Randomness Extractors Seminar **December 29, 2016**

Explicit Construction of 2-source Extractors - Resilient Function

Leader: KM Chung **Notes: Chi-Ning Chou**

We are going to see some how to construct a good resilient function.

From the overview of the construction of 2-source extractors, we saw that *resilient function* is one of the key ingredient. Since it is interesting on its own, here we are going to focus on how to construct a good resilient function. We will show how to use resilient function to construct 2-source extractor next time.

1 Definition and historical development

Resilient function was introduced by Ben-Or and Linial [BOL85] in the context of collective-coin flipping, which had been defined last time. Intuitively, resilient function is a boolean function that are not easily affected by any not too large subset of input bits. The following formally define this notion.

Definition 1 (influence)**.** *Let $f : \{0,1\}^n \to \{0,1\}$ be a boolean function, $Q \subseteq [n]$, and $\mathcal{D}$ is a distribution over $\{0,1\}^n$. Define the influence of f w.r.t. Q over distribution $\mathcal{D}$ as*

$$I_{Q,\mathcal{D}} := \mathbb{P}_{x \leftarrow \mathcal{D}}[f \text{ is undetermined after fixing bits of } x \text{ in } \bar{Q}]. \tag{1}$$

When we do not specify, we assume $\mathcal{D} = U_n$. For any $q \in [n]$, we can further define

$$I_{q,\mathcal{D}} := \max_{Q \subseteq [n],\ |Q|=q} I_{Q,\mathcal{D}}. \tag{2}$$

Resilient function is simply function that has low influence on any not too large subset of input.

Definition 2 (resilient function)**.** *Let $f : \{0,1\}^n \to \{0,1\}$ be a boolean function and $q \in [n]$. We said f is $(q,\epsilon)-$resilient if $I_q(f) \leq \epsilon$.*

As one can see, if f is a constant function, it's trivially a n-resilient function. However, it's uninterested and useless. In most of the cases, we also want f to be almost unbiased[1].

Remark 3. Here, we consider resilient to uniform input. For 2-source extractors, we actually consider more complicated source (if you remember, the NOBF source). To build such resilient function from resilient function w.r.t. uniform input require monotonicity and will have several error tradeoff.

The following table summarized historical and recent development in resilient function.

[1] A.k.a. almost *balanced*.

Reference	Type	Resilient
[AL93]	Existence, non-monotone	$\Omega(n/\log^2 n)$
[Mek09]	Depth logarithmic, non-monotone	$\Omega(n^{1-\delta})$
[CZ15]	Depth 4, monotone	$\Omega(n^{1-\delta})$
[Mek15]	Depth 3, monotone	$\Omega(n/\log^2 n)$

Table 1: Historical and recent development in resilient function.

Remark 4. I will index the theorems and lemmas in the following as the same as in [CZ15].

2 Explicit construction of resilient function in [CZ15]

In [CZ15], Chattopadhyay and Zuckerman explicitly construct a new constant depth resilient function for $\Omega(n^{1-\delta})$ bad portions. The high-level idea is derandomizing the probabilistic construction in [AL93] by utilizing the good structure of Trevisan extractors. Let's first formally state the result of them.

Theorem (**5.1** construction of good resilient function)**.** *For any $\delta > 0$, and large enough n, there exists a poly-time computable monotone function $f : \{0,1\}^n \to \{0,1\}$ satisfying:*

- *(small circuit) f is a depth 4 circuit in AC^0 of size $n^{O(1)}$.*
- *(small bias) $|\mathbb{E}_{x\sim U_n}[f(x)] - \frac{1}{2}| \leq \frac{1}{n^{\Omega(1)}}$.*
- *(small influence to size $n^{1-\delta}$) For any $q > 0$, $I_q(f) \leq \frac{q}{n^{1-\delta}}$.*

We are going to start with the Ajtai-Linial existence construction in section 2.1. Then, the explicit construction in [CZ15] will be introduced in Section 2.2 and be rigorously analyzed in Section 3.

2.1 Ajtai-Linial existence construction

The construction of Ajtai-Linial can be divided into two steps.

Step 1 Consider a partition $\mathcal{P}$ of $[n]$, *i.e.,* P consists of M disjoint blocks $P_1, \ldots, p_M$ of size B such that $[n] = \cup_{j\in[M]} P_j$ and $n = MB$. Define the tribe function of P as

$$T_P(x) := \bigvee_{j\in[M]} \bigwedge_{\ell\in P_j} x_\ell. \tag{3}$$

Step 1 Now, pick R random permutations $\mathcal{P}^1, \ldots, \mathcal{P}^R$ on $[n]$ and define the corresponding Ajtai-Linial function as

$$\begin{aligned} f(x) &:= \bigwedge_{i\in[R]} f_{\mathcal{P}^i} \\ &= \bigwedge_{i\in[R]} \bigvee_{j\in[M]} \bigwedge_{\ell\in P_j^i} x_\ell. \end{aligned} \tag{4}$$

Pictorially, we can visualize the tribe function and Ajtai-Linial function as follows.

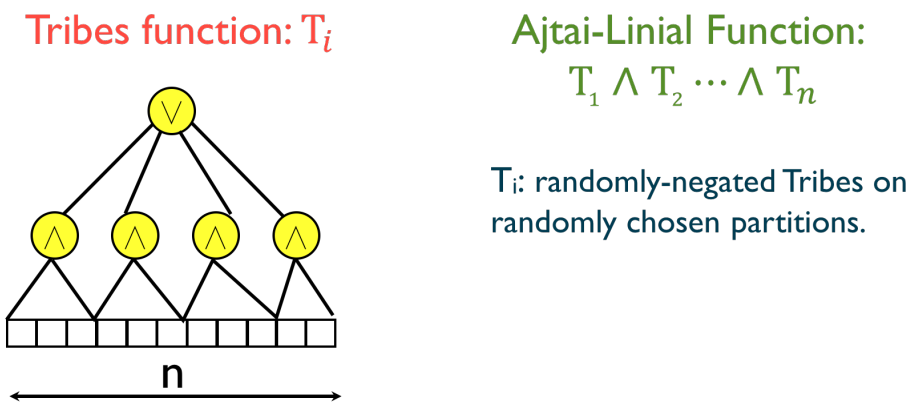

Figure 1: Tribe function and Ajtai-Linial function.

When properly choosing the parameters, Ajtai and Linial [AL93] proved that Ajtai-Linial function is $\Omega(n/\log^2 n)$-resilient with nonzero probability. However, two major drawbacks of Ajtai-Linial function make itself difficult to be applied in practice.

- The construction is probabilistic. To find good tribe functions by brute-force search deterministically requires $2^{O(n^2)}$ time.
- The function is not guaranteed to be monotone since there are random negation in the bottom layer. Thus, we cannot generalize the resilience to NOBF source with known techniques.

To resolve these issues, we choose the tribe functions, i.e. choose partitions, deterministically and nicely so that the resulting function is monotone and has large resilience. Formally, we want the partitions to enjoy the following three properties:

- (Simple and Monotone) The construction should be poly-time computable and the resulting function should be monotone.
- (Bound influence) Any small subsets ($< n^{1-\delta}$) of $[n]$ has small number of intersections with most partitions.
- (Bound bias) The partitions are pairwise pseudorandom: the interaction of any two blocks from distinct partitions is bounded by $0.9B$.

2.2 Chattopadhyay-Zuckerman explicit construction

The idea of [CZ15] to deterministically find proper partitions is quite cute: using the structure of Trevisan extractor! I believe most of the reader won't have any idea when seeing this sentence, let's find the partitions step by step. In the following, we consider derandomizing Ajtai-Linial function on s bits.

Step 1 Let $TExt : \{0,1\}^r \times \{0,1\}^b \to \{0,1\}^m$ be a Trevisan extractors with parameters set in Section 3.1. Consider its dependency graph G_{TExt} defined as what we did before. Extend it to G'_{TExt} where the right vertex set is the Cartesian product of seed and output. See Figure 2.

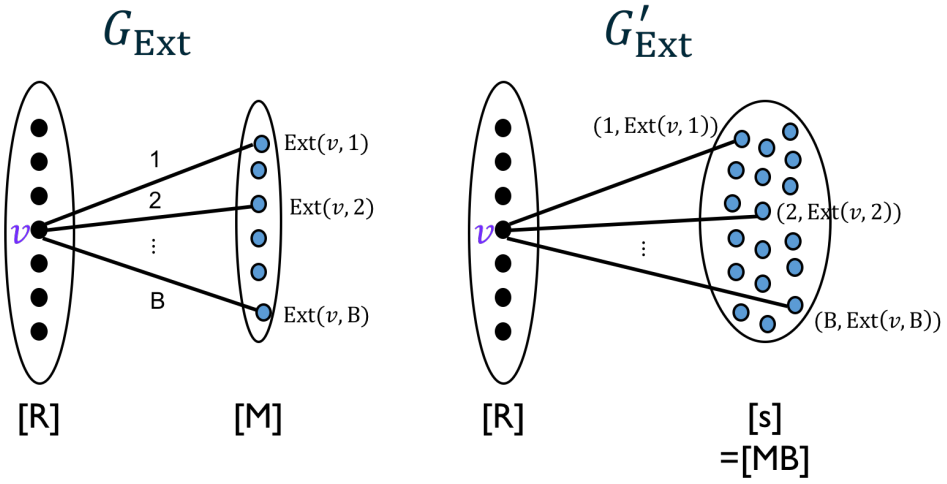

Figure 2: Trevisan extractor's dependency graph G_{TExt} and its extension.

Step 2 Next, let $s = MB$ and thus one can think of the right vertex set of G'_{TExt} as a $M \times B$ matrix or even an s bit string. See Figure 3.

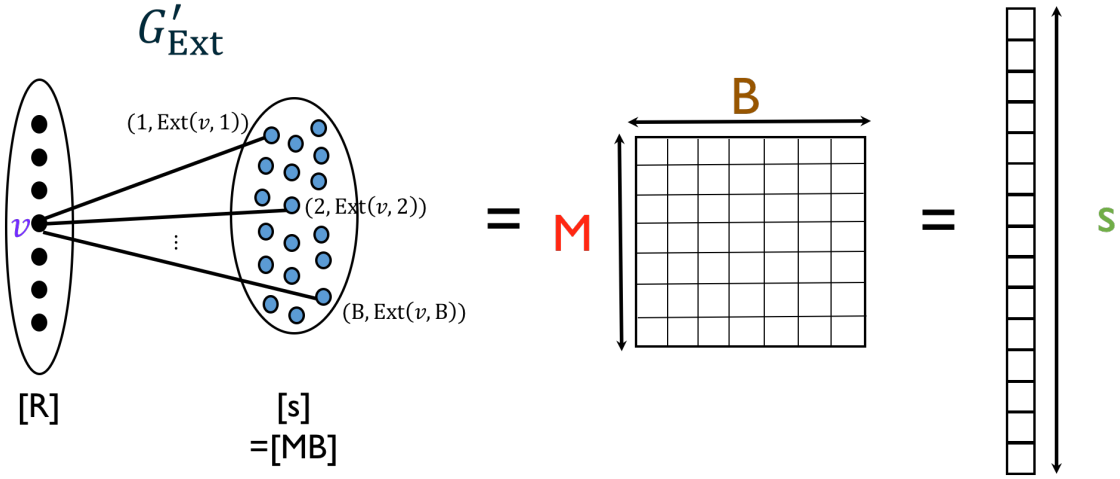

Figure 3: Think of the right vertex set of G'_{TExt} as a $M \times B$ matrix or even an s bit string.

Step 3 For each $i \in \{0,1\}^r$, observe that $\{(z, TExt(i,z)) : z \in \{0,1\}^b\}$ slices the $\{0,1\}^m \times \{0,1\}^b$ matrix as in the left of Figure 4. Next, by *shifting* this slicing through out the whole matrix, we get a partition on $\{0,1\}^m \times \{0,1\}^b$, or equivalently on $[s]$.

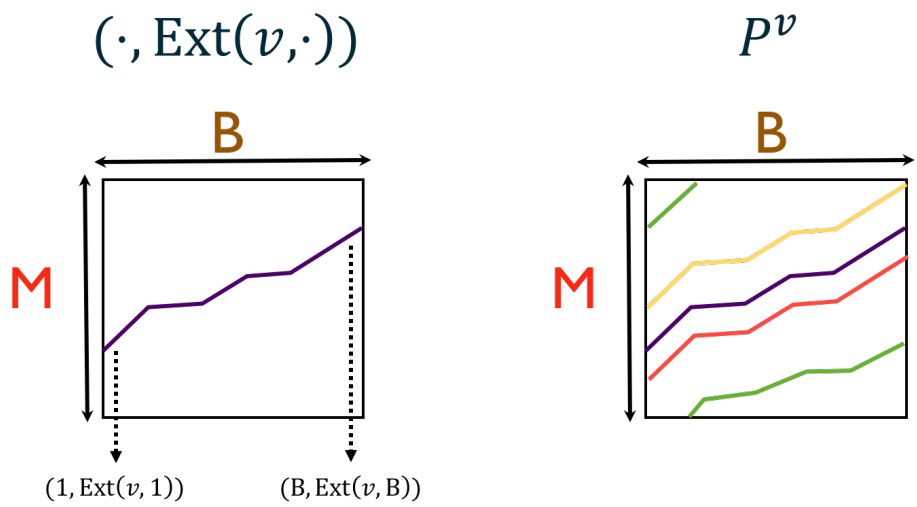

Figure 4: (left) For each $i \in \{0,1\}^r$, the every possible output slices the matrix. (right) By shifting the slicing, each $i \in \{0,1\}^r$ forms a partition on $[s]$.

Step 4 Let's formally define the above partition. For each $i \in \{0,1\}^r$, define the corresponding partition $\mathcal{P}^i = \{P^i_j : \ j \in \{0,1\}^m\}$ where

$$P^i_j := \{(z, TExt(i,z) \oplus j) : \ z \in \{0,1\}^b\} \tag{5}$$

As a result, the derandomized Ajtai-Linial function is

$$f_{TExt}(y) := \bigwedge_{i \in \{0,1\}^r} \bigvee_{j \in \{0,1\}^m} \bigwedge_{\ell \in P^i_j} y_\ell. \tag{6}$$

Step 5 However, f_{TExt} does not perform well on uniform input. If fact, it behaves well on Bernoulli input with higher probability to be 1 due to the parameter of Trevisan extractor. To fix this problem, we introduce another CNF for each y_ℓ in order to transform uniform input to Bernoulli input. Concretely, for each $\ell \in [s]$,

$$y_\ell := \bigwedge_{g_1 \in [h_1]} \bigvee_{g_2 \in [h_2]} x_{\ell, g_1, g_2}. \tag{7}$$

As we pick $n = sh_1h_2$, the final Chattopadhyay-Zuckerman function is

$$f(x) := \bigwedge_{i \in \{0,1\}^r} \bigvee_{j \in \{0,1\}^m} \bigwedge_{\ell \in P^i_j,\ g_1 \in [h_1]} \bigvee_{g_2 \in [h_2]} x_{\ell, g_1, g_2}. \tag{8}$$

3 Analysis of Chattopadhyay-Zuckerman construction

Now, we want to prove that the construction in Section 2.2 satisfies the properties in Theorem 5.1. Before we tune the parameter and get ourselves dirty, it's simple to see that the Chattopadhyay-Zuckerman function f is monotone and has depth 4 and polynomial size.

As we mentioned earlier, f actually performs well on Bernoulli source. The following lemma provides a way to approximate Bernoulli source with uniform source.

Lemma (**5.7** from uniform to Bernoulli)**.** *For any $0 < \gamma < 0.9$ and $\nu > 0$, there exists explicit size h monotone CNF C on h bits, where $h = O(\frac{1}{\nu} \ln \frac{1}{\nu})$, such that $\gamma - \nu \leq \mathbb{P}_{x \sim U_h}[C(x) = 0] < \gamma$. Namely, if $x \sim U_h$, $C(x)$ is ν-close to Bernoulli $1 - \gamma$.*

Next, define parameter

$$\gamma := \frac{\ln M - \ln \ln(R/\ln 2)}{B}. \tag{9}$$

The following two lemmas bound the influence and bias of f_{TExt} with Bernoulli input.

Proof. See the mathematics background note. □

Lemma (**5.3** bound influence)**.** *Let $TExt$ be the Trevisan extractor with parameters set in Section 3.1, for any $\epsilon_1 > 0$, and $(1 - B^{-\epsilon_1})\gamma \leq p_1 \leq \gamma$. There exists constant $\delta > 0$ such that for any $0 < q < s^{1-\delta}$,*

$$I_{q, Ber(s, 1-p_1)}(f_{TExt}) \leq \frac{q}{s^{1-\delta}}. \tag{10}$$

Proof. See Section 3.2. □

Lemma (**5.5** bound bias)**.** *Let $TExt$ be the Trevisan extractor with parameters set in Section 3.1, for any $0 < q < s^{1-\delta}$, for any $\epsilon_1 > 0$, and $(1 - B^{-\epsilon_1})\gamma \leq p_1 \leq \gamma$. $|\mathbb{E}_{y \in Ber(s, 1-p_1)}[f_{TExt}(y)] - \frac{1}{2}| \leq B^{-\Omega(1)}$.*

Proof. See Section 3.3. □

With Lemma 5.3, Lemma 5.5, and Lemma 5.7, we can prove Theorem 5.1. See Figure 5 for the visualization of the proof structure

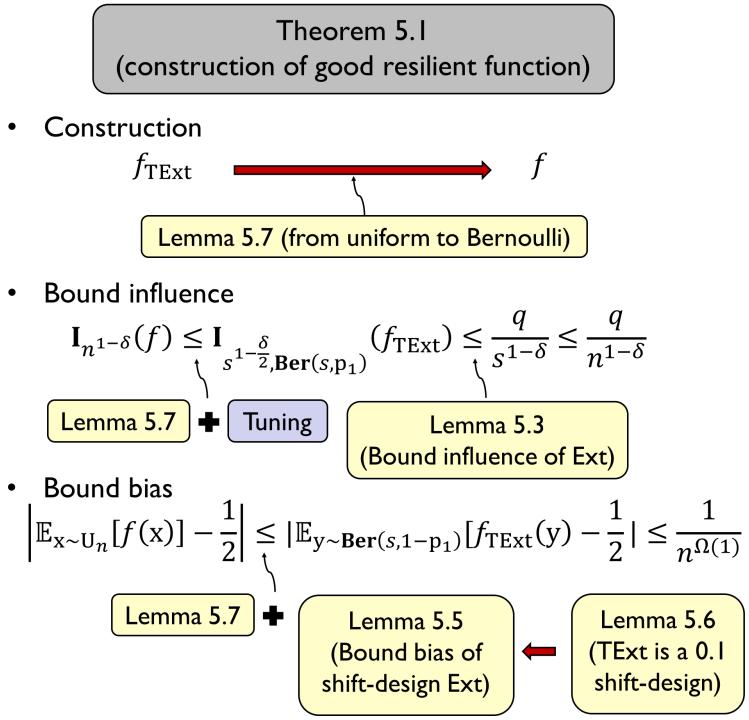

Figure 5: The proof structure of Theorem 5.1.

In Section 3.1 we first introduce the parameters we are going to use. In Section 3.2 and Section 3.3, we are going to bound the influence and bias of f respectively.

3.1 Parameters

Before we rigorously prove the three important lemmas, lets first see the relationship among parameters.

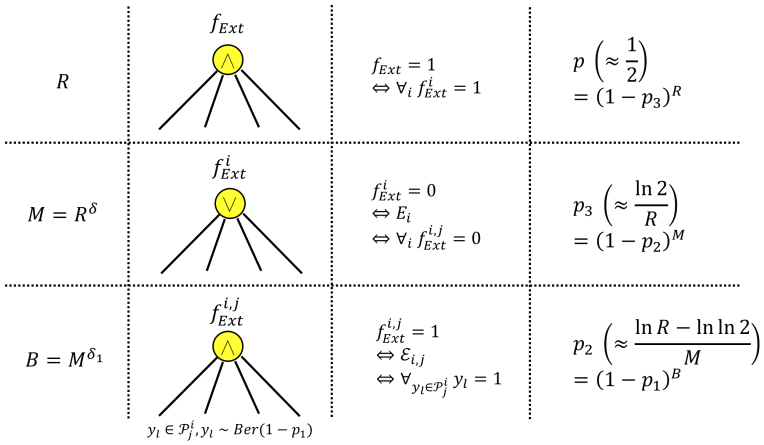

Figure 6: The parameters we are going to use.

We define and discuss the parameters of Trevisan extractor and the probability of each layers of Chattopadhyay-Zuckerman function in two parts.

Parameters of Trevisan extractor Let $\delta > 0$ be the parameter in Theorem 5.1 and $TExt : \{0,1\}^r \times \{0,1\}^b \to \{0,1\}^m$ be Trevisan extractor for weak-source with min-entropy at least $k = 2\delta r$ with error $\epsilon \leq \delta/4$, $b = \delta_1 m$, $\delta_1 = \delta/20$. The output length $m = \delta r$. Let $s = BM$. Thus, $s = M^{1+\delta_1}$. See Table 2 for a summary.

	Small character(# bits)	Large character(# instances)
r	r	R
k	$k = 2\delta r$	$M = R^{2\delta}$
m	$m = \delta r$	$M = R^{\delta}$
b	$b = \delta_1 m = delta\delta_1 r$	$B = M^{\delta_1} = R^{\delta\delta_1}$
s	$s = BM = M^{1+\delta_1} = R^{\delta+\delta\delta_1}$	

Table 2: Parameters of Trevisan extractor

Probability in Chattopadhyay-Zuckerman function Denote the probabilities in each layers of Chattopadhyay-Zuckerman function as follows. Note that by symmetric, nodes at the same layer have the same probability.

- $p_1 := \mathbb{P}_{x \sim U_h}[y(x) = 0]$, *i.e.,* the probability at the bottom layer of f_{TExt}. We want p_1 to be close to γ defined in (9).

- $p := \mathbb{P}_{y\sim Ber(s,1-p_1)}[f_{TExt}(y) = 1]$. We want p to be close to $\frac{1}{2}$.
- $p_3 := \mathbb{P}_{y\sim Ber(s,1-p_1)}[f^i_{TExt}(y) = 0]$. We want p_3 to be close to $\frac{\ln 2}{R}$.
- $p_2 := \mathbb{P}_{y\sim Ber(s,1-p_1)}[f^{i,j}_{TExt}(y) = 1]$. We want p_2 to be close to $\frac{\ln R - \ln\ln 2}{M}$.

We leave the details of the proof about why these probabilities are close to the desire one in mathematical background notes. Here, we will only see the intuition why we want these probabilities. First, let's write down the relation between p, p_1, p_2, p_3 by De Morgan's law as follows.

$$p \approx^2 (1-p_3)^R,\ p_3 = (1-p_2)^M,\ p_2 = (1-p_1)^B. \tag{11}$$

Recall a simple fact about natural exponential function.

$$\lim_{n\to\infty}(1-\frac{x}{n})^n = e^{-x},\ \forall x. \tag{12}$$

As we want $p = \frac{1}{2}$, it would be natural to let p_3 be close to $\frac{\ln 2}{R}$ since as R large, p will then close to 2 as we desired. Similarly, we would want p_2 be close to $\frac{\ln R - \ln\ln 2}{M}$ and p_1 be close to $\frac{\ln M - \ln\ln(R-\ln 2)}{B}$.

3.2 Bound influence

Now, we are going to prove Lemma 5.3, *i.e.,* bound the influence of f_{TExt} on Bernoulli input.

First, observe that the influence of f_{TExt} can be upper bounded by the summation of the influence of f^i_{TExt}, *i.e.,* $I_{q,Ber(s,1-p_1)}(f_{TExt}) \le \sum_{i\in[R]} I_{q,Ber(s,1-p_1)}(f^i_{TExt})$. Thus, lets consider the influence of each tribe function f^i_{Ext}.

Consider arbitrary set $Q \subseteq [s]$ of size at most $q < s^{1-\delta}$. As there are $M > s$ blocks in the partition $\mathcal{P}^i$, at least $M - q$ do not contain any variable from Q. Now, observe that, f^i_{TExt} is undetermined if the following two events happen simultaneously.

- All the blocks in $\mathcal{P}^i$ that do not contain variable from Q output 0. Namely,

$$U^i_1 := \{y :\ \forall j \in \{0,1\}^m,\ P^i_j \cap Q = \emptyset,\ f^{i,j}_{TExt}(y) = 0\}. \tag{13}$$

- Exists one block that contain variable from Q such that the non-Q variables are all set to 1.

$$U^i_2 := \{y :\ \exists j \in \{0,1\}^m,\ P^i_j \cap Q \neq \emptyset,\ \forall (j,z) \notin Q,\ y_{j,z} = 1\}. \tag{14}$$

Observe that since each block are disjoint to each other, the two events are independent. Namely, the influence of f^i_{TExt} is upper bounded by $\mathbb{P}[U^i_1]\cdot\mathbb{P}[U^i_2]$. The following upper bound the probability of two events respectively.

Claim (5.11). *For any $i \in \{0,1\}^r$ and $q \le s^{1-\delta}$, $\mathbb{P}[U^i_1] \le \frac{1}{R}$.*

[2] As each partitions is slightly correlated to each other, the equality won't hold. In Lemma 5.5 we will deal with the error.

Proof. Recall that, for each $i \in \{0,1\}^r$ and $j \in \{0,1\}^m$, $\mathbb{P}[f_{TExt}^{i,j}(y) = 1] = p_2$. Since there are at least $M - q$ blocks in $\mathcal{P}^i$ begin disjoint to Q, we have

$$\mathbb{P}[U_1^i] = \prod_{j \in \{0,1\}^m,\ P_j^i \cap Q = \emptyset} \mathbb{P}[f_{TExt}^{i,j}(t) = 0] \leq (1-p_2)^{M-q} \leq \frac{1}{R}. \tag{15}$$

The last inequality involves several steps of probabilistic argument, please refer to the note for mathematical background for details. □

Claim. *There are at least $R - KM$ partitions $i \in \{0,1\}^r$ such that $\mathbb{P}[U_2^i] \leq \frac{q}{2s^{1-\delta}}$.*

Proof. The proof consists of one definition and two steps.

Definition 5 (good/bad block/partition)**.** *A block P_j^i is a good block w.r.t. Q if $\forall j \in \{0,1\}^m$, $|P_j^i \cap Q| < 2\epsilon B$; otherwise it is bad. A partition $\mathcal{P}^i$ is a good partition w.r.t. Q if for any $j \in \{0,1\}^m$ P_j^i is a good block; otherwise it is bad.*

Claim (5.14). *Let $\mathcal{P}^i$ be a good partition w.r.t. Q. If $q \leq s^{1-\delta}$, then $\mathbb{P}[U_2^i] \leq \frac{q}{2s^{1-\delta}}$.*

Proof. Let $\mathcal{P}^i$ be a good partition w.r.t. Q. As there are at most q blocks in $\mathcal{P}^i$ intersects with Q and each of the intersecting block has at most $2\epsilon B$ overlapping. We can union bound the probability of U_2^i as follows.

$$\mathbb{P}[U_2^i] \leq \sum_{j \in \{0,1\}^m,\ P_j^i \cap Q \neq \emptyset} \mathbb{P}[\forall (j,z) \notin y_{j,z} = 1] \leq q(1-p_1)^{B(1-2\epsilon)} \leq \frac{q}{2s^{1-\delta}}. \tag{16}$$

The last inequality involves several steps of probabilistic argument, please refer to the note for mathematical background for details. □

Claim (5.13). *If $q \leq s^{1-\delta}$, then at most KM bad partitions w.r.t. Q.*

Proof. Lets prove by contradiction. Suppose there are at least KM bad partitions w.r.t. Q. As each partition has M blocks, by the pigeonhole principle, exists $j \in \{0,1\}^m$ such that there are at least K bad blocks among $\{P_j^i : i \in \{0,1\}^r\}$. Now, consider the jth shift of $TExt$ defined as $TExt_j(i,z) := TExt(i,z) \oplus j$. Observe that $TExt_j$ is also a seeded extractor for k-source with error ϵ. Pick out the partitions whose j-th block is bad w.r.t. Q,

$$BAD := \{i \in \{0,1\}^r :\ P_j^i \text{ is bad w.r.t. } Q\}. \tag{17}$$

By the choice of j, we know that $|BAD| \geq K$. However, note that Q is defined on the extension $\{0,1\}^m \times \{0,1\}^b$ of the range of the extractor. Thus, we *project* Q back to the original range $\{0,1\}^m$ of the extractor.

$$Q' := \{j \in \{0,1\}^m :\ \exists z \in \{0,1\}^b,\ (j,z) \in Q\}. \tag{18}$$

Next, define a k-source X_{BAD} on a size K subset of BAD. By the property of seeded extractor, $Ext_j(X_{BAD}, U_b)$ is ϵ-close to U_m. Namely, $|\mathbb{P}[Ext_j(X_{BAD}, U_b) \in Q'] - \mathbb{P}[U_m \in Q']| \leq \epsilon$. Observe

that

$$\mathbb{P}[TExt_j(X_{BAD}, U_b) \in Q'] = \frac{1}{KB} \sum_{i \in Supp(X_{BAD})} \sum_{z \in \{0,1\}^b} \mathbf{1}_{TExt_j(i,z) \in Q'} \tag{19}$$

$$= \sum_{i \in Supp(X_{BAD})} \frac{|N_{TExt_j}(i) \cap Q'|}{KB}. \tag{20}$$

By the definition of BAD and (20), we have

$$\mathbb{P}[Ext_j(X_{BAD}, U_b) \in Q'] \geq 2\epsilon. \tag{21}$$

Moreover, as $|Q'| \leq q \leq s^{1-\delta} \leq (M^{1+\delta_1})^{1-\delta} \leq M^{18\delta/19}$, we have

$$\mathbb{P}[U_m \in Q'] \leq M^{-\delta/19} < \epsilon. \tag{22}$$

Namely, $\mathbb{P}[Ext_j(X_{BAD}, U_b) \in Q'] - \mathbb{P}[U_m \in Q'] > \epsilon$, which is a contradiction. Thus, there are less than KM bad blocks. □

□

Finally, with Claim 5.11, Claim 5.13, and Claim 5.14, we can prove Lemma 5.3 as follows. For any $Q \subseteq [s]$ and $|Q| \leq q \leq s^{1-\delta}$,

$$I_{Q,Ber(s,1-p_1)}(f_{TExt}) \leq \sum_{i:\ P^i \text{ is bad w.r.t. } Q} I_{Q,Ber(s,1-p_1)}(f^i_{TExt}) \tag{23}$$

$$+ \sum_{i:\ P^i \text{ is good w.r.t. } Q} I_{Q,Ber(s,1-p_1)}(f^i_{TExt}) \tag{24}$$

$$\leq KM \cdot \frac{1}{R} + R \cdot \frac{1}{R} \cdot \frac{q}{2s^{1-\delta}} \tag{25}$$

$$\leq \frac{q}{s^{1-\delta}}. \tag{26}$$

The last inequality involves several steps of probabilistic argument, please refer to the note for mathematical background for details.

3.3 Bound bias

Now, we are going to prove Lemma 5.5, *i.e.,* bound the bias of f_{TExt} on Bernoulli input.

Before we start the proof, we are going to utilize the property of Trevisan extractor in a black box way as follows.

Lemma (5.19). *Consider partitions $\mathcal{P}^1, \ldots, \mathcal{P}^R$ constructed in Section 2.2, for any $i, i' \in \{0,1\}^r$ and $j, j' \in \{0,1\}^m$ where $i \neq i'$, we have*

$$|P^i_j \cap P^{i'}_{j'}| \leq 0.9B. \tag{27}$$

Proof. The proof is based on Lemma 5.6 which won't be introduced here. □

We also assume the following fact about the probability of each tribe function. Please refer to the mathematics background note for details.

Claim (5.15). *Recall that* $p_3 = \mathbb{P}_{y\sim Ber(s,1-p_1)}[f^i_{TExt}(y) = 0]$ *for any* $i \in \{0,1\}^r$. *We have*

$$|p_3 - \frac{\ln 2}{R}| \leq \frac{1}{R \cdot B^{\Omega(1)}}. \tag{28}$$

Now, we can proceed to prove Lemma 5.5[3].

Proof of Lemma 5.5. As we mentioned before, since each partitions on $[s]$ is slightly correlated to each other, we cannot simply apply De Morgan's law to yield p, which is the probability of f_{TExt} to be 1 on Bernoulli $1-p_1$ input. However, ideally p should be very close to the probability when every partition is independent. Namely, $(1-p_3)^R$, where p_3 is the probability of f^i_{TExt} to be 0.

Since directly dealing with the p involve too complicated correlation among every partition, the trick here is to use *inclusion-exclusion principle* to decompose the highly-correlated[4] event into small but many events. Concretely, define the event

$$E_i := \{y : \ f^i_{TExt}(y) = 0\}. \tag{29}$$

Consider[5],

$$\begin{aligned} 1 - p = \mathbb{P}[f_{TExt}(y) = 0] &= \mathbb{P}[\vee_{i\in[R]} E_i] && (30)\\ &= \sum_{i\in[R]} \mathbb{P}[E_i] - \sum_{1\leq i_1<i_2\leq R} \mathbb{P}[E_{i_1} \wedge E_{i_2}] + \cdots && (31)\\ &= \sum_{c=[R]} (-1)^{c-1} \sum_{1\leq i_1<\cdots<i_c\leq R} \mathbb{P}[\wedge_{g\in[c]} E_{i_g}]. && (32) \end{aligned}$$

For $c \in [R]$, let

$$S_c := \sum_{1\leq i_1<\cdots<i_c\leq R} \mathbb{P}[\wedge_{g\in[c]} E_{i_g}]. \tag{33}$$

Inclusion-exclusion principle actually guarantee an interlacing upper/lower bounds as follows. For every integer $a < \frac{R}{2}$,

$$\sum_{c\in[2a]} (-1)^{c-1} S_c \leq 1 - p \leq \sum_{c\in[2a+1]} (-1)^{c-1} S_c. \tag{34}$$

The following claim bounds each term of the above approximation.

Claim (5.20). *There exists constant* $\beta_1, \beta_2 > 0$ *such that for any* $c \leq s^{\beta_1}$ *and arbitrary* $1 \leq i_1 < \cdots < i_c \leq R$, *the following holds:*

$$p_3^c \leq \mathbb{P}[\wedge_{g\in[c]} E_{i_g}] \leq p_3^c(1 + \frac{1}{M^{\beta_2}}). \tag{35}$$

Furthermore,

$$\binom{R}{c} p_3^c \leq S_c \leq \binom{R}{c} p_3^c (1 + \frac{1}{M^{\beta_2}}). \tag{36}$$

[3] In [CZ15], they generalize the result to the *pairwise-good* partition. Here, I omit it for simplicity.

[4] Here, the highly-correlated notion means that there are many events correlated to each other, not the correlation is large.

[5] As the input is always $Ber(s, 1-p_1)$, we omit the notation in the following.

Proof. This lemma is proved by *Janson's inequality* which provides tight bound when the number of slightly-correlated events are not too much. That is, the property in Lemma 5.19 can be used to upper bound $\mathbb{P}[E_i \cap E_{i'}]$ for any $i \neq i'$. We defer the details in the mathematical background note. □

Lemma 5.20 implies that when c is not too large, each probability term is very close to the situation when each partition is independent. Let $a = \left\lfloor \frac{s^{\beta_3}}{2} \right\rfloor$, we sum up each terms and see how's the approximation for $1 - p$ by inclusion-exclusion principle in (34).

Lemma (5.22). $(1 - e^{-Rp_3}) - \frac{1}{M^{\beta_2/2}} \leq \sum_{c \in [2a]} (-1)^{c-1} S_c \leq 1 - p \leq \sum_{c \in [2a+1]} S_c \leq (1 - e^{-Rp_3}) + \frac{1}{M^{\beta_2/2}}$.

Proof. A key observation is applying Taylor's expansion on e^{-Rp_3}. We have

$$1 - e^{-Rp_3} = \sum_{c=1}^{\infty} (-1)^{c-1} \frac{R^c p_3^c}{c!}. \tag{37}$$

When R is large and c is small, $R^c/c! \approx \binom{R}{c}$, which matches S_c. The details and rest of the steps require complicated probabilistic argument, please refer to the note for mathematical background for details. □

From Lemma 5.20 and Lemma 5.22, we have $|(1-p) - (1 - e^{-Rp_3})| \leq \frac{1}{M^{\Omega(1)}}$. From Claim 5.15, we have $|(1 - e^{-Rp_3}) - \frac{1}{2}| \leq \frac{1}{B^{\Omega(1)}}$. By properly pick the parameters and triangle inequality, we have $|(1-p) - \frac{1}{2}| \leq \frac{1}{B^{\Omega(1)}}$. □

References

[AL93] Miklós Ajtai and Nathan Linial. The influence of large coalitions. *Combinatorica*, 13(2):129–145, 1993.

[BOL85] Michael Ben-Or and Nathan Linial. Collective coin flipping, robust voting schemes and minima of banzhaf values. In *Foundations of Computer Science, 1985., 26th Annual Symposium on*, pages 408–416. IEEE, 1985.

[CZ15] Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functions. In *Electronic Colloquium on Computational Complexity (ECCC)*, volume 22, page 119, 2015.

[Mek09] Raghu Meka. Explicit coin flipping protocols. *Unpublished manuscript*, 2009.

[Mek15] Raghu Meka. Explicit resilient functions matching ajtai-linial. *arXiv preprint arXiv:1509.00092*, 2015.