Electronic Colloquium on Computational Complexity, Report No. 183 (2015)

Non-Malleable Extractors – New Tools and Improved Constructions

Gil Cohen*

November 16, 2015

Abstract

A non-malleable extractor is a seeded extractor with a very strong guarantee – the output of a non-malleable extractor obtained using a typical seed is close to uniform even conditioned on the output obtained using any other seed. The first contribution of this paper consists of two new and improved constructions of non-malleable extractors:

- We construct a non-malleable extractor with seed-length $O(\log n \cdot \log\log n)$ that works for entropy $\Omega(\log n)$. This improves upon a recent exciting construction by Chattopadhyay, Goyal, and Li (ECCC'15) that has seed length $O(\log^2 n)$ and requires entropy $\Omega(\log^2 n)$.
- Secondly, we construct a non-malleable extractor with optimal seed length $O(\log n)$ for entropy $n/\text{polylog}\, n$. Prior to this construction, non-malleable extractors with a logarithmic seed length, due to Li (FOCS'12), required entropy $0.49n$. Even non-malleable condensers with seed length $O(\log n)$, by Li (STOC'12), could only support linear entropy.

We further devise several tools for enhancing a given non-malleable extractor in a black-box manner. One such tool is an algorithm that reduces the entropy requirement of a non-malleable extractor at the expense of a slightly longer seed. A second algorithm increases the output length of a non-malleable extractor from constant to linear in the entropy of the source. We also devise an algorithm that transforms a non-malleable extractor to the so-called t-non-malleable extractor for any desired t. Besides being useful building blocks for our constructions, we consider these modular tools to be of independent interest.

*Computing and Mathematical Sciences Department, Caltech. Email: coheng@gmail.com.

ISSN 1433-8092

Contents

1 Introduction

A non-malleable extractor is a seeded extractor with a very strong property – the output of a non-malleable extractor obtained using a typical seed is close to uniform even given the output obtained using any other seed. Constructing non-malleable extractors gained a significant attention in the literature, with original motivation coming from privacy amplification protocols due to Dodis and Wichs [DW09]. Recently, non-malleable extractors were used as a key component in the breakthrough construction of two-source extractors by Chattopadhyay and Zuckerman [CZ15]. Before giving the formal definition of a non-malleable extractor, we recall the more basic notion of seeded extractors (see [Sha11, Vad11] for a more elaborated discussion).

Seeded extractors, introduced by Nisan and Zuckerman [NZ96], are central objects in pseudorandomness with many applications in theoretical computer science. Informally speaking, a seeded extractor is a randomized algorithm that uses only few bits of internal randomness, called the seed, to extract pure randomness from a weak random source.

For a formal treatment, we recall the notion of min-entropy, introduced by Chor and Goldreich [CG88]. A random variable X has min-entropy k if no point is sampled by X with probability larger than 2^{-k}. When X is supported on n bit strings, we say that X is an (n,k)-source. With this notion of entropy, we recall the definition of a seeded extractor.

Definition 1.1 (Seeded extractors)**.** *A function* $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is called a* seeded extractor *for entropy* k *if for any* (n,k)*-source* X *and an independent random variable* Y *that is uniformly distributed over* $\{0,1\}^d$*, it holds that* $\mathsf{Ext}(X,Y) \approx U_m$*.*

In the definition above, and throughout the paper, U_m stands for the uniform distribution over m bit strings. Further, by writing $A \approx B$ we mean that A and B are two distributions that are close in statistical distance. Throughout the introduction we will be vague about how close distributions are exactly, and the reader is advised to think of A, B as being, say, $1/10$-close. In some cases, constants that appear in the results described in this section hide $\mathrm{polylog}(1/\varepsilon)$ factors, where ε is the error guarantee.

The second input to Ext is called the *seed*. The general goal is to design efficiently computable seeded extractors with short seeds for low entropy sources, having many output bits. By a straightforward application of the probabilistic method one can prove the existence of a seeded extractor that works for any entropy $k = \Omega(1)$ with seed length $d = \log(n) + O(1)$, and $m = k - O(1)$ output bits. By now, following a long line of research initiated by [NZ96] and that has accumulated to [GUV09, DKSS09, TSU12], it is known how to construct seeded extractors with seed length $O(\log n)$ for any entropy $k = \Omega(1)$, with $m = 0.99k$ output bits.

For many applications, it is desired that the output of a seeded extractor will be close to uniform even given the seed that was used for the extraction. A seeded extractor that has this property is called *strong*.

Definition 1.2 (Strong seeded extractors)**.** *A function* $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is called a* strong seeded extractor *for entropy* k *if for any* (n,k)*-source* X *and an independent random variable* Y *that is uniform over* $\{0,1\}^d$*, it holds that* $(\mathsf{Ext}(X,Y),Y) \approx (U_m,Y)$*.*

In the definition above, U_m stands for a random variable that is uniformly distributed over m bit strings and is independent of Y, namely, (U_m, Y) is a product distribution. The explicit constructions mentioned above [GUV09, DKSS09, TSU12] are in fact strong. In particular, it is known how to construct a strong seeded extractor for any entropy $k = \Omega(1)$ with seed length $d = O(\log n)$ and $m = 0.99k$ output bits. Moreover, there is a black-box transformation that produces a strong seeded extractor given a seeded extractor (which not necessarily strong) with essentially the same parameters [RSW00].

1.1 Non-malleable extractors

It is straightforward to show that if $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a strong seeded extractor for entropy k then for any (n,k)-source X, there exists a small subset of seeds $B \subset \{0,1\}^d$ such that for any $y \notin B$, it holds that $\mathsf{Ext}(X,y)$ is close to uniform. That is, one can associate with any source X a small set of "bad" seeds such that for any seed y that is not bad, $\mathsf{Ext}(X,y)$ is close to uniform.

This dichotomic point of view on strong seeded extractors is frequently used in the literature. Taking this view, we note that nothing in the definition of a strong seeded extractor prevents $\mathsf{Ext}(X,y)$ from being arbitrarily correlated with $\mathsf{Ext}(X,y')$ for some good seeds y, y'. Namely, there is no guarantee on the correlation (or the lack of) between the outputs of a strong seeded extractor when applied with two distinct good seeds. One can then contemplate an even stronger notion of seeded extractors in which the output $\mathsf{Ext}(X,y)$ is uniform even conditioned $\mathsf{Ext}(X,y')$ for any good seed y and for any $y' \neq y$. This point of view leads to the definition of non-malleable extractors. We choose to present next an equivalent definition, which is the one originally suggested by Dodis and Wichs [DW09]. In Lemma 4.14 we show that the original definition and the dichotomic one described above are equivalent. On top being natural, we make frequent use of the dichotomic definition in our proofs.

Definition 1.3 (Non-malleable extractors)**.** *A function* $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is called a* non-malleable extractor *for entropy* k *if for any* (n,k)*-source* X *and a function* $\mathcal{A}\colon \{0,1\}^d \to \{0,1\}^d$ *with no fixed points, it holds that*

$$(\mathsf{Ext}(X,Y), \mathsf{Ext}(X,\mathcal{A}(Y)), Y) \approx (U_m, \mathsf{Ext}(X,\mathcal{A}(Y)), Y),$$

where Y *is uniformly distributed over* $\{0,1\}^d$ *and is independent of* X*.*

As suggested in [CRS14], one can consider the generalization to t-non-malleable extractors in which $\mathsf{Ext}(X,y)$ is close to uniform even conditioned on $\mathsf{Ext}(X,y^1), \ldots, \mathsf{Ext}(X,y^t)$ for any good seed y and arbitrary seeds $y^1, \ldots, y^t \in \{0,1\}^d \setminus \{y\}$, or equivalently, where $\mathsf{Ext}(X,Y)$ looks uniform even given $\mathsf{Ext}(X,\mathcal{A}_1(Y)), \ldots, \mathsf{Ext}(X,\mathcal{A}_t(Y))$ for arbitrary functions $\{\mathcal{A}_i\colon \{0,1\}^d \to \{0,1\}^d\}_{i=1}^t$ with no fixed points. Note that a strong seeded extractor can be viewed as a 0-non-malleable extractor. Although this generalization is useful for some applications (e.g., [CZ15] uses $t = \operatorname{polylog} n$), in this section we consider only the standard definition of non-malleable extractors, namely, the case $t = 1$. In fact, one of our contributions is an algorithm that transforms a "standard" non-malleable extractor (namely, a

1-non-malleable extractor) to a t-non-malleable extractor, for any desired $t > 1$, in a black-box manner (see Lemma 2.5). Thus, it is not only for simplicity that the reader can focus on standard non-malleable extractors.

Construction	Seed length	Supported entropy
[DW09] (non-constructive)	$\log(n) + O(1)$	$\Omega(\log\log n)$
[LWZ11]	n	$(0.5+\delta)\cdot n$ for any constant $\delta > 0$
[CRS14, DLWZ14, Li12a]	$O(\log n)$	$(0.5+\delta)\cdot n$ for any constant $\delta > 0$
[Li12c]	$O(\log n)$	$(0.5-\alpha)\cdot n$ for some small constant $0 < \alpha < 0.5$
[CGL15]	$O(\log^2 n)$	$\Omega(\log^2 n)$
Theorem 2.1	$O(\log n \cdot \log\log n)$	$\Omega(\log n)$
Theorem 2.2	$O(\log n)$	$\Omega(n/\log^c n)$ for any constant $c > 0$

Table 1: Summary of explicit non-malleable extractors from the literature as well as our contribution.

Dodis and Wichs [DW09], who introduced the notion of non-malleable extractors, left the problem of constructing such extractors to future research, yet showed that such extractors, with great parameters, do exist. More precisely [DW09] proved the existence of a non-malleable extractor with seed length $d = \log(n) + O(1)$ that supports any entropy $k = \Omega(\log\log n)$, having $m = k/2 - O(1)$ output bits.

Since then, several explicit constructions of non-malleable extractors appeared in the literature, as summarized in Table 1. Moreover, different objects related to non-malleable extractors were considered in the literature as well [Li12a, Li12b, Coh15a, AHL15]. Up until the recent work of Chattopadhyay, Goyal, and Li [CGL15], all constructions of non-malleable extractors worked for entropy roughly $n/2$. The non-malleable extractor of [CGL15] substantially improved upon previous results by supporting min-entropy $O(\log^2 n)$.

Unfortunately, unlike most previous constructions, the seed length required by the non-malleable extractor of [CGL15] is $O(\log^2 n)$ as apposed to the desired $O(\log n)$. Thus, the exciting result of [CGL15] sets the next natural goal at obtaining non-malleable extractors with logarithmic seed length for poly-logarithmic or even lower entropy. Besides being a natural goal, reducing the seed length to logarithmic in n is desired as in many constructions of pseudorandom objects that appear in the literature (e.g., [BRSW12, Rao09, Li11, Li13b, Li13a, Coh15a, Coh15b, CZ15, Li15b, Li15a]) one cycles over all possible seeds of a strong seeded extractor to obtain and further process all 2^d possible outputs. Such techniques are inefficient whenever the seed length d is super-logarithmic.

2 Our Contribution

In this paper we give two constructions of non-malleable extractors that improve upon existing knowledge (see Theorem 2.1 and Theorem 2.2). Moreover, we devise several tools that we consider to be of independent interest. The first tool is an algorithm that reduces the entropy requirement of a given non-malleable extractor at the expense of slightly increasing its seed length (see Lemma 2.3). Our second algorithm increases the output length of a given non-malleable extractor from constant to optimal up to constant factors, where the constants depend only on the error guarantee (see Lemma 2.4). A third algorithm, already mentioned above, transforms a non-malleable extractor to a t-non-malleable extractor, for any desired $t > 1$ in a black-box manner (see Lemma 2.5). We now elaborate.

2.1 Two new constructions of non-malleable extractors

The first contribution of this work is a construction of a non-malleable extractor with quasi-logarithmic seed length. Our extractor also has the advantage of supporting logarithmic entropy, which is lower than that supported by the extractor of [CGL15]. More precisely, we prove the following.

Theorem 2.1. *There exists an explicit non-malleable extractor* $\mathsf{NMExt}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with seed length* $d = O(\log n \cdot \log\log n)$ *for entropy* $k = \Omega(\log n)$*, having* $m = \Omega(k)$ *output bits.*

We note that Theorem 2.1 improves upon [CGL15] both in seed length and in the required entropy. In particular, the seed length is optimal up to a multiplicative factor of $O(\log\log n)$. Our second contribution is a construction of non-malleable extractors with optimal seed length, up to a constant factor, that work for sources with entropy $n/\mathrm{polylog}\, n$. Prior to this construction, the lowest entropy supported by a non-malleable extractor with a logarithmic seed length was $0.49n$ [Li12c]. Furthermore, even non-malleable condensers with logarithmic seed length [Li12a] did not support sub-linear entropy.

Theorem 2.2. *For any constant* $c > 0$ *there exists an explicit non-malleable extractor* $\mathsf{NMExt}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with seed length* $d = O(\log n)$ *for entropy* $k = \Omega(n/\log^c n)$*, having* $\Omega(k)$ *output bits.*

In fact, the parameter c in Theorem 2.2 can be taken to be slightly super-constant so that the resulted non-malleable extractor can support entropy $k = n/(\log n)^{\omega(1)}$. This, however, will increase the seed length as it has exponential dependence in c.

2.2 Reducing the entropy requirement of a non-malleable extractor

A tool that we develop for proving Theorem 2.1 and Theorem 2.2, which we find to be of independent interest, is an algorithm that reduces the entropy requirement of a non-malleable

extractor at the expense of slightly increasing its seed length. We state here a special case that is used in order to prove Theorem 2.2.

Lemma 2.3. *There exist constants $0 < \alpha < 1 < c$ and an efficient algorithm that given a non-malleable extractor with seed length d for entropy $k = \Omega(d^{1+\alpha})$ having c output bits, produces a non-malleable extractor with seed length $O(d)$ for a lower entropy $k' = k/d^{\alpha}$.*

For a more general and formal statement, see Lemma 6.1. We are not aware of such an "entropy-seed tradeoff" being considered in previous works on seeded extractors. What is known is how to increase the output length at the expense of a longer seed. Next we consider this transformation in the context of non-malleable extractors.

2.3 Increasing the output length of a non-malleable extractor

A second tool we develop is a general method for increasing the output length of non-malleable extractors. In fact, the algorithm in the following lemma is able to increase the output length from a constant (more precisely, from $\Omega(\log(1/\varepsilon))$, where ε is the desired error guarantee) to linear in the entropy.

Lemma 2.4. *There exists a constant c and an efficient algorithm that given a non-malleable extractor with seed length d for entropy $k = \Omega(\log n)$ and c output bits, produces a non-malleable extractor with seed length $O(d)$ for the same entropy k having $\Omega(k)$ output bits.*

A more formal statement and its proof are given in Section 7. Increasing the output length of seeded extractors is a useful tool introduced already by Nisan and Zuckerman [NZ96]. Using the framework set in [NZ96], Li [Li12a] showed how to increase the output length of non-malleable extractors. However, the latter only works for high entropy sources and requires the output length one starts with to depend on the input length n. Our technique does not follow the method of Nisan and Zuckerman and involves new ideas which allows us to obtain our result.

2.4 From non-malleable extractors to t-non-malleable extractors

As mentioned, for some applications one requires an even stronger notion of non-malleability, where the output of the non-malleable extractor obtained using a typical seed is uniform even conditioned on the outputs obtained using any other t seeds for some desired parameter $t \geq 1$.

Several known constructions of non-malleable extractors are in fact t-non-malleable. Usually proving that a non-malleable extractor is a t-non-malleable extractor for some $t > 1$ is straightforward yet requires to make some changes in the proof. In other cases (e.g., [Li12c]) one needs to make some changes in the construction itself rather than in the analysis alone.

Our next result is a black-box reduction from t-non-malleable extractors to standard (namely, $t = 1$) non-malleable extractors. Having such a reduction allows one to focus only on constructing non-malleable extractors.

Lemma 2.5. *There exists a constant c and an efficient algorithm that given an integer $t \geq 1$ and a non-malleable extractor for entropy k with seed length d and c output bits, such that $k = \Omega(\log n + t \cdot \log(td))$, produces a t-non-malleable extractor for entropy k with seed length $O(t^2 d)$.*

A more general and formal statement and its proof appear in Section 10.

3 Proof Overview

In this section we give an informal proof overview for our results. Our techniques build on novel ideas from [CGL15] which in turn make use of the flip-flop primitive that was introduced in [Coh15a]. To get a broad perspective, we believe it is instructive to start by describing this primitive.

3.1 The flip-flop primitive

Informally speaking, the flip-flop primitive uses a weak-source of randomness to break correlations between random variables. To this end, the flip-flop also requires an "advice bit". More precisely, a flip-flop is a function

$$\mathsf{FF}\colon \{0,1\}^n \times \{0,1\}^\ell \times \{0,1\} \to \{0,1\}^m$$

with the following property. Assume that Y, Y' are two arbitrarily correlated random variables on ℓ bit strings such that Y is uniform, and let X be an (n,k)-source that is independent of the joint distribution (Y, Y'). Then, the guarantee of the flip-flop primitive is that $\mathsf{FF}(X, Y, 0)$ looks uniform even conditioned on $\mathsf{FF}(X, Y', 1)$. Similarly, $\mathsf{FF}(X, Y, 1)$ looks uniform even conditioned on $\mathsf{FF}(X, Y', 0)$. So, informally speaking, as long as the advice bit, that is passed as the third argument to the flip-flop primitive, is different in the two applications, the flip-flop can use the weak-source X to break the correlation Y' has with Y. As mentioned, we think of the third input bit as an advice.

The construction of FF, which is implicit in [Coh15a], is based on alternating extraction – a technique that was introduced by Dziembowski and Pietrzak [DP07] and has found several applications in the literature since then [DW09, Li13a, Li15c]. We will treat FF as an atomic operation and will not get into the details of its construction here. We remark that the construction and its analysis are not very complicated. Nevertheless, we believe that thinking of FF as an atomic operation is the right level of abstraction for this discussion.

Quantitatively speaking, in [Coh15a], an explicit construction of FF was given for any n as long as $\ell = \Omega(\log n)$ and $k = \Omega(\log \ell)$, with $m = \Omega(\ell)$ output bits. In particular, if one is willing to output $O(\log n)$ bits (which usually suffices for the purpose of compositions with other pseudo-random objects), the required entropy from X is surprisingly low, namely, one only needs $k = \Omega(\log \log n)$.

3.2 Correlation breakers with advice

Informally speaking, the flip-flop primitive breaks the correlation between random variables as above, using a weak-source of randomness and an advice bit. At this point, it is not at all clear where do we expect this advice to come from when designing a non-malleable extractor. In fact, following [CGL15], in the construction of our non-malleable extractors we will not be able to generate an advice *bit* but rather an advice *string*. More formally, we say that a function

$$\mathsf{AdvCB}\colon \{0,1\}^n \times \{0,1\}^\ell \times \{0,1\}^a \to \{0,1\}^m$$

is called a *correlation breaker with advice* if for any two ℓ-bit random variables Y, Y' such that Y is uniform and for any independent (n,k)-source X, it holds that $\mathsf{FF}(X,Y,\alpha)$ looks uniform even conditioned on $\mathsf{FF}(X,Y',\alpha')$ for any distinct $\alpha,\alpha' \in \{0,1\}^a$ (for a formal definition the reader is referred to Definition 4.11).

Note that a correlation breaker with advice of length $a = 1$ is exactly the flip-flop primitive. Clearly, it is easier to generate long advices than shorter ones. Nevertheless, one can implement an AdvCB using the flip-flop primitive. We will not delve into the details of the reduction here, and will be satisfied by stating that this reduction, as was done implicity in [Coh15a, CGL15], works for every n, a with $\ell = \Omega(a \cdot \log(an))$, $k = \Omega(a \cdot \log(a \log n))$, and has $m = \Omega(\log n)$ output bits (see Theorem 4.12 for a formal statement).

In fact, as in [CGL15], we will need a somewhat stronger guarantee. Namely, not only $\mathsf{AdvCB}(X,Y,\alpha)$ should be uniform even conditioned on $\mathsf{AdvCB}(X,Y',\alpha')$ with the notation set as above, but rather $\mathsf{AdvCB}(X,Y,\alpha)$ should look uniform even after given $\mathsf{AdvCB}(X',Y',\alpha')$, where X' may correlate arbitrarily with the (n,k)-source X, as long as the joint distribution (X,X') is independent of the joint distribution (Y,Y').

3.3 The [CGL15] reduction from non-malleable extractors to advice generators

In this section we introduce the notion of an *advice generator* that is implicit in [CGL15], and present the novel reduction by [CGL15] from non-malleable extractors to advice generators. In the following section we introduce our improved reduction. We start by defining the notion of an *advice generator* (for a formal treatment, see Definition 5.1). A function

$$\mathsf{AdvGen}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^a$$

is called an advice generator if for any X, Y as above and for any function $\mathcal{A}\colon \{0,1\}^d \to \{0,1\}^d$ with no fixed points, it holds that $\mathsf{AdvGen}(x,y) \neq \mathsf{AdvGen}(x,\mathcal{A}(y))$ with high probability over $x \sim X$, $y \sim Y$. The general idea in [CGL15] is to compute an advice using x, y and feed that advice to a correlation breaker with advice. Namely, given an advice generator AdvGen and a correlation breaker with advice AdvCB, the non-malleable extractor is defined as

$$\mathsf{NMExt}(x,y) = \mathsf{AdvCB}(x,y,\mathsf{AdvGen}(x,y)). \tag{3.1}$$

Indeed, with high probability, the advices $\mathsf{AdvGen}(X,Y)$ and $\mathsf{AdvGen}(X,\mathcal{A}(Y))$ are distinct, and so one may carelessly conclude that AdvCB guarantees that $\mathsf{NMExt}(X,Y)$ is uniform even conditioned on $\mathsf{NMExt}(X,\mathcal{A}(Y))$. Of course, the problem with this argument is that there are correlations between the advices and between X,Y.

To salvage the argument above, one needs to make sure that even conditioned on the fixings of the advices $\mathsf{AdvGen}(X,Y)$, $\mathsf{AdvGen}(X,\mathcal{A}(Y))$, it holds that X and Y remain independent. So there is a strong limitation on the type of computation that can be carried by AdvGen. Even having such a guarantee there are a couple of problems with such a general method for constructing a non-malleable extractor. First, we must make sure that conditioned on the fixings of $\mathsf{AdvGen}(X,Y)$, $\mathsf{AdvGen}(X,\mathcal{A}(Y))$, it holds that X has enough entropy as required by AdvCB. Typically, this is a non-issue. Second, we need Y to remain uniform even after these fixings. Nevertheless, by constructing an advice generator that has a suitable interplay with AdvCB, a construction having the general form above was used by [CGL15] for their construction of non-malleable extractors.

Quantitatively speaking, [CGL15] constructed an advice generator with advice length $a = O(\log n)$ (see Section 8.1) that, using the reduction above, can be shown to yield a non-malleable extractor for min-entropy $\Omega(\log^2 n)$ with seed length $O(\log^2 n)$. In the next section we describe our improved reduction from non-malleable extractors to advice generators.

3.4 An improved reduction

We now present a different way of constructing a non-malleable extractor given an advice generator. Our reduction will enable us to obtain non-malleable extractors with shorter seeds that work for lower min-entropies compared to [CGL15].

A building block that we use is the seeded extractor of Raz [Raz05] that works with weak-seeds. This is a strong seeded extractor $\mathsf{Raz}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ that has the same guarantee as standard strong seeded extractors even if the seed is not uniform, but rather has min-entropy $0.6d$. Raz [Raz05] gave an explicit construction of such an extractor with seed length $d = O(\log n)$ that supports any entropy $k = \Omega(d)$. See Theorem 4.3 for a formal statement.

With this building block, we are ready to define our reduction. First, we divide the seed y to 3 parts $y = y_1 \circ y_2 \circ y_3$, where y_i has length d_i. We only assume that d_1 is very small compared to d (taking $d_1 \leq d/1000$ will do) and set $9d_2 = d_3$. Our reduction make use of an advice generator $\mathsf{AdvGen}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^a$ that has the following extra guarantee. For any function $\mathcal{A}\colon \{0,1\}^d \to \{0,1\}^d$ with no fixed points, it holds that with high probability over the fixing of $\mathsf{AdvGen}(X,Y)$, $\mathsf{AdvGen}(X,\mathcal{A}(Y))$:

- The random variables X,Y remain independent;
- X has not lost more than, say, half of its min-entropy;
- The random variable $Y_2 \circ Y_3$ has min-entropy rate 0.99.

Given any such "nice" advice generator, we define our non-malleable extractor by

$$\mathsf{NMExt}(x, y) = \mathsf{AdvCB}\left(y_3, \mathsf{Raz}(x, y_2), \mathsf{AdvGen}(x, y)\right). \tag{3.2}$$

It is worthwhile to compare the above definition with the reduction given by Equation (3.1). The most important difference being the "switch" that was done between the roles of the source and the seed. Namely, the seed Y to the non-malleable extractor takes the role of a source in AdvCB as (a suffix of) it is being passed as the first argument, whereas the seed to AdvCB is this function $\mathsf{Raz}(X, Y_2)$ of both X and Y. This switch is what makes the reduction more efficient in the sense that the resulted non-malleable extractor has a shorter seed and can support a lower entropy. Informally speaking, the reason for this is that Y_3 makes a much shorter source than X as the latter consists of n bits whereas we will end up setting Y to have length which is logarithmic in n.

3.4.1 Analyzing the reduction

We now give a sketch of the analysis for the reduction given by Equation (3.2). First, according to the definition of AdvGen, by aggregating a small error, we may assume that $\alpha = \mathsf{AdvGen}(X, Y)$ and $\alpha' = \mathsf{AdvGen}(X, \mathcal{A}(Y))$ are distinct fixed strings. Further, the three extra properties of AdvGen hold.

By the third property, $Y_2 \circ Y_3$ has min-entropy rate 0.99. Since $d_2 = (d_2 + d_3)/10$, we argue that with high probability over Y_3, it holds that Y_2 has min-entropy rate 0.9. To see why a claim of this sort should be true, think of the special case where 0.99 fraction of the bits of $Y_2 \circ Y_3$ are distributed uniformly and independently at random, and the remaining 0.01 fraction of the bits behave adversarially. Since Y_2 is a block of density 0.1 in $Y_2 \circ Y_3$, even in the worst case where Y_2 contains all the "bad" bits, their fraction within Y_2 is at most $0.01/0.1 = 0.1$, and so 0.9 fraction of the bits in Y_2 are uniform and independent of each other, leaving Y_2 with min-entropy rate of 0.9. A somewhat more careful argument can be carried out to handle the more general case where we only assume that the min-entropy rate of $Y_2 \circ Y_3$ is 0.99.

Once we have established that Y_2 has min-entropy rate 0.9, we have that $\mathsf{Raz}(X, Y_2)$ is close to uniform. For this we use the guarantees that the entropy of X remained high after the fixings of the advices, and that these fixings have not introduced correlations between X and Y_2. In fact, since Raz is strong, with high probability over the fixing of $y_2 \sim Y_2$ we have that $\mathsf{Raz}(X, y_2)$ is close to uniform. Since $\mathsf{Raz}(X, y_2)$ is a deterministic function of X, we can further fix $\mathcal{A}(Y)_2$ without affecting $\mathsf{Raz}(X, y_2)$ and without introducing correlations between X, Y. One can then show that these fixings of Y_2 and $\mathcal{A}(Y)_2$ can only reduce the min-entropy of Y_3 by roughly $2d_2$, and so the min-entropy of Y_3 is at least $0.99(d_2 + d_3) - 2d_2 > 0.8d_3$. Namely, Y_3 is a $(d_3, 0.8d_3)$-source.

Note that by now, $\mathsf{Raz}(X, Y_2)$ and $\mathsf{Raz}(X, \mathcal{A}(Y)_2)$ are deterministic functions of X whereas Y_3, $\mathcal{A}(Y)_3$ are independent of X. Further, $\mathsf{Raz}(X, y_2)$ is close to uniform and Y_3 is has min-entropy rate 0.8. Thus, the hypothesis of AdvCB is met and we conclude that $\mathsf{NMExt}(X, Y)$ looks uniform even conditioned on $\mathsf{NMExt}(X, \mathcal{A}(Y))$, as desired.

3.5 Reducing the entropy requirement of non-malleable extractors

In this section we describe another contribution of this paper stated as Lemma 2.3, which is a black-box transformation that given a non-malleable extractor with seed length d for entropy $k = \Omega(d^{1+\alpha})$, produces a non-malleable extractor for a lower entropy $k' = k/d^{\alpha}$ with seed length $O(d)$. Here $\alpha > 0$ is some small universal constant. Our reduction is composed of two steps. In the first step we construct an advice generator for entropy k' given a non-malleable extractor for entropy k. We then apply our reduction from Section 3.4 to obtain a non-malleable extractor for entropy k' using the advice generator.

To describe this "reversed" reduction, namely, the reduction from advice generators to non-malleable extractors with higher entropy, we make use of several building blocks, the first of which is a somewhere condenser. Informally speaking, this is a sequence of functions $\{\mathsf{Cond}_i \colon \{0,1\}^n \to \{0,1\}^n\}_{i=1}^r$ with the following property. Let $\delta > 0$. Then, for any $(n, \delta k)$-source X there exists $g \in [r]$ such that $\mathsf{Cond}_g(X)$ is an (n,k)-source. It is known [BKS+05, Zuc07] how to construct such a somewhere condenser with $r = \mathrm{poly}(1/\delta)$ (see Theorem 4.5). Building on [CGL15], we also make use of a strong seeded extractor Ext and a binary error correcting code ECC with relative distance, say, $1/4$ having a constant rate.

Given these building blocks, say we are given a non-malleable extractor $\mathsf{NMExt} \colon \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}^{\log m}$ for entropy k, where m will be set later on. Our advice generator is defined as follows. Split the seed y to two substrings $y = y_1 \circ y_2$, where y_1 is of length d_1 and $d_2 = 100 d_1$. We define

$$\mathsf{AdvGen}(x, y) = \mathsf{NMExt}(\mathsf{Cond}_1(x), y_1) \circ \cdots \circ \mathsf{NMExt}(\mathsf{Cond}_r(x), y_1) \circ \mathsf{ECC}(y_2)_{\mathsf{Ext}(x,y_1)},$$

where we interpret the output of $\mathsf{Ext}(x, y_1)$ as a size $\log m$ subset of the index set $[D_2]$ and use $\mathsf{ECC}(y_2)_{\mathsf{Ext}(x,y_1)}$ to denote the projection of the string $\mathsf{ECC}(y_2)$ on to that set of indices. Note that for this we need the output of Ext to consists of $O(\log m \cdot \log d_1)$ bits.

The construction above is influenced by the advice generator construction of [CGL15]. In particular, with the notation set above, the advice generator of [CGL15] can be written as $\mathsf{AdvGen}(x, y) = y_1 \circ \mathsf{ECC}(y_2)_{\mathsf{Ext}(x,y_1)}$ (see Section 8.1).

3.5.1 Analyzing the entropy reduction transformation

In this section we give an informal analysis showing that the function AdvGen is indeed an advice generator for entropy δk. To this end we consider an $(n, \delta k)$-source X and a function $\mathcal{A} \colon \{0,1\}^d \to \{0,1\}^d$ with no fixed points. We start by fixing $y_1 \sim Y_1$ and $y_1' \sim \mathcal{A}(Y)_1$ and consider two cases according to whether or not $y_1 = y_1'$.

Case 1 – $y_1 = y_1'$. In this case, following [CGL15], we show that with high probability $\mathsf{ECC}(Y_2)_{\mathsf{Ext}(X,y_1)} \neq \mathsf{ECC}(\mathcal{A}(Y)_2)_{\mathsf{Ext}(x,y_1)}$, which in particular will guarantee that with high probability $\mathsf{AdvGen}(X, Y) \neq \mathsf{AdvGen}(X, \mathcal{A}(Y))$ in this case. To see why this is true, note that since $y_1 = y_1'$ we have that $Y_2 \neq \mathcal{A}(Y)_2$ and so the two codewords $\mathsf{ECC}(Y_2)$, $\mathsf{ECC}(\mathcal{A}(Y)_2)$ agree on at most $3/4$ of the indices. In particular, by projecting each of these codewords to

a random set of indices of size $\log m$, we will get the same string with a probability bound that decrease polynomially with $1/m$. Of course, we do not (and cannot) sample a truly uniform projection. Nevertheless, as Ext is a strong seeded extractor, for most fixings of y_1 it holds that $\mathsf{Ext}(X, y_1)$ is close to a random subset of $[D_2]$ which suffices for the argument above to go through.

Case 2 – $y_1 \neq y_1'$. For analyzing this case, we recall that NMExt is a non-malleable extractor for entropy k and that there is some $g \in [r]$ for which $\mathsf{Cond}_g(X)$ has min-entropy k. Using the dichotomic point of view on non-malleable extractors (see Lemma 4.14), one can show that $\mathsf{NMExt}(\mathsf{Cond}_g(X), y_1)$ is close to uniform even conditioned on $\mathsf{NMExt}(\mathsf{Cond}_g(X), y_1')$ for most choices of y_1. In particular, the probability that the two strings $\mathsf{NMExt}(\mathsf{Cond}_g(X), y_1)$, $\mathsf{NMExt}(\mathsf{Cond}_g(X), y_1')$ are equal is polynomially small in m.

By taking $m = \mathrm{poly}(1/\varepsilon)$ we can bound the error of AdvGen by ε. This choice of m yields an advice length $a = O(r \cdot \log(1/\varepsilon)) = \mathrm{poly}(1/\delta) \cdot \log(1/\varepsilon)$.

So far we gave an informal proof showing that AdvGen is an advice generator for entropy δk. Recall that to use the advice generator in our reduction from Section 3.4, AdvGen must have some extra guarantees. Perhaps the most subtle of which is that conditioned on the fixings of $\mathsf{AdvGen}(X, Y)$, $\mathsf{AdvGen}(X, \mathcal{A}(Y))$, the random variables X, Y must remain independent. We assure the reader that this is the case with our construction due to the "alternating" fashion of the computation involving AdvGen, though we will skip the details in this proof overview and refer the reader to Section 6.

3.6 Increasing the output length of a non-malleable extractor

In this section we briefly describe our algorithm that increases the output length of a given non-malleable extractor described in Lemma 2.4. Being a bit more formal, for a desired error guarantee ε, we show how to increase the output length of a non-malleable extractor NMExt from $O(\log(1/\varepsilon))$ to $\Omega(k/\log(1/\varepsilon))$. Here, k is the entropy supported by NMExt. As with our entropy reduction transformation described in Section 3.5, here too the general idea is to use the given non-malleable extractor NMExt so to obtain an advice generator AdvGen which in turn will be used to construct the desired non-malleable extractor NMExt' using our reduction from Section 3.4. More precisely, borrowing notation from previous sections, we define

$$\mathsf{AdvGen}(x, y) = \mathsf{NMExt}(x, y_1) \circ \mathsf{ECC}(y_2)_{\mathsf{Ext}(x, y_1)}.$$

A similar argument to the one used in Section 3.5 shows that AdvGen is an advice generator for entropy k (in fact, this is a special case of the argument from Section 3.5). In particular, we show that if one aims for an error guarantee ε, it suffices that the output length of NMExt consists of $O(\log(1/\varepsilon))$ bits. At this point we can apply the reduction from Section 3.4 to AdvGen. This results in a non-malleable extractor NMExt' that supports the same entropy k, though it has the advantage of having output length $\Omega(k/\log(1/\varepsilon))$.

3.7 Proof overview for Theorem 2.1 and Theorem 2.2

In this section we give an overview for the proofs of Theorem 2.1 and Theorem 2.2, starting with the first theorem. As our starting point, we apply our improved reduction given in Section 3.4 with the advice generator of [CGL15]. This already yields a non-malleable extractor with seed length $O(\log n \cdot \log\log n)$ that supports entropy $\Omega(\log n \cdot \log\log n)$. Our second step is to apply the entropy reduction transformation so to obtain a second non-malleable extractor that supports a lower entropy. By choosing the parameters correctly, one can show that the resulted non-malleable extractor can support entropy $\Omega(\log n)$ while maintaining a seed of length $O(\log n \cdot \log\log n)$. As our final step we apply the transformation for increasing the output length that was described in the previous section to yield Theorem 2.1.

For the proof of Theorem 2.2, our starting point is any of the constructions of non-malleable extractors for entropy $0.6n$ with seed length $O(\log n)$ (e.g., the one given in Theorem 4.6) and denote this non-malleable extractor by NMExt_0. We now apply the entropy reduction transformation described in Section 3.5 to NMExt_0 so to obtain a new non-malleable extractor, which we denote by NMExt_1. Working out the parameters, NMExt_1 can be shown to support entropy $n/(\log n)^{\alpha}$ for some small universal constant $\alpha > 0$. Further, NMExt_1 has seed length $d_1 = O(d) = O(\log n)$.

We continue by applying the entropy reduction transformation again, this time to NMExt_1 and obtain a new non-malleable extractor NMExt_2 that has seed length $O(d_1) = O(\log n)$ and supports entropy $n/(\log n)^{2\alpha}$. By repeating this process, we construct a sequence of non-malleable extractors where each extractor supports lower entropy than its predecessor. After r steps, we obtain a non-malleable extractor NMExt_r that supports entropy $n/(\log n)^{\alpha r}$ and has seed length $2^{O(r)} \cdot \log n$. The proof of Theorem 2.2 follows by taking $r = c/\alpha$, where c is the desired constant.

3.8 From non-malleable extractor to t-non-malleable extractors

We turn to say a few words about our reduction from non-malleable extractors to t-non-malleable extractors for any $t > 1$ stated in Lemma 2.5. Recall that our construction of non-malleable extractors from Section 3.4 consists of two steps. First, we construct a "nice" advice generator. Second, the generated advice is passed to a correlation breaker with advice.

One can generalize the notions of advice generators and correlation breakers with advice to t-advice generators and t-correlation breakers with advice in the natural way for any $t \geq 1$. One can then show that the idea presented in Section 3.4 of constructing non-malleable extractors based on advice generators and correlation breakers with advice can be extended to any $t > 1$. Namely, given a t-advice generator and t-correlation breaker with advice, one can obtain a t-non-malleable extractor using the exact same reduction (see Lemma 10.4).

We already know how to construct a t-correlation breaker with advice (see Theorem 4.12) for any $t \geq 1$. A key observation we make is that for any $t \geq 1$ one can construct a t-advice generator using a standard non-malleable extractor. This allows us to reduce the problem of constructing t-non-malleable extractors to the problem of constructing non-malleable

extractors. For further details see Section 10.

4 Preliminaries

Unless stated otherwise, the logarithm in this paper is always taken base 2. For every natural number $n \geq 1$, define $[n] = \{1, 2, \ldots, n\}$. Throughout the paper we avoid the use of floor and ceiling in order not to make the equations cumbersome.

Random variables and distributions. We sometimes abuse notation and syntactically treat random variables and their distribution as equal, specifically, we denote by U_m a random variable that is uniformly distributed over $\{0,1\}^m$. Furthermore, if U_m appears in a joint distribution (U_m, X) then U_m is independent of X. When m is clear from context, we omit it from the subscript and write U.

Let X, Y be two random variables. We say that Y is a *deterministic function of* X if the value of X determines the value of Y. Namely, there exists a function f such that $Y = f(X)$. Let $X, Y, Z_1, \ldots, Z_r$ be random variables. We use the following shorthand notation and write $(X, Z_1, \ldots, Z_r) \approx_\varepsilon (Y, \cdot)$ for $(X, Z_1, \ldots, Z_r) \approx_\varepsilon (Y, Z_1, \ldots, Z_r)$.

Statistical distance. The *statistical distance* between two distributions X, Y on the same domain D is defined by $\mathsf{SD}(X, Y) = \max_{A \subseteq D} \{|\, \mathbf{Pr}[X \in A] - \mathbf{Pr}[Y \in A] \,|\}$. If $\mathsf{SD}(X, Y) \leq \varepsilon$ we write $X \approx_\varepsilon Y$ and say that X and Y are ε-close.

Min-entropy. The *min-entropy* of a random variable X, denoted by $H_\infty(X)$, is defined by $H_\infty(X) = \min_{x \in \mathsf{supp}(X)} \log_2(1/\mathbf{Pr}[X = x])$. If X is supported on $\{0,1\}^n$, we define the *min-entropy rate* of X by $H_\infty(X)/n$. In such case, if X has min-entropy k or more, we say that X is an (n, k)-source.

4.1 Pseudorandom objects we use

Definition 4.1 (Seeded extractors)**.** *A function* $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is called a* seeded extractor *for entropy* k*, with error* ε*, if for any* (n,k)*-source* X *it holds that* $\mathsf{Ext}(X, S) \approx_\varepsilon U_m$*, where* S *is uniformly distributed over* $\{0,1\}^d$ *and is independent of* X*. We say that* Ext *is a* strong seeded-extractor *if* $(\mathsf{Ext}(X, S), S) \approx_\varepsilon (U_m, U_d)$*.*

Throughout the paper we make use of the following explicit pseudorandom objects.

Theorem 4.2 ([GUV09])**.** *There exists a universal constant* $c > 0$ *such that the following holds. For all positive integers* n, k *and* $\varepsilon > 0$*, there exists an efficiently-computable strong seeded-extractor* $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *for entropy* k*, with error* ε*, seed length* $d = c \cdot \log(n/\varepsilon)$*, and* $m = 0.99 \cdot k$ *output bits.*

Theorem 4.3 ([Raz05])**.** *For all integers* n, k, d *and for any* $\varepsilon > 0$ *such that* $d = \Omega(\log(n/\varepsilon))$ *and* $k = \Omega(d)$*, there exists an efficiently-computable function* $\mathsf{Raz}\colon \{0,1\}^n \times \{0,1\}^d \to$

$\{0,1\}^{k/2}$ *with the following property. Let* X *be an* (n,k)*-source, and let* Y *be an independent* $(d,0.6d)$*-source. Then,* $(\mathsf{Raz}(X,Y),Y) \approx_\varepsilon (U,Y)$.

Theorem 4.4. *There exists a universal constant* c *such that the following holds. For all integers* n*, there exists an explicit error correcting code* $\mathsf{ECC}\colon \{0,1\}^n \to \{0,1\}^{cn}$ *with relative distance* $1/4$.

Theorem 4.5 ([BKS+05, Zuc07])**.** *For any integer* n *and any* $\delta > 0$ *there exists a sequence of efficiently computable functions* $\{\mathsf{Cond}_i\colon \{0,1\}^n \to \{0,1\}^m\}_{i=1}^{\Delta}$ *with* $\Delta = \mathrm{poly}(1/\delta)$ *and* $m = n \cdot \mathrm{poly}(\delta)$ *such that the following holds. For any* $(n,\delta n)$*-source* X*, the joint distribution of* $\{\mathsf{Cond}_i(X)\}_{i=1}^r$ *is* $2^{-\Omega(\delta^2 n)}$*-close to a convex combination such that for any participant* $(Y_1,\ldots,Y_r)$ *in the combination, there exists* $g \in [\Delta]$ *such that* Y_g *has min-entropy rate* 0.6.

Theorem 4.6 ([CRS14])**.** *For all integers* n,m,t *such that* $n = \Omega(mt)$ *and for any* $\varepsilon > 0$ *there exists a* $\mathrm{poly}(n)$*-time computable* t*-non-malleable extractor* $\mathsf{CRS}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *for* $(n,0.6n)$*-sources, with error* 2^{-m} *and seed length* $d = tm + 2\log n$.

4.2 Average conditional min-entropy

We make use of the notion of average min-entropy and some basic properties of it.

Definition 4.7. *Let* X,W *be two random variables. The* average conditional min-entropy *of* X *given* W *is defined as* $\widetilde{H}_\infty(X \mid W) = -\log_2\left(\mathbf{E}_{w\sim W}\left[\max_x \mathbf{Pr}\left[X = x \mid W = w\right]\right]\right)$.

Lemma 4.8 ([DORS08])**.** *Let* X,Y,Z *be random variables such that* Y *has support size at most* 2^ℓ*. Then,* $\widetilde{H}_\infty(X \mid (Y,Z)) \geq \widetilde{H}_\infty(X \mid Z) - \ell$*. In particular,* $\widetilde{H}_\infty(X \mid Y) \geq H_\infty(X) - \ell$.

Lemma 4.9 ([DORS08])**.** *For any two random variables* X,Y *and any* $\varepsilon > 0$*, it holds that*

$$\mathop{\mathbf{Pr}}_{y\sim Y}\left[H_\infty(X \mid Y = y) < \widetilde{H}_\infty(X \mid Y) - \log(1/\varepsilon)\right] \leq \varepsilon.$$

We further make use of the following simple lemma.

Lemma 4.10. *Let* X,Y,Z *be random variables such that for any* $y \in \mathsf{supp}(Y)$*, the random variables* $(X \mid Y = y)$ *and* $(Z \mid Y = y)$ *are independent. Assume that* X *is supported on* $\{0,1\}^n$*. Then,* $\mathsf{SD}\left((X,Y,Z),(U_n,Y,Z)\right) = \mathsf{SD}\left((X,Y),(U_n,Y)\right)$.

4.3 Correlation breakers with advice

In this section we introduce the notion of *correlation breakers with advice* which is a variant of local correlation breakers [Coh15a] that is implicit in [CGL15]. We then state the parameters of the explicit construction obtained by following the proof of [CGL15].

Definition 4.11. *For an integer $t \geq 1$ a* t-correlation-breaker with advice *for entropy k and error ε is a function*

$$\mathsf{AdvCB}\colon \{0,1\}^w \times \{0,1\}^\ell \times \{0,1\}^a \to \{0,1\}^m$$

with the following property. Let $X^0, X^1, \ldots, X^t$ be random variables distributed over $\{0,1\}^w$ such that X^0 has min-entropy k. Let $Y^0, Y^1, \ldots, Y^t$ be random variables over $\{0,1\}^\ell$ that are jointly independent of $(X^0, X^1, \ldots, X^t)$ such that Y^0 is uniform. Then, for any strings $s^0, s^1, \ldots, s^t \in \{0,1\}^a$ such that $s^0 \notin \{s^1, \ldots, s^t\}$, it holds that

$$\left(\mathsf{AdvCB}(X^0, Y^0, s^0), \{\mathsf{AdvCB}(X^i, Y^i, s^i)\}_{i=1}^t\right) \approx_\varepsilon (U_m, \cdot)\,.$$

The third argument to the function AdvCB *is called the* advice.

Theorem 4.12. *For all integers ℓ, w, a, t and for any $\varepsilon \in (0,1)$ such that*

$$\ell = \Omega\left(at \cdot \log\left(\frac{aw}{\varepsilon}\right)\right), \tag{4.1}$$

there exists a $\mathrm{poly}(\ell, w)$-time computable t-correlation-breaker with advice $\mathsf{AdvCB}\colon \{0,1\}^w \times \{0,1\}^\ell \times \{0,1\}^a \to \{0,1\}^m$, for entropy

$$k = \Omega\left(at \cdot \log\left(\frac{a\ell}{\varepsilon}\right)\right), \tag{4.2}$$

with error ε and $m = \Omega(\ell/(at))$ output bits.

4.4 An equivalent definition for t-non-malleable extractors

In this section we give an equivalent definition for t-non-malleable extractors. We make use of this equivalence in some of our proofs, and in general, we find this alternative definition to be more convenient to work with than the original definition of non-malleable extractors.

Definition 4.13 (Dichotomic t-non-malleable extractors)**.** *A function $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is called a* dichotomic t-non-malleable extractor *for entropy k with error ε if for any (n,k)-source X there exists a set $B \subset \{0,1\}^d$ of size at most $\varepsilon \cdot 2^d$ such that the following holds. For any $y \notin B$ and any $y^1, \ldots, y^t \in \{0,1\}^d \setminus \{y\}$ it holds that*

$$\left(\mathsf{Ext}(X, y), \left\{\mathsf{Ext}(X, y^i)\right\}_{i=1}^t\right) \approx_\varepsilon (U_m, \cdot)\,.$$

The following simple lemma that shows the equivalence between the definition of non-malleable extractors and dichotomic non-malleable extractors, up to some loss in the error guarantee, builds on ideas by [CZ15].

Lemma 4.14. *Let $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ be some function.*

- *If* Ext *is a* t*-non-malleable extractor for entropy* k *with error* ε *then* Ext *is a dichotomic* t*-non-malleable extractor for entropy* k *with error* $\sqrt{\varepsilon}$*.*
- *If* Ext *is a dichotomic* t*-non-malleable extractor for entropy* k *with error* ε *then* Ext *is a* t*-non-malleable extractor for entropy* k *with error* 2ε*.*

Proof. We start by proving the first item. Let X be an (n,k)-source. Define B to be the set of all $y \in \{0,1\}^d$ for which there exist $y^1, \ldots, y^t \in \{0,1\}^d \setminus \{y\}$ such that

$$\left(\mathsf{Ext}(X,y), \{\mathsf{Ext}(X,y^i)\}_{i=1}^t\right) \not\approx_{\sqrt{\varepsilon}} (U_m, \cdot)\,. \tag{4.3}$$

We want to prove that $\beta \triangleq |B|/2^d \leq \sqrt{\varepsilon}$. To this end, for every $i \in [t]$ define the function $\mathcal{A}_i \colon \{0,1\}^d \to \{0,1\}^d$ as follows. For $y \notin B$ define $A_i(y)$ arbitrarily, only ensuring that there are no fixed points. For $y \in B$, let $y^1, \ldots, y^t \in \{0,1\}^d \setminus \{y\}$ be a sequence of seeds for which Equation (4.3) holds, and set $A_i(y) = y^i$. Note that by the definition of B,

$$\left(\mathsf{Ext}(X,Y), \{\mathsf{Ext}(X,\mathcal{A}_i(Y))\}_{i=1}^t\right) \not\approx_{\beta\cdot\sqrt{\varepsilon}} (U_m, \cdot)\,.$$

On the other hand, as Ext is a t-non-malleable extractor with error ε

$$\left(\mathsf{Ext}(X,Y), \{\mathsf{Ext}(X,\mathcal{A}_i(Y))\}_{i=1}^t\right) \approx_{\varepsilon} (U_m, \cdot)\,,$$

which concludes the proof of the first item.

As for the second item, let $\mathcal{A}_1, \ldots, \mathcal{A}_t \colon \{0,1\}^d \to \{0,1\}^d$ be functions with no fixed points, and let X be an (n,k)-source. As Ext is a dichotomic t-non-malleable extractor for entropy k with error ε, there exists a set $B \subset \{0,1\}^d$ of size $|B| \leq \varepsilon \cdot 2^d$ such that for any $y \notin B$ it holds that

$$\left(\mathsf{Ext}(X,y), \{\mathsf{Ext}(X,\mathcal{A}_i(y))\}_{i=1}^t\right) \approx_{\varepsilon} (U_m, \cdot)\,.$$

As $|B| \leq \varepsilon \cdot 2^d$ we conclude that

$$\left(\mathsf{Ext}(X,Y), \{\mathsf{Ext}(X,\mathcal{A}_i(Y))\}_{i=1}^t\right) \approx_{2\varepsilon} (U_m, \cdot)\,,$$

which concludes the proof of the second item. □

5 A New Reduction From Non-Malleable Extractors to Advice Generators

In this section we describe our reduction from non-malleable extractors to advice generators. Most of our results make use of this reduction by plugging in different advice generators (some of which are constructed using other non-malleable extractors). We start by giving a formal definition of advice generators.

Definition 5.1 (Advice generators)**.** *A function* $\mathsf{AdvGen}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^a$ *is called an* advice generator *for entropy* k *with error* ε *if the following holds. For any* (n,k)*-source* X*, an independent random variable* Y *that is uniform over* $\{0,1\}^d$*, and a function* $\mathcal{A}\colon \{0,1\}^d \to \{0,1\}^d$ *with no fixed points, it holds that*

$$\Pr_{\substack{x\sim X\\ y\sim Y}}[\mathsf{AdvGen}(x,y) = \mathsf{AdvGen}(x,\mathcal{A}(y))] \leq \varepsilon.$$

The second input to AdvGen *is called the* seed.

For our reduction to work, some extra guarantee is needed from the advice generator. Informally speaking, it is required that even conditioned on the fixings of the advices, the random variables X, Y remain independent and have a sufficient amount of entropy. The formal guarantee is encapsulated in the following definition.

Definition 5.2 (Nice advice generators)**.** *An advice generator* $\mathsf{AdvGen}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^a$ *for entropy* k *with error* ε *is said to be* d_1*-nice if the following holds. Let* X *be an* (n,k)*-source, let* Y *be a random variable that is independent of* X *and is uniformly distributed over* $\{0,1\}^d$*, and let* $\mathcal{A}\colon \{0,1\}^d \to \{0,1\}^d$ *be a function with no fixed points. Then, except with probability* ε *over the fixings of* $\mathsf{AdvGen}(X,Y)$*,* $\mathsf{AdvGen}(X,\mathcal{A}(Y))$ *it holds that:*

- X, Y *are independent.*
- $H_\infty(X) \geq 0.99k$*.*
- *The length* $d - d_1$ *suffix of* Y *has min-entropy rate* 0.99*.*

In the following lemma we present our reduction from non-malleable extractors to nice advice generators.

Lemma 5.3. *There exist universal constants* $0 < c < 1 < c', c''$ *such that the following holds. Let* $\mathsf{AdvGen}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^a$ *be an explicit advice generator for entropy* k *with error* ε *that is* d_1*-nice, with* $d_1 \leq d/2$*. Then, for any integer* m *such that*

$$\begin{aligned} m &\leq c \cdot k/a \\ d &\geq c' \cdot \max\left(a \cdot \log\left(\frac{am}{\varepsilon}\right), \log(n/\varepsilon)\right), \\ k &\geq c'' \cdot \max\left(a \cdot \log\left(\frac{ad}{\varepsilon}\right), \log(n/\varepsilon)\right), \end{aligned}$$

there exists an explicit non-malleable extractor $\mathsf{NMExt}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *for entropy* k*, with error* $O(\sqrt{\varepsilon})$*.*

Proof. We start by describing the construction of NMExt and then turn to the analysis. Given a string $y \in \{0,1\}^d$, we partition y to three consecutive substrings $y = y_1 \circ y_2 \circ y_3$, where $|y_1| = d_1$, $|y_2| = d_2 = \Omega(\log(n/\varepsilon))$ is a sufficient length for a seed of the extractor from Theorem 4.3 set with error ε, and $|y_3| = d_3 = 9d_2$. By choosing a sufficiently large constant c', d is large enough so to satisfy these properties. We make use of the following building blocks:

- Let $\mathsf{Raz}\colon \{0,1\}^n \times \{0,1\}^{d_2} \to \{0,1\}^\ell$ be the extractor from Theorem 4.3, where

$$\ell = c''' \cdot \max\left(am, a\log(ad/\varepsilon)\right)$$

  for some suitable constant c''' to be chosen next. By our choice of d_2, the error of Raz is bounded above by ε.

- Let $\mathsf{AdvCB}\colon \{0,1\}^{d_3} \times \{0,1\}^\ell \times \{0,1\}^a \to \{0,1\}^m$ be the correlation breaker with advice from Theorem 4.12 set with error ε. By Theorem 4.12, the constant c''' can be chosen such that the output length of AdvCB is indeed m.

With the notation set and using the building blocks above, we define

$$\mathsf{NMExt}(x,y) = \mathsf{AdvCB}\left(y_3, \mathsf{Raz}(x,y_2), \mathsf{AdvGen}(x,y)\right).$$

We now turn to the analysis. Let X be an (n,k)-source, let Y be an independent random variable that is uniformly distributed over $\{0,1\}^d$, and let $\mathcal{A}\colon \{0,1\}^d \to \{0,1\}^d$ be a function with no fixed points. As AdvGen is a d_1-nice advice generator with error ε, we have that except with probability ε over the fixings $\alpha \sim \mathsf{AdvGen}(X,Y)$, $\alpha' \sim \mathsf{AdvGen}(X,\mathcal{A}(Y))$, it holds that

- $\alpha \neq \alpha'$.
- X, Y remain independent.
- $H_\infty(X) \geq 0.99k$.
- The length $d - d_1$ suffix of Y has min-entropy rate 0.99.

We condition on such fixing. Next, we argue that except with probability ε over $y_3 \sim Y_3$ it holds that $Y_2 \mid (Y_3 = y_3)$ has min-entropy rate at least 0.6. To see this, apply Lemma 4.8 to obtain

$$\widetilde{H}_\infty(Y_2 \circ Y_3 \mid Y_3) \geq H_\infty(Y_2 \circ Y_3) - |Y_3| \geq 0.99(d_2+d_3) - d_3 = 0.9d_2.$$

Thus, by Lemma 4.9, except with probability ε over $y_3 \sim Y_3$ it holds that

$$H_\infty(Y_2 \mid Y_3 = y_3) = H_\infty(Y_2 \circ Y_3 \mid Y_3 = y_3) \geq 0.9d_2 - \log(1/\varepsilon) \geq 0.6d_2.$$

Therefore, except with probability ε over the fixing of Y_3, the min-entropy rate of Y_2 is bounded below by 0.6. For the remaining of the proof we assume that the min-entropy rate of Y_2 is at least 0.6, and aggregate an additional error of ε to the total error.

By setting the constant c'' to be large enough, we can guarantee that $H_\infty(X) \geq 0.99k \geq 2\ell$ and that $H_\infty(X) = \Omega(d_2)$. Since Y_2 is a $(d_2, 0.6d_2)$-source with $d_2 = \Omega(\log(n/\varepsilon))$, we can apply Theorem 4.3 and conclude that

$$(\mathsf{Raz}(X,Y_2), Y_2) \approx_\varepsilon (U_\ell, Y_2).$$

As $\mathsf{Raz}(X, Y_2)$ is independent of $\mathcal{A}(Y)_2$ conditioned on the fixing of Y_2, Lemma 4.10 implies that

$$(\mathsf{Raz}(X, Y_2), Y_2, \mathcal{A}(Y)_2) \approx_\varepsilon (U_\ell, \cdot)\,.$$

Thus, except with probability $\sqrt{\varepsilon}$ over the fixings of $Y_2, \mathcal{A}(Y)_2$ it holds that $\mathsf{Raz}(X, Y_2)$ is $\sqrt{\varepsilon}$-close to uniform. As for the entropy loss of Y_3 incurred by these fixings,

$$\widetilde{H}_\infty\left(Y_3 \mid Y_2, \mathcal{A}(Y)_2\right) = \widetilde{H}_\infty\left(Y_2 \circ Y_3 \mid Y_2, \mathcal{A}(Y)_2\right) \geq 0.99(d_2 + d_3) - 2d_2 \geq 0.8d_3,$$

and so by Lemma 4.9, except with probability ε over the fixings of $Y_2, \mathcal{A}(Y)_2$, it holds that Y_3 has min-entropy rate larger than 0.5.

To summarize, except with probability $O(\sqrt{\varepsilon})$ over all fixings done so far, we have that

- The joint distribution of $\mathsf{Raz}(X, Y_2)$, $\mathsf{Raz}(X, \mathcal{A}(Y)_2)$ is independent of the joint distribution of $Y_3, \mathcal{A}(Y)_3$.
- The min-entropy of Y_3 is bounded below by

$$\frac{d_3}{2} \geq \frac{9d}{20} = \Omega\left(a \cdot \log\left(\frac{am}{\varepsilon}\right)\right) = \Omega\left(a \cdot \log\left(\frac{a\ell}{\varepsilon}\right)\right), \tag{5.1}$$

  where we used the lemma hypothesis on d for the second inequality and that $d \geq 2d_1$ for the first inequality. The last equality follows by our choice of ℓ.
- $\mathsf{Raz}(X, Y_2)$ is $O(\sqrt{\varepsilon})$-close to uniform.

Therefore, we can apply Theorem 4.12 and conclude that

$$(\mathsf{NMExt}(X, Y), \mathsf{NMExt}(X, \mathcal{A}(Y)), Y) \approx_{O(\sqrt{\varepsilon})} (U_m, \cdot).$$

Note that the hypothesis of Theorem 4.12 holds. In particular, Equation (4.1) holds by our choice of ℓ, and Equation (4.2) follows by Equation (5.1). This concludes the proof. □

6 Reducing the Entropy Requirement of Non-Malleable Extractors

In this section we prove the following lemma which is a formal restatement of Lemma 2.3.

Lemma 6.1. *There exists a universal constant $\alpha > 0$ such that the following holds. Let $\mathsf{NMExt}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^{\log(1/\varepsilon)}$ be an explicit non-malleable extractor with error ε for entropy k. Let m be any integer. Assume that*

$$\begin{aligned} k &= \Omega(d^\alpha \cdot \log(n/\varepsilon)), \\ d &= \Omega\left(\log^4(1/\varepsilon) \cdot \log^2 m\right), \\ m &= O\left(\sqrt{k}/\log(1/\varepsilon)\right). \end{aligned}$$

Then, there exists an explicit non-malleable extractor $\mathsf{NMExt}'\colon \{0,1\}^n \times \{0,1\}^{d'} \to \{0,1\}^m$ for entropy $k' = k/d^\alpha$ with seed length $d' = O(d)$ and error $O(\varepsilon^{1/4})$.

The proof of Lemma 6.1 consists of two steps. First, we show how to construct an advice generator for entropy k' given a non-malleable extractor for entropy $k > k'$. This is done in the next subsection. Then, we apply Lemma 5.3 to obtain a non-malleable extractor for entropy k' using this advice generator. This second step is covered in Section 6.2.

6.1 From non-malleable extractors to advice generators for lower entropy

In this section we prove the following lemma.

Lemma 6.2. *There exists a universal constant $c > 1$ such that the following holds. Let $\mathsf{NMExt}\colon \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}^{\log(1/\varepsilon)}$ be an explicit non-malleable extractor for entropy k with error ε. Let $\delta > 0$, and set $\Delta = \delta^{-c}$. Assume that*

$$\delta k = \Omega((\Delta + \log d_1) \cdot \log(1/\varepsilon)). \tag{6.1}$$

Then, there exists an explicit d_1-nice advice generator $\mathsf{AdvGen}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^a$ for entropy δk with error $O(\sqrt{\varepsilon}) + 2^{-\Omega(\delta^2 n)}$, seed length $d = O(d_1)$, and $a = O(\Delta \cdot \log(1/\varepsilon))$ output bits.

Proof. Let $d_2 = 1000 d_1$ and set $d = d_1 + d_2$. For the construction of AdvGen we make use of the following building blocks:

- Let $\{\mathsf{Cond}_i\colon \{0,1\}^n \to \{0,1\}^u\}_{i=1}^{\Delta}$ be the sequence of efficiently computable functions given by Theorem 4.5 when applied with n and δ. By Theorem 4.5, $u = n \cdot \mathrm{poly}(\delta)$ and $\Delta = \delta^{-c}$ for some universal constant c. This constant will be the constant c introduced in the statement of the lemma.
- Let $\mathsf{ECC}\colon \{0,1\}^{d_2} \to \colon \{0,1\}^{D_2}$ be the error correcting code from Theorem 4.4 set with relative distance $1/4$. By Theorem 4.4, $D_2 = O(d_2)$.
- Let $r = \log_{4/3}(1/\varepsilon)$ and set $m = r \cdot \log_2 D_2$. Let $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}^m$ be the extractor from Theorem 4.2. Note that we use a seed of the same length d_1 as was used for the non-malleable extractor NMExt. This suffices for us since by Theorem 4.2, a seed of that length is sufficient for Ext to have error ε. By identifying $\{0,1\}^m$ with $[D_2]^r$, we interpret the output of Ext as an r-tuple in $[D_2]$.

Set $a = \Delta \cdot \log_2(1/\varepsilon) + \log_{4/3}(1/\varepsilon)$. We define the function $\mathsf{AdvGen}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^a$ as follows:

$$\mathsf{AdvGen}(x, y) = \mathsf{NMExt}(\mathsf{Cond}_1(x), y_1) \circ \cdots \circ \mathsf{NMExt}(\mathsf{Cond}_\Delta(x), y_1) \circ \mathsf{ECC}(y_2)_{\mathsf{Ext}(x, y_1)}.$$

Note that we feed as a first argument to NMExt u bit strings rather than the n bit strings it expects. We do so for simplicity of presentation. This minor technical issue can be overcome

by appending zeros to the u bit string so to obtain an n bit string, and instructing the extractor to ignore these zeros.

Having the definition of AdvGen at hand, we turn to the analysis. Let X be an $(n, \delta k)$-source and let Y be an independent random variable that is uniformly distributed over $\{0,1\}^d$. Consider a function $\mathcal{A}\colon \{0,1\}^d \to \{0,1\}^d$ with no fixed points. By Theorem 4.5 (and ignoring the convexity, for ease of readability) there exists $g \in [\Delta]$ such that $\mathsf{Cond}_g(X)$ is $2^{-\Omega(\delta^2 n)}$-close to having min-entropy k. Therefore, by Lemma 4.14, there exists a set $B \subset \{0,1\}^{d_1}$ of density $\sqrt{\varepsilon}$ such that for any $y_1 \notin B$ and any d_1-bit string $y_1' \neq y_1$, it holds that

$$(\mathsf{NMExt}(\mathsf{Cond}_g(X), y_1), \mathsf{NMExt}(\mathsf{Cond}_g(X), y_1')) \approx_{\sqrt{\varepsilon}+2^{-\Omega(\delta^2 n)}} (U, \cdot)\,. \tag{6.2}$$

We now fix $y_1 \sim Y_1$ and $y_1' \sim \mathcal{A}(Y)_1$. Clearly, these fixings do not introduce dependencies between X, Y. Furthermore, by the above, we can aggregate $\sqrt{\varepsilon}$ to the total error and assume that $y_1 \notin B$. We continue by considering two cases.

Case 1 – $y_1 \neq y_1'$. As the output length of NMExt is $\log(1/\varepsilon)$, Equation (6.2) implies that the probability that $\mathsf{NMExt}(\mathsf{Cond}_g(X), y_1) = \mathsf{NMExt}(\mathsf{Cond}_g(X), y_1')$ is bounded above by $O(\sqrt{\varepsilon}) + 2^{-\Omega(\delta^2 n)}$. Thus, in this case, except with probability $O(\sqrt{\varepsilon}) + 2^{-\Omega(\delta^2 n)}$ we have that $\mathsf{AdvGen}(X, Y) \neq \mathsf{AdvGen}(X, \mathcal{A}(Y))$.

Case 2 – $y_1 = y_1'$. This case follows the same idea as in the proofs of Theorem 8.1 and Lemma 7.1. Conditioned on $y_1 = y_1'$ we have that $Y_2 \neq \mathcal{A}(Y)_2$. Hence, the codewords $\mathsf{ECC}(Y_2), \mathsf{ECC}(\mathcal{A}(Y)_2)$ agree on at most $3/4$ of the coordinates of $[D_2]$. Hence, the set of r-tuples over $[D_2]$ for which $\mathsf{ECC}(Y_2)$ agrees with $\mathsf{ECC}(\mathcal{A}(Y)_2)$ on all r coordinates of the tuple has density at most $(3/4)^r = \varepsilon$ within $[D_2]^r$. We denote this set of r-tuples by $B' \subseteq [D_2]^r$.

Recall that Ext is a strong seeded extractor with ε. Thus, except for probability $\sqrt{\varepsilon}$ over the choice of y_1, we have that $\mathsf{Ext}(X, y_1)$ is $\sqrt{\varepsilon}$-close to uniform. Therefore, for such y_1, $\mathbf{Pr}[\mathsf{Ext}(X, y_1) \in B'] = O(\sqrt{\varepsilon})$. Hence, except with probability $O(\sqrt{\varepsilon})$ over the fixings done so far, we have that also in this case, $\mathsf{AdvGen}(X, Y) \neq \mathsf{AdvGen}(X, \mathcal{A}(Y))$.

As for niceness property, by Lemma 4.8, the fixings of $Y_1, \mathcal{A}(Y)_1$ reduce the average min-entropy of Y_2 by a most $2d_1$. Once $Y_1, \mathcal{A}(Y)_1$ are fixed, we have that $\mathsf{Ext}(X, Y_1)$ and $\mathsf{Ext}(X, \mathcal{A}(Y)_1)$ are deterministic functions of X. Thus, we can fix the latter random variables without introducing dependencies between X, Y. Further, by Lemma 4.8, the average min-entropy of X decreases by at most $2m$. After these fixings, $\mathsf{ECC}(Y_2)_{\mathsf{Ext}(X,Y_1)}$ and $\mathsf{ECC}(\mathcal{A}(Y)_2)_{\mathsf{Ext}(X,\mathcal{A}(Y)_1)}$ are deterministic functions of Y that consist of r bits each. Thus, fixing these random variables will reduce the average min-entropy of Y by at most $2r$. Further, these fixings do not introduce any dependencies between X, Y.

Finally, after all of the fixings done so far, $\mathsf{AdvGen}(X, Y)$ and $\mathsf{AdvGen}(X, \mathcal{A}(Y))$ are deterministic functions of X. We can therefore fix these random variables, which will result in an entropy-loss of at most $2\Delta \cdot \log(1/\varepsilon)$. Again, these last fixings do not introduce any dependencies between X, Y.

To summarize, in the process of fixing $\mathsf{AdvGen}(X, Y)$, $\mathsf{AdvGen}(X, \mathcal{A}(Y))$, the random variable Y lost an average entropy of $2d_1 + 2\log_{4/3}(1/\varepsilon)$. Thus, by the choice of d_2, except

with probability ε over these fixings, Y_2 has min-entropy rate 0.99. As for X, the fixings reduced its average min-entropy by

$$2\Delta \log(1/\varepsilon) + 2m = O\left(\Delta \log(1/\varepsilon) + \log(d)\log(1/\varepsilon)\right),$$

and so by Equation (6.1), except with probability ε over the fixings of $\mathsf{AdvGen}(X, Y)$, $\mathsf{AdvGen}(X, \mathcal{A}(Y))$, the source X has min-entropy rate 0.99. This concludes the proof. □

6.2 Proof of Lemma 6.1

Proof of Lemma 6.1. Let c be the constant from Lemma 6.2. Set $\alpha = 1/(4c)$ and set $\delta = d^{-\alpha}$. We borrow the notation from Lemma 6.2 and write $\Delta = \delta^{-c} = d^{1/4}$. First, we apply Lemma 6.2 with the non-malleable extractor NMExt and δ as set above. To show that this application is valid one needs to verify that

Claim 6.3.

$$\delta k = \Omega((\Delta + \log d) \cdot \log(1/\varepsilon)).$$

Proof. Note that $\Delta = d^{1/4} = \Omega(\log d)$. Thus, to prove the claim it suffices to show that $\delta k = \Omega(\Delta \cdot \log(1/\varepsilon))$. To verify that this inequality holds, it suffices to show that $k = \Omega(\Delta^2 \cdot \log(1/\varepsilon))$, or equivalently that $k = \Omega(\sqrt{d} \cdot \log(1/\varepsilon))$, which indeed follows by our assumption. □

Lemma 6.2 transforms the given NMExt to an efficiently computable d-nice advice generator $\mathsf{AdvGen}\colon \{0,1\}^n \times \{0,1\}^{O(d)} \to \{0,1\}^a$ for entropy δk with advice length $a = O(\Delta \cdot \log(1/\varepsilon))$ and error $O(\sqrt{\varepsilon}) + 2^{-\Omega(\delta^2 n)} = O(\sqrt{\varepsilon})$. Next, we would like to apply Lemma 5.3 to AdvGen so to obtain a non-malleable extractor $\mathsf{NMExt}'\colon \{0,1\}^n \times \{0,1\}^{O(d)} \to \{0,1\}^m$ for entropy δk, with error $O(\varepsilon^{1/4})$. To this end, we need to verify that the hypothesis of the lemma holds, which is guaranteed by the following cliam.

Claim 6.4.

$$\begin{aligned} m &= O(\delta k/a), \\ d &= \Omega\left(a \cdot \log\left(\frac{am}{\varepsilon}\right) + \log(n/\varepsilon)\right), \\ \delta k &= \Omega\left(a \cdot \log\left(\frac{ad}{\varepsilon}\right) + \log(n/\varepsilon)\right), \end{aligned}$$

Proof. To prove the first inequality it suffices to show that $m = O(k/(\Delta^2 \cdot \log(1/\varepsilon)))$. Since $\Delta = d^{1/4}$ and $k > d$, it suffices to show that $m = O(\sqrt{k}/\log(1/\varepsilon))$, which follows by the hypothesis of the lemma. As for the second inequality, first note that $d = \Omega(\log(n/\varepsilon))$ as d is a seed for the non-malleable extractor NMExt. Thus, it suffices to verify that $d = \Omega(a \cdot \log(am/\varepsilon))$. Since $a = O(\Delta \cdot \log(1/\varepsilon))$, this inequality holds as long as $d = \Omega(\Delta^2 \cdot \log^2(1/\varepsilon) \cdot \log m)$. Since $\Delta^2 = \sqrt{d}$, it suffices to verify that $d = \Omega(\log^4(1/\varepsilon) \cdot \log^2 m)$, which holds by assumption.

As for the last inequality, we first show that $\delta k = \Omega(a \cdot \log(ad/\varepsilon))$ and afterwards turn to verify that $\delta k \geq \log(n/\varepsilon)$. For the first inequality, it suffices to show that $k = \Omega(\Delta^2 \cdot \log^2(1/\varepsilon) \cdot \log d)$. As $\Delta^2 = \sqrt{d}$ and since $\sqrt{d} = \Omega(\log^2(1/\varepsilon))$, it suffices to show that $k = \Omega(d \cdot \log d)$ which follows by assumption. Further, as $\delta = d^{-\alpha}$, the inequality $\delta k \geq \log(n/\varepsilon)$ follows. □

By the above claim, NMExt' is indeed a non-malleable extractor for min-entropy δk, with seed length $O(d)$, error $O(\varepsilon^{1/4})$ and m output bits. This concludes the proof. □

7 Increasing the Output Length of a Non-Malleable Extractor

A general tool we use is an algorithm that increases the output length of a given non-malleable extractor in a black-box manner. This is given by the following lemma which is a formal restatement of Lemma 2.4.

Lemma 7.1. *There exists a universal constant $\alpha > 0$ such that the following holds. Let $\mathsf{NMExt}\colon \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}^{\log(1/\varepsilon)}$ be an explicit non-malleable extractor for entropy k with error ε such that*

$$k = \Omega\left(\log(d_1/\varepsilon) \cdot \log(1/\varepsilon) + \log(n/\varepsilon)\right).$$

Then, for any $m < \alpha k / \log(1/\varepsilon)$ there exists an explicit non-malleable extractor $\mathsf{NMExt}'\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ for entropy k with error $O(\varepsilon^{1/4})$, having seed length

$$d = O\left(d_1 + \log(m/\varepsilon) \cdot \log(1/\varepsilon)\right).$$

Note that Lemma 2.4 follows by Lemma 7.1 for constant ε by setting $m = \Omega(k)$. Indeed, the expression $\log(m/\varepsilon) \cdot \log(1/\varepsilon)$ in the resulted seed length d is $O(\log k)$ which is always smaller than d_1 (as the seed length of any seeded extractor, in particular NMExt, is at least $\log(n-k)$), and so in the setting of Lemma 2.4, $d = O(d_1)$.

Proof of Lemma 7.1. During the proof we make use of the following notation. Given a string $y \in \{0,1\}^d$, we write $y = y_1 \circ y_2$ where $|y_1| = d_1$ and define $d_2 = d - d_1 = 500 d_1$. We make use of the following building blocks:

- Let $\mathsf{ECC}\colon \{0,1\}^{d_2} \to \colon \{0,1\}^{D_2}$ be the error correcting code from Theorem 4.4 set with relative distance $1/4$. By Theorem 4.4, $D_2 = O(d_2)$.
- Let $r = \log_{4/3}(1/\varepsilon)$ and set $v = r \cdot \log_2 D_2$. Let $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}^v$ be the extractor from Theorem 4.2. Note that we use a seed of the same length d_1 as was used for the non-malleable extractor NMExt. By identifying $\{0,1\}^v$ with $[D_2]^r$, we interpret the output of Ext as an r-tuple over $[D_2]$.

We proceed by proving the following claim.

Claim 7.2. *The function*

$$\mathsf{AdvGen}(x,y) = \mathsf{NMExt}(x,y_1) \circ \mathsf{ECC}(y_2)_{\mathsf{Ext}(x,y_1)}$$

is a d_1-nice advice generator for entropy k with error $O(\sqrt{\varepsilon})$.

Proof. By Lemma 4.14, there exists a set $B \subset \{0,1\}^{d_1}$ of density $\sqrt{\varepsilon}$ such that for any $y_1 \notin B$ and any d_1-bit string $y_1' \neq y_1$, it holds that

$$(\mathsf{NMExt}(X,y_1), \mathsf{NMExt}(X,y_1')) \approx_{\sqrt{\varepsilon}} (U,\cdot)\,. \tag{7.1}$$

We now fix $y_1 \sim Y_1$ and $y_1' \sim \mathcal{A}(Y)_1$. Clearly, these fixings do not introduce dependencies between X,Y. Furthermore, by the above, we can aggregate $\sqrt{\varepsilon}$ to the total error and assume that $y_1 \notin B$. We continue by considering two cases.

Case 1 – $y_1 \neq y_1'$. In this case Equation (7.1) holds. In particular, as NMExt has output length $\log(1/\varepsilon)$, the probability that $\mathsf{NMExt}(X,y_1) = \mathsf{NMExt}(X,y_1')$ is bounded above by $O(\sqrt{\varepsilon})$. Thus, in this case, except with probability $O(\sqrt{\varepsilon})$ we have that $\mathsf{AdvGen}(X,Y) \neq \mathsf{AdvGen}(X,\mathcal{A}(Y))$.

Case 2 – $y_1 = y_1'$. Here we follow the idea of [CGL15] from Theorem 8.1. Conditioned on $y_1 = y_1'$ we have that $Y_2 \neq \mathcal{A}(Y)_2$, and so the codewords $\mathsf{ECC}(Y_2), \mathsf{ECC}(\mathcal{A}(Y)_2)$ agree on at most $3/4$ of the coordinates of $[D_2]$. Hence, the set of r-tuples over $[D_2]$ for which $\mathsf{ECC}(Y_2)$ agrees with $\mathsf{ECC}(\mathcal{A}(Y)_2)$ on all r coordinates of the tuple has density at most $(3/4)^r = \varepsilon$ within $[D_2]^r$. We denote this set of r-tuples by $B' \subseteq [D_2]^r$.

Recall that Ext is a strong seeded extractor with error ε. Moreover, $H_\infty(X) \geq k = \Omega(v)$, and so except for probability $\sqrt{\varepsilon}$ over the choice of y_1, we have that $\mathsf{Ext}(X,y_1)$ is $\sqrt{\varepsilon}$-close to uniform. For any such y_1 we have that $\mathbf{Pr}[\mathsf{Ext}(X,y_1) \in B'] = O(\sqrt{\varepsilon})$. Thus, except with probability $O(\sqrt{\varepsilon})$ over the fixings done so far, we have that also in this case $\mathsf{AdvGen}(X,Y) \neq \mathsf{AdvGen}(X,\mathcal{A}(Y))$.

As for the niceness property, by Lemma 4.8, the fixings of $Y_1, \mathcal{A}(Y)_1$ reduce the average min-entropy of Y_2 by a most $2d_1$. Once $Y_1, \mathcal{A}(Y)_1$ are fixed, we have that $\mathsf{Ext}(X,Y_1)$, $\mathsf{Ext}(X,\mathcal{A}(Y)_1)$, $\mathsf{NMExt}(X,Y_1)$, and $\mathsf{NMExt}(X,\mathcal{A}(Y)_1)$ are all deterministic functions of X. Thus, we can fix the latter random variables without introducing dependencies between X,Y. Further, by Lemma 4.8, the average min-entropy of X decreases by at most $2v + 2\log(1/\varepsilon) = O(\log(1/\varepsilon) \cdot \log d_1)$.

After these fixings, $\mathsf{ECC}(Y_2)_{\mathsf{Ext}(X,Y_1)}$ and $\mathsf{ECC}(\mathcal{A}(Y)_2)_{\mathsf{Ext}(X,\mathcal{A}(Y)_1)}$ are deterministic functions of Y, each consists of r bits. Thus, fixing these random variables will reduce the average min-entropy of Y by at most $2r = O(\log(1/\varepsilon))$. Further, these fixings do not introduce any dependencies between X,Y. Note that after all of the fixings done so far, $\mathsf{AdvGen}(X,Y)$ and $\mathsf{AdvGen}(X,\mathcal{A}(Y))$ are fixed.

To summarize, in the process of fixing $\mathsf{AdvGen}(X,Y)$, $\mathsf{AdvGen}(X,\mathcal{A}(Y))$, the random variable Y_2 lost an average entropy of $2d_1 + 2r$. Since $d_2 = 500d_1$ we have that except with

probability ε over these fixings, Y_2 has min-entropy rate 0.99. As for X, the fixings reduced its average min-entropy by $O(\log(1/\varepsilon) \cdot \log d_1)$, and so except with probability ε, X has min-entropy rate 0.99 conditioned on these fixings. □

To conclude the proof we apply Lemma 5.3 with AdvGen defined above and the parameter m. The hypothesis of Lemma 5.3 is met due to our hypothesis on m, d, k and since $a = O(\log(1/\varepsilon))$. □

8 Proof of Theorem 2.1

In this section we prove Theorem 2.1. For the proof we make use of the advice generator of [CGL15] that is given by the following theorem.

Theorem 8.1 ([CGL15])**.** *For any integer n and all $\varepsilon > 0$ there exists a $O(\log(n/\varepsilon))$-nice advice generator $\mathsf{AdvGen}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^a$ for entropy*

$$k = \Omega\left(\log(1/\varepsilon) \cdot \log\log(n/\varepsilon)\right) \tag{8.1}$$

with error ε, seed length $d = O(\log(n/\varepsilon))$, and $a = O(\log(n/\varepsilon))$ output bits.

We defer the proof of Theorem 8.1 to Section 8.1 and start by proving Theorem 2.1.

Proof of Theorem 2.1. Our first step is to apply Lemma 5.3 to the advice generator AdvGen given by Theorem 8.1. For simplicity, we consider a constant error ε. One can easily verify that this gives us a non-malleable extractor NMExt_0 for entropy $\Omega(\log n \cdot \log\log n)$ having seed length $O(\log n \cdot \log\log n)$.

Our second step would be to reduce the entropy requirement to $\Omega(\log n)$. To this end, we apply Lemma 6.2 to NMExt_0 with $\delta = O(1/\log\log n)$. One can easily verify that the hypothesis of Lemma 6.2 holds with this choice of δ. Thus, we obtain an advice generator with seed length $O(\log n \cdot \log\log n)$ and advice length $a = \operatorname{poly}\log\log n$ for entropy $\Omega(\log n)$.

We now apply Lemma 5.3 to AdvGen with constant output length m so to obtain a non-malleable extractor NMExt_1 with seed length $O(\log n \cdot \log\log n)$ for entropy $\Omega(\log n)$. One can easily verify that the hypothesis of Lemma 5.3 are met by our choice of δ.

To obtain our final non-malleable extractor, denoted by NMExt_2, we apply Lemma 7.1 to NMExt_1 with $m = \Omega(\log n)$. One can again easily verify that all the conditions of Lemma 7.1 hold and that the resulting non-malleable extractor, NMExt_2, supports entropy $\Omega(\log n)$, has seed length $O(\log n \cdot \log\log n)$, and has output length $\Omega(\log n)$. □

8.1 The [CGL15] advice generator

In this section we prove Theorem 8.1. We give a full proof here since the theorem as stated is somewhat implicit in [CGL15]. Nevertheless, we stress that all the ideas already appear in [CGL15].

Proof of Theorem 8.1. We start by describing the construction of AdvGen and then turn to the analysis. Let c be the universal constant from Theorem 4.2. Split $y = y_1 \circ y_2$, where y_1 consists of $d_1 = c \cdot \log(n/\varepsilon)$ bits, and set $d_2 = d - d_1$, where $d = c' \cdot d_1$ for some large enough constant c'. We define $\mathsf{AdvGen}(x, y) = y_1 \circ \phi(x, y)$, where $\phi(x, y)$ is described next. For the definition of ϕ we make use of the following building blocks:

- Let $\mathsf{ECC}\colon \{0,1\}^{d_2} \to \colon \{0,1\}^{D_2}$ be the error correcting code from Theorem 4.4 set with relative distance $1/4$. By Theorem 4.4, $D_2 = O(d_2)$.
- Let $r = \log_{4/3}(1/\varepsilon)$ and set $m = r \cdot \log_2 D_2$. Let $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}^m$ be the extractor from Theorem 4.2, set with error ε. Recall that we set d_1 to be large enough as required by a seed for Ext. Moreover, one can verify that by our assumption on k given by Equation (8.1), $k \geq 2m$.

Let $z = \mathsf{Ext}(x, y_1)$. We identify $\{0,1\}^m$ with $[D_2]^r$ and let $i_1(z), \ldots, i_r(z)$ be elements in $[D_2]$ corresponding to the r consecutive length $\log_2 D_2$ substrings of z. For $j = 1, \ldots, r$, we define

$$\phi(x, y)_j = \mathsf{ECC}(y_2)_{i_j(z)}.$$

We now turn to the analysis. First, note that the output length of AdvGen is $a = O(\log(n/\varepsilon))$ as stated. Indeed, the output is a concatenation of y_1 with $\phi(x, y)$, where $|y_1| = d_1 = O(\log(n/\varepsilon))$ and $\phi(x, y)$ consists of $r = O(\log(1/\varepsilon))$ bits. Now, by the strongness of Ext we have that

$$(\mathsf{Ext}(X, Y_1), Y_1) \approx_\varepsilon (U_m, \cdot)\,.$$

Further, by Lemma 4.10

$$(\mathsf{Ext}(X, Y_1), Y_1, \mathcal{A}(Y)_1) \approx_\varepsilon (U_m, \cdot)\,,$$

Indeed, the hypothesis of Lemma 4.10 is met as conditioned on any fixing of Y_1, the random variable $\mathsf{Ext}(X, Y_1)$ is independent of $\mathcal{A}(Y)_1$. Furthermore, by Lemma 4.8,

$$\widetilde{H}_\infty\left(Y_2 \mid Y_1, \mathcal{A}(Y)_1\right) \geq d_2 - 2d_1.$$

Thus, except with probability $2\sqrt{\varepsilon}$ over the fixing of $y_1 \sim Y_1$, $y_1' \sim \mathcal{A}(Y)_1$, it holds that $\mathsf{Ext}(X, y_1)$ is $\sqrt{\varepsilon}$-close to uniform and that

$$H_\infty(Y_2) \geq d_2 - 2d_1 - \log(1/\varepsilon) \geq 0.999 d_2. \tag{8.2}$$

From this point on we condition on a fixings of y_1, y_1' for which $\mathsf{Ext}(X, y_1)$ is $\sqrt{\varepsilon}$-close to uniform and for which Equation (8.2) holds, and aggregate $2\sqrt{\varepsilon}$ to the total error.

As y_1 is a prefix of $\mathsf{AdvGen}(x, y)$ and y_1' is a prefix of $\mathsf{AdvGen}(x, \mathcal{A}(y))$, we have that if $y_1 \neq y_1'$ then $\mathsf{AdvGen}(X, Y) \neq \mathsf{AdvGen}(X, \mathcal{A}(Y))$. Therefore, we may assume that $y_1 = y_1'$. Since $\mathcal{A}$ has no fixed points it holds that $Y_2 \neq \mathcal{A}(Y)_2$. Therefore, the codewords $\mathsf{ECC}(Y_2), \mathsf{ECC}(\mathcal{A}(Y)_2)$ agree on at most $3/4$ fraction of the coordinates of $[D_2]$, and so the

set of r-tuples over $[D_2]$ in which $\mathsf{ECC}(Y_2)$ equals $\mathsf{ECC}(\mathcal{A}(Y)_2)$ in all r coordinates has density at most $(3/4)^r = \varepsilon$ within $[D_2]^r$. We denote this set of "bad" r-tuples by $B \subseteq [D_2]^r$.

As $\mathsf{Ext}(X, y_1)$ is $\sqrt{\varepsilon}$-close to uniform, we have that

$$\mathbf{Pr}[\mathsf{Ext}(X, y_1) \in B] \leq \varepsilon + \sqrt{\varepsilon} \leq 2\sqrt{\varepsilon},$$

and so

$$\mathop{\mathbf{Pr}}_{\substack{x\sim X\\ y\sim Y}}[\mathsf{AdvGen}(x, y) = \mathsf{AdvGen}(x, \mathcal{A}(y))] = O(\sqrt{\varepsilon}).$$

As for the niceness property, note that conditioned on the fixings done so far, namely, the fixings of Y_1 and $\mathcal{A}(Y)_1$ it holds that both $\mathsf{Ext}(X, Y_1)$, $\mathsf{Ext}(X, \mathcal{A}(Y)_1)$ are deterministic functions of X. As these random variables consist of $2m$ bits altogether, we have that conditioned on the further fixings of $\mathsf{Ext}(X, Y_1)$, $\mathsf{Ext}(X, \mathcal{A}(Y)_1)$, the average min-entropy of X is bounded below by $k - 2m$. Hence, by Lemma 4.9, except with probability ε over the further fixings of these random variables,

$$H_\infty(X) \geq k - 2m - \log(1/\varepsilon) \geq 0.99k.$$

Note that the fixing of $\mathsf{Ext}(X, Y_1)$, $\mathsf{Ext}(X, \mathcal{A}(Y)_1)$ does not reduce the entropy of Y_2 and does not introduce any correlation between X, Y.

Conditioned on the fixings done so far, we have that $\mathsf{Ext}(X, Y_1)$, $\mathsf{Ext}(X, \mathcal{A}(Y)_1)$ are fixed, and so $\phi(X, Y)$, $\phi(X, \mathcal{A}(Y))$ are deterministic functions Y that consist of $2r$ bits. Thus, we can further condition the fixings of $\phi(X, Y)$, $\phi(X, \mathcal{A}(Y))$, which results in the fixings of $\mathsf{AdvGen}(X, Y)$ and $\mathsf{AdvGen}(X, \mathcal{A}(Y))$. Furthermore, as $2r + \log(1/\varepsilon) \leq 0.009d_2$, conditioned on these fixings we have that Y_2 has min-entropy rate 0.99 except with probability ε. Note that these fixings do not introduce dependencies between X, Y. Further, note that the total error incurred so far can be reduced from $O(\sqrt{\varepsilon})$ to ε without need for any change in the hypothesis of the theorem. This concludes the proof of the theorem. □

9 Proof of Theorem 2.2

Building on results developed so far, in this section we prove Theorem 2.1.

Proof of Theorem 2.2. Set $m = \log n$. Our starting point is the explicit non-malleable extractor $\mathsf{NMExt}_0 \colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ from Theorem 4.6 that supports entropy $0.6n$, has error $1/\log n$, and seed length $d = O(\log n)$. We apply Lemma 6.1 to NMExt_0 with m as set above so to obtain a second non-malleable extractor $\mathsf{NMExt}_1 \colon \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}^m$, where $d_1 = O(d)$. One can easily verify that the hypothesis of Lemma 6.1 holds, and so Lemma 6.1 guarantees that NMExt_1 is a non-malleable extractor for entropy $k_1 = k_0/d_0^\alpha = \Omega(n/(\log n)^\alpha)$, where α is the universal constant from Lemma 6.1. By Lemma 6.1, the error of NMExt_1 is $\varepsilon_1 = O((\log n)^{-1/4})$.

We apply Lemma 6.1 again, now to NMExt_1 with m as before. One can verify that the hypothesis of this application of Lemma 6.1 holds as well, and so we obtain a third non-malleable extractor $\mathsf{NMExt}_2 \colon \{0,1\}^n \times \{0,1\}^{d_2} \to \{0,1\}^m$, where $d_2 = O(d_1) = O(d)$, for min-entropy $k_2 = k_1/d_1^\alpha = \Omega(n/(\log n)^{2\alpha})$. The error of NMExt_2 is $\varepsilon_2 = O((\log n)^{-1/4^2})$

We repeat this process, producing a sequence of non-malleable extractors, always with m output bits. After r iterations we obtain a non-malleable extractor $\mathsf{NMExt}_r\colon \{0,1\}^n \times \{0,1\}^{d_r} \to \{0,1\}^m$, where $d_r = 2^{O(r)} \cdot \log n$, having error $\varepsilon_r = (\log n)^{-1/4^r}$ for entropy $k_r = \Omega\left(n/(\log n)^{\alpha r}\right)$. One can prove by induction that indeed for any constant r, these sequence of applications of Lemma 6.1 is valid. Notice that for any constant r the error is bounded above by ε – the desired constant error guarantee, assuming n is large enough. Thus, by setting $r = c/\alpha$, we obtain a non-malleable extractor with seed length $O(\log n)$ for entropy $\Omega(n/\log^c n)$ with error ε.

Lastly, we increase the output length of NMExt_r by applying Lemma 7.1 with $m = \Omega(k)$ to NMExt_r so to obtain our final non-malleable extractor $\mathsf{NMExt}'\colon \{0,1\}^n \times \{0,1\}^{d'} \to \{0,1\}^m$. One can easily verify that the hypothesis of Lemma 7.1 is met and that $d' = O(\log n)$. □

10 From Non-Malleable Extractors to t-Non-Malleable Extractors

In this section we prove the following lemma, which is a formal restatement of Lemma 2.5.

Lemma 10.1. *Let $t \geq 1$ be an integer. Let $\mathsf{NMExt}\colon \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}^{\log(1/\varepsilon)}$ be an explicit non-malleable extractor for entropy k with error ε such that*

$$k = \Omega\left(t \cdot \log(td_1/\varepsilon) \cdot \log(1/\varepsilon) + \log(n/\varepsilon)\right).$$

Then, for any $m = O(k/(t \cdot \log(1/\varepsilon)))$ there exists an explicit t-non-malleable extractor $\mathsf{NMExt}'\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ for entropy k with error $O(t \cdot \varepsilon^{1/4})$, having seed length

$$d = O\left(t^2 d_1 + t \cdot \log(tm/\varepsilon) \cdot \log(1/\varepsilon)\right).$$

The proof of Lemma 10.1 builds on what we call t-advice generators that generalize Definition 5.1.

Definition 10.2 (t-advice generators)**.** *For an integer $t \geq 1$, a function $\mathsf{AdvGen}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^a$ is called a* t-advice generator *for entropy k with error ε if the following holds. For any (n,k)-source X, an independent random variable Y that is uniform over $\{0,1\}^d$, and any functions $\{\mathcal{A}_i\colon \{0,1\}^d \to \{0,1\}^d\}_{i=1}^t$ with no fixed points, it holds that*

$$\Pr_{\substack{x\sim X\\ y\sim Y}}\left[\exists i \in [t] \quad \mathsf{AdvGen}(x,y) = \mathsf{AdvGen}(x, \mathcal{A}_i(y))\right] \leq \varepsilon.$$

Note that a 1-advice generator is an advice generator as defined in Definition 5.1. Similarly to our reduction in Lemma 5.3, some extra guarantee from the t-advice generator is needed for the reduction from t-non-malleable extractors to t-advice generators. This is encapsulated in the following definition.

Definition 10.3 (Nice t-advice generators)**.** *A t-advice generator* $\mathsf{AdvGen}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^a$ *for entropy k with error ε is said to be d_1-nice if the following holds. Let X be an (n,k)-source, let Y be a random variable that is independent of X and is uniformly distributed over $\{0,1\}^d$, and let $\{\mathcal{A}_i\colon \{0,1\}^d \to \{0,1\}^d\}_{i=1}^t$ be functions with no fixed points. Then, except with probability ε over the fixings of $\mathsf{AdvGen}(X,Y)$, $\{\mathsf{AdvGen}(X,\mathcal{A}_i(Y))\}_{i=1}^t$ it holds that:*

- *X, Y are independent.*
- *$H_\infty(X) \geq 0.99k$.*
- *The length $d - d_1$ suffix of Y has min-entropy rate $1 - 1/(100t)$.*

Note that a nice 1-advice generator is a nice advice generator as defined in Section 5. Mimicking the proof of Lemma 5.3 we obtain the following lemma.

Lemma 10.4. *There exist universal constants $0 < c < 1 < c', c''$ such that the following holds. Let $\mathsf{AdvGen}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^a$ be an explicit t-advice generator for entropy k with error ε that is d_1-nice, with $d_1 \leq d/2$. Then, for any integer m such that*

$$\begin{aligned} m &\leq c \cdot k/(at) \\ d &\geq c't \cdot \max\left(a \cdot \log\left(\frac{atm}{\varepsilon}\right), \log(n/\varepsilon)\right), \\ k &\geq c'' \cdot \max\left(at \cdot \log\left(\frac{ad}{\varepsilon}\right), \log(n/\varepsilon)\right), \end{aligned}$$

there exists a t-non-malleable extractor $\mathsf{NMExt}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ for entropy k with error $O(\sqrt{\varepsilon})$.

Proof. We start by describing the construction of NMExt and then turn to the analysis. Given a string $y \in \{0,1\}^d$, we partition y to three consecutive substrings $y = y_1 \circ y_2 \circ y_3$, where $|y_1| = d_1$, $|y_2| = d_2 = \Omega(\log(n/\varepsilon))$ is a sufficient length for a seed of the extractor from Theorem 4.3 set with error ε, and $|y_3| = d_3 = (10t-1)d_2$. By our hypothesis, d is large enough so to satisfy these properties. We make use of the following building blocks:

- Let $\mathsf{Raz}\colon \{0,1\}^n \times \{0,1\}^{d_2} \to \{0,1\}^\ell$ be the extractor from Theorem 4.3, where

  $$\ell = c''' \cdot \max(atm, at\log(ad/\varepsilon))$$

  for some suitable constant c''' to be chosen next. By our choice of d_2, the error of Raz is bounded above by ε.

- Let $\mathsf{AdvCB}\colon \{0,1\}^{d_3} \times \{0,1\}^\ell \times \{0,1\}^a \to \{0,1\}^m$ be the t-correlation breaker with advice from Theorem 4.12 set with error ε. By Theorem 4.12, c''' can be chosen such that the output length of AdvCB is indeed m.

With the notation set and using the building blocks above, we define

$$\mathsf{NMExt}(x,y) = \mathsf{AdvCB}\left(y_3, \mathsf{Raz}(x,y_2), \mathsf{AdvGen}(x,y)\right).$$

We now turn to the analysis. Let X be an (n,k)-source, let Y be an independent random variable that is uniformly distributed over $\{0,1\}^d$, and let $\{\mathcal{A}_i \colon \{0,1\}^d \to \{0,1\}^d\}_{i=1}^t$ be functions with no fixed points. As AdvGen is a d_1-nice t-advice generator with error ε, we have that except with probability ε over the fixings of $\alpha \sim \mathsf{AdvGen}(X,Y)$, $\{\alpha^i \sim \mathsf{AdvGen}(X,\mathcal{A}_i(Y))\}_{i=1}^t$, it holds that

- $\alpha \notin \{\alpha^1,\ldots,\alpha^t\}$.
- X, Y remain independent.
- $H_\infty(X) \geq 0.99k$.
- The length $d-d_1$ suffix of Y has min-entropy rate $1-1/(100t)$.

We condition on such fixings. Next, we argue that except with probability ε over $y_3 \sim Y_3$ it holds that $Y_2 \mid (Y_3 = y_3)$ has min-entropy rate at least 0.6. To see this, apply Lemma 4.8 to obtain

$$\widetilde{H}_\infty(Y_2 \circ Y_3 \mid Y_3) \geq H_\infty(Y_2 \circ Y_3) - |Y_3| \geq \left(1 - \frac{1}{100t}\right)(d_2+d_3) - d_3 = 0.9d_2.$$

Thus, by Lemma 4.9, except with probability ε over $y_3 \sim Y_3$ it holds that

$$H_\infty(Y_2 \mid Y_3 = y_3) = H_\infty(Y_2 \circ Y_3 \mid Y_3 = y_3) \geq 0.9d_2 - \log(1/\varepsilon) \geq 0.6d_2.$$

Therefore, except with probability ε over the fixing of Y_3, the min-entropy rate of Y_2 is bounded below by 0.6. For the remaining of the proof we assume that the min-entropy rate of Y_2 is at least 0.6, and aggregate an additional error of ε to the total error.

As $H_\infty(X) \geq 0.99k \geq 2\ell$, $H_\infty(X) = \Omega(d_2)$, and since Y_2 is a $(d_2, 0.6d_2)$-source with $d_2 = \Omega(\log(n/\varepsilon))$, Theorem 4.3 implies that

$$(\mathsf{Raz}(X,Y_2), Y_2) \approx_\varepsilon (U_\ell, Y_2).$$

As $\mathsf{Raz}(X,Y_2)$ is independent of the joint distribution of $\{(\mathcal{A}_i(Y))_2\}_{i=1}^t$ conditioned on the fixing of Y_2, Lemma 4.10 implies that

$$\left(\mathsf{Raz}(X,Y_2), Y_2, \{(\mathcal{A}_i(Y))_2\}_{i=1}^t\right) \approx_\varepsilon (U_\ell, \cdot).$$

Thus, except with probability $\sqrt{\varepsilon}$ over the fixings of $Y_2, \{(\mathcal{A}_i(Y))_2\}_{i=1}^t$ it holds that $\mathsf{Raz}(X,Y_2)$ is $\sqrt{\varepsilon}$-close to uniform. As for the entropy loss of Y_3 resulted by these fixings,

$$\widetilde{H}_\infty\left(Y_3 \mid Y_2, \{(\mathcal{A}_i(Y))_2\}_{i=1}^t\right) \geq \left(1 - \frac{1}{100t}\right)(d_2+d_3) - (t+1)d_2 \geq 0.8d_3$$

and so except with probability ε over $Y_2, \{(\mathcal{A}_i(Y))_2\}_{i=1}^t$ it holds that Y_3 has min-entropy rate larger than 0.5. To summarize, except with probability $O(\sqrt{\varepsilon})$ over all fixings done so far, we have that

- The joint distribution of $\mathsf{Raz}(X, Y_2)$, $\{\mathsf{Raz}(X, (\mathcal{A}_i(Y))_2)\}_{i=1}^t$ is independent of the joint distribution of $Y_3, \{(\mathcal{A}_i(Y))_3\}_{i=1}^t$.
- The min-entropy of Y_3 is bounded below by

$$\frac{d_3}{2} \geq \frac{9d}{20} = \Omega\left(at \cdot \log\left(\frac{atm}{\varepsilon}\right)\right) = \Omega\left(at \cdot \log\left(\frac{a\ell}{\varepsilon}\right)\right), \tag{10.1}$$

  where we used the hypothesis on d and the choice of m for the second inequality and that $d \geq 2d_1$ for the first inequality. For the last inequality we used our choice of ℓ.
- $\mathsf{Raz}(X, Y_2)$ is $O(\sqrt{\varepsilon})$-close to uniform.

Therefore, we can apply Theorem 4.12 and conclude that

$$\left(\mathsf{NMExt}(X, Y), \{\mathsf{NMExt}(X, \mathcal{A}_i(Y))\}_{i=1}^t, Y\right) \approx_{O(\sqrt{\varepsilon})} (U_m, \cdot).$$

Note that indeed the hypothesis of Theorem 4.12 holds. In particular, Equation (4.1) holds by our choice of ℓ, and Equation (4.2) follows by Equation (10.1). This concludes the proof. □

We are now ready to prove Lemma 10.1

Proof of Lemma 10.1. Write $d = d_1 + d_2$, where $d_2 = 500t^2 d_1$. For the proof we make use of the following building blocks:

- Let $\mathsf{ECC}\colon \{0,1\}^{d_2} \to \colon \{0,1\}^{D_2}$ be the error correcting code from Theorem 4.4 set with relative distance $1/4$. By Theorem 4.4, $D_2 = O(d_2)$.
- Let $r = \log_{4/3}(1/\varepsilon)$ and set $v = r \cdot \log_2 D_2$. Let $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}^v$ be the extractor from Theorem 4.2, set with error ε. Note that we set d_1 to be large enough as required by a seed for Ext. Moreover, one can verify that by our assumption on k, given by Equation (8.1), $k \geq 2v$ as required by Theorem 4.2.

We proceed by proving the following claim.

Claim 10.5. *The function*

$$\mathsf{AdvGen}(x, y) = \mathsf{NMExt}(x, y_1) \circ \mathsf{ECC}(y_2)_{\mathsf{Ext}(x, y_1)}$$

is a d_1-nice t-advice generator for entropy k with error $O(t\sqrt{\varepsilon})$.

Proof. Let X be an (n, k)-source, let Y be a random variable that is independent of X and is uniformly distributed over $\{0,1\}^d$, and let $\{A_i\colon \{0,1\}^d \to \{0,1\}^d\}_{i=1}^t$ be functions with no fixed points. By Lemma 4.14, there exists a set $B \subset \{0,1\}^{d_1}$ of density $\sqrt{\varepsilon}$ such that for any $y_1 \notin B$ and any d_1-bit string $y_1' \neq y_1$, it holds that

$$(\mathsf{NMExt}(X, y_1), \mathsf{NMExt}(X, y_1')) \approx_{\sqrt{\varepsilon}} (U, \cdot)\,. \tag{10.2}$$

We now fix $y_1 \sim Y_1$ and $y_1^i \sim (\mathcal{A}_i(Y))_1$ for $i = 1, \ldots, t$. Clearly, these fixings do not introduce dependencies between X, Y. Furthermore, by the above, we can aggregate $\sqrt{\varepsilon}$ to the total error and assume that $y_1 \notin B$. Let I be the set of $i \in [t]$ such that $y_1 \neq y_1^i$.

Fix $i \in I$. By Equation (10.2) it holds that $\mathsf{NMExt}(X, y_1)$ is $\sqrt{\varepsilon}$-close to uniform even conditioned on $\mathsf{NMExt}(X, y_1^i)$. In particular, as NMExt has output length $\log(1/\varepsilon)$, the probability that $\mathsf{NMExt}(X, y_1) = \mathsf{NMExt}(X, y_1^i)$ is bounded above by $O(\sqrt{\varepsilon})$. By the union bound over all $i \in I$, we have that except with probability $O(t\sqrt{\varepsilon})$, for all $i \in I$, $\mathsf{AdvGen}(X, Y) \neq \mathsf{AdvGen}(X, \mathcal{A}_i(Y))$.

Consider now $i \notin I$. Conditioned on $y_1 = y_1^i$ we have that $Y_2 \neq (\mathcal{A}_i(Y))_2$, and so the codewords $\mathsf{ECC}(Y_2), \mathsf{ECC}((\mathcal{A}_i(Y))_2)$ agree on at most $3/4$ of the coordinates of $[D_2]$. Hence, the set of r-tuples over $[D_2]$ for which $\mathsf{ECC}(Y_2)$ agrees with $\mathsf{ECC}((\mathcal{A}_i(Y))_2)$ on all r coordinates of the tuple has density at most $(3/4)^r = \varepsilon$ within $[D_2]^r$. By the union bound over all $i \notin I$, at most εt fraction of the r-tuples in $[D_2]^r$ are such that $\mathsf{ECC}(Y_2)$ agrees with $\mathsf{ECC}((\mathcal{A}_i(Y))_2)$ for some $i \notin I$. We denote this set of r-tuples by $B' \subseteq [D_2]^r$.

Recall that Ext is a strong seeded extractor with error ε, and so except for probability $\sqrt{\varepsilon}$ over the choices of y_1, we have that $\mathsf{Ext}(X, y_1)$ is $\sqrt{\varepsilon}$-close to uniform. For any such y_1 we have that $\mathbf{Pr}[\mathsf{Ext}(X, y_1) \in B'] \leq \varepsilon t + O(\sqrt{\varepsilon})$. Thus, except with probability $O(t\sqrt{\varepsilon})$ we have that also for all $i \notin I$, $\mathsf{AdvGen}(X, Y) \neq \mathsf{AdvGen}(X, \mathcal{A}_i(Y))$.

As for niceness property, by Lemma 4.8, the fixings of $Y_1, \{(\mathcal{A}_i(Y))_1\}_{i=1}^t$ reduce the average min-entropy of Y_2 by a most $(t+1)d_1$. Once $Y_1, \{(\mathcal{A}_i(Y))_1\}_{i=1}^t$ are fixed, we have that $\mathsf{Ext}(X, Y_1)$, $\{\mathsf{Ext}(X, (\mathcal{A}_i(Y))_1)\}_{i=1}^t$, $\mathsf{NMExt}(X, Y_1)$, and $\{\mathsf{NMExt}(X, (\mathcal{A}_i(Y))_1)\}_{i=1}^t$ are all deterministic functions of X. Thus, we can fix the latter random variables without introducing dependencies between X, Y. Further, by Lemma 4.8, the average min-entropy of X decreases by at most $O(t \cdot \log(1/\varepsilon) \cdot \log d)$.

After these fixings, $\mathsf{ECC}(Y_2)_{\mathsf{Ext}(X,Y_1)}$ and $\{\mathsf{ECC}((\mathcal{A}_i(Y))_2)_{\mathsf{Ext}(X,(\mathcal{A}_i(Y))_1)}\}_{i=1}^t$ are deterministic functions of Y, each consists of r bits. Thus, fixing these random variables will reduce the average min-entropy of Y by at most $(t+1)r = O(t \cdot \log(1/\varepsilon))$. Further, these fixings do not introduce any dependencies between X, Y. Note that after all of the fixings done so far, $\mathsf{AdvGen}(X, Y)$ and $\{\mathsf{AdvGen}(X, (\mathcal{A}_i(Y)))\}_{i=1}^t$ are all fixed.

To summarize, in the process of fixing $\mathsf{AdvGen}(X, Y)$, $\{\mathsf{AdvGen}(X, (\mathcal{A}_i(Y)))\}_{i=1}^t$, the random variable Y_2 lost an average entropy of $(t+1)(d_1 + r)$. As we set $d_2 = 500t^2 d_1$ we have that except with probability ε over these fixings, Y_2 has min-entropy rate $1 - 1/(100t)$. As for X, the fixings reduced its average min-entropy by $O(t \cdot \log(1/\varepsilon) \cdot \log d)$, and so except with probability ε, X has min-entropy rate 0.99 conditioned on these fixings. □

To conclude the proof we apply Lemma 10.4 with AdvGen defined above and the parameter m. The hypothesis of Lemma 10.4 is met due to our hypothesis on m, d, k and since $a = O(\log(1/\varepsilon))$.

□

11 Summary and Open Problems

The study of seeded extractors came a long way in the 20 years since the influential paper by Nisan and Zuckerman [NZ96]. The accumulation of many different ideas and competitive routes of attack eventually led to explicit constructions of seeded extractors with very close to optimal parameters [GUV09, DKSS09, TSU12], exploiting a variety of elegant ideas and insightful connections with other pseudorandom objects.

The notion of non-malleable extractors, introduced by Dodis and Wichs [DW09], rechallenged our understanding of seeded extractors, and up until the exciting result of Chattopadhyay, Goyal, and Li [CGL15], all the techniques that were developed in the course of studying seeded extractors only led to non-malleable extractors for entropy roughly $n/2$ [CRS14, DLWZ14, Li12a, Li12c]. The result of [CGL15] got the entropy requirement down to $\Omega(\log^2 n)$, and this improvement was a key ingredient in the two-source extractor construction by Chattopadhyay and Zuckerman [CZ15], giving yet another application for non-malleable extractors.

In this work we further contributed to the study of non-malleable extractors. On top of devising new modular tools for enhancing non-malleable extractors (see Lemma 2.4, Lemma 2.3 and Lemma 2.5), we constructed a non-malleable extractor with seed length $O(\log n \cdot \log\log n)$ for min-entropy $\Omega(\log n \cdot \log\log n)$ (Theorem 2.1). We also constructed a non-malleable extractor with optimal seed length, up to constant factors, though the supported entropy is $n/\text{polylog}n$ (Theorem 2.2). These results set the next natural goal at constructing a non-malleable extractor with logarithmic seed length for poly-logarithmic or even lower entropy.

A second problem that we leave for future research concerns the error of the extractor. In all of our constructions, the dependence of the seed length on the error ε is of the form $\Omega(\log^2(1/\varepsilon))$. This is also the case with the construction of [CGL15], for to the same reason. It would be interesting to construct non-malleable extractors having seed with a better dependence in ε. In particular, an optimal dependence of $\log(1/\varepsilon)$.

A third question that we find intriguing concerns the entropy that can be supported by non-malleable extractors. Consider a fixed error ε. The existential proof for non-malleable extractors by Dodis and Wichs [DW09] can only yield non-malleable extractors for entropy $\Omega(\log\log n)$. This is in contrast to strong seeded extractors that can support any entropy. It would be nice to either improve this bound or to show that it is necessary.

Acknowledgement

We wish to thank Ronen Shaltiel for enjoyable conversations we had regarding this work during his visit at Caltech.

References

[AHL15] D. Aggarwal, K. Hosseini, and S. Lovett. Affine-malleable extractors, spectrum doubling, and application to privacy amplification. In *Electronic Colloquium on*

Computational Complexity (ECCC), page 179, 2015.

[BKS+05] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, and A. Wigderson. Simulating independence: New constructions of condensers, Ramsey graphs, dispersers, and extractors. In *Proceedings of the thirty-seventh annual ACM Symposium on Theory of Computing*, pages 1–10. ACM, 2005.

[BRSW12] B. Barak, A. Rao, R. Shaltiel, and A. Wigderson. 2-source dispersers for $n^{o(1)}$ entropy, and Ramsey graphs beating the Frankl-Wilson construction. *Annals of Mathematics*, 176(3):1483–1544, 2012.

[CG88] B. Chor and O. Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM Journal on Computing*, 17(2):230–261, 1988.

[CGL15] E. Chattopadhyay, V. Goyal, and X. Li. Non-malleable extractors and codes, with their many tampered extensions. *arXiv preprint arXiv:1505.00107*, 2015.

[Coh15a] G. Cohen. Local correlation breakers and applications to three-source extractors and mergers. In *Electronic Colloquium on Computational Complexity (ECCC)*, page 38, 2015.

[Coh15b] G. Cohen. Two-source dispersers for polylogarithmic entropy and improved Ramsey graphs. *arXiv preprint arXiv:1506.04428*, 2015.

[CRS14] G. Cohen, R. Raz, and G. Segev. Nonmalleable extractors with short seeds and applications to privacy amplification. *SIAM Journal on Computing*, 43(2):450–476, 2014.

[CZ15] E. Chattopadhyay and D. Zuckerman. Explicit two-source extractors and resilient functions. *Electronic Colloquium on Computational Complexity (ECCC)*, 2015.

[DKSS09] Z. Dvir, S. Kopparty, S. Saraf, and M. Sudan. Extensions to the method of multiplicities, with applications to Kakeya sets and mergers. In *50th Annual IEEE Symposium on Foundations of Computer Science*, pages 181–190. IEEE, 2009.

[DLWZ14] Y. Dodis, X. Li, T. D. Wooley, and D. Zuckerman. Privacy amplification and nonmalleable extractors via character sums. *SIAM Journal on Computing*, 43(2):800–830, 2014.

[DORS08] 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*, 38(1):97–139, 2008.

[DP07] S. Dziembowski and K. Pietrzak. Intrusion-resilient secret sharing. In *48th Annual IEEE Symposium on Foundations of Computer Science*, pages 227–237, 2007.

[DW09] Y. Dodis and D. Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In *Proceedings of the forty-first annual ACM Symposium on Theory of Computing*, pages 601–610. ACM, 2009.

[GUV09] V. Guruswami, C. Umans, and S. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *Journal of the ACM*, 56(4):20, 2009.

[Li11] X. Li. Improved constructions of three source extractors. In *IEEE 26th Annual Conference on Computational Complexity*, pages 126–136, 2011.

[Li12a] X. Li. Design extractors, non-malleable condensers and privacy amplification. In *Proceedings of the forty-fourth annual ACM Symposium on Theory of Computing*, pages 837–854, 2012.

[Li12b] X. Li. Non-malleable condensers for arbitrary min-entropy, and almost optimal protocols for privacy amplification. *arXiv preprint arXiv:1211.0651*, 2012.

[Li12c] X. Li. Non-malleable extractors, two-source extractors and privacy amplification. In *IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 688–697, 2012.

[Li13a] X. Li. Extractors for a constant number of independent sources with polylogarithmic min-entropy. In *IEEE 54th Annual Symposium on Foundations of Computer Science*, pages 100–109, 2013.

[Li13b] X. Li. New independent source extractors with exponential improvement. In *Proceedings of the forty-fifth annual ACM Symposium on Theory of Computing*, pages 783–792. ACM, 2013.

[Li15a] X. Li. Extractors for affine sources with polylogarithmic entropy. In *Electronic Colloquium on Computational Complexity (ECCC)*, page 121, 2015.

[Li15b] X. Li. Improved constructions of two-source extractors. In *Electronic Colloquium on Computational Complexity (ECCC)*, page 125, 2015.

[Li15c] X. Li. Three-source extractors for polylogarithmic min-entropy. *Electronic Colloquium on Computational Complexity (ECCC)*, 2015.

[LWZ11] X. Li, T. D. Wooley, and D. Zuckerman. Privacy amplification and nonmalleable extractors via character sums. *arXiv preprint arXiv:1102.5415*, 2011.

[NZ96] N. Nisan and D. Zuckerman. Randomness is linear in space. *Journal of Computer and System Sciences*, 52(1):43–52, 1996.

[Rao09] A. Rao. Extractors for a constant number of polynomially small min-entropy independent sources. *SIAM Journal on Computing*, 39(1):168–194, 2009.

[Raz05] R. Raz. Extractors with weak random seeds. In *Proceedings of the thirty-seventh annual ACM Symposium on Theory of Computing*, pages 11–20, 2005.

[RSW00] O. Reingold, R. Shaltiel, and A. Wigderson. Extracting randomness via repeated condensing. In *Proceedings. 41st Annual Symposium on Foundations of Computer Science, 2000*, pages 22–31. IEEE, 2000.

[Sha11] R. Shaltiel. An introduction to randomness extractors. In *Automata, languages and programming*, pages 21–41. Springer, 2011.

[TSU12] A. Ta-Shma and C. Umans. Better condensers and new extractors from Parvaresh-Vardy codes. In *IEEE 27th Annual Conference onComputational Complexity (CCC)*, pages 309–315. IEEE, 2012.

[Vad11] Salil P. Vadhan. Pseudorandomness. *Foundations and Trends in Theoretical Computer Science*, 2011.

[Zuc07] D. Zuckerman. Linear degree extractors and the inapproximability of max clique and chromatic number. *Theory of Computing*, 3:103–128, 2007.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de