An Entropy Lower Bound for Non-Malleable Extractors

Tom Gur * Igor Shinkar *

January 9, 2018

Abstract

A \((k, \epsilon)\)-non-malleable extractor is a function \(\text{nmExt} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}\) that takes two inputs, a weak source \(X \sim \{0, 1\}^n\) of min-entropy \(k\) and an independent uniform seed \(s \in \{0, 1\}^d\), and outputs a bit \(\text{nmExt}(X, s)\) that is \(\epsilon\)-close to uniform, even given the seed \(s\) and the value \(\text{nmExt}(X, s')\) for an adversarially chosen seed \(s' \neq s\). Dodis and Wichs (STOC 2009) showed the existence of \((k, \epsilon)\)-non-malleable extractors with seed length \(d = \log(n - k - 1) + 2 \log(1/\epsilon) + 6\) that support sources of entropy \(k > \log(d) + 2 \log(1/\epsilon) + 8\).

We show that the foregoing bound is essentially tight, by proving that any \((k, \epsilon)\)-non-malleable extractor must satisfy the entropy bound \(k > \log(d) + 2 \log(1/\epsilon) - \log \log(1/\epsilon) - C\) for an absolute constant \(C\). In particular, this implies that non-malleable extractors require min-entropy at least \(\Omega(\log \log(n))\). This is in stark contrast to the existence of strong seeded extractors that support sources of entropy \(k = O(\log(1/\epsilon))\).

Our techniques strongly rely on coding theory. In particular, we reveal an inherent connection between non-malleable extractors and error correcting codes, by proving a new lemma which shows that any \((k, \epsilon)\)-non-malleable extractor with seed length \(d\) induces a code \(C \subseteq \{0, 1\}^{2^d}\) with relative distance \(0.5 - 2\epsilon\) and rate \(\frac{d - 1}{2^d}\).

1 Introduction

Randomness extractors are central objects in the theory of computation. Loosely speaking, a seeded extractor [NZ96] is a randomized algorithm that extracts nearly uniform bits from biased random sources, using a short seed of randomness. A non-malleable extractor [DW09] is a seeded extractor that satisfies a very strong requirement regarding the lack of correlations of the output of the extractor with respect to different seeds.

More accurately, a \((k, \epsilon)\)-non-malleable extractor is a function \(\text{nmExt} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}\) such that for every (weak) source \(X\) of min-entropy \(k\) and a random variable \(s\) uniformly distributed on \(\{0, 1\}^d\) it holds that \(\text{nmExt}(X, s)\) is \(\epsilon\)-close to uniform, even given the seed \(s \in \{0, 1\}^d\) and the value \(\text{nmExt}(X, s')\) for any seed \(s' \neq s\) that is determined as an arbitrary function of \(s\). More generally, if \(\text{nmExt}(X, s)\) is \(\epsilon\)-close to uniform, even given \(\text{nmExt}(X, s'_1), \ldots, \text{nmExt}(X, s'_t)\) for \(t\) adversarially chosen seeds such that \(s'_i \neq s\) for all \(i \in [t]\), we say it is a \((k, \epsilon)\)-\(t\)-non-malleable extractor [CRS14].

The notion of non-malleable extractors is strongly motivated by applications to privacy amplification protocols, as well as proven to be a fundamental notion in the theory of pseudorandomness,
for some absolute constant $c$.

Theorem 1 (Main result). Let $(k,\varepsilon)$ be parameters such that $t = 2^{d/2}$, and let $\varepsilon \in (0, c_0)$ for some absolute constant $c_0$. If $\text{nmExt} : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}$ is a $(k,\varepsilon)$-non-malleable extractor, then $d > \log(n-k) + 2 \log(1/\varepsilon) - C$ and $k \geq \log(d) + 2 \log(1/\varepsilon) + \log(1/\varepsilon) + \log(t) - C$ for an absolute constant $C$.

We remark that by a recent result of Ben-Aroya et al. [BCD+17] (see Theorem 2.4), the lower bound on $d$ in the theorem is tight up to an additive factor of $O(\log(t))$, and our lower bound on $k$ is almost tight in $\varepsilon$, up to an additive factor of $\log\log(1/\varepsilon)$. Furthermore, since as we mentioned

Question: Is it true that in any $(k,\varepsilon)$-non-malleable extractor the entropy $k$ must grow with $n$?

In this paper we give a positive answer to this question, as well as reveal a simple yet fundamental connection between non-malleable extractors and error-correcting codes, which we believe to be of independent interest.

1.1 Our results

Our main result is a lower bound on the entropy required by non-malleable extractors, which essentially matches the one obtained by the probabilistic construction. In particular, we show that any $(k,\varepsilon)$-non-malleable extractor requires the source entropy $k$ to be at least $\log\log(n) - (2 - o_0(1))\log(1/\varepsilon)$. In fact, we prove the entropy lower bound for the more general notion of $t$-non-malleable extractors.

Let $n,k,d,t \in \mathbb{N}$ be parameters such that $t \leq 2^{d/2}$, and let $\varepsilon \in (0, c_0)$ for some absolute constant $c_0$. If $\text{nmExt} : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}$ is a $(k,\varepsilon)$-t-non-malleable extractor, then $d > \log(n-k) + 2 \log(1/\varepsilon) - C$ and $k \geq \log(d) + 2 \log(1/\varepsilon) - \log\log(1/\varepsilon) + \log(t) - C$ for an absolute constant $C$.

We remark that by a recent result of Ben-Aroya et al. [BCD+17] (see Theorem 2.4), the lower bound on $d$ in the theorem is tight up to an additive factor of $O(\log(t))$, and our lower bound on $k$ is almost tight in $\varepsilon$, up to an additive factor of $\log\log(1/\varepsilon)$. Furthermore, since as we mentioned
above, there exist (strong) seeded extractors for sources of entropy $k = 2 \log(1/\varepsilon) + O(1)$, Theorem 1 implies a chasm between non-malleable extractors and (strong) seeded extractors; in particular, it rules out the possibility of transforming seeded extractors into non-malleable extractors, while preserving the parameters.

A key technical tool that we use to prove Theorem 1 is a lemma, which shows that any non-malleable extractor induces an error correcting code with a good distance. We believe this lemma is of independent interest.

**Lemma 2.** If there exists a $(k, \varepsilon)$-non-malleable extractor $\text{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}$, then there exists an error correcting code $C \subseteq \{0,1\}^{2k}$ with relative distance $0.5 - 2\varepsilon$ and rate $\frac{d-1}{2k}$.

In fact, we actually prove a more general lemma, which shows that $t$-non-malleable extractors induce codes with rate that grows with $t$. See Section 4 for details.

### 1.2 Technical overview

We provide a high-level overview of the proof of our main result, the entropy lower bound in Theorem 1 for the simple case of $t = 1$ (i.e., for standard non-malleable extractors). See Section 4 for the complete details of the proof for the general case. We assume basic familiarity with coding theory and extractors (see Section 2 for the necessary preliminaries).

Consider a non-malleable extractor $\text{nmExt}$. Our strategy for showing a lower bound on the source entropy of $\text{nmExt}$ consists of the following two steps.

1. Derive a binary code $C$ with high distance and rate from $\text{nmExt}$, as captured by Lemma 2.
2. Show refined bounds on the rate of binary codes with a given minimum distance, and apply them to $C$ to obtain an entropy lower bound.

That is, we show that if the parameters of $\text{nmExt}$ were too good, then the implied code $C$ would have parameters that would violate the rate bounds in the second step. Below, we elaborate on each of the steps.

**Deriving codes from non-malleable extractors.** We start with a $(k, \varepsilon)$-non-malleable extractor $\text{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}$. Denote $K = 2^k$, and consider a (flat) source $X$, which we view as a collection of $K$ vectors $X \subseteq \{0,1\}^n$. We show that there is a large subset $S$ of the seeds such that the evaluations of $\text{nmExt}$, with respect to $X$ and $S$, constitute a code with high distance and rate.

More accurately, denote by $w(s)$ the evaluation vector of $\text{nmExt}$ on the source $X$ and seed $s \in \{0,1\}^d$; that is, $w(s) = (\text{nmExt}(x,s))_{x \in X}$. We show that there exists a large subset of seeds $S \subseteq \{0,1\}^d$ such that

$$C \overset{\text{def}}{=} \{w(s) : s \in S\}$$

is a code with distance $0.5 - 2\varepsilon$ and rate $(d-1)/K$.

As a warmup, it is instructive to note that the definition of (standard) seeded extractors only requires that a random coordinate of a random $w(s)$ is nearly uniformly distributed. Strong seeded extractors also imply that most evaluation vectors are roughly balanced (i.e., contain a similar
Figure 1: Truth table of a \((k,\varepsilon)\)-non-malleable extractor \(\text{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}\). Rows correspond to the \(D = 2^d\) seeds. Columns correspond to all \(n\)-bit vectors, out of which we highlight the \(K = 2^k\) vectors of the flat source \(X\). Each vector \(w(s) = (\text{nmExt}(x, s))_{x \in X}\) consists of the values corresponding to seed \(s\) and all vectors of \(X\). The vectors \(w(s_i)\) and \(w(s_i')\) correspond to a pair of “bad” seeds \(s_i, s_i' \in B\), and hence they are close to each other.

The key observation is that the structure of \textit{non-malleable extractors} asserts that there exists a large subset of seeds whose corresponding evaluation vectors are (close to) pairwise uncorrelated, and hence constitute a code with large distance. Details follow.

Denote the number of seeds by \(D = 2^d\). We wish to show that there exists a subset \(S \subset \{0,1\}^d\) of \(D/2\) seeds whose corresponding evaluation vectors are pairwise \((0.5 - 2\varepsilon)\)-far. Suppose the contrary, i.e., that every set \(S\) of \(D/2\) seeds contains at least two distinct seeds \(s, s'\) such that \(w(s)\) is \((0.5 - 2\varepsilon)\)-close to \(w(s')\). This means that we can iteratively select a set of \(D/2\) “bad” seeds \(B = \{s_1, \ldots, s_{D/4}, s'_1, \ldots, s'_{D/4}\}\) such that \(w(s_i)\) and \(w(s'_i)\) are \((0.5 - 2\varepsilon)\)-close in Hamming distance, for every \(i \in [D/4]\). (See Fig. 1.)

The crux is that having many pairs of correlated evaluation vectors violates the assumption that \(\text{nmExt}\) is a non-malleable extractor. Intuitively, this holds because for each \(w(s_i)\) corresponding to a bad seed \(s_i \in B\), the output of \(\text{nmExt}(X, s_i)\) is biased given \(\text{nmExt}(X, s'_i)\). Hence, a non-malleable extractor cannot have a large set of bad seeds.

In Section 4.1 we make this intuition precise by exhibiting an adversarial function \(A : \{0,1\}^d \to \{0,1\}^d\) (with no fixed points) that matches pairs of bad seeds such that we can construct a distinguisher that, for a random variable \(U_d\) uniformly distributed on the seeds \(\{0,1\}^d\), can tell apart with confidence \(\varepsilon\) between \(\text{nmExt}(X, U_d)\) and a uniform bit, even when given \(\text{nmExt}(X, A(U_d))\) and \(U_d\).

\textbf{Refined rate bounds for binary codes.} After we derived a binary code \(C\) with distance \(0.5 - 2\varepsilon\) and rate \((d - 1)/K\) from a \((k,\varepsilon)\)-non-malleable extractor \(\text{nmExt}\), we wish to apply upper bounds on the rate of binary codes, which will in turn imply entropy lower bounds on the entropy that \(\text{nmExt}\) requires.

\footnote{We stress that elements of a set of nearly-balanced vectors are not necessarily pairwise-far, unless this set is a \textit{linear space}. Hence, the foregoing property of strong seeded extractors does \textit{not} imply a good code in general.}
Our starting point is the state-of-the-art upper bound of McEliece, Rodemich, Rumsey and Welch [MRR+77], which, loosely speaking, states that any binary code with relative distance $0.5 - \varepsilon$ has rate $O(\varepsilon^2 \log(1/\varepsilon))$ for all sufficiently small $\varepsilon > 0$.

Alas, the aforementioned bound does not suffice for the entropy lower bound, as we need a quantitative bound in terms of the blocklength of the code. We, thus, prove the following theorem, which provides the refined bound that we need.

**Theorem 3.** Fix a constant $c \in (0, 1/20)$, and let $\varepsilon \in (0, c)$. For $K > \frac{c}{\varepsilon^5}$ let $\mathcal{C} \subseteq \{0, 1\}^K$ be a code with relative distance $\delta = 0.5 - \varepsilon$. Then $|\mathcal{C}| < 2^{\frac{21}{c} \varepsilon^2 \log(1/\varepsilon) K}$.

We prove Theorem 3 in Section 3 relying on the spectral approach of Navon and Samorodnitsky [NS09].

To conclude the proof of the entropy lower bound, we argue that if the non-malleable extractor \textsc{nmExt} could support entropy that is smaller than stated in Theorem 1, then the code $\mathcal{C}$ we derive via Lemma 2 would have rate that would violate the lower bound in Theorem 3.

**1.3 Organization**

In Section 2 we present the required preliminaries. In Section 3 we prove the refined bounds on the rate of binary codes. Finally, in Section 4 we prove our main result, Theorem 1, as well as Lemma 2 which captures the connection between non-malleable extractors and error correcting codes.

**2 Preliminaries**

We cover the notation and basic definitions used in this paper.

**2.1 Notation**

For $n \in \mathbb{N}$, we denote by $[n]$ the set $\{1, \ldots, n\}$, and by $U_n$ the random variable that is uniformly distributed over $\{0,1\}^n$. Throughout, $\log(x)$ is defined as $\log_2(x)$. The binary entropy function $H: [0,1] \to [0,1]$ is given by $H(x) = -x \log(x) - (1-x) \log(1-x)$. We denote by $1_E$ the indicator of an event $E$. For a finite set $X$, we denote by $\Pr_{x \in X}[\cdot]$ the probability over an element $x$ that is chosen uniformly at random from $X$.

**Distance.** The relative Hamming distance (or just distance), over alphabet $\Sigma$, between two vectors $x, y \in \Sigma^n$ is denoted $\text{dist}(x, y) \overset{\text{def}}{=} \frac{|\{i \in [n]: x_i \neq y_i\}|}{n}$. If $\text{dist}(x, y) \leq \varepsilon$, we say that $x$ is $\varepsilon$-close to $y$, and otherwise we say that $x$ is $\varepsilon$-far from $y$. Similarly, the relative distance of $x \in \Sigma^n$ from a non-empty set $S \subseteq \Sigma^n$ is denoted $\text{dist}(x, S) \overset{\text{def}}{=} \min_{y \in S} \text{dist}(x, y)$. If $\text{dist}(x, S) \leq \varepsilon$, we say that $x$ is $\varepsilon$-close to $S$, and otherwise we say that $x$ is $\varepsilon$-far from $S$.

The total variation distance between two random variables $X_1, X_2$ over domain $\Omega$ is denoted by $\text{dist}_{TV}(X_1, X_2) \overset{\text{def}}{=} \sup_{S \subseteq \Omega} |\Pr[X_1 \in S] - \Pr[X_2 \in S]|$, and is equivalent, up to a factor 2, to their $\ell_1$ distance $\|X_1 - X_2\|_1 \overset{\text{def}}{=} \sum_{\omega \in \Omega} |\Pr[X_1 = \omega] - \Pr[X_2 = \omega]|$. We say that $X_1$ is $\varepsilon$-close to $X_2$ if $\text{dist}_{TV}(X_1, X_2) \leq \varepsilon$, and otherwise we say that $X_1$ is $\varepsilon$-far from $X_2$.

**Remark.** In order to show that $X_1$ is $\varepsilon$-far from $X_2$ it suffices to show a randomized distinguisher $D: \Omega \to \{0,1\}$ such that $|\Pr[D(X_1) = 1] - \Pr[D(X_2) = 1]| > \varepsilon$, where the probabilities are over
the random variables $X_1, X_2$ and the randomness of $D$. Note that if such randomized distinguisher exists, then, by averaging, there is also a deterministic distinguisher with the same property. This, naturally, defines the event $S_D = \{ \omega \in \Omega : D(\omega) = 1 \} \subseteq \Omega$. for which we have $\text{dist}_{TV}(X_1, X_2) = \sup_{S \subseteq \Omega} |\Pr[X_1 \in S] - \Pr[X_2 \in S]| \geq |\Pr[X_1 \in S_D] - \Pr[X_2 \in S_D]| > \varepsilon$, and hence $X_1$ is $\varepsilon$-far from $X_2$.

2.2 Error correcting codes

Let $k, n \in \mathbb{N}$, and let $\Sigma$ be a finite alphabet. An error correcting code is a set $C \subseteq \Sigma^n$, and the elements of $C$ are called its codewords. The parameter $n$ is called the blocklength of $C$, and $k = \log_{|\Sigma|}(|C|)$ is the dimension of $C$. The relative distance of a code $C$ is the minimal relative Hamming distance between its codewords, and is denoted by $\delta = \min_{c \neq c'} \{ \text{dist}(c, c') \}$. The rate of the code, measuring the redundancy of the encoding, is the ratio of its dimension and blocklength, and is denote by $\rho = k/n$. If the alphabet is binary, i.e., $\Sigma = \{0,1\}$, we say that $C$ is a binary code.

2.3 Randomness extractors

We recall the standard definitions of random sources and several types of extractors, as well as state known bounds that we will need.

Weak sources. For integers $n > k$, an $(n,k)$-random source $X$ of min-entropy $k$ is a random variable taking values in $\{0,1\}^n$ such that for every $x \in \{0,1\}^n$ holds that $\Pr[X = x] \leq 2^{-k}$. An $(n,k)$-random source $X$ is flat if it is uniformly distributed over some subset $S \subseteq \{0,1\}^n$ of size $2^k$.

It is well known [CG88] that the distribution of any $(n,k)$-random source is a convex combination of distributions of flat $(n,k)$-random sources, and thus it typically suffices to consider flat sources. We follow the literature, restrict our attention to flat $(n,k)$-random sources, and refer to them simply as $(n,k)$-sources.

Seeded extractors. A function $\text{Ext}: \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}$ is a $(k,\varepsilon)$-seeded extractor if for any $(n,k)$-source $X$, the distribution of $\text{Ext}(X, U_d)$ is $\varepsilon$-close to $U_1$, i.e., $\text{dist}_{TV}(\text{Ext}(X, U_d), U_1) \leq \varepsilon$.

(Recall that $U_m$ denotes the random variable that is uniformly distributed on $\{0,1\}^m$.)

A function $\text{Ext}: \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}$ is a $(k,\varepsilon)$-strong seeded extractor if for any $(n,k)$-source $X$ the distribution of $(\text{Ext}(X, U_d), U_d)$ is $\varepsilon$-close to $U_{d+1}$. We will need the following lower bound on the source entropy required by strong seeded extractors, due to Radhakrishnan and Ta-Shma [RT00] (see also [NZ96]).

**Theorem 2.1** ([RT00] Theorem 1.9). Let $\text{Ext}: \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}$ be a $(k,\varepsilon)$-strong seeded extractor. Then, it holds that

$$d > \log(n - k) + 2\log(1/\varepsilon) - c \quad \text{and} \quad k \geq 2\log(1/\varepsilon) - c,$$

for some absolute constant $c \in \mathbb{R}$.
Non-malleable extractors. Informally, a non-malleable extractor \( \text{nmExt} \) is a seeded extractor that for any source \( X \) and seed \( s \) outputs a bit \( \text{nmExt}(X, s) \) that is nearly uniform even if given the seed \( s \) and value \( \text{nmExt}(X, s') \) for an adversarially selected seed \( s' \).

Formally, we say that a function \( A : \{0,1\}^d \to \{0,1\}^d \) is an adversarial function if it has no fixed points, i.e., if \( A(s) \neq s \) for all \( s \in \{0,1\}^d \). Non-malleable extractors are defined as follows.

**Definition 2.2.** A function \( \text{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\} \) is a \((k,\varepsilon)\)-non-malleable extractor if for any \((n,k)\)-source \( X \), and for any adversarial function \( A : \{0,1\}^d \to \{0,1\}^d \), it holds that the distribution of the 3-tuple \( (\text{nmExt}(X, U_d), \text{nmExt}(X, A(U_d)), U_d) \) is \( \varepsilon \)-close to \((U_1, \text{nmExt}(X, A(U_d)), U_d)\); that is,

\[
\text{dist}_{TV} \left( (\text{nmExt}(X, U_d), \text{nmExt}(X, A(U_d)), U_d), (U_1, \text{nmExt}(X, A(U_d)), U_d) \right) \leq \varepsilon.
\]

We will also consider the more general notion of \( \tau \)-non-malleable extractors, in which it is possible to extract randomness even given multiple (namely, \( \tau \)) outputs of the extractor with respect to adversarially chosen seeds.

**Definition 2.3.** A function \( \text{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\} \) is a \((k,\varepsilon,\tau)\)-non-malleable extractor if for any \((n,k)\)-source \( X \) and for any \( \tau \) adversarial functions \( A_1, \ldots, A_{\tau} : \{0,1\}^d \to \{0,1\}^d \) it holds that

\[
\text{dist}_{TV} \left( (\text{nmExt}(X, U_d), \text{nmExt}(X, A_i(U_d)))_{i=1}^\tau, U_d), (U_1, (\text{nmExt}(X, A_i(U_d)))_{i=1}^\tau, U_d) \right) \leq \varepsilon.
\]

We conclude this section by stating a recent result, due to Ben-Aroya et al. \cite{BCD+17}, extending a result by Dodis and Wichs \cite{DW09}, which complements our Theorem 1 by showing that the lower bound on the seed length \( d \) in the Theorem 1 is tight up to an additive factor of \( O(\log(t)) \), and the lower bound on \( k \) is almost tight in \( \varepsilon \), up to an additive factor of \( \log \log(1/\varepsilon) \).

**Theorem 2.4 \((\cite{BCD+17}, \cite{DW09})\).** Let \( \varepsilon > 0 \) be sufficiently small, and let \( n, k, d, t \in \mathbb{N} \). There exists a \((k,\varepsilon,\tau)\)-non-malleable extractor \( \text{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\} \) with

\[
d \leq \log(n) + 2\log(1/\varepsilon) + 2\log(t) + O(1) \quad \text{and} \quad k \leq \log(d) + 2\log(1/\varepsilon) + t + O(\log(t)).
\]

3 Refined coding bounds

As we mentioned in the technical overview (Section 1.2), we prove our entropy lower bound for non-malleable extractors by deriving codes from extractors and bounding the rate of these codes. To this end, in this section we prove refined bounds on the rate of binary codes with a given minimum distance. Our starting point is the seminal result of McEliece, Rodemich, Rumsey and Welch \cite{MRR+77}.

**Theorem 3.1 \((\cite{MRR+77})\).** Any code \( C \subseteq \{0,1\}^n \) with relative distance \( \delta \in (0, \frac{1}{2}) \) has rate at most

\[
H \left( \frac{1}{2} - \sqrt{\delta(1-\delta)} \right) + o(1), \quad \text{where } o(1) \text{ is some function that tends to zero as } n \text{ grows to infinity.}
\]

Observe that in particular, by plugging in \( \delta = 0.5 - \varepsilon \) for sufficiently small \( \varepsilon > 0 \), and letting \( n \) be sufficiently large Theorem 3.1 implies that any family of binary codes with blocklength \( n \) and relative distance \( \frac{1}{2} - \varepsilon \) has rate \( \rho = O(\varepsilon^2 \log(1/\varepsilon)) \).

However, the above does not suffice for our needs, as to prove our main result (Theorem 1) we need a quantitative bound on \( n \). We thus prove the following theorem, which provides the refined bound that we seek.
Theorem 3.2. Fix some constant \( c \in (0,1/20) \), and let \( \varepsilon \in (0,c) \). For \( n > \frac{c^2}{\varepsilon} \), let \( C \subseteq \{0,1\}^n \) be a code with relative distance \( \delta = \frac{1}{2} - \varepsilon \). Then \( |C| < 2^{\frac{23c^2}{\varepsilon^2} \log(1/\varepsilon)n} \).

Proof. The proof follows the general approach of Navon and Samorodnitsky [NS09], who provide a spectral graph theoretic framework to prove upper bounds on the rate of binary codes.

We will need the following definition, which generalizes the notion of a maximal eigenvalue to subsets of the hypercube.

**Definition 3.3.** Let \( A \in \{0,1\}^{2^n \times 2^n} \) be the adjacency matrix of the hypercube graph; that is, \( A_{x,y} = 1 \) if and only if \( x \in \{0,1\}^n \) and \( y \in \{0,1\}^n \) differ in exactly one coordinate. Given a set \( B \subseteq \{0,1\}^n \), we define

\[
\lambda_B = \max_{f : \{0,1\}^n \to \mathbb{R}} \langle Af, f \rangle \quad \text{supp}(f) \subseteq B.
\]

To better understand the definition of \( \lambda_B \), it is convenient to consider the subgraph \( H_B \) of the hypercube graph \( \{0,1\}^n \) induced by the vertices in \( B \), and observe that \( \lambda_B \) is the maximal eigenvalue of the adjacency matrix of \( H_B \). Navon and Samorodnitsky [NS09] prove the following result.

**Proposition 3.4 ([NS09] Proposition 1.1).** Let \( C \subseteq \{0,1\}^n \) be a code with relative distance \( \delta > 0 \), and let \( \varepsilon > 0 \). Suppose that for a subset \( B \subseteq \{0,1\}^n \) it holds that \( \lambda_B \geq (1 - 2\delta + \varepsilon)n \). Then \( |C| \leq |B|/\varepsilon \).

The foregoing theorem naturally suggest the following proof strategy: to upper bound the rate of a binary code \( C \) with relative distance \( \delta = 0.5 - \varepsilon \), it suffices to exhibit a (small as possible) set \( B \subseteq \{0,1\}^n \) whose corresponding maximal eigenvalue satisfies \( \lambda_B \geq 3\varepsilon n \); note that the smaller \( B \) is, the better upper bound we get on the rate of \( C \).

Towards this end, let \( r \in [n] \) be a parameter to be chosen later, and let

\[
B = \{ x \in \{0,1\}^n : |x| \in \{r,r+1\} \}.
\]

We lower bound the maximal eigenvalue \( \lambda_B \) by showing a particular function \( f \) that is supported on \( B \), such that \( \langle Af, f \rangle \geq 3\varepsilon n \). Specifically, for some \( a,b \in \mathbb{R} \) to be chosen later, we define \( f : \{0,1\}^n \to \mathbb{R} \) as

\[
f(x) = \begin{cases} a & \text{if } |x| = r \\ b & \text{if } |x| = r + 1 \\ 0 & \text{otherwise} \end{cases}.
\]

Clearly \( \text{supp}(f) \subseteq B \). Observe that

\[
\frac{\langle Af, f \rangle}{\langle f, f \rangle} = \frac{ab \binom{n}{r} \cdot (n-r)}{a^2 \binom{n}{r} + b^2 \binom{n}{r+1}} = \frac{ab \binom{n}{r} \cdot (n-r)}{a^2 \binom{n}{r} + b^2 \binom{n}{r+1}} > \frac{ab \cdot r(n-r)}{a^2 \cdot r + b^2 \cdot (n-r)}.
\]

By choosing \( r \) to be an integer in the interval \( \left[ \frac{9c^2}{\varepsilon} n, \frac{10c^2}{\varepsilon} n \right] \) and letting \( b = a \sqrt{\frac{r}{n}} \) we get that

\[
\frac{\langle Af, f \rangle}{\langle f, f \rangle} > \frac{a^2 \sqrt{r/n} \cdot r(n-r)}{a^2 r + a^2 \cdot (r/n) \cdot (n-r)} = \frac{\sqrt{r} n (n-r)}{2n-r} > 3\varepsilon n,
\]

\footnote{Note that by the assumption in the theorem we have \( 1 < \frac{c^2}{\varepsilon} n < n \). In particular, the interval \( \left[ \frac{9c^2}{\varepsilon} n, \frac{10c^2}{\varepsilon} n \right] \) contains an integer.}
where the last inequality uses the assumptions that \( \varepsilon < c < 1/20 \), which implies that \( r \leq \frac{10c^2}{c-n} < \frac{n}{2} \).

Therefore, by applying Proposition 3.4 we get that

\[
|C| \leq \frac{|B|}{\varepsilon} = \frac{\binom{n}{r} + \binom{\binom{n}{r} + 1}{r+1}}{\varepsilon} \leq \left(\frac{n}{r}\right) \frac{n}{r\varepsilon} \leq \frac{c}{9\varepsilon^3} \left(\frac{10c^2}{e^2}\right) \leq \frac{c}{9\varepsilon^3} \left(\frac{ce}{10e^2}\right) \frac{10c^2}{e^2} n < 2^{\frac{20c^2\log(1/\varepsilon)}{\varepsilon}} n ,
\]

which concludes the proof of Theorem 3.2.

\[\square\]

4 Proof of Theorem 1

In this section we prove Theorem 1, which we restate here with slightly more specific parameters than those stated above.

**Theorem 1 (restated):** Let \( n, k, d, t \in \mathbb{N} \) be parameters such that \( t \leq 2^{d/2} \), and let \( \varepsilon \in (0, c_0/2) \) for \( c_0 = \min\{1/2^2, 1/20\} \), where \( c > 0 \) is the constant from Theorem 2.1. If \( \text{nmExt} : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\} \) is a \((k,\varepsilon)\)-non-malleable extractor, then

\[
d > \log(n-k) + 2\log(1/\varepsilon) - O(1) \text{ and } k \geq \log(d) + 2\log(1/\varepsilon) - \log\log(1/\varepsilon) + \log(t) - O(1).
\]

We start, in Section 4.1, with the proof of Theorem 1 for the special case where \( t = 1 \) (i.e., for standard non-malleable extractors). Then, in Section 4.2, we provide the full proof for general values of \( t \).

4.1 Proof of Theorem 1 for \( t = 1 \)

Following the outline provided in Section 1.2, we start the proof with the following lemma, showing that any non-malleable extractor induces an error correcting code with good distance.

**Lemma 4.1 (Lemma 2 restated).** If there exists a \((k,\varepsilon)\)-non-malleable extractor \( \text{nmExt} : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\} \), then there exists an error correcting code \( C \subseteq \{0,1\}^{2k} \) with relative distance \( 0.5 - 2\varepsilon \) and rate \( \frac{d-1}{2^k} \).

**Proof.** Let \( \text{nmExt} : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\} \) be a \((k,\varepsilon)\)-non-malleable extractor, and let \( X \) be an \((n,k)\)-source. That is, \( X \subseteq \{0,1\}^n \) is a collection of \( K = 2^k \) vectors, which we denote by \( X = \{x_1, \ldots, x_K\} \subseteq \{0,1\}^n \). For each seed \( s \in \{0,1\}^d \), let \( w(s) \in \{0,1\}^K \) be the \( K \)-bit evaluation vector defined as

\[
w(s) = (\text{nmExt}(x_i, s))_{i \in \{1,\ldots,K\}}.
\]

We claim that the (multi-)set \( \{w(s) : s \in \{0,1\}^d\} \subseteq \{0,1\}^K \) contains an error correcting code \( C \subseteq \{0,1\}^K \) with relative distance \( 0.5 - 2\varepsilon \) and rate \( \frac{d-1}{2^k} \).

**Claim 4.2.** There exists a subset \( S \subseteq \{0,1\}^d \) of size \( 2^{d-1} \) such that for every two distinct \( s, s' \in S \) it holds that \( \text{dist}(w(s), w(s')) \geq 0.5 - 2\varepsilon \).

**Proof.** Suppose towards contradiction that for every subset \( S' \subseteq \{0,1\}^d \) of size at least \( 2^{d-1} \) there exist distinct seeds \( s, s' \in S' \) such that \( \text{dist}(w(s), w(s')) < 0.5 - 2\varepsilon \). We show below that this contradicts the assumption that \( \text{nmExt} \) is a \((k,\varepsilon)\)-non-malleable extractor.
Indeed, by the assumption, we can find $s_1, s'_1 \in \{0,1\}^d$ such that $\text{dist}(w(s_1), w(s'_1)) < 0.5 - 2\varepsilon$. Then, we can remove $s_1, s'_1$ from $\{0,1\}^d$, and apply the assumption again, to obtain $s_2, s'_2 \in \{0,1\}^d \setminus \{s_1, s'_1\}$ such that $\text{dist}(w(s_2), w(s'_2)) < 0.5 - 2\varepsilon$. By iteratively repeating this argument $D/4$ times, where $D = 2^d$, we obtain $D/4$ pairs of distinct elements $(s_1, s'_1), \ldots, (s_{D/4}, s'_{D/4})$ such that
\[
\forall j \in [D/4] \quad \text{dist} \left( w(s_j), w(s'_j) \right) < 0.5 - 2\varepsilon .
\] (1)

Let $B = \{ s_j, s'_j : j \in [D/4] \} \subseteq \{0,1\}^d$ denote the set of all such “bad” seeds, and define an adversarial function $A : \{0,1\}^d \rightarrow \{0,1\}^d$ that matches each pair of bad seeds by mapping $A(s_j) = s'_j$ and $A(s'_j) = s_j$ for all $j \in [D/4]$, and defining $A(s)$ arbitrarily for all other seeds $s \notin B$.

Next we prove that $\text{nmExt}$ is not a $(k, \varepsilon)$-non-malleable extractor by arguing that the distribution of the random variable consisting of the 3-tuple $(\text{nmExt}(X, U_d), \text{nmExt}(X, \mathcal{A}(U_d)), U_d)$ is $\varepsilon$-far from $(U_1, \text{nmExt}(X, \mathcal{A}(U_d)), U_d)$, where recall that $U_m$ denotes the random variable that is uniformly distributed over $\{0,1\}^m$. Indeed, consider the following distinguisher $D : \{0,1\} \times \{0,1\} \times \{0,1\}^d \rightarrow \{0,1\}$, defined as
\[
D(b, b', s) = \begin{cases} 1_{b=b'} & \text{if } s \in B \\ U_1 & \text{otherwise} \end{cases}.
\]
Clearly $\Pr[D(U_1, \text{nmExt}(X, \mathcal{A}(U_d)), U_d) = 1] = 0.5$. On the other hand, by Eq. (1), for $s$ sampled from $U_d$ we have
\[
\Pr[D(\text{nmExt}(X, s), \text{nmExt}(X, \mathcal{A}(s)), s) = 1] \geq (0.5 + 2\varepsilon) \Pr[s \in B] + 0.5 \Pr[s \notin B] \geq 0.5 + \varepsilon,
\]
thus contradicting the assumption that $\text{nmExt}$ is a $(k, \varepsilon)$-non-malleable extractor. This concludes the proof of Claim 4.2.

Therefore, by Claim 4.2 there exists a set $C = \{ w(s) : s \in S \} \subseteq \{0,1\}^K$ of size $2^{d-1}$ such that for every $x, y \in C$ it holds that $\text{dist}(x, y) \geq 0.5 - 2\varepsilon$, i.e., $C$ is an error correcting code with relative distance $0.5 - 2\varepsilon$ and rate $\frac{d-1}{2^K}$, which completes the proof of Lemma 4.1.

By applying the bound from Theorem 3.2 to the code obtained in Lemma 4.1 we prove Theorem 1 for the case of $t = 1$.

Proof of Theorem 1 for $t = 1$. Since every non-malleable extractor is, in particular, a strong seeded extractor, then by Theorem 2.1 it holds that the seed length is $d > \log(n - k) + 2\log(1/\varepsilon) - c$, as required. Furthermore, Theorem 2.1 also implies that
\[
k \geq 2\log(1/\varepsilon) - c .
\] (2)

By Lemma 4.1, if $\text{nmExt} : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}$ is a $(k, \varepsilon)$-non-malleable extractor, then there exists an error correcting code $C \subseteq \{0,1\}^{2^k}$ with relative distance $0.5 - 2\varepsilon$ and rate $\frac{d-1}{2^K}$.

Next, we wish to apply Theorem 3.2 to the code $C$. Recall that by the assumption it holds that $\varepsilon < c_0$ and $c_0 < 1/2\varepsilon$, and observe that by Eq. (2) we have $2^k \geq \frac{2 - \varepsilon}{\varepsilon} > \frac{c_0}{2}$. Therefore, by applying Theorem 3.2 with respect to $c_0$ (recall that $c_0 < 1/20$) and $2\varepsilon < c_0$ we get that
\[
2^{d-1} \leq |C| < 2^{\frac{c_0}{20} - (2\varepsilon)^2 \log(1/\varepsilon) 2^k},
\]
and thus $k \geq \log(d) + 2\log(1/\varepsilon) - \log(1/\varepsilon) - O(1)$, as required.
4.2 Proof of Theorem 1 for general \( t \)

Next, we extend the idea presented in Section 4.1 to larger values of \( t \). The key step is the following lemma.

**Lemma 4.3.** If there exists a \((k, \varepsilon)\)-t-non-malleable extractor \( \text{nmExt} : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\} \), then, there exists an error correcting code \( C \subseteq \{0,1\}^k \) with relative distance \( 0.5 - 2\varepsilon \) such that \( |C| \geq (2^{d-1}/t)\lceil t/2 \rceil \).

**Proof.** Let \( \text{nmExt} : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\} \) be a \((k, \varepsilon)\)-t-non-malleable extractor. Similarly to the proof of Lemma 4.1, we set \( K = 2^k \), and let \( X \) be an \((n,k)\)-source, which we view as a collection of vectors \( X = \{x_1, \ldots, x_K\} \subseteq \{0,1\}^n \). For each seed \( s \in \{0,1\}^d \), let \( w(s) \in \{0,1\}^K \) be the \( K \)-bit evaluation vector, defined as \( w(s) = (\text{nmExt}(x_i, s))_{i \in \{1, \ldots, K\}} \). Hereafter, all sums involving binary vectors are summations over \( \text{GF}(2) \). For \( x \in \{0,1\}^n \), we denote by \( \text{weight}(x) \) the (absolute) Hamming weight of \( x \).

Whereas before, in the proof of Lemma 4.1, we showed that the multi-set of evaluation vectors \( \{w(s) : s \in \{0,1\}^d\} \subseteq \{0,1\}^K \) simply contains an error correcting code with good parameters, here we will derive our code by considering all \( \text{GF}(2) \)-linear combinations of \( \lceil t/2 \rceil \) elements of a carefully selected subset of the evaluation vectors.

Towards that end, the next claim shows that there exists a large subset of seeds such that any linear combination of \( t+1 \) of the evaluation vectors that corresponds to these seeds has large Hamming weight.

**Claim 4.4.** There is a subset \( S \subseteq \{0,1\}^d \) of size \( 2^{d-1} \) such that for every subset \( I \subseteq S \) of size \( |I| \leq t + 1 \) it holds that \( \text{weight} \left( \sum_{s \in I} w(s) \right) \geq (0.5 - 2\varepsilon)K \).

**Proof.** Assume towards contradiction that for every subset \( S' \subseteq \{0,1\}^d \) of size at least \( 2^{d-1} \) there are \( t' \leq t + 1 \) distinct seeds \( s_1, \ldots, s_{t'} \in S' \) such that

\[
\Pr_{x \in X} \left[ \sum_{j=1}^{t'} \text{nmExt}(x, s_j) = 0 \right] < 0.5 - 2\varepsilon .
\]

We show below that this contradicts the assumption that \( \text{nmExt} \) is a \((k, \varepsilon)\)-t-non-malleable extractor.

By our assumption, there is a subset of seeds \( S_1 \subseteq \{0,1\}^d \) for which there exists \( I_1 \subseteq S_1 \) of size \( |I_1| = t_1' \leq t \) such that \( \text{weight} \left( \sum_{s \in I_1} w(s) \right) < (0.5 - 2\varepsilon)K \). We remove \( I_1 \) from \( \{0,1\}^d \), and apply the assumption again to obtain \( I_2 \subseteq \{0,1\}^d \) of size \( |I_2| = t_2' \leq t + 1 \) such that \( \text{weight} \left( \sum_{s \in I_2} w(s) \right) < (0.5 - 2\varepsilon)K \). We then remove \( I_2 \) from \( \{0,1\}^d \setminus I_1 \), and apply the assumption again with respect to \( \{0,1\}^d \setminus (I_1 \cup I_2) \). By repeating this argument as long as \( |\cup_j I_j| < 2^{d-1} \), we obtain \( R \) disjoint subsets \( I_1, \ldots, I_R \), where the size of each \( I_j \) is \( t_j' \leq t + 1 \), such that \( \sum_{j=1}^{R} |I_j| \geq 2^{d-1} \) and

\[
\text{weight} \left( \sum_{s \in I_j} w(s) \right) < (0.5 - 2\varepsilon)K ,
\]

for all \( j \in [R] \). Analogously to the proof of Lemma 4.1 the set \( I_1 \cup \ldots \cup I_R \) consists of the “bad seeds” that correspond to evaluation vectors whose \((t+1)\)-element linear combinations are of low weight.
To prove that the foregoing collection of “bad seeds” violates the assumption that $\text{nmExt}$ is a $(k, \varepsilon)$-$t$-non-malleable extractor, we exhibit $t$ adversarial functions $A_1, \ldots, A_t : \{0, 1\}^d \rightarrow \{0, 1\}^d$ (with no fixed points) for which there exists a function that distinguishes between the random variables consisting of the $(t + 2)$-tuples
\[
\left( \text{nmExt}(X, U_d), \left( \text{nmExt}(X, A_\ell(U_d)) \right)_{\ell \in [t]}, U_d \right)
\]
with confidence $\varepsilon$, where recall that $U_m$ denotes the random variable that is uniformly distributed over $\{0, 1\}^m$.

We define the family $\{A_\ell\}_{\ell \in [t]}$ in the natural way, by mapping each of the bad seeds to the set of seeds with which its linear combination is a low weight vector. That is, for each $j \in [R]$ let $I_j = \{s_1, \ldots, s_{t_j}'\}$, where $t_j' \leq t + 1$. Then, for all $\ell \in [t]$ we define
\[
A_\ell(s_i) = \begin{cases} 
    s_i + \ell \pmod{t_j'}, & \text{for } s_i \in I_j, j \in [R] \\
    \text{arbitrary}, & \text{for } s \in \{0, 1\}^d \setminus (\cup_{j \in [R]} I_j).
\end{cases}
\]
Note that by definition of the $A_\ell$'s, for all $j \in [R]$ and $s \in I_j$ it holds that $\{s\} \cup \{A_\ell(s) : \ell \in [t_j' - 1]\} = I_j$, and so, by Eq. (3) we have that
\[
\Pr_{x \in X} \left[ \text{nmExt}(x, s) = \sum_{i=1}^{t_j'-1} \text{nmExt}(x, A_i(s)) \right] = \frac{\text{weight} \left( \sum_{s \in I_j} w(s) \right)}{K} < (0.5 - 2\varepsilon)K.
\]

Next, we define the distinguisher $D : \{0, 1\} \times \{0, 1\}^t \times \{0, 1\}^d \rightarrow \{0, 1\}$ as
\[
D(b, b_1, \ldots, b_t, s) = \begin{cases} 
    1_{b = \sum_{i \in [t_j'-1]} b_i}, & \text{if } s \in I_j \text{ for some } j \in [R] \\
    U_1, & \text{otherwise}.
\end{cases}
\]
Clearly $\Pr \left[ D \left( U_1, \left( \text{nmExt}(X, A_\ell(U_d)) \right)_{\ell \in [t]}, U_d \right) = 1 \right] = 0.5$. On the other hand, for $s$ sampled from $U_d$ we have
\[
\Pr \left[ D \left( \text{nmExt}(X, s), \left( \text{nmExt}(X, A_\ell(s)) \right)_{\ell \in [t]}, s \right) = 1 \right] 
\geq (0.5 + 2\varepsilon) \Pr \left[ s \in \cup_{j \in [R]} I_j \right] + 0.5 \Pr \left[ s \in \{0, 1\}^d \setminus \cup_{j \in [R]} I_j \right] \geq 0.5 + \varepsilon,
\]
thus contradicting the assumption that $\text{nmExt}$ is a $(k, \varepsilon)$-$t$-non-malleable extractor. This concludes the proof of Claim 4.4.$\square$

Let $S \subseteq \{0, 1\}^d$ be the set guaranteed by Claim 4.4 and consider the code
\[
C \overset{\text{def}}{=} \left\{ \sum_{s \in I} w(s) : I \subseteq S, |I| \leq \lfloor t/2 \rfloor \subseteq \{0, 1\}^K \right\}.
\]
Note that for $D = 2^d$ we have $|C| \geq \left( \frac{D}{|t/2|} \right) \geq (D/2t)^{t/2}$. By the guarantee of Claim 4.4 for every distinct $x, y \in C$ it holds that $\text{dist}(x, y) \geq 0.5 - 2\varepsilon$; that is $C \subseteq \{0, 1\}^K$ is an error correcting code with relative distance $0.5 - 2\varepsilon$, which completes the proof of Lemma 4.3.$\square$
We prove Theorem 1 by applying the bound from Theorem 3.2 to the code obtained in Lemma 4.3, analogously to the way we proved the theorem for the restricted case of \( t = 1 \) before.

**Proof of Theorem 1 (general case).** Since every \( t \)-non-malleable extractor is, in particular, a strong seeded extractor, then by Theorem 2.1 it holds that the seed length is \( d > \log(n-k) + 2 \log(1/\varepsilon) - c \), as required. Furthermore, Theorem 2.1 also implies that \( k \geq 2 \log(1/\varepsilon) - c \).

By Lemma 4.3, if \( \text{nmExt} : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\} \) is a \((k,\varepsilon)\)-non-malleable extractor, then there exists an error correcting code \( C \subseteq \{0,1\}^{2^k} \) with relative distance \( 0.5 - 2\varepsilon \) such that \( |C| \geq (2^{d-1}/t)^{t/2} \).

We wish to apply Theorem 3.2 to the code \( C \). Recall that by the assumption it holds that \( \varepsilon < c_0 \) and \( c_0 < 1/2^c \), and observe that according to the bound on \( k \) given by Theorem 2.1, we have that \( 2^k \geq \frac{2 - \varepsilon}{\varepsilon^2} > \frac{c_0}{\varepsilon^2} \). Therefore, by applying Theorem 3.2 with respect to \( c_0 \) (recall that \( c_0 < 1/20 \)) and \( 2\varepsilon < c_0 \), we get that

\[
(2^{d-1}/t)^{t/2} \leq |C| < 2^{23} \cdot (2\varepsilon)^2 \log(1/2\varepsilon)2^k,
\]

and by the assumption that \( \log(t) < d/2 \) we get that

\[
\frac{23}{c_0} \cdot (2\varepsilon)^2 \log(1/2\varepsilon)2^k \geq (d - 2 - \log(t)) \cdot \lfloor t/2 \rfloor \geq \Omega(d \cdot t).
\]

This implies that \( k \geq \log(d) + \log(t) + 2 \log(1/\varepsilon) - \log \log(1/\varepsilon) - O(1) \), as required.

\( \square \)

**Acknowledgements**

We are thankful to Gil Cohen for helpful discussions. We also thank Venkatesan Guruswami for a discussion regarding the MRRW bounds.

**References**


