output lightness, we introduce a related notion, of R-invertible functions.

Definition VI.18 (R-invertible function)**.** *A function $f : \{0,1\}^n \to \{0,1\}^m$ is R-invertible if for every $z \in \{0,1\}^m$, it holds that $|\{x \in \{0,1\}^n : f(x) = z\}| \leq R$.*

We record the observation that R-invertible functions are also R-output light.

Observation VI.19. *Let $\mathsf{Ext} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ be a (k_1, k_2, ε)-two source extractor. If Ext is R-invertible, then Ext is R-output-light.*

We now show that a random function is optimally invertible, hence concluding a random function is also output light.

Lemma VI.20. *Let $f : \{0,1\}^n \to \{0,1\}^m$ be a random function where $m \leq n - \log n$. Then, with probability $1 - o(1)$, f will be 2^{n-m+c}-invertible where c is a universal constant.*

ACKNOWLEDGEMENTS

We want to thank Ran Raz for illuminating discussions.

REFERENCES

[1] D. Aggarwal, M. Obremski, J. Ribeiro, L. Siniscalchi, and I. Visconti, "How to Extract Useful Randomness from Unreliable Sources," en, in *Advances in Cryptology – EUROCRYPT 2020*, A. Canteaut and Y. Ishai, Eds., ser. Lecture Notes in Computer Science, Cham: Springer International Publishing, 2020, pp. 343–372, ISBN: 978-3-030-45721-1. DOI: 10.1007/978-3-030-45721-1_13.

[2] D. Doron, D. Moshkovitz, J. Oh, and D. Zuckerman, "Almost Chor-Goldreich Sources and Adversarial Random Walks," in *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, ser. STOC 2023, New York, NY, USA: Association for Computing Machinery, Jun. 2023, pp. 1–9, ISBN: 978-1-4503-9913-5. DOI: 10.1145/3564246.3585134. [Online]. Available: https://doi.org/10.1145/3564246.3585134 (visited on 06/01/2023).

[3] Y. Dodis, S. J. Ong, M. Prabhakaran, and A. Sahai, "On the (im)possibility of cryptography with imperfect randomness," in *45th Annual IEEE Symposium on Foundations of Computer Science*, ISSN: 0272-5428, Oct. 2004, pp. 196–205. DOI: 10.1109/FOCS.2004.44. [Online]. Available: https://ieeexplore.ieee.org/document/1366239 (visited on 11/05/2023).

[4] D. Zuckerman, "General weak random sources," in *Proceedings of the 31st Annual Symposium on Foundations of Computer Science*, ser. SFCS '90, USA: IEEE Computer Society, Oct. 1990, 534–543 vol.2, ISBN: 978-0-8186-2082-9. DOI: 10.1109/FSCS.1990.89574. [Online]. Available: https://doi.org/10.1109/FSCS.1990.89574 (visited on 11/05/2023).

[5] M. Santha and U. V. Vazirani, "Generating quasi-random sequences from semi-random sources," *Journal of Computer and System Sciences*, vol. 33, no. 1, pp. 75–87, Aug. 1986, ISSN: 0022-0000. DOI: 10.1016/0022-0000(86)90044-9. [Online]. Available: https://doi.org/10.1016/0022-0000(86)90044-9 (visited on 11/05/2023).

[6] B. Chor and O. Goldreich, "Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 230–261, Apr. 1988, Publisher: Society for Industrial and Applied Mathematics, ISSN: 0097-5397. DOI: 10.1137/0217015. [Online]. Available: https://epubs.siam.org/doi/abs/10.1137/0217015 (visited on 11/05/2023).

[7] O. Reingold, S. Vadhan, and A. Wigderson, "A Note on Extracting Randomness from Santha-Vazirani Sources," en, Tech. Rep., 2004.

[8] M. Ball, O. Goldreich, and T. Malkin, "Randomness Extraction from Somewhat Dependent Sources," in *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, M. Braverman, Ed., ser. Leibniz International Proceedings in Informatics (LIPIcs), ISSN: 1868-8969, vol. 215, Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022, 12:1–12:14, ISBN: 978-3-95977-217-4. DOI: 10.4230/LIPIcs.ITCS.2022.12. [Online]. Available: https://drops.dagstuhl.de/opus/volltexte/2022/15608 (visited on 11/05/2023).

[9] A. Ben-Aroya, G. Cohen, D. Doron, and A. Ta-Shma, "Two-Source Condensers with Low Error and Small Entropy Gap via Entropy-Resilient Functions," en, in *DROPS-IDN/v2/document/10.4230/LIPIcs.APPROX-RANDOM.2019.43*, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2019. DOI: 10.4230/LIPIcs.APPROX-RANDOM.2019.43. [Online]. Available: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.APPROX-RANDOM.2019.43 (visited on 04/02/2024).

[10] J. Radhakrishnan and A. Ta-Shma, "Bounds for Dispersers, Extractors, and Depth-Two Superconcentrators," *SIAM Journal on Discrete Mathematics*, vol. 13,

no. 1, pp. 2–24, Jan. 2000, Publisher: Society for Industrial and Applied Mathematics, ISSN: 0895-4801. DOI: 10.1137/S0895480197329508. [Online]. Available: https://epubs.siam.org/doi/10.1137/S0895480197329508 (visited on 08/29/2023).

[11] O. Reingold, R. Shaltiel, and A. Wigderson, "Extracting Randomness via Repeated Condensing," *SIAM Journal on Computing*, vol. 35, no. 5, pp. 1185–1209, Jan. 2006, Publisher: Society for Industrial and Applied Mathematics, ISSN: 0097-5397. DOI: 10.1137/S0097539703431032. [Online]. Available: https://epubs.siam.org/doi/abs/10.1137/S0097539703431032 (visited on 07/10/2023).

[12] D. Zuckerman, "Linear Degree Extractors and the Inapproximability of Max Clique and Chromatic Number," *Theory of Computing*, vol. 3, pp. 103–128, Aug. 2007, Number: 6 Publisher: Theory of Computing. DOI: 10.4086/toc.2007.v003a006. [Online]. Available: https://theoryofcomputing.org/articles/v003a006/ (visited on 11/06/2023).

[13] A. Ta-Shma, C. Umans, and D. Zuckerman, "Lossless Condensers, Unbalanced Expanders, And Extractors," en, *Combinatorica*, vol. 27, no. 2, pp. 213–240, Mar. 2007, ISSN: 1439-6912. DOI: 10.1007/s00493-007-0053-2. [Online]. Available: https://doi.org/10.1007/s00493-007-0053-2 (visited on 11/05/2023).

[14] V. Guruswami, C. Umans, and S. Vadhan, "Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes," *Journal of the ACM*, vol. 56, no. 4, 20:1–20:34, Jul. 2009, ISSN: 0004-5411. DOI: 10.1145/1538902.1538904. [Online]. Available: https://dl.acm.org/doi/10.1145/1538902.1538904 (visited on 11/05/2023).

[15] O. Reingold, S. Vadhan, and A. Wigderson, "Entropy waves, the zig-zag graph product, and new constant-degree expanders," *Annals of Mathematics*, vol. 155, no. 1, pp. 157–187, 2002, ISSN: 0003486X. [Online]. Available: http://www.jstor.org/stable/3062153 (visited on 03/29/2024).

[16] S. P. Vadhan, "Pseudorandomness," English, *Foundations and Trends® in Theoretical Computer Science*, vol. 7, no. 1–3, pp. 1–336, Dec. 2012, Publisher: Now Publishers, Inc., ISSN: 1551-305X, 1551-3068. DOI: 10.1561/0400000010. [Online]. Available: https://www.nowpublishers.com/article/Details/TCS-010 (visited on 11/05/2023).

[17] B. Barak, Y. Dodis, H. Krawczyk, *et al.*, "Leftover Hash Lemma, Revisited," en, in *Advances in Cryptology – CRYPTO 2011*, P. Rogaway, Ed., Berlin, Heidelberg: Springer, 2011, pp. 1–20, ISBN: 978-3-642-22792-9. DOI: 10.1007/978-3-642-22792-9_1.

[18] Y. Dodis, T. Ristenpart, and S. Vadhan, "Randomness Condensers for Efficiently Samplable, Seed-Dependent Sources," en, in *Theory of Cryptography*, R. Cramer, Ed., Berlin, Heidelberg: Springer, 2012, pp. 618–635, ISBN: 978-3-642-28914-9. DOI: 10.1007/978-3-642-28914-9_35.

[19] Y. Dodis and Y. Yu, "Overcoming Weak Expectations," en, in *Theory of Cryptography*, A. Sahai, Ed., Berlin, Heidelberg: Springer, 2013, pp. 1–22, ISBN: 978-3-642-36594-2. DOI: 10.1007/978-3-642-36594-2_1.

[20] Y. Dodis, K. Pietrzak, and D. Wichs, "Key Derivation without Entropy Waste," en, in *Advances in Cryptology – EUROCRYPT 2014*, P. Q. Nguyen and E. Oswald, Eds., Berlin, Heidelberg: Springer, 2014, pp. 93–110, ISBN: 978-3-642-55220-5. DOI: 10.1007/978-3-642-55220-5_6.

[21] J. Garay, A. Kiayias, and N. Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications," en, in *Advances in Cryptology - EUROCRYPT 2015*, E. Oswald and M. Fischlin, Eds., vol. 9057, Series Title: Lecture Notes in Computer Science, Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 281–310, ISBN: 978-3-662-46803-6. DOI: 10.1007/978-3-662-46803-6_10. [Online]. Available: http://link.springer.com/10.1007/978-3-662-46803-6_10 (visited on 03/28/2024).

[22] R. Pass, L. Seeman, and A. Shelat, "Analysis of the Blockchain Protocol in Asynchronous Networks," en, in *Advances in Cryptology – EUROCRYPT 2017*, J.-S. Coron and J. B. Nielsen, Eds., Cham: Springer International Publishing, 2017, pp. 643–673, ISBN: 978-3-319-56614-6. DOI: 10.1007/978-3-319-56614-6_22.

[23] J. Cook and D. Moshkovitz, *Explicit Time and Space Efficient Encoders Exist Only With Random Access*, en, ISSN: 1433-8092, Feb. 2024. [Online]. Available: https://eccc.weizmann.ac.il/report/2024/032/ (visited on 02/23/2024).

[24] D. Gavinsky and P. Pudlák, "Santha-Vazirani sources, deterministic condensers and very strong extractors," en, *Theory of Computing Systems*, vol. 64, no. 6, pp. 1140–1154, Aug. 2020, ISSN: 1433-0490. DOI: 10.1007/s00224-020-09975-8. [Online]. Available: https://doi.org/10.1007/s00224-020-09975-8 (visited on 11/09/2023).

[25] B. Chor, O. Goldreich, J. Hasted, J. Freidmann, S. Rudich, and R. Smolensky, "The bit extraction problem or t-resilient functions," in *Proceedings of the 26th Annual Symposium on Foundations of Computer Science*, ser. SFCS '85, USA: IEEE Computer Society, Oct. 1985, pp. 396–407. DOI: 10.1109/SFCS.1985.55. [Online]. Available: https://doi.org/10.1109/SFCS.1985.55 (visited on 04/02/2024).

[26] E. Chattopadhyay and D. Zuckerman, "Explicit two-source extractors and resilient functions," *Annals of Mathematics*, vol. 189, no. 3, pp. 653–705, May 2019, Publisher: Department of Mathematics of Princeton University, ISSN: 0003-486X, 1939-8980. DOI: 10.4007/annals.2019.189.3.1. [Online]. Available: https://projecteuclid.org/journals/annals-of-mathematics/volume-189/issue-3/Explicit-two-source-extractors-

and-resilient-functions/10.4007/annals.2019.189.3.1. full (visited on 07/18/2023).

[27] M. Ben-Or and N. Linial, "Collective Coin Flipping," *Advances In Computing Research*, vol. 5, pp. 91–115, 1989. [Online]. Available: https://www.cs.huji.ac.il/~nati/PAPERS/coll_coin_fl.pdf (visited on 03/30/2024).

[28] J. Kahn, G. Kalai, and N. Linial, "The influence of variables on Boolean functions," in *[Proceedings 1988] 29th Annual Symposium on Foundations of Computer Science*, Oct. 1988, pp. 68–80. DOI: 10.1109/SFCS.1988.21923.

[29] E. Friedgut, "Influences in Product Spaces: KKL and BKKKL Revisited," en, *Combinatorics, Probability and Computing*, vol. 13, no. 1, pp. 17–29, Jan. 2004, ISSN: 1469-2163, 0963-5483. DOI: 10.1017/S0963548303005832. [Online]. Available: https://www.cambridge.org/core/journals/combinatorics-probability-and-computing/article/influences-in-product-spaces-kkl-and-bkkkl-revisited/F91C9636C0496CB42669265F744E83AE (visited on 03/28/2024).

[30] J. Bourgain, J. Kahn, G. Kalai, Y. Katznelson, and N. Linial, "The influence of variables in product spaces," en, *Israel Journal of Mathematics*, vol. 77, no. 1, pp. 55–64, Feb. 1992, ISSN: 1565-8511. DOI: 10.1007/BF02808010. [Online]. Available: https://doi.org/10.1007/BF02808010 (visited on 11/06/2023).

[31] M. Ben-Or and N. Linial, "Collective coin flipping, robust voting schemes and minima of Banzhaf values," in *26th Annual Symposium on Foundations of Computer Science (sfcs 1985)*, ISSN: 0272-5428, Oct. 1985, pp. 408–416. DOI: 10.1109/SFCS.1985.15. [Online]. Available: https://ieeexplore.ieee.org/document/4568166 (visited on 11/09/2023).

[32] M. Ajtai and N. Linial, "The influence of large coalitions," en, *Combinatorica*, vol. 13, no. 2, pp. 129–145, Jun. 1993, ISSN: 1439-6912. DOI: 10.1007/BF01303199. [Online]. Available: https://doi.org/10.1007/BF01303199 (visited on 11/09/2023).

[33] R. Meka, "Explicit Resilient Functions Matching Ajtai-Linial," in *Proceedings of the 2017 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, ser. Proceedings, Society for Industrial and Applied Mathematics, Jan. 2017, pp. 1132–1148. DOI: 10.1137/1.9781611974782.73. [Online]. Available: https://epubs.siam.org/doi/10.1137/1.9781611974782.73 (visited on 07/13/2023).

[34] S. Kopparty and V. N, "Extracting mergers and projections of partitions," in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2023, September 11-13, 2023, Atlanta, Georgia, USA*, N. Megow and A. D. Smith, Eds., ser. LIPIcs, vol. 275, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023, 52:1–52:22. DOI: 10.4230/LIPICS.APPROX/RANDOM.2023.52. [Online]. Available: https://doi.org/10.4230/LIPIcs.APPROX/RANDOM.2023.52.

[35] E. Chattopadhyay, V. Goyal, and X. Li, "Nonmalleable Extractors and Codes, with Their Many Tampered Extensions," *SIAM Journal on Computing*, vol. 49, no. 5, pp. 999–1040, Jan. 2020, Publisher: Society for Industrial and Applied Mathematics, ISSN: 0097-5397. DOI: 10.1137/18M1176622. [Online]. Available: https://epubs.siam.org/doi/10.1137/18M1176622 (visited on 04/02/2024).

[36] U. V. Vazirani, "Towards a strong communication complexity theory or generating quasi-random sequences from two communicating slightly-random sources (extended abstract)," in *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA*, R. Sedgewick, Ed., ACM, 1985, pp. 366–378. DOI: 10.1145/22145.22186. [Online]. Available: https://doi.org/10.1145/22145.22186.

[37] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions (extended abstracts)," in *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washington, USA*, D. S. Johnson, Ed., ACM, 1989, pp. 12–24. DOI: 10.1145/73007.73009. [Online]. Available: https://doi.org/10.1145/73007.73009.

[38] E. Chattopadhyay, "Explicit Two-Source Extractors and More," PhD thesis, The University of Texas at Austin, Austin, TX, May 2016. [Online]. Available: https://repositories.lib.utexas.edu/items/9fd88fea-a4e7-4953-92a9-ad233c661458.

[39] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, Jan. 2008, Publisher: Society for Industrial and Applied Mathematics, ISSN: 0097-5397. DOI: 10.1137/060651380. [Online]. Available: https://epubs.siam.org/doi/10.1137/060651380 (visited on 03/06/2024).