Electronic Colloquium on Computational Complexity, Report No. 38 (2015)

Local Correlation Breakers and Applications to Three-Source Extractors and Mergers

Gil Cohen*

March 11, 2015

Abstract

We introduce and construct a pseudorandom object which we call a *local correlation breaker (LCB)*. Informally speaking, an LCB is a function that gets as input a sequence of r (arbitrarily correlated) random variables and an independent weak-source. The output of the LCB is a sequence of r random variables with the following property. If the i^{th} input random variable is uniform then the i^{th} output variable is uniform even given a bounded number of any other output variables. That is, an LCB uses the weak-source to "break" local correlations between random variables. Using our construction of LCBs, we obtain the following results:

- We construct a three-source extractor where one of the sources is only assumed to have a double-logarithmic entropy. More precisely, for any integer n and constant $\delta > 0$, we construct a three-source extractor for entropies δn, $O(\log n)$ and $O(\log \log n)$. As the third source is required to have tantalizingly low entropy, we hope that further ideas can be used to eliminate the need for this source altogether.
- We construct a merger with weak-seeds that merges r random variables using an independent (n, k)-weak-source with $k = \widetilde{O}(r) \cdot \log \log n$. A previous construction by Barak *et al.* [Ann. Math'12] assumes $k \geq \Omega(r^2) + \mathrm{polylog}(n)$.

*Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel. Email: gil.cohen@weizmann.ac.il. Partially supported by an ISF grant and by the I-CORE program of the planning and budgeting committee. Part of this work was done while the author was visiting Microsoft Research Silicon Valley.

ISSN 1433-8092

Contents

1 Introduction

A central theme in pseudorandomness concerns the design of efficient algorithms that transform one or more sources of randomness to a source with a desired property. Extractors, dispersers, mergers and condensers are examples of this theme, and have received a significant attention in the literature. In this work we introduce and construct a pseudorandom primitive that we call a *local correlation breaker* (LCB for short), and present applications of LCBs to the construction of three-source extractors and for mergers with weak-seeds.

Informally speaking, an LCB is a deterministic algorithm that gets as input a sequence of r (arbitrarily correlated) random variables, and an independent weak-source. The output of the LCB is a sequence of r random variables with the following property: If the i^{th} input random variable is uniform then the i^{th} output variable is uniform even given some bounded number of any other output variables. That is, an LCB uses the weak-source to "break" local correlations between random variables. For the formal definition of LCBs we make use of standard definitions from the literature such as min-entropy, statistical distance, and (n,k)-weak-sources (see the Preliminaries).

Definition 1.1 (Local correlation breakers)**.** *A* t-local correlation breaker (t-LCB) *for min-entropy k, with error ε, is a function*

$$\mathsf{LCB}\colon \left(\{0,1\}^{\ell}\right)^{r} \times \{0,1\}^{n} \to \left(\{0,1\}^{m}\right)^{r},$$

with the following property. Let $X = (X_1, \ldots, X_r)$ be a sequence of random variables, each supported on $\{0,1\}^{\ell}$. Let Y be an independent (n,k)-weak-source. Denote the output $\mathsf{LCB}(X,Y)$ by $Z_1, \ldots, Z_r$, where each Z_i is supported on $\{0,1\}^m$. Let $g \in [r]$ be such that X_g is uniform. Let $I \subseteq [r] \setminus \{g\}$ be any set of size $t-1$. Then,

$$\left(Z_g, \{Z_i\}_{i \in I}\right) \approx_{\varepsilon} \left(U_m, \{Z_i\}_{i \in I}\right).$$

A pseudorandom object related to LCBs appears (implicitly) in the analysis of Li's multi-source extractor [Li13]. The difference between LCBs and Li's pseudorandom object is that the latter only guarantees that an output variable Z_g that corresponds to a uniform input variable X_g is statistically-close to uniform given output variables that correspond to $t-1$ other *uniform* input variables. In other words, in Li's pseudorandom object, the set I in Definition 1.1 is assumed to contain indices only of uniform input variables. For the applications we consider, it is crucial that Z_g is close to uniform even given output variables $\{Z_i\}$ that correspond to possibly non-uniform input variables.

Our first result is an explicit construction of LCBs. Our proof builds on the work of [Li13], together with some new ideas required so to guarantee the stronger property. In Section 6.1 we give a high-level comparison between the ideas used in [Li13] and those used in our construction of LCBs. In terms of parameters, Theorem 1.2 gives LCBs with somewhat better parameters compared to Li's pseudorandom object. For simplicity, the theorem below is stated for a constant error.

Theorem 1.2 (Explicit LCBs; informal statement)**.** *For all integers n, r, t, there exists an explicit t-local correlation breaker* $\mathsf{LCB}\colon \left(\{0,1\}^\ell\right)^r \times \{0,1\}^n \to (\{0,1\}^m)^r$ *with*

$$\ell = O\left(t^2 \cdot \log(nr) \cdot \log r\right),$$
$$m = \Omega\left(\ell/(t \cdot \log r)\right),$$

for entropy

$$k = O\left(t \cdot \log(r) \cdot \log(r \log n)\right).$$

Note that the dependence of the entropy k in n is double-logarithmic. For a complete and formal statement of Theorem 1.2, see Section 6. We turn to present our applications of LCBs.

1.1 Three-source extractors with a double-logarithmic entropy source

Chor and Goldreich [CG88] introduced the notion of two-source extractors. Informally speaking, a function $f\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ is called a *two-source extractor* if for any two independent sources X, Y over $\{0,1\}^n$, with sufficient min-entropy, it holds that $f(X, Y)$ is statistically-close to uniform. By a standard probabilistic argument, one can prove the existence of a two-source extractor for any entropies k_1, k_2 such that $\min(k_1, k_2) > \log n + O(1)$.

Chor and Goldreich [CG88] gave an explicit construction of a two-source extractor for any entropies k_1, k_2 such that $k_1 + k_2 > (1+\delta) \cdot n$, where $\delta > 0$ is an arbitrarily small constant. In particular, one can take $k_1 = k_2 > (1/2 + \delta) \cdot n$, for any constant $\delta > 0$. This construction is far from optimal (ignoring the computational aspect). Nevertheless, it took almost 20 years before any improvement was made. Raz [Raz05] gave an explicit construction of a two-source extractor for sources with entropies k_1, k_2, with $k_1 = O(\log n)$ and $k_2 > (1/2 + \delta) \cdot n$, where $\delta > 0$ is an arbitrarily small constant. An incomparable result was obtained by Bourgain [Bou05] who constructed a two-source extractor for entropies $k_1 = k_2 > (1/2 - \alpha) \cdot n$, where $\alpha > 0$ is some (small) universal constant.

Given the difficulty of explicitly constructing two-source extractors for low entropy, a significant research effort was directed towards the construction of t-source extractors for $t > 2$. The next natural goal is constructing three-source extractors. A simple probabilistic argument can be used to prove the existence of an extractor for three independent $(n, \log(n)/2 + O(1))$-weak-sources. Barak *et al.* [BKS[+]05] gave an explicit construction of a three-source extractor, where the entropy of each of the sources is δn, for any constant $\delta > 0$. This was improved by Raz [Raz05], who requires only one of the sources to have entropy δn, while the other two sources can have entropy $O(\log n)$. Here, again, $\delta > 0$ is an arbitrarily small constant. Raz's extractor supports a constant error, and in a subsequent work, Rao [Rao09] showed how to support exponentially small error, assuming the second and third sources have entropy $O(\log^4 n)$. Furthermore, Rao [Rao09] constructed a three-source extractor, where the entropy of each of the sources is $n^{0.9}$. This was later improved by Li [Li11] to $n^{1/2+\delta}$, where $\delta > 0$ is an arbitrarily small constant.

In a recent breakthrough, Li [Li15] constructed a three-source extractor for poly-logarithmic entropy. This exciting result sets the next natural goal in multi-source extractors on improving the constructions of two-source extractors by Raz [Raz05] and Bourgain [Bou05]. Towards this goal, as an application of LCBs, we construct a three-source extractor where one of the sources is only assumed to have double-logarithmic entropy. This can also be seen as an improvement over Raz's three-source extractor [Raz05] that assumes the third source has entropy $\Omega(\log n)$.

Theorem 1.3 (Explicit three-source extractors; informal statement)**.** *For any integer n and $\delta > 0$, there exists an explicit three-source extractor $\mathsf{3Ext}\colon (\{0,1\}^n)^3 \to \{0,1\}^m$ for entropies*

$$\begin{aligned} k_1 &= \delta n, \\ k_2 &= \mathrm{poly}(1/\delta) \cdot \log n, \\ k_3 &= \mathrm{poly}(1/\delta) \cdot \log \log n, \end{aligned}$$

with $m = \mathrm{poly}(1/\delta) \cdot \log n$ output bits.

A formal statement of Theorem 1.3 and its proof appear in Section 8. Although during the introduction we omit the error of the extractors, in order to compare our extractor with Rao's extractor [Rao09], we mention here that the error of the three-source extractor in Theorem 1.3 is exponentially small.

As the third source fed to our three-source extractor is required to have a tantalizingly small entropy, we hope that further ideas can be used to eliminate the need for this third source altogether.

Improved three-source extractors for poly-logarithmic entropy As mentioned, Li [Li15] constructed a three-source extractor for poly-logarithmic entropy. More precisely, the entropy required by Li's construction is $O(\log^{12} n)$. For his construction, Li uses a pseudorandom object that is related to LCBs, introduced in [Li13], as well as the merger with weak-seeds of [BRSW12]. As our construction of LCBs has better parameters than Li's related pseudorandom object (see Section 6.1) and since our merger with weak-seeds improves that of [BRSW12], by using our results as building blocks in Li's three-source extractor, one can obtain a three-source extractor for a somewhat lower entropy $O(\log^c n)$, where $c < 12$ is some constant. We made no attempt at pinpointing the value of the constant c.

1.2 Mergers with weak-seeds

Motivated by the construction of seeded extractors, Ta-Shma [TS96] introduced the notion of a merger. Informally speaking, a merger is a function that gets as input a sequence of (arbitrarily correlated) random variables, at least one of which is uniform. The goal of a merger is to "merge" the random variables into a single random variable that is statistically-close to uniform. [1] It is not hard to show that randomness is a necessity for merging.

[1] Variants of mergers (which are also called mergers in the literature) assume that one of the random variables is not necessarily uniform, yet has high entropy-rate.

Constructing mergers with short seeds (namely, short strings that are uniform and independent of the random variables we wish to merge) has been studied in several works [TS96, LRVW03, Raz05, DS07, Zuc07, DR08, DW11, DKSS09]. The state of the art construction of Dvir and Wigderson [DW11] merges r random variables, supported on $\{0,1\}^\ell$, using a seed of length $O(\log(r\ell))$. An incomparable result was obtained by Dvir, Kopparty, Saraf and Sudan [DKSS09], who use a seed of length $O(\log(r)/\delta)$ to output a string that has entropy-rate $1-\delta$. As a building block for their two-source disperser, Barak, Rao, Shaltiel and Wigderson [BRSW12] constructed, what we call, mergers with weak-seeds. [2]

Definition 1.4 (Mergers with weak-seeds)**.** *A* merger with weak-seeds *for entropy k, with error ε, is a function*

$$\mathsf{Merg}\colon \left(\{0,1\}^\ell\right)^r \times \{0,1\}^n \to \{0,1\}^m,$$

with the following property. Let $X = (X_1,\ldots,X_r)$ be a sequence of random variables, supported on $\{0,1\}^\ell$, such that at least one of them is uniform. Let Y be an independent (n,k)-weak-source. Then, $\mathsf{Merg}(X,Y) \approx_\varepsilon U_m$.

In [BRSW12], a construction of a merger with weak-seeds is given, assuming $k = \ell > \Omega(r^2) + \mathrm{polylog}(n)$. [3] A probabilistic argument can be used to show that there exists a merger with weak-seeds for parameters

$$\begin{aligned}\ell &= \log n + O(1),\\ k &= \log r + \log\log n + O(1).\end{aligned}$$

In particular, the entropy k is only required to be double-logarithmic in n.

We note that constructing mergers with weak-seeds given an LCB is trivial. Indeed, one can apply an r-LCB to $X_1,\ldots,X_r$ and Y so to obtain random variables $Z_1,\ldots,Z_r$. The output of the merger is simply the XOR of all Z_i's. To see that this reduction works, note that if X_g is uniform then, by the guarantee of the LCB, Z_g is statistically-close to uniform even given all other Z_i's. Therefore, the XOR of all Z_i's is statistically-close to uniform. We use Theorem 1.2 with this simple idea (together with a bit more work so to improve the output length) and obtain the following result.

Theorem 1.5 (Explicit mergers with weak-seeds; informal statement)**.** *For all integers n, r, there exists an explicit merger with weak-seeds* $\mathsf{Merg}\colon \left(\{0,1\}^\ell\right)^r \times \{0,1\}^n \to \{0,1\}^m$, *with*

$$\begin{aligned}\ell &= O\left(r^2\cdot\log(r)\cdot\log(nr)\right),\\ k &= O\left(r\cdot\log(r)\cdot\log(r\cdot\log n)\right),\\ m &= \Omega(\ell/r).\end{aligned}$$

A formal statement of Theorem 1.5 and its proof appear in Section 7. In Section 5 we give a warm up for the proof of Theorem 1.5, and show how to merge $r = 3$ rows of

[2] In [BRSW12] this object is called an extractor for a general source and a somewhere-random source.

[3] In fact, the construction of [BRSW12] works even assuming one of the X_i's has entropy-rate $1-o(1)$.

length $\ell = O(\log n)$ using an independent weak-source with entropy $k = O(\log\log n)$ (see Theorem 5.1). This "toy-example" also demonstrates most of the ideas used in the proof of Theorem 1.2.

The merger of Barak *et al.* [BRSW12] and ours are incomparable. On one hand, the merger of [BRSW12] works even if one of the rows has min-entropy rate $1 - o(1)$. On the other hand, Theorem 1.5 has a quadratically improved dependence of k in r, and more importantly, an exponentially improved dependence of k in n, which matches the probabilistic construction. This feature allows us to obtain a three-source extractor with double-logarithmic entropy source. Moreover, we believe our construction and analysis are somewhat simpler and more intuitive than the construction of [BRSW12] which uses a completely different set of ideas.

1.3 Organization of this paper

The paper is organized as follows. In Section 2 we give formal definitions and state some of the results from previous works that we use. In Section 3 we prove some technical lemmata on probabilistic processes that appear again and again throughout the paper. In Section 4 we present a restricted version of look-ahead extractors.

Before constructing LCBs and mergers with weak-seeds in their full generality, we start with a warm up – in Section 5 we give a construction of a merger with weak-seeds for only three random variables. Section 5 is meant only for building up intuition and presenting the underling ideas behind the constructions of our mergers with weak-seeds and LCBs, without getting into all the details. The reader may freely skip this section at any point as we make no use of the results that appear in this section. In Section 6 we present the construction of LCBs (Theorem 1.2). In Section 7, we present our construction of mergers with weak-seeds (Theorem 1.5). In Section 8 we give our construction of three-source extractors (Theorem 1.3).

2 Preliminaries

The logarithm in this paper is always taken base 2. For every natural number $n \geq 1$, define $[n] = \{1, 2, \ldots, n\}$. For a string $x \in \{0,1\}^n$ and an integer $1 \leq s \leq n$, we write $x|_s$ for the length s prefix of x. For an $r \times \ell$ matrix x and $1 \leq s \leq \ell$, we let $x|_s$ denote the matrix composed of the s leftmost columns of x. For $i \in [r]$, we denote by x_i the i^{th} row of x. Throughout the paper we almost always 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 introduce 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 $\mathsf{SD}(X, Y) \le \varepsilon$ we write $X \approx_\varepsilon Y$ and say that X is ε-close to Y.

Min-entropy. The *min-entropy* of a random variable X is defined by

$$H_\infty(X) = \min_{x \in \mathsf{supp}(X)} \log_2 \left(\frac{1}{\mathbf{Pr}[X = x]} \right).$$

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)-weak-source.

Somewhere-random sources. A random variable X that has the form of an $r \times \ell$ matrix is called a *somewhere-random source* if there exists $g \in [r]$ such that X_g is uniformly distributed over $\{0,1\}^\ell$. In this case we say that X_g is a *good* row of X. We think of a somewhere-random source as a sequence of (arbitrarily correlated) random variables given by its rows $X_1, \ldots, X_r$.

Extractors and condensers

Definition 2.1 (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)*-weak-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* $(\mathsf{Ext}(X, S), S) \approx_\varepsilon (U_m, U_d)$*, where* X *and* S *are as above.*

Throughout the paper we make an extensive (black-box) use of the following strong seeded-extractor by Guruswami, Umans and Vadhan [GUV09].

Theorem 2.2 ([GUV09])**.** *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* $d = \log n + O(\log(k/\varepsilon))$*, and* $m = 0.99 \cdot k$ *output bits.*

Definition 2.3 (Multi-source extractors)**.** *A function* $\mathsf{Ext}\colon (\{0,1\}^n)^t \to \{0,1\}^m$ *is called a* t-source extractor *for entropies* $k_1, \ldots, k_t$*, with error* ε*, if for any* t *independent* n*-bit weak-sources* $X_1, \ldots, X_t$*, where* $H_\infty(X_i) \ge k_i$*, it holds that* $\mathsf{Ext}(X_1, \ldots, X_t) \approx_\varepsilon U_m$*. For a subset* $I \subseteq [t]$*, we say that* Ext *is strong in* I *if* $(\mathsf{Ext}(X_1, \ldots, X_t), \{X_i\}_{i \in I}) \approx_\varepsilon (U_m, \cdot)$*.*

Basic lemmata in probability

Throughout the paper we make a frequent use of the following simple and well-known lemmata.

Lemma 2.4. *Let X, Y be two independent random variables on a common domain D. Let f be a function with domain D. Then, $\mathsf{SD}\left(f(X), f(Y)\right) \le \mathsf{SD}\left(X, Y\right)$. Moreover, the inequality above holds also for f which is a random function, where the internal randomness of f is independent of (X, Y).*

Lemma 2.5. *For all random variables X, Y, Z, it holds that*

$$\mathsf{SD}\left((X,Y),(Z,Y)\right) = \mathop{\mathbf{E}}_{y\sim Y}\left[\mathsf{SD}\left((X \mid Y = y),(Z \mid Y = y)\right)\right].$$

Lemma 2.6. *Let X, Y, Z be random variables such that X is independent of Y and Z is independent of Y. Then, $\mathsf{SD}\left((X,Y),(Z,Y)\right) = \mathsf{SD}\left(X, Z\right)$. In particular, if X is supported on $\{0,1\}^a$ then $\mathsf{SD}\left((X,Y),(U_a,Y)\right) = \mathsf{SD}\left(X, U_a\right)$.*

Lemma 2.7. *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 $\{0,1\}^a$. Then,*

$$\mathsf{SD}\left((X,Y,Z),(U_a,Y,Z)\right) = \mathsf{SD}\left((X,Y),(U_a,Y)\right).$$

Lemma 2.8. *Let X, Z be random variables on a common domain. Let Y be some random variable. Then, $\mathsf{SD}\left(X, Z\right) \le \mathsf{SD}\left((X,Y),(Z,Y)\right)$.*

Lemma 2.9. *Let X, Y be two random variables on a common domain D. Let $f \colon D \to \mathbb{R}$ be a function with non-negative range, that is, $f(z) \ge 0$ for all $z \in D$. Then,*

$$\left|\mathop{\mathbf{E}}_{x\sim X}\left[f(x)\right] - \mathop{\mathbf{E}}_{y\sim Y}\left[f(y)\right]\right| \le \max_{z \in D}|f(z)| \cdot \mathsf{SD}(X,Y).$$

Lemma 2.10 ([Li12], Lemma 3.20)**.** *Let (X, Y) be a joint distribution. Let Z be a random variable with the same range as X. Then, there exists a joint distribution (Z, Y) such that $\mathsf{SD}\left((X,Y),(Z,Y)\right) = \mathsf{SD}(X,Z)$.*

Average conditional min-entropy

Definition 2.11. *Let X, W be two random variables. The* average conditional min-entropy *of X given W is defined as*

$$\begin{aligned}\widetilde{H}_\infty(X \mid W) &= -\log_2\left(\mathop{\mathbf{E}}_{w\sim W}\left[\max_x \mathbf{Pr}\left[X = x \mid W = w\right]\right]\right)\\ &= -\log_2\left(\mathop{\mathbf{E}}_{w\sim W}\left[2^{-H_\infty(X \mid W = w)}\right]\right).\end{aligned}$$

Lemma 2.12 ([DORS08])**.** *Let X, Y, Z be random variables such that Y has support size at most 2^ℓ. Then,*

$$\widetilde{H}_\infty(X \mid (Y, Z)) \geq \widetilde{H}_\infty((X, Y) \mid Z) - \ell \geq \widetilde{H}_\infty(X \mid Z) - \ell.$$

In particular, $\widetilde{H}_\infty(X \mid Y) \geq H_\infty(X) - \ell$.

Lemma 2.13 ([DORS08])**.** *For any two random variables X, Y and any $\varepsilon > 0$, it holds that*

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

We also need the following simple lemma.

Lemma 2.14. *Let X, Y, Z be random variables such that for any $y \in \mathsf{supp}(Y)$ it holds that $(X \mid Y = y)$ and $(Z \mid Y = y)$ are independent. Then, $\widetilde{H}_\infty(X \mid (Y, Z)) = \widetilde{H}_\infty(X \mid Y)$. In particular, if X and Z are independent then $\widetilde{H}_\infty(X \mid Z) = H_\infty(X)$.*

3 (L, R)-Histories

In this section we introduce the notion of an (L, R)-*history* and some technical lemmata concerning it that we use repeatedly throughout the paper.

Definition 3.1 ((L, R)-histories)**.** *Let L, R be two independent random variables. A sequence of random variables $\mathcal{H} = (H_t, H_{t-1}, \ldots, H_1)$ is called an* (L, R)-history *if for any $i \in [t]$, H_i is either a deterministic function of $H_{i-1}, \ldots, H_1, L$ or otherwise H_i is a deterministic function of $H_{i-1}, \ldots, H_1, R$.*

Some remarks and notations:

- Throughout the paper we assume that each H_i is supported on bit strings of some common length, which we can then denote by $|H_i|$.
- We note that if H_{i+1}, H_i are two consecutive random variables in some (L, R)-history, such that H_i is a deterministic function of $H_{i-1}, \ldots, H_1, L$ (resp. $H_{i-1}, \ldots, H_1, R$) and H_{i+1} is a deterministic function of $H_i, \ldots, H_1, L$ (resp. $H_{i-1}, \ldots, H_1, R$), then one can replace H_{i+1}, H_i by a single random variable which is their joint distribution. This yields a new (L, R)-history. We allow ourselves to apply this operation freely during the proofs.
- Given two (L, R)-histories $\mathcal{H} = (H_t, \ldots, H_1)$ and $\mathcal{H}' = (H'_{t'}, \ldots, H'_1)$, one can consider the (L, R)-history which is the concatenation of $\mathcal{H}, \mathcal{H}'$, namely, $H'_{t'}, \ldots, H'_1, H_t, \ldots, H_1$. When we do not want to refer to the random variables in $\mathcal{H}$ but do want to refer to the random variables in $\mathcal{H}'$ (which is quite frequent), we write this concatenated (L, R)-history as $(H'_{t'}, \ldots, H'_1, \mathcal{H})$.

The following lemma states that conditioned on any fixing of an (L,R)-history, the random variables L,R remain independent. We omit the proof, which is done by a straightforward induction.

Lemma 3.2. *Let L,R be two independent random variables, and let $\mathcal{H}$ be an (L,R)-history. Then, for any $h \in \mathsf{supp}(\mathcal{H})$, the random variables $(L \mid \mathcal{H}=h)$ and $(R \mid \mathcal{H}=h)$ are independent.*

In the rest of this section we state and prove two technical lemmata for (L,R)-histories. Before giving the formal statement of the first lemma, we present the lemma in an informal manner so to give some intuition about what the lemma aims to abstract. A common scenario in our proofs is the following. Let L,R be two independent random variables. We think of L,R as two independent sources of randomness from which we extract randomness again and again and preform various computations on the sequence. We denote by $\mathcal{H}=(H_t,\dots,H_1)$ the (L,R)-history that captures the random variables obtained from L,R so far. Typically we will know that some random variable P is statistically-close to uniform even given $\mathcal{H}$, namely, $(P,\mathcal{H}) \approx (U,\mathcal{H})$. Furthermore, P is either a deterministic function of $L,\mathcal{H}$ or otherwise P is a deterministic function of $R,\mathcal{H}$. Assume, without loss of generality, that P is a deterministic function of $L,\mathcal{H}$. Let Ext be a strong seeded extractor. The following lemma states that if M is a deterministic function of $R,\mathcal{H}$ and $\widetilde{H}_\infty(M \mid \mathcal{H})$ is sufficiently high, then $(\mathsf{Ext}(M,P),P,\mathcal{H}) \approx (U,P,\mathcal{H})$.

The proof of this technical lemma is fairly simple. Nevertheless, we apply the lemma frequently and believe that our proofs are cleaner and conceptually simpler by identifying the operation that is described and analyzed by the lemma as an atomic operation.

Lemma 3.3. *Let L,R be two independent random variables, and let $\mathcal{H}$ be an (L,R)-history. Let P be a random variable over $\{0,1\}^p$ which is a deterministic function of $L,\mathcal{H}$.* [4] *Assume that*

$$(P,\mathcal{H}) \approx_\delta (U_p,\mathcal{H})\,. \tag{3.1}$$

Let M be a random variable over $\{0,1\}^m$ which is a deterministic function of $R,\mathcal{H}$, such that

$$\widetilde{H}_\infty(M \mid \mathcal{H}) \geq k + \log(1/\varepsilon). \tag{3.2}$$

Let $\mathsf{Ext}\colon \{0,1\}^m \times \{0,1\}^p \to \{0,1\}^f$ be a strong seeded extractor for entropy k with error ε. Define $F = \mathsf{Ext}(M,P)$. Then, $P,\mathcal{H}$ is an (L,R)-history, and

$$(F,P,\mathcal{H}) \approx_{\delta+2\varepsilon} (U_f,P,\mathcal{H})\,.$$

Proof. Let $h \in \mathsf{supp}(\mathcal{H})$. For the sake of readability, for a random variable T, we denote the random variable $(T \mid H=h)$ by T_h. Let $\delta_h = \mathsf{SD}(P_h,U_p)$. By Lemma 2.5 and Equation (3.1),

$$\mathop{\mathbf{E}}_{h\sim\mathcal{H}}[\delta_h] = \mathop{\mathbf{E}}_{h\sim\mathcal{H}}[\mathsf{SD}(P_h,U_p)] = \mathsf{SD}((P,\mathcal{H}),(U_p,\mathcal{H})) \leq \delta.$$

[4] Note that any (L,R)-history is also an (R,L)-history, and so an analog statement of the lemma in which P is a deterministic function of $R,\mathcal{H}$ readily follows.

Note that the random variables M_h, P_h are independent. Indeed, Lemma 3.2 implies that the random variables L_h, R_h are independent, and M is a deterministic function of $R, \mathcal{H}$ whereas P is a deterministic function of $L, \mathcal{H}$. Therefore, by Lemma 2.5,

$$\mathsf{SD}\left(\left(F_h, P_h\right), \left(U_f, P_h\right)\right) = \mathop{\mathbf{E}}_{s \sim P_h}\left[\mathsf{SD}\left(F_h \mid P_h = s, U_f\right)\right] = \mathop{\mathbf{E}}_{s \sim P_h}\left[\mathsf{SD}\left(\mathsf{Ext}\left(M_h, s\right), U_f\right)\right]. \quad (3.3)$$

Since $\mathsf{SD}\left(P_h, U_p\right) = \delta_h$ and since the range of the function $g(s) = \mathsf{SD}\left(\mathsf{Ext}\left(M_h, s\right), U_f\right)$ is contained in the interval $[0,1]$, Lemma 2.9 implies that

$$\mathop{\mathbf{E}}_{s \sim P_h}\left[\mathsf{SD}\left(\mathsf{Ext}\left(M_h, s\right), U_f\right)\right] \leq \mathop{\mathbf{E}}_{s \sim U_p}\left[\mathsf{SD}\left(\mathsf{Ext}\left(M_h, s\right), U_f\right)\right] + \delta_h. \quad (3.4)$$

Equation (3.3) and Equation (3.4) imply that

$$\mathsf{SD}\left(\left(F_h, P_h\right), \left(U_f, P_h\right)\right) \leq \mathop{\mathbf{E}}_{s \sim U_p}\left[\mathsf{SD}\left(\mathsf{Ext}\left(M_h, s\right), U_f\right)\right] + \delta_h.$$

As we assume that $\widetilde{H}_\infty\left(M \mid \mathcal{H}\right) \geq k + \log(1/\varepsilon)$, Lemma 2.13 implies that

$$\mathop{\mathbf{Pr}}_{h \sim \mathcal{H}}\left[H_\infty\left(M_h\right) \geq k\right] \geq 1 - \varepsilon.$$

We say that h is *good* if $H_\infty(M_h) \geq k$. Since Ext is a strong seeded extractor for entropy k with error ε, for any good h it holds that

$$\mathsf{SD}\left(\left(F_h, P_h\right), \left(U_f, P_h\right)\right) \leq \varepsilon + \delta_h.$$

By Lemma 2.5,

$$\mathsf{SD}\left(\left(F, P, \mathcal{H}\right), \left(U_f, P, \mathcal{H}\right)\right) = \mathop{\mathbf{E}}_{h \sim \mathcal{H}}\left[\mathsf{SD}\left(\left(F_h, P_h\right), \left(U_f, P_h\right)\right)\right].$$

The right hand side is bounded above by

$$\mathop{\mathbf{E}}_{h \sim \mathcal{H}}\left[\mathsf{SD}\left(\left(F_h, P_h\right), \left(U_f, P_h\right)\right) \;\middle|\; h \text{ is good}\right] \cdot \mathop{\mathbf{Pr}}_{h \sim \mathcal{H}}\left[h \text{ is good}\right] + \mathop{\mathbf{Pr}}_{h \sim \mathcal{H}}\left[h \text{ is not good}\right] \leq \delta + 2\varepsilon,$$

as stated. The fact that $P, \mathcal{H}$ is an (L, R)-history readily follows since $\mathcal{H}$ is an (L, R)-history and P is a deterministic function of $L, \mathcal{H}$. □

The following lemma is also used frequently in our proofs.

Lemma 3.4. *Let L, R be two independent random variables, and let $\mathcal{H}$ be an (L, R)-history. Let P be a random variable that is a deterministic function of $R, \mathcal{H}$. Let J be a random variable that is a deterministic function of $L, \mathcal{H}$. Then,*

$$\mathsf{SD}\left(\left(P, J, \mathcal{H}\right), \left(U, J, \mathcal{H}\right)\right) = \mathsf{SD}\left(\left(P, \mathcal{H}\right), \left(U, \mathcal{H}\right)\right).$$

Moreover, $J, \mathcal{H}$ is an (L, R)-history.

Proof. The fact that $J, \mathcal{H}$ is an (L,R)-history readily follows since $\mathcal{H}$ is an (L,R)-history and J is a deterministic function of $L, \mathcal{H}$. Now, by Lemma 2.5,

$$\mathsf{SD}\left((P,J,\mathcal{H}),(U,J,\mathcal{H})\right) = \mathop{\mathbf{E}}_{h\sim\mathcal{H}}\left[\mathsf{SD}\left(((P,J) \mid \mathcal{H}=h),(U,J \mid \mathcal{H}=h)\right)\right].$$

For any $h \in \mathsf{supp}(\mathcal{H})$, the random variable $(P \mid \mathcal{H}=h)$ is a deterministic function of R whereas $(J \mid \mathcal{H}=h)$ is a deterministic function of L. Since $(L \mid \mathcal{H}=h)$, $(R \mid \mathcal{H}=h)$ are independent, as guaranteed by Lemma 3.2, we have that $(P \mid \mathcal{H}=h)$ and $(J \mid \mathcal{H}=h)$ are independent. Thus, Lemma 2.6 implies that

$$\mathsf{SD}\left((P,J,\mathcal{H}),(U,J,\mathcal{H})\right) = \mathop{\mathbf{E}}_{h\sim\mathcal{H}}\left[\mathsf{SD}\left(P \mid (\mathcal{H}=h),U\right)\right],$$

which concludes the proof, as by Lemma 2.5, the right hand side of the above equation equals to $\mathsf{SD}\left((P,\mathcal{H}),(U,\mathcal{H})\right)$. ◻

4 Two-Steps Look-Ahead Extractors

In this section we present a restricted version of look-ahead extractors. Building on the idea of alternating extraction [DP07], Dodis and Wichs [DW09] introduced the notion of look-ahead extractors. Look-ahead extractors were further used by Li [Li13, Li15] for his multi-source extractors. In these cases, the look-ahead extractors were applied for some non-constant number of "steps" or "rounds". We construct our LCBs using look-ahead extractors with only two steps. This in turn allows us to present relatively simple constructions of LCBs, which are also easier to analyze. Since we need only this very restricted version, and since we use it in the analysis of our constructions in a white-box manner, we give in this section the construction for two-steps look-ahead extractors.

Let n, a, h be integers and let $\varepsilon > 0$ be such that $a = \Omega(\log(h/\varepsilon))$ and $h = \Omega(\log(n/\varepsilon))$. Set $s = \Theta(\log(n/\varepsilon))$, where some appropriately chosen large enough universal constant is hidden under the Θ notation. Let $\mathsf{Ext}_1 \colon \{0,1\}^n \times \{0,1\}^s \to \{0,1\}^a$ and $\mathsf{Ext}_2 \colon \{0,1\}^h \times \{0,1\}^a \to \{0,1\}^s$ be strong seeded extractors from Theorem 2.2, both with error ε. Note that the choice of s and the assumption on a guarantee that the seed lengths of Ext_1 and Ext_2 are sufficient. Moreover, by Theorem 2.2, Ext_1 is an extractor for entropy $2a$ and Ext_2 is an extractor for entropy $2s$. Define the function

$$\mathsf{LookAheadExt} \colon \{0,1\}^h \times \{0,1\}^n \to \{0,1\}^a \times \{0,1\}^a$$

as follows. Given $W \in \{0,1\}^h$ and $Y \in \{0,1\}^n$, let

$$\begin{aligned} A &= \mathsf{Ext}_1(Y, W|_s), \\ Z &= \mathsf{Ext}_2(W, A), \\ B &= \mathsf{Ext}_1(Y, Z). \end{aligned}$$

Define

$$\mathsf{LookAheadExt}(W,Y) = (A,B).$$

With notations as above, we have the following lemma.

Lemma 4.1. *Let r be an integer. Let X, Y be two independent random variables, and let $\mathcal{H}$ be an (X,Y)-history such that*

$$\widetilde{H}_\infty(Y \mid \mathcal{H}) \geq (r+2)a + \log(1/\varepsilon). \tag{4.1}$$

Let W be a random variable of the form of an $r \times h$ matrix, which is a deterministic function of $X, \mathcal{H}$, where

$$h \geq (r+2)s + \log(1/\varepsilon). \tag{4.2}$$

Assume further that there exists $g \in [r]$ such that

$$(W_g, \mathcal{H}) \approx_\delta (U_h, \mathcal{H}). \tag{4.3}$$

For each $i \in [r]$, let (A_i, B_i) be the output $\mathsf{LookAheadExt}(W_i, Y)$*. Then the following holds:*

- $\mathcal{H}' = (W, Z_g, \{A_i\}_{i=1}^r, W|_s, \mathcal{H})$ *is an (X,Y)-history.*
- $(B_g, \mathcal{H}') \approx_{2\delta+6\varepsilon} (U_a, \mathcal{H}')$.
- $\widetilde{H}_\infty(Y \mid \mathcal{H}') \geq \widetilde{H}_\infty(Y \mid \mathcal{H}) - ra$.
- *For any random variable N which is a deterministic function of $X, \mathcal{H}$, it holds that $\widetilde{H}_\infty(N \mid \mathcal{H}') \geq \widetilde{H}_\infty(N \mid \mathcal{H}) - rh$.*

As mentioned, Lemma 4.1 is not new and general versions of it appear in the literature. Nevertheless, as we consider a restricted setting and since the lemma as stated uses the notion of (L,R)-histories (which is new), a direct proof for the lemma above does not appear in the literature (though existing proofs can be adopted in a straightforward manner). Thus, for completeness, we give a proof for Lemma 4.1 in Appendix A.

5 A Warm Up – Merging Three Rows

In order to convey the ideas underling our LCBs, we present in this section a construction of a merger with weak-seeds for a somewhere-random source with only three rows. This toy example allows us to present some of the ideas used in the actual constructions of our mergers with weak-seeds (Theorem 1.5) and LCBs (Theorem 1.2). This section is meant only for building up intuition, and presenting the underling ideas behind our constructions without getting into all the details.

During this section we ignore the error analysis as this does not affect the parameters and slightly complicates the presentation. In particular, when applying Lemma 3.3 and Lemma 4.1 we ignore the expression $\log(1/\varepsilon)$ in Equation (3.2) and in Equation (4.1).

In this section we prove the following theorem which, roughly speaking, states that one can efficiently and deterministically merge the rows of a $3 \times \ell$ somewhere-random source, using an independent (n,k)-weak-source, even when $\ell = \Theta(\log n)$ and $k = \Omega(\log \log n)$.

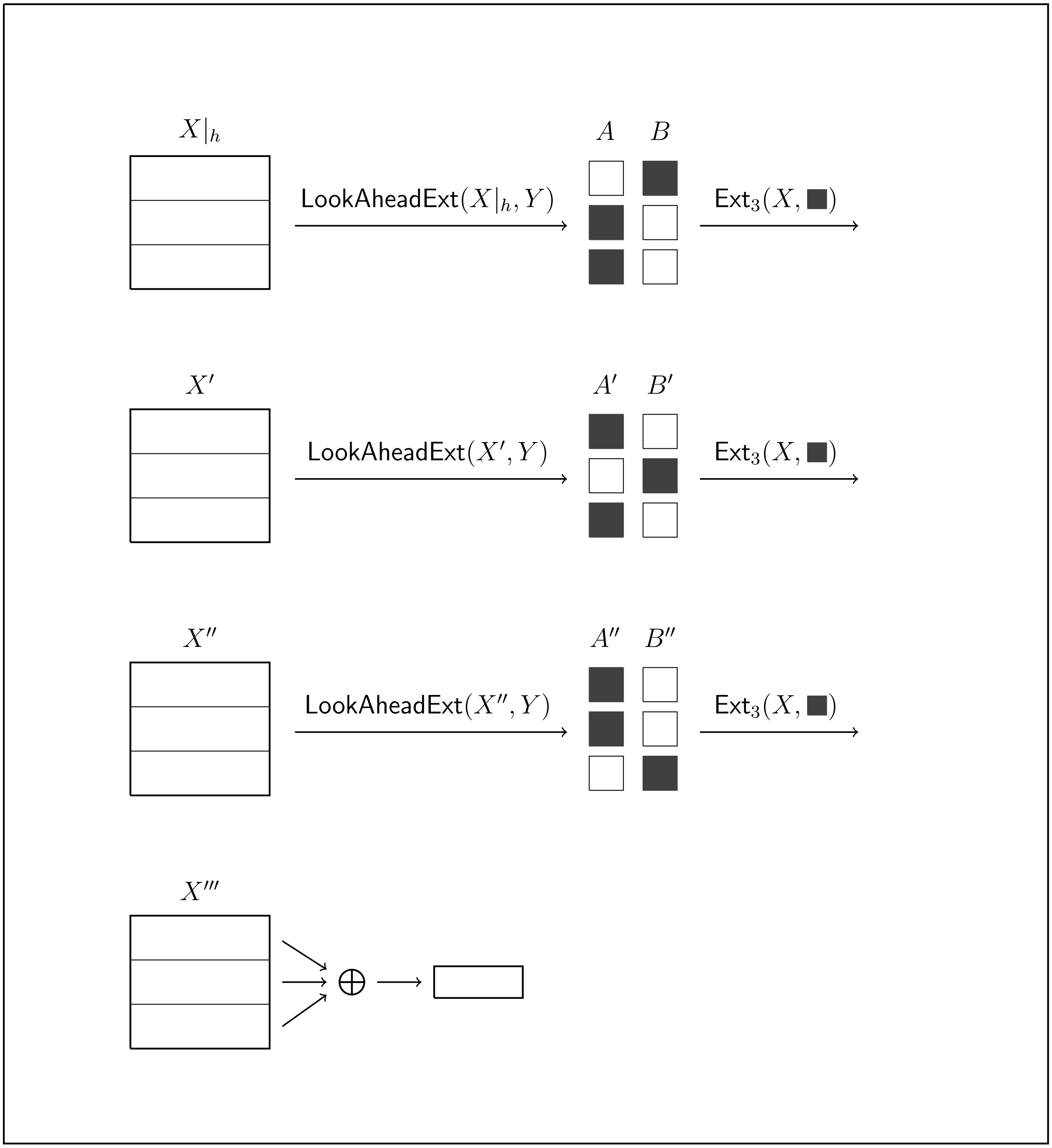

Figure 1: A schematic diagram of the three rows merger Merg_3.

Theorem 5.1 (Merging three rows)**.** *For any integer n, there exists a* poly(n)*-time computable function*

$$\mathsf{Merg}_3 \colon \left(\{0,1\}^{\ell}\right)^3 \times \{0,1\}^n \to \{0,1\}^m,$$

where $\ell = \Theta(\log n)$ and $m = \Omega(\ell)$, with the following property. Let X be a $3 \times \ell$ somewhere-random source. Let Y be an independent (n,k)-weak-source with $k = \Omega(\log\log n)$. Then, $\mathsf{Merg}_3(X,Y) \approx U_m$.

Proof. During the proof of this toy example we assume that the second row, X_2, is good. Of course, the algorithm Merg_3 will not rely on this assumption (or otherwise the algorithm can simply output X_2). We use the assumption that X_2 is uniform only for the analysis. We exemplify this with the good row being the second row just to avoid introducing more indices. Since the second row is not the first or the last row, this will enable us to demonstrate all the ideas needed to prove the theorem for any number of rows.

We turn to present the construction of Merg_3. For the reader's convenience, the construction is depict in Figure 1. As mentioned, the problem of merging the 3 rows X_1, X_2, X_3, with X_2 being the good row, is reduced to the problem of obtaining random variables X_1''', X_2''', X_3''', where each X_i''' is a function of X_i and Y, with the following property: $(X_2''', X_1''', X_3''') \approx (U, X_1''', X_3''')$, namely, constructing 3-LCBs for 3 rows. Once this independence is obtained, one can simply output

$$\mathsf{Merg}_3(X,Y) = X_1''' \oplus X_2''' \oplus X_3'''.$$

Set h to be just large enough for the two-steps look-ahead extractor from Section 4 with $r = 3$. Taking $h = \Theta(\log n)$ will do. Set $a = \Theta(\log\log n)$ and note that this choice of a satisfies the hypothesis of the two-steps look-ahead extractor. We now compute

$$\begin{aligned}(A_1, B_1) &= \mathsf{LookAheadExt}\left((X_1)|_h, Y\right),\\ (A_2, B_2) &= \mathsf{LookAheadExt}\left((X_2)|_h, Y\right),\\ (A_3, B_3) &= \mathsf{LookAheadExt}\left((X_3)|_h, Y\right),\end{aligned}$$

and then compute

$$\begin{aligned}X_1' &= \mathsf{Ext}_3(X_1, B_1),\\ X_2' &= \mathsf{Ext}_3(X_2, A_2),\\ X_3' &= \mathsf{Ext}_3(X_3, A_3),\end{aligned}$$

where $\mathsf{Ext}_3 \colon \{0,1\}^{\ell} \times \{0,1\}^a \to \{0,1\}^h$ is the strong seeded extractor from Theorem 2.2 for entropy $2h$. [5] This was the first iteration of the algorithm Merg_3, in which we produced the random variables X_1', X_2' and X_3' from X_1, X_2, X_3 and Y. In the second iteration we will compute X_1'', X_2'' and X_3'' from X_1', X_2', X_3' and X, Y in a similar way. The difference will be

[5] We use the name Ext_3 because during the proof we will argue about the random variables obtained by the two-steps look-ahead extractor from Section 4, which uses two strong seeded extractors we denoted by Ext_1 and Ext_2.

that instead of taking the B variable as a seed for the first row and the corresponding A variables to the other rows, we will take the B variable as a seed for the *second* row and the corresponding A variables to the other two rows. More formally, we compute

$$\begin{aligned}(A'_1, B'_1) &= \mathsf{LookAheadExt}\left(X'_1, Y\right),\\ (A'_2, B'_2) &= \mathsf{LookAheadExt}\left(X'_2, Y\right),\\ (A'_3, B'_3) &= \mathsf{LookAheadExt}\left(X'_3, Y\right),\end{aligned}$$

and then set

$$\begin{aligned}X''_1 &= \mathsf{Ext}_3(X_1, A'_1),\\ X''_2 &= \mathsf{Ext}_3(X_2, B'_2),\\ X''_3 &= \mathsf{Ext}_3(X_3, A'_3).\end{aligned}$$

The algorithm continues for one more iteration, and computes

$$\begin{aligned}(A''_1, B''_1) &= \mathsf{LookAheadExt}\left(X''_1, Y\right),\\ (A''_2, B''_2) &= \mathsf{LookAheadExt}\left(X''_2, Y\right),\\ (A''_3, B''_3) &= \mathsf{LookAheadExt}\left(X''_3, Y\right),\end{aligned}$$

and then computes

$$\begin{aligned}X'''_1 &= \mathsf{Ext}_3(X_1, A''_1),\\ X'''_2 &= \mathsf{Ext}_3(X_2, A''_2),\\ X'''_3 &= \mathsf{Ext}_3(X_3, B''_3).\end{aligned}$$

Informally speaking, we want to show that if there is enough entropy in Y and in X_2 (namely, ℓ is large enough), then X'''_2 is close to uniform even given X'''_1, X'''_3. This is formalized by the following claim. By the discussion above, once we prove Claim 5.2, Theorem 5.1 will follow.

Claim 5.2. *If $k \geq 11a$ and $\ell \geq 13h$, then*

$$(X'''_2, X'''_1, X'''_3) \approx (U_h, X'''_1, X'''_3).$$

Before proving Claim 5.2, we present the high-level strategy of the proof, which consists of three steps.

- First, we show that in iterations that precede the "good" iteration (that is, the iteration in which the good row is given the B variable, which in our case is the second iteration) the assumption on the input is preserved. Namely, at the end of each such iteration, an output row that corresponds to a good input row is uniform, and the joint distribution of the rows is independent of Y.

- In the second step we show that after the good iteration was executed, the respective output row "gains its independence". That is, an output row that corresponds to a good input row is uniform even conditioned on all other output rows. Moreover, the joint distribution of the rows is independent of Y.

- In the third step we show that the independence of the good row is "preserved" throughout the remaining iterations. Namely, an output row that corresponds to a good input row remains uniform even conditioned on all other output rows, and moreover, the joint distribution of all output rows is independent of Y.

Proof of Claim 5.2. The proof will follow the three iterations of the algorithm. In the first iteration we give the "lead", namely the B variable, to the "wrong" row X_1. We show that nothing bad happens by letting X_1 have the lead, in the following sense: after this iteration, we have that the joint distribution (X'_1, X'_2, X'_3) is independent of Y (more formally, this independence holds conditioned on any fixing of carefully chosen (X, Y)-history), and X'_2 is close to uniform. So besides losing some entropy in Y and in X_2, and observing some error, we maintain the assumption we had initially about our input – the second row X'_2 is uniform, and the joint distribution of the three rows is independent of Y. Thus, in some sense we can "skip" to the iteration in which we give the lead to the good row, which in our case is the second row. This easily generalizes to any number of rows that precede the good row.

Analyzing the first iteration. Recall that $A_2 = \mathsf{Ext}_1(Y, (X_2)|_s)$. Moreover, Y and $(X_2)|_s$ are independent, and $H_\infty(Y) = k \geq 11a$. Since Ext_1 is a strong seeded extractor for entropy $2a$, we have that

$$(A_2, (X_2)|_s) \approx (U_a, \cdot).$$ [6]

Note further that conditioned on any fixing of $(X_2)|_s$, the random variables A_2 and $X|_h$ are independent. Thus, we can apply Lemma 2.7 and conclude that

$$(A_2, X|_h) \approx (U_a, \cdot). \tag{5.1}$$

Recall that $X'_2 = \mathsf{Ext}_3(X_2, A_2)$. We apply Lemma 3.3 to the (X, Y)-history $X|_h$ with $P = A_2$, $M = X_2$ and the extractor Ext_3. The hypothesis of Lemma 3.3 is met since A_2 is a deterministic function of Y and $X|_h$. Moreover, since Ext_3 is an extractor for entropy $2h$, and since

$$\widetilde{H}_\infty(X_2 \mid (X|_h)) \geq \ell - 3h \geq 10h,$$

Equation (3.2) of Lemma 3.3 holds. Therefore, Lemma 3.3 together with Equation (5.1) imply that

$$(X'_2, A_2, X|_h) \approx (U_h, \cdot).$$

Moreover, $A_2, X|_h$ is an (X, Y)-history.

[6] Recall that our notation dictates that $(X, Z_1, \ldots, Z_r) \approx (Y, \cdot)$ is a shorthand for $(X, Z_1, \ldots, Z_r) \approx (Y, Z_1, \ldots, Z_r)$

We now apply Lemma 3.4 with $P = X_2'$, $J = (B_1, A_3)$ and the (X, Y)-history $A_2, X|_h$. Since X_2' is a deterministic function of X and A_2 and since B_1, A_3 are deterministic functions of Y and $X|_h$, Lemma 3.4 implies that $\mathcal{H}_1 = (B_1, A_2, A_3, X|_h)$ is an (X, Y)-history and that

$$(X_2', \mathcal{H}_1) \approx (U_h, \cdot). \tag{5.2}$$

Since each of B_1, A_2, A_3 consists of a bits and since Y is independent of $X|_h$, Lemma 2.12 and Lemma 2.14 imply that

$$\widetilde{H}_\infty(Y \mid \mathcal{H}_1) \geq \widetilde{H}_\infty(Y \mid (X|_h)) - 3a = H_\infty(Y) - 3a \geq 8a. \tag{5.3}$$

Similarly, conditioned on any fixing of $X|_h$, the random variables B_1, A_2, A_3 are deterministic functions of Y, whereas X_2 is a deterministic function of X. Hence, Lemma 2.14 implies that $\widetilde{H}_\infty(X_2 \mid \mathcal{H}_1) = \widetilde{H}_\infty(X_2 \mid (X|_h))$. Since $X|_h$ consists of $3h$ bits, we have that

$$\widetilde{H}_\infty(X_2 \mid \mathcal{H}_1) \geq H_\infty(X_2) - 3h = 10h. \tag{5.4}$$

This concludes the first iteration. Note that after the first iteration X_2' is close to uniform (Equation (5.2)). Moreover, Y and X_2 still have (enough) entropy (Equation (5.3), Equation (5.4)).

Analyzing the second iteration. We reached the iteration in which we give the lead to the good row – X_2. We want to show that after this iteration, $(X_2'', X_1'', X_3'') \approx (U_h, X_1'', X_3'')$. Namely, the good row "gains its independence" in the iteration in which it takes the lead.

We continue from Equation (5.2) and apply Lemma 4.1 to the (X, Y)-history $\mathcal{H}_1$, with the $3 \times h$ matrix X' and the weak-source Y. Equation (4.1) of Lemma 4.1 holds by Equation (5.3). Since $h \geq 5s$, Equation (4.2) of Lemma 4.1 holds as well. Therefore, Lemma 4.1 together with Equation (5.2) imply that

$$\mathcal{H}_1' = (X', Z_2', A_1', A_2', A_3', (X')|_s, \mathcal{H}_1)$$

is an (X, Y)-history, and that

$$(B_2', \mathcal{H}_1') \approx (U_a, \cdot).$$

Furthermore, the third item of Lemma (4.1) together with Equation (5.3) imply that

$$\widetilde{H}_\infty(Y \mid \mathcal{H}_1') \geq \widetilde{H}_\infty(Y \mid \mathcal{H}_1) - 3a \geq 5a. \tag{5.5}$$

The fourth item of Lemma 4.1, applied with $N = X_2$, together with Equation (5.4), implies that

$$\widetilde{H}_\infty(X_2 \mid \mathcal{H}_1') \geq \widetilde{H}_\infty(X_2 \mid \mathcal{H}_1) - 3h \geq 7h. \tag{5.6}$$

We now apply Lemma 3.4 to the (X, Y)-history $\mathcal{H}_1'$ with $P = B_2'$ and $J = (X_1'', X_3'')$. Lemma 3.4 is applicable since B_2' is a deterministic function of Y, X_2', and the latter is contained in $\mathcal{H}_1'$. Moreover, X_1'', X_3'' are deterministic functions of X, A_1', A_3', and A_1', A_3' are contained in $\mathcal{H}_1'$. Thus, Lemma 3.4 implies that

$$(B_2', X_1'', X_3'', \mathcal{H}_1') \approx (U_a, \cdot), \tag{5.7}$$

and that $X_1'', X_3'', \mathcal{H}_1'$ is an (X,Y)-history.

Recall that $X_2'' = \mathsf{Ext}_3(X_2, B_2')$. We now apply Lemma 3.3 to the (X,Y)-history $X_1'', X_3'', \mathcal{H}_1'$ with $P = B_2'$, $M = X_2$ and the extractor Ext_3. The hypothesis of the lemma holds since B_2' is a deterministic function of Y and X_2', and the latter is contained in $\mathcal{H}_1'$. By Equation (5.6) and Lemma 2.12, it holds that

$$\widetilde{H}_\infty(X_2 \mid X_1'', X_3'', \mathcal{H}_1') \geq \widetilde{H}_\infty(X_2 \mid \mathcal{H}_1') - 2h \geq 5h. \tag{5.8}$$

Since Ext_3 is a strong seeded extractor for entropy $2h$, Equation (3.2) of Lemma 3.3 holds. Therefore, Lemma 3.3 together with Equation (5.7) imply that

$$(X_2'', \mathcal{H}_2) \approx (U_h, \cdot), \tag{5.9}$$

where $\mathcal{H}_2 = (B_2', X_1'', X_3'', \mathcal{H}_1')$ is an (X,Y)-history. In terms of entropy-loss,

$$\widetilde{H}_\infty(Y \mid \mathcal{H}_2) \geq \widetilde{H}_\infty(Y \mid X_1'', X_3'', \mathcal{H}_1') - a = \widetilde{H}_\infty(Y \mid \mathcal{H}_1') - a \geq 4a, \tag{5.10}$$

where the first inequality follows by Lemma 2.12 and the fact that $|B_2'| = a$. The second equality follows by Lemma 2.14 and the fact that conditioned on any fixing of $\mathcal{H}_1'$, the random variables X_1'', X_3'' are deterministic functions of X, and are thus independent of Y. The last inequality follows by Equation (5.5).

Similarly, since B_2' is independent of X_2 conditioned on any fixing of $\mathcal{H}_1'$, we have that

$$\widetilde{H}_\infty(X_2 \mid \mathcal{H}_2) = \widetilde{H}_\infty(X_2 \mid X_1'', X_3'', \mathcal{H}_1') \geq 5h, \tag{5.11}$$

where the last inequality follows by Equation (5.8). Since X_1'', X_3'' are contained in $\mathcal{H}_2$, this proves what we wanted for this iteration. Namely, after the second iteration, in which the good row takes the lead, $(X_2'', X_1'', X_3'') \approx (U_h, X_1'', X_3'')$.

Analyzing the third iteration. We now show that the independence of the good row X_2'' is "preserved" throughout the following iteration, where again another row takes the lead. We continue from Equation (5.9). We note that conditioned on any fixing of $\mathcal{H}_2$, the random variables A_1'', B_3'' are deterministic functions of Y (as X_1'', X_3'' are contained in $\mathcal{H}_2$). On the other hand, conditioned on any fixing of $\mathcal{H}_2$, the random variable X_2'' is a deterministic function of X (as B_2' is contained in $\mathcal{H}_2$). Thus, by Lemma 3.4 applied to the (X,Y)-history $\mathcal{H}_2$ with $P = X_2''$ and $J = (A_1'', B_3'')$, it holds that

$$(X_2'', A_1'', B_3'', \mathcal{H}_2) \approx (U_h, \cdot).$$

Furthermore, $A_1'', B_3'', \mathcal{H}_2$ is an (X,Y)-history. By Lemma 2.12 and Equation (5.10), it holds that

$$\widetilde{H}_\infty(Y \mid A_1'', B_3'', \mathcal{H}_2) \geq \widetilde{H}_\infty(Y \mid \mathcal{H}_2) - 2a \geq 2a. \tag{5.12}$$

Recall that $A_2'' = \mathsf{Ext}_1(Y, (X_2'')|_s)$. We apply Lemma 3.3 to the (X,Y)-history $A_1'', B_3'', \mathcal{H}_2$ with $P = (X_2'')|_s$, $M = Y$ and the extractor Ext_1. Since Ext_1 is an extractor for entropy $2a$, Equation (3.2) of Lemma 3.3 holds by Equation (5.12). Furthermore, $(X_2'')|_s$ is a deterministic function of X and B_2', which is contained in $\mathcal{H}_2$. Thus, the hypothesis of Lemma 3.3 is met, and we get that

$$(A_2'', X_2'', A_1'', B_3'', \mathcal{H}_2) \approx (U_a, \cdot),$$

and $X_2'', A_1'', B_3'', \mathcal{H}_2$ is an (X,Y)-history. In terms of entropy-loss, since $|X_2''| = h$ and since A_1'', B_3'' are deterministic functions of Y conditioned on any fixing of X_1'', X_3'', which are contained in $\mathcal{H}_2$, Lemma 2.12 together with Equation (5.11) imply that

$$\widetilde{H}_\infty(X_2 \mid X_2'', A_1'', B_3'', \mathcal{H}_2) \geq \widetilde{H}_\infty(X_2 \mid A_1'', B_3'', \mathcal{H}_2) - h = \widetilde{H}_\infty(X_2 \mid \mathcal{H}_2) - h \geq 4h. \quad (5.13)$$

We now apply Lemma 3.4 to the (X,Y)-history $X_2'', A_1'', B_3'', \mathcal{H}_2$ with $P = A_2''$ and $J = X_1''', X_3'''$. Recall that $X_1''' = \mathsf{Ext}_3(X_1, A_1'')$ and $X_3''' = \mathsf{Ext}_3(X_3, B_3'')$. Thus, conditioned on any fixing of A_1'', B_3'', it holds that X_1''', X_3''' are deterministic functions of X, whereas A_2'' is a deterministic function of Y conditioned on any fixing of X_2''. Thus, Lemma 3.4 implies that

$$(A_2'', X_1''', X_3''', \mathcal{H}_2') \approx (U_a, \cdot),$$

where $\mathcal{H}_2' = (X_2'', A_1'', B_3'', \mathcal{H}_2)$ is an (X,Y)-history. In terms of entropy-loss, by Equation (5.13) and Lemma 2.12, we have that

$$\widetilde{H}_\infty(X_2 \mid X_1''', X_3''', \mathcal{H}_2') \geq \widetilde{H}_\infty(X_2 \mid X_2'', A_1'', B_3'', \mathcal{H}_2) - 2h \geq 2h. \quad (5.14)$$

Recall that $X_2''' = \mathsf{Ext}_3(X_2, A_2'')$. We apply Lemma 3.3 to the (X,Y)-history $X_1''', X_3''', \mathcal{H}_2'$, with $P = A_2''$, $M = X_2$ and the extractor Ext_3. Note that A_2'' is a deterministic function of Y and X_2'', which is contained in $\mathcal{H}_2'$. Equation (3.2) of Lemma 3.3 follows by Equation (5.14) and the fact that Ext_3 is an extractor for entropy $2h$. Lemma 3.3 then implies that

$$(X_2''', A_2'', X_1''', X_3''', \mathcal{H}_2') \approx (U_h, \cdot).$$

By Lemma 2.8 it follows that

$$(X_2''', X_1''', X_3''') \approx (U_h, \cdot),$$

which concludes the proof of the claim. □

As mentioned above, the proof of Theorem 5.1 readily follows by Claim 5.2. □

5.1 Merging r rows – an overview

Generalizing the proof of the three-rows merger presented above to $r > 3$ rows is straightforward. Instead of three iterations, we can apply the algorithm above for r iterations, where at the i^{th} iteration we give the lead to row i. Working out the parameters, one can show that this generalization works for $\ell = O(r^4 \cdot \log n)$ and $k = O(r^3 \cdot \log\log n)$. We now explain how one can improve this, and construct a merger for $\ell = \tilde{O}(r^2) \cdot \log n$ and $k = \tilde{O}(r) \cdot \log\log n$, as we obtain in the actual construction (Theorem 7.2).

For the purpose of constructing mergers with weak-seeds, this improvement, although desired, is not crucial, especially when r is small. This, for example, is the case in the construction of our three-source extractor. Thus, in these cases, the simpler merger depicted above is sufficient. However, for our construction of LCBs the somewhat more involved construction is necessary, and so in the rest of this section we give an informal overview of the actual construction.

Consider the complete graph on r vertices, where vertex $i \in [r]$ represents the i^{th} row of X. In the straightforward generalization of the three rows merger to r rows, we (implicitly) considered r cuts of this graph, where the i^{th} cut is $(\{i\}, [r] \setminus \{i\})$. The construction in Theorem 5.1 guarantees that if X_i is good then after the i^{th} iteration, row i is uniform even given all other rows (and remains as such throughout the following iterations). In the actual construction of our merger (and LCBs) we generalize this idea and guarantee that the following stronger property holds. For any cut (S, S^c) of $[r]$, the i^{th} row is independent of all rows with indices that are separated from i by the cut (S, S^c). Notice that when we used the cuts of the form $(\{i\}, [r] \setminus \{i\})$, we knew that at some iteration the good row $g \in [r]$ is separated from all other rows, and moreover, we knew on which side of the cut g will be (the side that contains the single vertex). By inspecting the construction above, one can see that the algorithm used this second piece of information. Indeed, in each iteration we gave the lead to the single row, namely, we gave the single row the B variable, and all other rows got the A variables.

When considering general cuts (S, S^c), we no longer know which side of the cut contains the good row g. Namely, to who should we give the B variables – to the rows in S or to the rows in S^c. We solve this problem by applying the construction used above twice, in a "flip-flop". Namely, we first give the B variables to the rows in S and the A variables to the rows in S^c, and then run one more round, giving the B variables to the rows in S^c and the A variables to the rows in S. We only then proceed to the next cut in the sequence.

Having the ability to use general cuts allows us to run for only $\log r$ iterations rather than for r iterations. Indeed, instead of choosing r (highly unbalanced) cuts, and run for r iterations, we use $q = \log r$ (efficiently computable) cuts $S_1, \ldots, S_q$ with the following property. For any two distinct $i, j \in [r]$, there exists $v \in [q]$ such that the cut (S_v, S_v^c) separates i from j. By working with these cuts, the same independence guarantee holds when the algorithm terminates. Indeed, after the v^{th} iteration, row i is uniform and independent of all rows that were separated from i by at least one of the cuts $(S_1, S_1^c), \ldots, (S_v, S_v^c)$. By the property of $S_1, \ldots, S_q$ it follows that after all q iterations were executed, row i is uniform and independent of all other rows. Since we run for only $q = \log r$ iterations, as apposed to r iterations, we obtain a multiplicative saving of roughly $r/\log r$ in both k, ℓ, which yields the desired improvement.

Our construction of LCBs follows the same idea as the construction of the mergers described above. The only difference is that the analysis is done "locally" on t rows, rather than on r rows. The fact that we run for $\log r$ iterations introduces only logarithmic factors of r into k, ℓ, as apposed to polynomial factors.

6 Local Correlation Breakers

In this section we prove Theorem 1.2. We start by giving a more formal and complete statement of the theorem.

Theorem 6.1. *For all integers n, r, t and any $\varepsilon > 0$, there exists a* $\mathrm{poly}(n, r, \log(1/\varepsilon))$*-time computable t-LCB*

$$\mathsf{LCB}\colon \left(\{0,1\}^{\ell}\right)^{r} \times \{0,1\}^{n} \to \left(\{0,1\}^{m}\right)^{r}$$

for entropy k, with error ε, where

$$\begin{aligned} \ell &= \Theta\left(t^2 \cdot \log\left(\frac{nr}{\varepsilon}\right) \cdot \log r\right), \\ m &= \Omega\left(\frac{\ell}{t \cdot \log r}\right), \\ k &= \Omega\left(t \cdot \log(r) \cdot \log\left(\frac{r \cdot \log n}{\varepsilon}\right)\right). \end{aligned}$$

In fact, we prove the following stronger theorem which readily implies Theorem 6.1.

Theorem 6.2. *Let n, r, t be integers, and let $\varepsilon > 0$. Set*

$$\begin{aligned} h &= \Theta\left(t \cdot \log\left(\frac{nr}{\varepsilon}\right)\right), \\ \ell &= \Theta\left(ht \cdot \log r\right) = \Theta\left(t^2 \cdot \log\left(\frac{nr}{\varepsilon}\right) \cdot \log r\right). \end{aligned}$$

There exists a function $\mathsf{LCB}\colon \left(\{0,1\}^{\ell}\right)^{r} \times \{0,1\}^{n} \to \left(\{0,1\}^{h}\right)^{r}$ with the following property. Let X be an $r \times \ell$ somewhere-random source. Assume that X_g is a good row of X. Let $\mathcal{I} = \{i_1, \ldots, i_{t-1}\} \subseteq [r] \setminus \{g\}$. Let Y be an (n, k)-weak-source that is independent of X, such that

$$k = \Omega\left(t \cdot \log(r) \cdot \log\left(\frac{r \cdot \log n}{\varepsilon}\right)\right). \tag{6.1}$$

Let $\bar{W} = \mathsf{LCB}(X, Y)$. Then, there exists an (X, Y)-history $\mathcal{H}$ that contains $\{\bar{W}_i \mid i \in \mathcal{I}\}$, such that the following holds:

- $\left(\bar{W}_g, \mathcal{H}\right) \approx_{\varepsilon} (U_h, \mathcal{H})$.
- $\widetilde{H}_{\infty}(X_g \mid \mathcal{H}) \geq 0.9 \cdot \ell$.
- $\widetilde{H}_{\infty}(Y \mid \mathcal{H}) \geq 0.9 \cdot k$. [7]
- *$\bar{W}_g$ is a deterministic function of X and $\mathcal{H}$.*

Furthermore, for any $i \in [r]$, $\bar{W}_i$ in computable in time $\mathrm{poly}(n, t, \log r, \log(1/\varepsilon))$.

[7] The constant 0.9 in the second and third items can be replaced by $1-\delta$ for any (not necessarily constant) $\delta > 0$, by taking ℓ to be $1/\delta$ times the stated ℓ, and by taking k to be $\log(1/\delta)/\delta$ times the stated k.

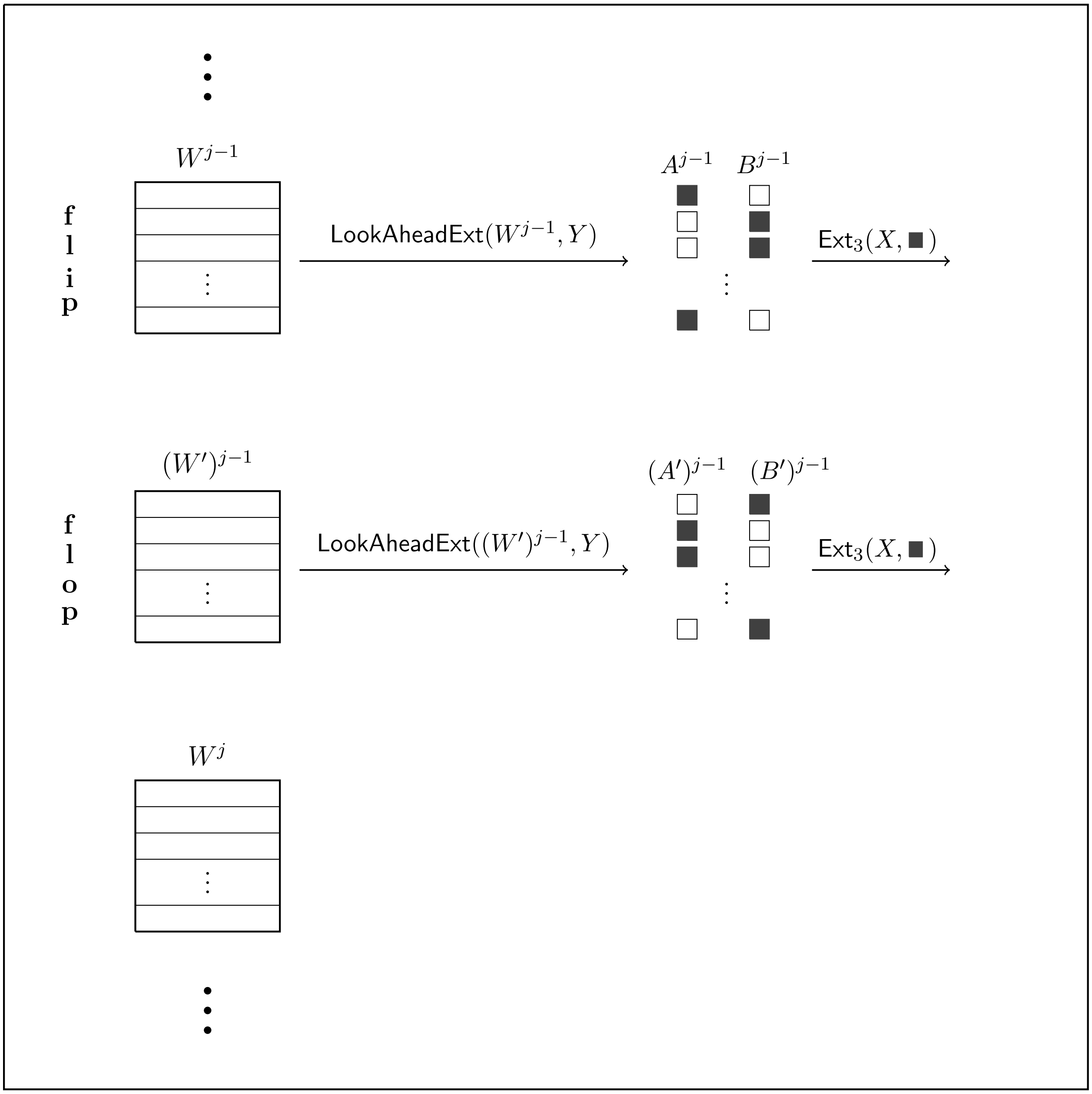

Figure 2: A schematic diagram of j^{th} iteration of LCB.

Proof. Let $\varepsilon' = \varepsilon/(32r)$. We make use of the following building blocks for the construction of LCB.

- Let $\mathsf{LookAheadExt}\colon \{0,1\}^h \times \{0,1\}^n \to \{0,1\}^a \times \{0,1\}^a$ be the two-steps look-ahead extractor from Section 4, set with error ε' and $a = \Theta(\log(\ell/\varepsilon'))$. Note that this choice of a satisfies the condition $a \geq \Omega(\log(h/\varepsilon'))$ (since $\ell \geq h$), as required by the two-steps look-ahead extractor. Note further that, by the choice of h, it holds that $h = \Omega(t \cdot \log(n/\varepsilon'))$. During the proof we apply Lemma 4.1 to somewhere-random sources with t rows, for which this setting of h is sufficient.

- Let $\mathsf{Ext}_3\colon \{0,1\}^\ell \times \{0,1\}^a \to \{0,1\}^h$ be the strong seeded-extractor from Theorem 2.2 for entropy $2h$, set with error ε'. Note that a was chosen to be large enough so that a seed of length a is sufficient for extracting entropy from length ℓ sources, with error ε'.

- Let $S_1, \ldots, S_q \subseteq [r]$ with the following property. For any two distinct $i, j \in [r]$, there exists $v \in [q]$ such that $|\{i,j\} \cap S_v| = 1$. We think of $S_1, \ldots, S_q$ as a sequence of cuts of the complete graph on vertex set $[r]$. The property above states that for any two distinct vertices $i, j \in [r]$, at least one of the cuts in the sequence separates i from j, namely, either $i \in S_v$, $j \notin S_v$ or $j \in S_v$, $i \notin S_v$, for some $v \in [q]$. We note that such a sequence, with length $q = \lceil \log_2 r \rceil$, can be constructed efficiently in the sense that given $i \in [r]$ and $v \in [q]$, one can determine whether or not $i \in S_v$ in time $\mathrm{polylog}(r)$. This can be done, for example, by taking S_v to be all $i \in [r]$ such that the v^{th} bit in the binary expansion of i is 1. This specific sequence of cuts was used in [Li13] for the construction of his multi-source extractor, though any sequence with the above property will do.

The algorithm LCB iteratively computes a sequence $W^0, W^1, \ldots, W^q$ of $r \times h$ matrices as follows. First, we set $W^0 = X|_h$. As depict in Figure 2, for any $j \geq 1$, the matrix W^j is computed as follows, given W^{j-1}. For each row $i \in [r]$ of W^{j-1}, we apply the two-steps look-ahead extractor together with the weak-source Y to obtain

$$\left(A_i^{j-1}, B_i^{j-1}\right) = \mathsf{LookAheadExt}\left(W_i^{j-1}, Y\right).$$

We then define

$$C_i^{j-1} = \begin{cases} A_i^{j-1}, & i \in S_j, \\ B_i^{j-1}, & i \notin S_j. \end{cases}$$

Next, we compute

$$(W')_i^{j-1} = \mathsf{Ext}_3\left(X_i, C_i^{j-1}\right).$$

We apply the two-steps look-ahead extractor for the second time, as follows

$$\left((A')_i^{j-1}, (B')_i^{j-1}\right) = \mathsf{LookAheadExt}\left((W')_i^{j-1}, Y\right),$$

and define

$$(C')_i^{j-1} = \begin{cases} (B')_i^{j-1}, & i \in S_j, \\ (A')_i^{j-1}, & i \notin S_j. \end{cases}$$

Note that the roles of A, B in this application of the two-steps look-ahead extractor were flipped, compared to the previous application. Finally, the i^{th} row of W^j is defined by

$$W_i^j = \mathsf{Ext}_3\left(X_i, (C')_i^{j-1}\right).$$

The output of LCB is then defined by $\mathsf{LCB}(X, Y) = W^q$.

We now turn to the analysis, starting with the running-time. First, note that row W_i^j is a function only of the corresponding rows W_i^{j-1}, X_i and the weak-source Y. For computing each row $i \in [r]$, the algorithm runs for $q = O(\log r)$ iterations. In each iteration it checks which side of the current cut contains i, and performs a constant number of calls to various seeded extractors (Ext_3 and the two extractors $\mathsf{Ext}_1, \mathsf{Ext}_2$ within the two calls to $\mathsf{LookAheadExt}$). Thus, the running-time for computing each output row is $\mathrm{poly}(n, t, \log r, \log(1/\varepsilon))$, as claimed.

For $j = 1, \dots, q$, define $I_j \subseteq \mathcal{I}$ by

$$I_j = \{i_v \in \mathcal{I} \,:\, |\{g, i_v\} \cap S_j| = 1\}.$$

That is, I_j contains all vertices in $\mathcal{I}$ that are separated from g by the cut S_j. We further define $I_0 = \emptyset$, and let $\mathcal{I}_j = \cup_{j'=0}^{j} I_{j'}$. Note that $\mathcal{I}_j$ is the set of vertices in $\mathcal{I}$ that are separated from g by at least one of the cuts $S_1, \dots, S_j$. By the property of the sequence $S_1, \dots, S_q$, we have that $\mathcal{I}_q = \mathcal{I}$. We prove the following claim by induction on j.

Claim 6.3. *There exists an (X, Y)-history $\mathcal{H}_j$ such that the following holds:*

- *$\mathcal{H}_j$ contains $\left\{W_i^j \mid i \in \mathcal{I}_j\right\}$.*
- *$\mathcal{H}_j$ contains $\left\{(C')_i^{j-1} \mid i \in \mathcal{I} \cup \{g\}\right\}$ for all $j \geq 1$.*
- *$\left(W_g^j, \mathcal{H}_j\right) \approx_{\varepsilon_j} (U_h, \mathcal{H}_j)$, where $\varepsilon_0 = 0$ and $\varepsilon_j \leq 2\varepsilon_{j-1} + 16\varepsilon'$ for all $j \geq 1$.*
- *$\widetilde{H}_\infty(X_g \mid \mathcal{H}_j) \geq \ell - 5htj$.*
- *$\widetilde{H}_\infty(Y \mid \mathcal{H}_j) \geq k - 5atj$.*

Proof of Claim 6.3. We prove the claim by induction on j. The claim readily follows for $j = 0$ with an empty (X, Y)-history $\mathcal{H}_0$. Consider $j \geq 1$ and assume the correctness of the claim for $j - 1$. By the induction hypothesis, we have that

$$\left(W_g^{j-1}, \mathcal{H}_{j-1}\right) \approx_{\varepsilon_{j-1}} (U_h, \cdot).$$

Recall that

$$W_g^{j-1} = \begin{cases} (X_g)\,|_h, & j = 1; \\ \mathsf{Ext}_3\left(X_g, (C')_g^{j-2}\right), & j > 1. \end{cases}$$

If $j = 1$ then clearly W_g^{j-1} is a deterministic function of X. For $j > 1$, by the induction hypothesis, $\mathcal{H}_{j-1}$ contains $(C')_g^{j-2}$ and so W_g^{j-1} is a deterministic function of $X, \mathcal{H}_{j-1}$. Moreover, by the induction hypothesis $\{W_i^{j-1} \mid i \in \mathcal{I}_{j-1}\}$ are all contained in $\mathcal{H}_{j-1}$. Since C_i^{j-1} is a deterministic function of W_i^{j-1} and Y, we have that $\{C_i^{j-1} \mid i \in \mathcal{I}_{j-1}\}$ are all deterministic functions of $\mathcal{H}_{j-1}$ and Y. Thus, we can apply Lemma 3.4 to the (X,Y)-history $\mathcal{H}_{j-1}$ with $P = W_g^{j-1}$ and $J = \{C_i^{j-1} \mid i \in \mathcal{I}_{j-1}\}$, and conclude that

$$\left(W_g^{j-1}, \left\{C_i^{j-1}\right\}_{i\in\mathcal{I}_{j-1}}, \mathcal{H}_{j-1}\right) \approx_{\varepsilon_{j-1}} (U_h, \cdot)\,, \tag{6.2}$$

and that $\left\{C_i^{j-1} \mid i \in \mathcal{I}_{j-1}\right\}, \mathcal{H}_{j-1}$ is an (X,Y)-history. In terms of entropy-loss, by Lemma 2.12 and by the induction hypothesis,

$$\begin{aligned} \widetilde{H}_\infty\left(Y \mid \left\{C_i^{j-1}\right\}_{i\in\mathcal{I}_{j-1}}, \mathcal{H}_{j-1}\right) &\geq \widetilde{H}_\infty\left(Y \mid \mathcal{H}_{j-1}\right) - |\mathcal{I}_{j-1}| \cdot a \\ &\geq k - 5atj + 4at + a, \end{aligned} \tag{6.3}$$

where we used the fact that $|\mathcal{I}_{j-1}| \leq |\mathcal{I}| \leq t-1$ and that $|C_i^{j-1}| = a$ for all $i \in \mathcal{I}_{j-1}$. As for the entropy of X_g, we have that

$$\widetilde{H}_\infty\left(X_g \mid \left\{C_i^{j-1}\right\}_{i\in\mathcal{I}_{j-1}}, \mathcal{H}_{j-1}\right) = \widetilde{H}_\infty\left(X_g \mid \mathcal{H}_{j-1}\right) \geq \ell - 5ht(j-1), \tag{6.4}$$

where the first equality holds by Lemma 2.14 and by the induction hypothesis. Indeed, the induction hypothesis implies that all random variables $\left\{W_i^{j-1} \mid i \in \mathcal{I}_{j-1}\right\}$ are contained in $\mathcal{H}_{j-1}$. Since C_i^{j-1} is a deterministic function of W_i^{j-1} and Y, it holds that conditioned on any fixing of $\mathcal{H}_{j-1}$, the random variables $\left\{C_i^{j-1} \mid i \in \mathcal{I}_{j-1}\right\}$ are deterministic functions of Y, and thus are independent of X_g. The second inequality follows by the induction hypothesis.

We proceed with the analysis by considering two cases, according to whether or not $g \in S_j$.

Case 1: $\mathbf{g} \in \mathbf{S_j}$. Recall that $A_g^{j-1} = \mathsf{Ext}_1(Y, (W_g^{j-1})|_s)$. We apply Lemma 3.3 to the (X,Y)-history $\left\{C_i^{j-1} \mid i \in \mathcal{I}_{j-1}\right\}, \mathcal{H}_{j-1}$, with $P = \left(W_g^{j-1}\right)|_s$, $M = Y$ and the extractor Ext_1. The hypothesis of Lemma 3.3 is met since, as explained above, W_g^{j-1} is a deterministic function of X and $\mathcal{H}_{j-1}$. Furthermore, Equation (3.2) of Lemma 3.3 follows by Equation (6.3), the fact that Ext_1 is a strong seeded extractor for entropy $2a$ with error ε', and our assumption on k, namely, Equation (6.1). Thus, Lemma 3.3 together with Equation (6.2) imply that

$$\left(A_g^{j-1}, \mathcal{H}'_{j-1}\right) \approx_{\varepsilon_{j-1}+2\varepsilon'} (U_a, \cdot)\,,$$

where

$$\mathcal{H}'_{j-1} = \left(W_g^{j-1}, \left\{C_i^{j-1}\right\}_{i\in\mathcal{I}_{j-1}}, \mathcal{H}_{j-1}\right)$$

is an (X,Y)-history. Note that we added W_g^{j-1} rather than $(W_g^{j-1})|_s$ to $\mathcal{H}'_{j-1}$. This can be done either by applying Lemma 3.4 or by considering the extractor Ext'_1 that takes W_g^{j-1} as the seed, ignore the length $h-s$ suffix of it and use $(W_g^{j-1})|_s$ as a seed for Ext_1. In terms of entropy-loss,

$$\widetilde{H}_\infty\left(X_g \mid \mathcal{H}'_{j-1}\right) \geq \widetilde{H}_\infty\left(X_g \mid \left\{C_i^{j-1}\right\}_{i\in\mathcal{I}_{j-1}}, \mathcal{H}_{j-1}\right) - \left|W_g^{j-1}\right| \geq \ell - 5htj + 5ht - h, \tag{6.5}$$

where the first inequality follows by Lemma 2.12, and the second inequality follows by Equation (6.4).

We now apply Lemma 3.4 to the (X, Y)-history $\mathcal{H}'_{j-1}$, with $P = A_g^{j-1}$ and

$$J = \left\{ (W')_i^{j-1} \mid i \in \mathcal{I}_{j-1} \right\} \cup \left\{ W_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_{j-1} \right\}.$$

To see that this application of Lemma 3.4 is valid, note that A_g^{j-1} is a deterministic function of Y and W_g^{j-1}, and the latter is contained in $\mathcal{H}'_{j-1}$ – the history to which we apply the lemma. On the other hand, each of the random variables in $\left\{ (W')_i^{j-1} \mid i \in \mathcal{I}_{j-1} \right\}$ is a deterministic function of X and $\left\{ C_i^{j-1} \mid i \in \mathcal{I}_{j-1} \right\}$, all of which are contained in $\mathcal{H}'_{j-1}$. Moreover, as explained above, $\left\{ W_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_{j-1} \right\}$ are all deterministic functions of X and $\mathcal{H}_{j-1}$ (this was shown for $i = g$ but can be easily shown to hold for all $i \in \mathcal{I} \cup \{g\}$). Thus, Lemma 3.4 implies that

$$\left(A_g^{j-1}, \left\{ (W')_i^{j-1} \right\}_{i \in \mathcal{I}_{j-1}}, \left\{ W_i^{j-1} \right\}_{i \in \mathcal{I} \setminus \mathcal{I}_{j-1}}, \mathcal{H}'_{j-1} \right) \approx_{\varepsilon_{j-1} + 2\varepsilon'} (U_a, \cdot),$$

and that $\left\{ (W')_i^{j-1} \mid i \in \mathcal{I}_{j-1} \right\}$, $\left\{ W_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_{j-1} \right\}$, $\mathcal{H}'_{j-1}$ is an (X, Y)-history. In terms of entropy-loss, Equation (6.5) together with Lemma 2.12 imply that

$$\begin{aligned} \widetilde{H}_\infty \left(X_g \mid \left\{ (W')_i^{j-1} \right\}_{i \in \mathcal{I}_{j-1}}, \left\{ W_i^{j-1} \right\}_{i \in \mathcal{I} \setminus \mathcal{I}_{j-1}}, \mathcal{H}'_{j-1} \right) &\geq \widetilde{H}_\infty \left(X_g \mid \mathcal{H}'_{j-1} \right) - |\mathcal{I}| \cdot h \\ &\geq \ell - 5htj + 4ht. \end{aligned} \tag{6.6}$$

Recall that $(W')_g^{j-1} = \mathsf{Ext}_3 \left(X_g, C_g^{j-1} \right)$. Since $g \in S_j$ it holds that $C_g^{j-1} = A_g^{j-1}$. We apply Lemma 3.3 to the (X, Y)-history $\left\{ (W')_i^{j-1} \mid i \in \mathcal{I}_{j-1} \right\}$, $\left\{ W_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_{j-1} \right\}$, $\mathcal{H}'_{j-1}$, with $P = A_g^{j-1} = C_g^{j-1}$, $M = X_g$ and the extractor Ext_3. The hypothesis of Lemma 3.3 is met since A_g^{j-1} is a deterministic function of Y and W_g^{j-1}, and the latter in contained in the (X, Y)-history to which we apply the lemma. Furthermore, Equation (3.2) of Lemma 3.3 follows by Equation (6.6) and our hypothesis on k, namely, Equation (6.1), and since Ext_3 is a strong seeded extractor for entropy $2h$ with error ε'. Therefore, Lemma 3.3 implies that

$$\left((W')_g^{j-1}, \mathcal{H}''_{j-1} \right) \approx_{\varepsilon_{j-1} + 4\varepsilon'} (U_h, \cdot),$$

where

$$\mathcal{H}''_{j-1} = \left(A_g^{j-1}, \left\{ (W')_i^{j-1} \right\}_{i \in \mathcal{I}_{j-1}}, \left\{ W_i^{j-1} \right\}_{i \in \mathcal{I} \setminus \mathcal{I}_{j-1}}, \mathcal{H}'_{j-1} \right).$$

In terms of entropy-loss,

$$\begin{aligned} \widetilde{H}_\infty \left(Y \mid \mathcal{H}''_{j-1} \right) &\geq \widetilde{H}_\infty \left(Y \mid \left\{ (W')_i^{j-1} \right\}_{i \in \mathcal{I}_{j-1}}, \left\{ W_i^{j-1} \right\}_{i \in \mathcal{I} \setminus \mathcal{I}_{j-1}}, \mathcal{H}'_{j-1} \right) - a \\ &= \widetilde{H}_\infty \left(Y \mid \mathcal{H}'_{j-1} \right) - a \\ &= \widetilde{H}_\infty \left(Y \mid \left\{ C_i^{j-1} \right\}_{i \in \mathcal{I}_{j-1}}, \mathcal{H}_{j-1} \right) - a \\ &\geq k - 5atj + 4at, \end{aligned} \tag{6.7}$$

where the first inequality follows by Lemma 2.12, and since $|A_g^{j-1}| = a$. The second equality follows by Lemma 2.14, which is applicable since conditioned on any fixing of the random variables $\left\{C_i^{j-1} \mid i \in \mathcal{I}_{j-1}\right\}$, all of which are all contained in $\mathcal{H}'_{j-1}$, the random variables $\left\{(W')_i^{j-1} \mid i \in \mathcal{I}_{j-1}\right\}$ are deterministic functions of X, and in particular are independent of Y. Moreover, as explained above, conditioned on any fixing of $\mathcal{H}'_{j-1}$, the random variables $\left\{W_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_{j-1}\right\}$ are deterministic functions of X. The third equality follows by Lemma 2.14 as W_g^{j-1} is a deterministic function of X and $\mathcal{H}_{j-1}$. The last inequality follows by Equation (6.3).

We now apply Lemma 3.4 to the (X,Y)-history $\mathcal{H}''_{j-1}$, with $P = (W')_g^{j-1}$ and

$$J = \left\{(C')_i^{j-1} \mid i \in \mathcal{I}_{j-1}\right\} \cup \left\{C_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_{j-1}\right\}.$$

This application of Lemma 3.4 is valid since $(W')_g^{j-1}$ is a deterministic function of X, C_g^{j-1}, and C_g^{j-1} is contained in the history to which we apply the lemma. This is because $C_g^{j-1} = A_g^{j-1}$ since $g \in S_j$. On the other hand, each random variable in $\left\{(C')_i^{j-1} \mid i \in \mathcal{I}_{j-1}\right\}$ is a deterministic function of Y and $(W')_i^{j-1}$, and all of the random variables $\left\{(W')_i^{j-1} \mid i \in \mathcal{I}_{j-1}\right\}$ are contained in the $\mathcal{H}''_{j-1}$. Furthermore, each of the random variables in $\left\{C_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_{j-1}\right\}$ is a deterministic function of Y and $\left\{W_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_{j-1}\right\}$, and the latter random variables are all contained in $\mathcal{H}''_{j-1}$. Thus, Lemma 3.4 implies that

$$\left((W')_g^{j-1}, \mathcal{H}'''_{j-1}\right) \approx_{\varepsilon_{j-1}+4\varepsilon'} (U_h, \cdot)\,, \tag{6.8}$$

where

$$\mathcal{H}'''_{j-1} = \left(\left\{(C')_i^{j-1}\right\}_{i \in \mathcal{I}_{j-1}}, \left\{C_i^{j-1}\right\}_{i \in \mathcal{I} \setminus \mathcal{I}_{j-1}}, \mathcal{H}''_{j-1}\right)$$

is an (X,Y)-history. By Lemma 2.12, Equation (6.7) and the fact that $|\mathcal{I}| = t-1$, it holds that

$$\widetilde{H}_\infty\left(Y \mid \mathcal{H}'''_{j-1}\right) \geq \widetilde{H}_\infty\left(Y \mid \mathcal{H}''_{j-1}\right) - |\mathcal{I}| \cdot a \geq k - 5atj + 3at + a. \tag{6.9}$$

Note that all random variables $\left\{C_i^{j-1} \mid i \in \mathcal{I} \cup \{g\}\right\}$ are contained in $\mathcal{H}'''_{j-1}$. Indeed, $\left\{C_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_{j-1}\right\}$ are contained in $\mathcal{H}'''_{j-1}$ by definition. Moreover, the random variables $\left\{C_i^{j-1} \mid i \in \mathcal{I}_{j-1}\right\}$ are contained in $\mathcal{H}'_{j-1}$ which in turn is contained in $\mathcal{H}'''_{j-1}$. Finally, since $g \in S_j$, it holds that $C_g^{j-1} = A_g^{j-1}$, and A_g^{j-1} is contained in $\mathcal{H}''_{j-1}$, and so it is also contained in $\mathcal{H}'''_{j-1}$.

We apply Lemma 4.1 to the (X,Y)-history $\mathcal{H}'''_{j-1}$, with W (in the notation of Lemma 4.1) equals to rows $\mathcal{I} \cup \{g\}$ of $(W')^{j-1}$. The hypothesis of Lemma 4.1 is met since these rows of $(W')^{j-1}$ are deterministic functions of X and $\left\{C_i^{j-1} \mid i \in \mathcal{I} \cup \{g\}\right\}$ which, by the above, are contained in $\mathcal{H}'''_{j-1}$. Furthermore, Equation (4.1) of Lemma 4.1 follows by Equation (6.9), and Equation (4.2) follows by our choice of h. Lemma 4.1 together with Equation (6.8) imply that

$$\left((B')_g^{j-1}, \mathcal{H}''''_{j-1}\right) \approx_{2\varepsilon_{j-1}+14\varepsilon'} (U_a, \cdot)\,,$$

where

$$\mathcal{H}''''_{j-1} = \left(\left\{(W')_i^{j-1}\right\}_{i \in \mathcal{I} \cup \{g\}}, (Z')_g^{j-1}, \left\{(A')_i^{j-1}\right\}_{i \in \mathcal{I} \cup \{g\}}, \left\{\left((W')_i^{j-1}\right)|_s\right\}_{i \in \mathcal{I} \cup \{g\}}, \mathcal{H}'''_{j-1}\right)$$

is an (X, Y)-history. Moreover, by the third item of Lemma 4.1 and Equation (6.9), we have that

$$\widetilde{H}_\infty\left(Y \mid \mathcal{H}''''_{j-1}\right) \geq \widetilde{H}_\infty\left(Y \mid \mathcal{H}'''_{j-1}\right) - |\mathcal{I} \cup \{g\}| \cdot a \geq k - 5atj + 2at + a. \tag{6.10}$$

As for the entropy-loss of X_g, it holds that

$$\begin{aligned}
\widetilde{H}_\infty\left(X_g \mid \mathcal{H}''''_{j-1}\right) &\geq \widetilde{H}_\infty\left(X_g \mid \mathcal{H}'''_{j-1}\right) - |\mathcal{I} \cup \{g\}| \cdot h \\
&= \widetilde{H}_\infty\left(X_g \mid \mathcal{H}'''_{j-1}\right) - th \\
&= \widetilde{H}_\infty\left(X_g \mid \mathcal{H}''_{j-1}\right) - th \\
&= \widetilde{H}_\infty\left(X_g \mid \left\{(W')_i^{j-1}\right\}_{i \in \mathcal{I}_{j-1}}, \left\{W_i^{j-1}\right\}_{i \in \mathcal{I} \setminus \mathcal{I}_{j-1}}, \mathcal{H}'_{j-1}\right) - th \\
&\geq \widetilde{H}_\infty\left(X_g \mid \mathcal{H}'_{j-1}\right) - (2t-1)h \\
&\geq \ell - 5htj + 2ht + h,
\end{aligned} \tag{6.11}$$

where the first inequality follows by the fourth item of Lemma 4.1, with $N = X_g$. The second equality follows since $|\mathcal{I} \cup \{g\}| = t$. The third equality follows by Lemma 2.14 and the fact that conditioned on any fixing of $\mathcal{H}''_{j-1}$, all random variables $\left\{(C')_i^{j-1} \mid i \in \mathcal{I}_{j-1}\right\}$, $\left\{C_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_{j-1}\right\}$ are deterministic functions of Y. The fourth equality follows by Lemma 2.14 since A_g^{j-1} is a deterministic function of Y conditioned on any fixing of $\mathcal{H}'_{j-1}$. The penultimate inequality follows by Lemma 2.12. The last inequality follows by Equation (6.6).

Recall that $\left\{(C')_i^{j-1} \mid i \in \mathcal{I}_{j-1}\right\}$ are contained in $\mathcal{H}''''_{j-1}$, as these random variables are already contained in $\mathcal{H}'''_{j-1}$. However, due to the application of Lemma 4.1 above, we have that $\left\{(C')_i^{j-1} \mid i \in \mathcal{I}_j\right\}$ are all contained in $\mathcal{H}''''_{j-1}$. To see this, note that after the application of the two-steps look-ahead extractor, $\left\{(A')_i^{j-1} \mid i \in \mathcal{I} \cup \{g\}\right\}$ are all contained in $\mathcal{H}''''_{j-1}$. However, $(A')_i^{j-1} = (C')_i^{j-1}$ for $i \notin S_j$, which is equivalent to $i \in I_j$ as $g \in S_j$. Since $\mathcal{I}_j = \mathcal{I}_{j-1} \cup I_j$, it follows that $(C')_i^{j-1}$ is contained in $\mathcal{H}''''_{j-1}$ for all $i \in \mathcal{I}_j$, as claimed.

We apply Lemma 3.4 to the (X, Y)-history $\mathcal{H}''''_{j-1}$ with $P = (B')_g^{j-1}$ and $J = \left\{W_i^j \mid i \in \mathcal{I}_j\right\}$, and conclude that

$$\left((B')_g^{j-1}, \left\{W_i^j\right\}_{i \in \mathcal{I}_j}, \mathcal{H}''''_{j-1}\right) \approx_{2\varepsilon_{j-1} + 14\varepsilon'} (U_a, \cdot)\,.$$

This application of Lemma 3.4 is valid since $(B')_g^{j-1}$ is a deterministic function of Y and $(W')_g^{j-1}$, which is contained in $\mathcal{H}''''_{j-1}$. Furthermore, the random variables $\left\{W_i^j \mid i \in \mathcal{I}_j\right\}$ are deterministic functions of X and $\left\{(C')_i^j \mid i \in \mathcal{I}_j\right\}$ which, by the above, are also contained in $\mathcal{H}''''_{j-1}$. By Equation (6.11) and Lemma 2.12, it holds that

$$\widetilde{H}_\infty\left(X_g \mid \left\{W_i^j\right\}_{i \in \mathcal{I}_j}, \mathcal{H}''''_{j-1}\right) \geq \widetilde{H}_\infty\left(X_g \mid \mathcal{H}''''_{j-1}\right) - (t-1)h \geq \ell - 5htj + ht + 2h. \tag{6.12}$$

We apply Lemma 3.3 to the (X, Y)-history $\left\{W_i^j \mid i \in \mathcal{I}_j\right\}, \mathcal{H}''''_{j-1}$ with $P = (B')_g^{j-1}$, $M = X_g$ and the extractor Ext_3. The hypothesis of Lemma 3.3 is met since $(B')_g^{j-1}$ is a deterministic function of Y and $(W')_g^{j-1}$, which is contained $\mathcal{H}''''_{j-1}$. Moreover, Equation (3.2) of Lemma 3.3 follows by Equation (6.12). Since $W_i^j = \mathsf{Ext}_3\left(X_i, (C')_i^{j-1}\right)$, and since $(C')_g^{j-1} = (B')_g^{j-1}$ (as $g \in S_j$), Lemma 3.3 implies that

$$\left(W_g^j, (B')_g^{j-1}, \left\{W_i^j\right\}_{i \in \mathcal{I}_j}, \mathcal{H}''''_{j-1}\right) \approx_{2\varepsilon_{j-1}+16\varepsilon'} (U_h, \cdot)\,.$$

Finally, we apply Lemma 3.4 to the (X, Y)-history $(B')_g^{j-1}$, $\left\{W_i^j \mid i \in \mathcal{I}_j\right\}$, $\mathcal{H}''''_{j-1}$, with $P = W_g^j$ and $J = \left\{(C')_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}$. This application of Lemma 3.4 is valid since W_g^j is a deterministic function of X and $(C')_g^{j-1}$, which is contained in the history to which we apply the lemma, since $(C')_g^{j-1} = (B')_g^{j-1}$ (recall that $g \in S_j$). Moreover, the random variables $\left\{(C')_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}$ are deterministic functions of Y and $\left\{(W')_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}$, all of which are contained in $\mathcal{H}''''_{j-1}$. Thus, Lemma 3.4 implies that

$$\left(W_g^j, \mathcal{H}_j\right) \approx_{2\varepsilon_{j-1}+16\varepsilon'} (U_h, \cdot)\,,$$

where

$$\mathcal{H}_j = \left(\left\{(C')_i^{j-1}\right\}_{i \in \mathcal{I} \setminus \mathcal{I}_j}, (B')_g^{j-1}, \left\{W_i^j\right\}_{i \in \mathcal{I}_j}, \mathcal{H}''''_{j-1}\right)$$

is an (X, Y)-history. This proves the third item of the claim. Note that $\mathcal{H}_j$ contains $\left\{W_i^j \mid i \in \mathcal{I}_j\right\}$, which proves the first item of the claim.

As for the second item, as proved above, $\left\{(C')_i^{j-1} \mid i \in \mathcal{I}_j\right\}$ are contained in $\mathcal{H}''''_{j-1}$ and therefore also contained in $\mathcal{H}_j$. Moreover, by definition, $\left\{(C')_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}$ are contained in $\mathcal{H}_j$, and so all random variables $\left\{(C')_i^{j-1} \mid i \in \mathcal{I}\right\}$ are contained in $\mathcal{H}_j$. Finally, since $g \in S_j$ it holds that $(C')_g^{j-1} = (B')_g^{j-1}$, and the latter is contained in $\mathcal{H}_j$. To summarize, all random variables $\left\{(C')_i^{j-1} \mid i \in \mathcal{I} \cup \{g\}\right\}$ are contained in $\mathcal{H}_j$, and so the second item of the claim follows.

The fourth item of the claim follows by Equation (6.12), Lemma 2.14 and the fact that $(B')_g^{j-1}$ and $\left\{(C')_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}$ are all deterministic functions of Y and $\left\{(W')_i^{j-1} \mid i \in \mathcal{I} \cup \{g\}\right\}$. As for the fifth item,

$$\begin{aligned}
\widetilde{H}_\infty\left(Y \mid \mathcal{H}_j\right) &\geq \widetilde{H}_\infty\left(Y \mid \left\{W_i^j\right\}_{i \in \mathcal{I}_j}, \mathcal{H}''''_{j-1}\right) - \left(|\mathcal{I} \setminus \mathcal{I}_j| + 1\right) \cdot a \\
&= \widetilde{H}_\infty\left(Y \mid \mathcal{H}'''_{j-1}\right) - \left(|\mathcal{I} \setminus \mathcal{I}_j| + 1\right) \cdot a \\
&\geq k - 5atj + at + a,
\end{aligned}$$

where the first inequality follows by Lemma 2.12. The second equality follows by Lemma 2.14, which is applicable as conditioned on any fixing of $\mathcal{H}''''_{j-1}$, the random variables $\{W_i^j \mid i \in \mathcal{I}_j\}$ are deterministic functions of X. Indeed, W_i^j is a deterministic function of X and $(C')_i^{j-1}$, and as shown above, all random variables $\{(C')_i^{j-1} \mid i \in \mathcal{I}_j\}$ are contained in $\mathcal{H}''''_{j-1}$. The last inequality follows by Equation (6.10).

Case 2: $\mathbf{g \notin S_j}$. We continue from Equation (6.2), and apply Lemma 4.1 to the (X,Y)-history $\left\{C_i^{j-1} \mid i \in \mathcal{I}_{j-1}\right\}, \mathcal{H}_{j-1}$, and rows $\mathcal{I} \cup \{g\}$ of W^{j-1}. We note that the hypothesis of Lemma 4.1 is met. Indeed, as shown above, for any $i \in \mathcal{I} \cup \{g\}$, W_i^{j-1} is a deterministic function of X and $\mathcal{H}_{j-1}$. Moreover, Equation (4.1) of Lemma 4.1 follows by Equation (6.3), and Equation (4.2) follows by our choice of h. Therefore, by Lemma 4.1 and Equation (6.2) we have that

$$\left(B_g^{j-1}, \mathcal{H}'_{j-1}\right) \approx_{2\varepsilon_{j-1}+6\varepsilon'} (U_a, \cdot),$$

where

$$\mathcal{H}'_{j-1} = \left(\left\{W_i^{j-1}\right\}_{i \in \mathcal{I} \cup \{g\}}, Z_g^{j-1}, \left\{A_i^{j-1}\right\}_{i \in \mathcal{I} \cup \{g\}}, \left\{\left(W_i^{j-1}\right)|_s\right\}_{i \in \mathcal{I} \cup \{g\}}, \left\{C_i^{j-1}\right\}_{i \in \mathcal{I}_{j-1}}, \mathcal{H}_{j-1}\right)$$

is an (X,Y)-history. Furthermore, by the third item of Lemma 4.1 and by Equation (6.3) it holds that

$$\widetilde{H}_\infty\left(Y \mid \mathcal{H}'_{j-1}\right) \ge \widetilde{H}_\infty\left(Y \mid \left\{C_i^{j-1}\right\}_{i \in \mathcal{I}_{j-1}}, \mathcal{H}_{j-1}\right) - |\mathcal{I} \cup \{g\}| \cdot a \ge k - 5atj + 3at + a. \quad (6.13)$$

The fourth item of Lemma 4.1, with $N = X_G$, together with Equation (6.4) imply that

$$\widetilde{H}_\infty\left(X_g \mid \mathcal{H}'_{j-1}\right) \ge \widetilde{H}_\infty\left(X_g \mid \left\{C_i^{j-1}\right\}_{i \in \mathcal{I}_{j-1}}, \mathcal{H}_{j-1}\right) - |\mathcal{I} \cup \{g\}| \cdot h \ge \ell - 5htj + 4ht. \quad (6.14)$$

Note that $\left\{C_i^{j-1} \mid i \in \mathcal{I}_{j-1}\right\}$ are all contained in $\mathcal{H}'_{j-1}$ even prior to the application of the two-steps look-ahead extractor. But in fact, after this application, all random variables in $\left\{C_i^{j-1} \mid i \in \mathcal{I}_j\right\}$ are contianed in $\mathcal{H}'_{j-1}$. To see this, recall that $A_i^{j-1} = C_i^{j-1}$ for all $i \in S_j$. Furthermore, $i \in S_j \iff i \in I_j$ as $g \notin S_j$. Since $\mathcal{I}_j = \mathcal{I}_{j-1} \cup I_j$, and since $\{A_i^{j-1} \mid i \in \mathcal{I} \cup \{g\}\}$ are all contained in $\mathcal{H}'_{j-1}$, the claimed assertion follows. Namely, for all $i \in \mathcal{I}_j$, the random variable C_i^{j-1} is contained in $\mathcal{H}'_{j-1}$.

We now apply Lemma 3.4 to the (X,Y)-history $\mathcal{H}'_{j-1}$, with $P = B_g^{j-1}$ and $J = \left\{(W')_i^{j-1} \mid i \in \mathcal{I}_j\right\}$. Lemma 3.4 is applicable as B_g^{j-1} is a deterministic function of Y and W_g^{j-1}, which is contained in $\mathcal{H}'_{j-1}$. Moreover, by the above, for each $i \in \mathcal{I}_j$, the random variable C_i^{j-1} is contained in $\mathcal{H}'_{j-1}$, and so $\left\{(W')_i^{j-1} \mid i \in \mathcal{I}_j\right\}$ are all deterministic functions of X and $\mathcal{H}'_{j-1}$. Thus, Lemma 3.4 implies that

$$\left(B_g^{j-1}, \left\{(W')_i^{j-1}\right\}_{i \in \mathcal{I}_j}, \mathcal{H}'_{j-1}\right) \approx_{2\varepsilon_{j-1}+6\varepsilon'} (U_a, \cdot).$$

In terms of entropy-loss, Lemma 2.12 together with Equation (6.14) imply that

$$\widetilde{H}_\infty\left(X_g \mid \left\{(W')_i^{j-1}\right\}_{i \in \mathcal{I}_j}, \mathcal{H}'_{j-1}\right) \ge \widetilde{H}_\infty\left(X_g \mid \mathcal{H}'_{j-1}\right) - |\mathcal{I}_j| \cdot h \ge \ell - 5htj + 3ht + h. \quad (6.15)$$

We now apply Lemma 3.3 to the (X,Y)-history $\left\{(W')_i^{j-1} \mid i \in \mathcal{I}_j\right\}, \mathcal{H}'_{j-1}$, with $P = B_g^{j-1}$, $M = X_g$ and the extractor Ext_3. Recall that $(W')_g^{j-1} = \mathsf{Ext}_3\left(X_g, C_g^{j-1}\right)$. Since $g \notin S_j$, it follows that $C_g^{j-1} = B_g^{j-1}$. Thus, Lemma 3.3 implies that

$$\left((W')_g^{j-1}, B_g^{j-1}, \left\{(W')_i^{j-1}\right\}_{i \in \mathcal{I}_j}, \mathcal{H}'_{j-1}\right) \approx_{2\varepsilon_{j-1}+8\varepsilon'} (U_h, \cdot).$$

Lemma 3.3 is applicable since B_g^{j-1} is a deterministic function of Y and W_g^{j-1}, which is contained in $\mathcal{H}'_{j-1}$. Furthermore, Equation (3.2) of Lemma 3.3 follows by Equation (6.15). In terms of entropy-loss, we have that

$$\begin{aligned}\widetilde{H}_\infty\left(Y \mid B_g^{j-1}, \left\{(W')_i^{j-1}\right\}_{i\in\mathcal{I}_j}, \mathcal{H}'_{j-1}\right) &\geq \widetilde{H}_\infty\left(Y \mid \left\{(W')_i^{j-1}\right\}_{i\in\mathcal{I}_j}, \mathcal{H}'_{j-1}\right) - a \\ &= \widetilde{H}_\infty\left(Y \mid \mathcal{H}'_{j-1}\right) - a \\ &\geq k - 5atj + 3at, \end{aligned} \tag{6.16}$$

where the first inequality follows by Lemma 2.12 and the fact that $\left|B_g^{j-1}\right| = a$. The second equality follows by Lemma 2.14 and the fact that conditioned on any fixing of $\mathcal{H}'_{j-1}$, each random variable in $\left\{(W')_i^{j-1} \mid i \in \mathcal{I}_j\right\}$ is a deterministic function of X. Indeed, as shown above, $\left\{C_i^{j-1} \mid i \in \mathcal{I}_j\right\}$ are all contained in $\mathcal{H}'_{j-1}$. The last inequality follows by Equation (6.13).

We now apply Lemma 3.4 to the (X,Y)-history B_g^{j-1}, $\left\{(W')_i^{j-1} \mid i \in \mathcal{I}_j\right\}$, $\mathcal{H}'_{j-1}$, with $P = (W')_g^{j-1}$ and

$$J = \left\{(C')_i^{j-1} \mid i \in \mathcal{I}_j\right\} \cup \left\{C_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}.$$

Lemma 3.4 is applicable since $(W')_g^{j-1}$ is a deterministic function of X and $C_g^{j-1} = B_g^{j-1}$, which is contained in $\mathcal{H}'_{j-1}$. On the other hand, each random variable in $\left\{(C')_i^{j-1} \mid i \in \mathcal{I}_j\right\}$ is a deterministic function of Y and $\left\{(W')_i^{j-1} \mid i \in \mathcal{I}_j\right\}$, and the latter are contained in the history to which we apply the lemma. Similarly, every random variable in $\left\{C_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}$ is a deterministic function of Y and $\left\{W_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}$, and the latter are contained in $\mathcal{H}'_{j-1}$. We conclude that

$$\left((W')_g^{j-1}, \mathcal{H}''_{j-1}\right) \approx_{2\varepsilon_{j-1}+8\varepsilon'} \left(U_h, \cdot\right),$$

where

$$\mathcal{H}''_{j-1} = \left(\left\{(C')_i^{j-1}\right\}_{i\in\mathcal{I}_j}, \left\{C_i^{j-1}\right\}_{i\in\mathcal{I}\setminus\mathcal{I}_j}, B_g^{j-1}, \left\{(W')_i^{j-1}\right\}_{i\in\mathcal{I}_j}, \mathcal{H}'_{j-1}\right).$$

In terms of entropy, Equation (6.16) together with Lemma 2.12 imply that

$$\begin{aligned}\widetilde{H}_\infty\left(Y \mid \mathcal{H}''_{j-1}\right) &\geq \widetilde{H}_\infty\left(Y \mid B_g^{j-1}, \left\{(W')_i^{j-1}\right\}_{i\in\mathcal{I}_j}, \mathcal{H}'_{j-1}\right) - |\mathcal{I}| \cdot a \\ &\geq k - 5atj + 2at + a. \end{aligned} \tag{6.17}$$

Recall that $(A')_g^{j-1} = \mathsf{Ext}_1(Y, ((W')_g^{j-1})|_s)$. We apply Lemma 3.3 to the (X,Y)-history $\mathcal{H}''_{j-1}$ with $P = ((W')_g^{j-1})|_s$, $M = Y$ and the extractor Ext_1. Lemma 3.3 is applicable since $(W')_g^{j-1}$ is a deterministic function of X and $C_g^{j-1} = B_g^{j-1}$, which is contained in $\mathcal{H}''_{j-1}$. Furthermore, Equation (3.2) of Lemma 3.3 holds by Equation (6.17). Thus, Lemma 3.3 implies that

$$\left((A')_g^{j-1}, (W')_g^{j-1}, \mathcal{H}''_{j-1}\right) \approx_{2\varepsilon_{j-1}+10\varepsilon'} \left(U_a, \cdot\right).$$

In terms of entropy-loss, we have that

$$\begin{aligned}\widetilde{H}_\infty\left(X_g \mid (W')_g^{j-1}, \mathcal{H}''_{j-1}\right) &\geq \widetilde{H}_\infty\left(X_g \mid \mathcal{H}''_{j-1}\right) - h \\ &= \widetilde{H}_\infty\left(X_g \mid \left\{(W')_i^{j-1}\right\}_{i\in\mathcal{I}_j}, \mathcal{H}'_{j-1}\right) - h \\ &\geq \ell - 5htj + 3ht, \end{aligned} \tag{6.18}$$

where the first inequality follows by Lemma 2.12 and the fact that $\left|(W')_g^{j-1}\right| = h$. The second equality follows by Lemma 2.14 which is applicable as conditioned on any fixing of $\mathcal{H}'_{j-1}$, all random variables $\left\{(C')_i^{j-1} \mid i \in \mathcal{I}_j\right\}$, $\left\{C_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}$ and B_g^{j-1} are deterministic functions of Y. The last inequality follows by Equation (6.15).

Next we apply Lemma 3.4 to the (X,Y)-history $(W')_g^{j-1}, \mathcal{H}''_{j-1}$, with $P = (A')_g^{j-1}$ and

$$J = \left\{W_i^j \mid i \in \mathcal{I}_j\right\} \cup \left\{(W')_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}$$

to conclude that

$$\left((A')_g^{j-1}, \left\{W_i^j\right\}_{i \in \mathcal{I}_j}, \left\{(W')_i^{j-1}\right\}_{i \in \{g\} \cup \mathcal{I} \setminus \mathcal{I}_j}, \mathcal{H}''_{j-1}\right) \approx_{2\varepsilon_{j-1}+10\varepsilon'} (U_a, \cdot)\,.$$

This application of Lemma 3.4 is valid since $(A')_g^{j-1}$ is a deterministic function of Y and $(W')_g^{j-1}$, which is contained in the history to which we apply the lemma. On the other hand, $\left\{W_i^j \mid i \in \mathcal{I}_j\right\}$ are all deterministic functions of X and $\left\{(C')_i^j \mid i \in \mathcal{I}_j\right\}$, all of which are contained in $\mathcal{H}''_{j-1}$. Furthermore, all random variables $\left\{(W')_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}$ are deterministic functions of X and $\left\{C_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}$, and these random variables are contained in $\mathcal{H}''_{j-1}$. As for the entropy-loss, Lemma 2.12 and Equation (6.18) imply that

$$\begin{aligned}\widetilde{H}_\infty\left(X_g \mid \left\{W_i^j\right\}_{i \in \mathcal{I}_j}, \left\{(W')_i^{j-1}\right\}_{i \in \{g\} \cup \mathcal{I} \setminus \mathcal{I}_j}, \mathcal{H}''_{j-1}\right) &\geq \widetilde{H}_\infty\left(X_g \mid (W')_g^{j-1}, \mathcal{H}''_{j-1}\right) - |\mathcal{I}| \cdot h \\ &\geq \ell - 5htj + 2ht + h. \end{aligned} \tag{6.19}$$

We apply Lemma 3.3 to the (X,Y)-history $\left\{W_i^j \mid i \in \mathcal{I}_j\right\}$, $\left\{(W')_i^{j-1} \mid i \in \{g\} \cup \mathcal{I} \setminus \mathcal{I}_j\right\}$, $\mathcal{H}''_{j-1}$, with $P = (A')_g^{j-1}$, $M = X_g$ and the extractor Ext_3. Recall that $W_g^j = \mathsf{Ext}_3\left(X_g, (C')_g^{j-1}\right)$. Since $g \notin S_j$, we have that $(C')_g^{j-1} = (A')_g^{j-1}$. Thus, Lemma 3.3 implies that

$$\left(W_g^j, (A')_g^{j-1}, \left\{W_i^j\right\}_{i \in \mathcal{I}_j}, \left\{(W')_i^{j-1}\right\}_{i \in \{g\} \cup \mathcal{I} \setminus \mathcal{I}_j}, \mathcal{H}''_{j-1}\right) \approx_{2\varepsilon_{j-1}+12\varepsilon'} (U_h, \cdot)\,.$$

We note that Lemma 3.3 is applicable since $(A')_g^{j-1}$ is a deterministic function of Y and $(W')_g^{j-1}$, which is contained in the history to which we apply the lemma. Furthermore, Equation (3.2) of Lemma 3.3 follows by Equation (6.19).

We apply Lemma 3.4 to the (X,Y)-history $(A')_g^{j-1}$, $\left\{W_i^j \mid i \in \mathcal{I}_j\right\}$, $\left\{(W')_i^{j-1} \mid i \in \{g\} \cup \mathcal{I} \setminus \mathcal{I}_j\right\}$, $\mathcal{H}''_{j-1}$, with $P = W_g^j$ and $J = \left\{(C')_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}$. Lemma 3.4 is applicable since W_g^j is a deterministic function of X and $(C')_g^{j-1}$. Recall that $(C')_g^{j-1} = (A')_g^{j-1}$ as $g \notin S_j$, and so $(C')_g^{j-1}$ is contained in the history to which we apply the lemma. Moreover, all random variables $\left\{(C')_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}$ are deterministic functions of Y and $\left\{(W')_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\right\}$ and these random variables are contained in the history to which we apply the lemma. Therefore, Lemma 3.4 implies that

$$\left(W_g^j, \mathcal{H}_j\right) \approx_{2\varepsilon_{j-1}+12\varepsilon'} (U_h, \cdot)\,,$$

where

$$\mathcal{H}_j = \left(\left\{(C')_i^{j-1}\right\}_{i \in \mathcal{I} \setminus \mathcal{I}_j}, (A')_g^{j-1}, \left\{W_i^j\right\}_{i \in \mathcal{I}_j}, \left\{(W')_i^{j-1}\right\}_{i \in \{g\} \cup \mathcal{I} \setminus \mathcal{I}_j}, \mathcal{H}''_{j-1}\right).$$

This proves the third item of the claim. The first item of the claim holds since $\mathcal{H}_j$ contains $\{W_i^j \mid i \in \mathcal{I}_j\}$. To see that the second item follows, recall that $\{(C')_i^{j-1} \mid i \in \mathcal{I}_j\}$ are contained in $\mathcal{H}''_{j-1}$. By the last application of Lemma 3.4, the random variables $\{(C')_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\}$ are also contained in $\mathcal{H}_j$. Finally, since $g \notin S_j$ we have that $(C')_g^{j-1} = (A')_g^{j-1}$, which is also contained in $\mathcal{H}_j$. Thus, $\{(C')_i^{j-1} \mid i \in \mathcal{I} \cup \{g\}\}$ are all contained in $\mathcal{H}_j$, and the second item of the claim holds.

The fourth item follows by Equation (6.19), Lemma 2.14 and the fact that $(A')_g^{j-1}$ is a deterministic function of Y conditioned on the fixing of $(W')_g^{j-1}$, and $\{(C')_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\}$ are deterministic functions of Y conditioned on the fixing of $\{(W')_i^{j-1} \mid i \in \mathcal{I} \setminus \mathcal{I}_j\}$. The fifth item follows since

$$\begin{aligned}
\widetilde{H}_\infty(Y \mid \mathcal{H}_j) &\geq \widetilde{H}_\infty\left(Y \mid \{W_i^j\}_{i \in \mathcal{I}_j}, \{(W')_i^{j-1}\}_{i \in \{g\} \cup \mathcal{I} \setminus \mathcal{I}_j}, \mathcal{H}''_{j-1}\right) - (1 + |\mathcal{I} \setminus \mathcal{I}_j|) \cdot a \\
&= \widetilde{H}_\infty\left(Y \mid \mathcal{H}''_{j-1}\right) - (1 + |\mathcal{I} \setminus \mathcal{I}_j|) \cdot a \\
&\geq k - 5atj + at + a,
\end{aligned}$$

where the first inequality follows by Lemma 2.12. The second equality follows by Lemma 2.14 and the fact that conditioned on any fixing of $\mathcal{H}''_{j-1}$, the random variables $\{W_i^j \mid i \in \mathcal{I}_j\}$, $\{(W')_i^{j-1} \mid i \in \{g\} \cup \mathcal{I} \setminus \mathcal{I}_j\}$ are deterministic functions of X. The third inequality follows by Equation (6.17).

This concludes the proof for the case $g \notin S_j$. The proof of the claim then follows. □

By Claim 6.3 applied with $j = q$, we have that $\mathcal{H} \triangleq \mathcal{H}_q$ contains $\{W_i^j \mid i \in \mathcal{I}\}$ as $\mathcal{I} = \mathcal{I}_q$. Furthermore,

- $(W_g^q, \mathcal{H}) \approx_\varepsilon (U_h, \mathcal{H})$. This follows since

  $$\varepsilon_q \leq (2^q - 1) \cdot 16 \cdot \varepsilon' \leq 32r \cdot \varepsilon' \leq \varepsilon,$$

  where the second inequality follows since $q = \lceil \log_2 r \rceil$, and the last inequality holds by our choice of ε'.

- $\widetilde{H}_\infty(X_g \mid \mathcal{H}) \geq \ell - 5htq \geq 0.9\ell$.

- $\widetilde{H}_\infty(Y \mid \mathcal{H}) \geq k - 5atq \geq 0.9k$.

Since $\bar{W} = W^q$, the first three items of the theorem follows. As for the fourth item, recall that $\bar{W}_g = W_g^q = \mathsf{Ext}_3\left(X_g, (C')_g^{q-1}\right)$. The second item of the claim states that $(C')_g^{q-1}$ is contained in $\mathcal{H}_q$, and so W_g^q is a deterministic function of X and $\mathcal{H}$, as stated. This concludes the proof of the theorem. □

6.1 A comparison with [Li13]

As mentioned, our construction of LCBs builds on ideas by Li [Li13]. For the construction of his multi-source extractor, Li constructs an object related to LCBs that has a weaker guarantee. Namely, an output variable that corresponds to a good input variable is uniform even given some bounded number of any other output variables which correspond to *good* input variables. Since both Li's construction and ours are fairly technical, it might be hard to pinpoint the new ideas required so to guarantee the stronger property, and so in this section we highlight the differences between the two constructions.

To review the ideas used so to guarantee the stronger property of LCBs, we first give a high-level overview of Li's argument used for the construction of his related object. Let X be a random variable that has the form of an $r \times \ell$ matrix with the following property: there exists $G \subseteq [r]$ such that for each $i \in G$, X_i is uniform. Let Y be an independent weak-source. Given a parameter $t \geq 1$, Li's pseudorandom object produces an $r \times m$ matrix Z with the following property. For any $S \subseteq G$ with size at most t, it holds that the joint distribution of $\{Z_i \mid i \in S\}$ is close to uniform. To this end, Li's algorithm runs for $O(\log_t r)$ iterations, where the input for iteration i is a matrix X^i as well as X, Y, and the output is a matrix X^{i+1}. The output matrix Z is defined to be the output matrix produced by the last iteration. We set X^1 to be the h leftmost columns of X, for some sufficiently large integer h. In each iteration, the algorithm is defined as follows.

First, the algorithm applies a look-ahead extractor for t steps to each row $\ell \in [r]$ of X^i and Y. The output is a sequence of t "blocks" which we denote by $R^i_{\ell,1}, \ldots, R^i_{\ell,t}$. Then, the algorithm selects for each row ℓ one of these blocks according to some rule. The selected block is used as a seed for extracting from X_ℓ to obtain the ℓ^{th} row of the output matrix X^{i+1}. The rule for selecting the block is based on the representation of ℓ in base t. More precisely, the selected block corresponds to the i^{th} digit in this representation.

The analysis is as follows. Let $S \subseteq G$ and let $i_1 > i_2 > \cdots > i_t$ be the elements in S. Li shows that at some iteration j_1, row i_1 of X^{j_1} is uniform even given the rows of X^{j_1} indexed by $i_2, \ldots, i_t$. Moreover, this property is preserved throughout the remaining iterations (namely, for X^j with $j > j_1$). Similarly, at some iteration $j_2 \geq j_1$, row i_2 of X^{j_2} is uniform even given the rows of X^{j_2} with indices $i_3, \ldots, i_t$. Therefore, after all iterations were executed, for every $v \in [t]$, Z_{i_v} is close to uniform even given $(Z_{i_1}, \ldots, Z_{i_{v-1}})$. Thus, the joint distribution of the rows of Z indexed by S is close to uniform.

To construct our LCBs, our first observation is that one can simply use two-steps look-ahead extractors in the construction above, and there is no reason to use look-ahead extractors for t steps, where t is the parameter that determines the independence guarantee. This observation can also be used to simplify Li's construction and analysis without deteriorating the parameters. In fact, it seems to improve the parameters as although with the two-steps look-ahead extractors one needs to run for $\log_2 r$ iterations rather than for $\log_t r$ iterations, in each iteration one needs to fix only $2t$ blocks rather than t^2 blocks. This saves a factor of $t/\log t$ in entropy-loss. In the setting used by Li, $t = \text{polylog}(n)$, and so this saves a $\text{polylog}(n)$ factor in entropy-loss.

Our second idea, which becomes somewhat more transparent given the observation above, is the "flip-flip" idea. Using the "flip-flip" idea we can guarantee the stronger property we need (without any asymptotical cost in parameters). Namely, as we work with only two blocks (which we call A, B), we can break the correlation between a good row and *any* other row by first giving the B variable to one of the rows and the A variable to the second row, and then flip. Regardless of which row is good, at the end of this process the good row will be uniform even given the other row. We note that when working with t blocks, one can apply an analog strategy which will require t iterations. Indeed, while two blocks induce a partition of the complete graph on r vertices to two parts, t blocks induce a partition of the graph to t parts. One can then consider a cyclic assignment of the blocks to the different parts in the partition (though this will deteriorate the entropy requirement by another factor of t).

7 Mergers with Weak-Seeds

In this section we prove Theorem 1.5 using Theorem 6.2. We start by giving a formal definition of mergers with weak-seeds using the definition of somewhere-random sources. We further define strong mergers with weak-seeds. We then give a complete and formal restatement of Theorem 1.5 and present its proof.

Definition 7.1 (Mergers with weak-seeds)**.** *A function*

$$\mathsf{Merg}\colon \left(\{0,1\}^{\ell}\right)^{r} \times \{0,1\}^{n} \to \{0,1\}^{m}$$

is called a merger with weak-seeds *for entropy k, with error ε, if the following holds. For any $r \times \ell$ somewhere-random source X and an independent (n,k)-weak-source Y, it holds that*

$$\mathsf{Merg}(X,Y) \approx_{\varepsilon} U_m.$$

We say that Merg *is* strong *if*

$$\left(\mathsf{Merg}(X,Y),Y\right) \approx_{\varepsilon} \left(U_m,Y\right).$$

Theorem 7.2. *For all integers n,r and for any $\varepsilon > 0$, there exists a* $\mathrm{poly}(n,r,\log(1/\varepsilon))$*-time computable strong merger with weak-seeds for entropy k, with error ε,*

$$\mathsf{Merg}\colon \left(\{0,1\}^{\ell}\right)^{r} \times \{0,1\}^{n} \to \{0,1\}^{m},$$

with

$$\begin{aligned}
\ell &= \Theta\left(r^2 \cdot \log(r) \cdot \log\left(\frac{nr}{\varepsilon}\right)\right), \\
k &= \Omega\left(r \cdot \log(r) \cdot \log\left(\frac{r \cdot \log n}{\varepsilon}\right)\right), \\
m &= \ell/(2r).
\end{aligned}$$

Before proving the theorem, we remark that if one is willing to output $\Omega(\ell/(r\log r))$ bits rather than $\Omega(\ell/r)$, one can construct a merger with weak-seeds using the LCB from Theorem 6.2 in a slightly simpler way. Indeed, one can compute $W = \mathsf{LCB}(X,Y)$ with $t = r$ and then output $\mathsf{Merg}(X,Y) = \oplus_{i=1}^{r} W_i$. That is, one can skip the extra "round" that has the purpose of increasing the output length.

Proof of Theorem 7.2. We first describe the construction of Merg, and then turn to the analysis. To this end, we need the following building blocks.

- Let $\mathsf{LCB}\colon \left(\{0,1\}^{\ell}\right)^r \times \{0,1\}^n \to \left(\{0,1\}^h\right)^r$ be the t-LCB from Theorem 6.2, set with $t = r$ and error ε. Note that the hypothesis of Theorem 6.2 is met by our choice of ℓ, k. Furthermore, by Theorem 6.2, $h = \Theta(r \cdot \log(nr/\varepsilon))$.
- Set $s = \Theta(\log(\ell/\varepsilon)) = \Theta(\log(r \cdot \log(n)/\varepsilon))$. Let $\mathsf{Ext}_4\colon \{0,1\}^n \times \{0,1\}^h \to \{0,1\}^s$ be the strong seeded extractor from Theorem 2.2 for entropy $2s$, with error ε. Note that $h = \Omega(\log(n/\varepsilon))$, and so a seed of length h suffices for Theorem 2.2.
- Let $\mathsf{Ext}_5\colon \{0,1\}^{\ell} \times \{0,1\}^s \to \{0,1\}^m$ be the extractor from Theorem 2.2 for entropy $2m$, set to extract with error ε. Note that s was chosen so that a seed of length s suffices for Theorem 2.2.

The function Merg is defined as follows. First, we compute the $r \times h$ matrix $W = \mathsf{LCB}(X, Y)$. For each $i \in [r]$, we compute

$$Z_i = \mathsf{Ext}_4(Y, W_i),$$
$$T_i = \mathsf{Ext}_5(X_i, Z_i).$$

The output of $\mathsf{Merg}(X, Y)$ is then defined to be

$$\mathsf{Merg}(X, Y) = \bigoplus_{i=1}^{r} T_i\,.$$

We now turn to the analysis. Let $g \in [r]$ be such that X_g is uniformly distributed. By Theorem 6.2, applied with $\mathcal{I} = [r] \setminus \{g\}$, there exists an (X, Y)-history $\mathcal{H}$ that contains $\{W_i \mid i \in [r] \setminus \{g\}\}$, such that the following holds:

- $(W_g, \mathcal{H}) \approx_{\varepsilon} (U_h, \mathcal{H})$.
- $\widetilde{H}_{\infty}(X_g \mid \mathcal{H}) \geq 0.9 \cdot \ell$.
- $\widetilde{H}_{\infty}(Y \mid \mathcal{H}) \geq 0.9 \cdot k$.
- W_g is a deterministic function of X and $\mathcal{H}$.

We apply Lemma 3.4 to the (X, Y)-history $\mathcal{H}$ with $P = W_g$ and $J = \{Z_i \mid i \in [r] \setminus \{g\}\}$. Lemma 3.4 is applicable since W_g is a deterministic function of X and $\mathcal{H}$. Moreover, since $Z_i = \mathsf{Ext}_4\left(Y, W_i\right)$ and since $\{W_i \mid i \in [r] \setminus \{g\}\}$ are all contained in $\mathcal{H}$, the random variables $\{Z_i \mid i \in [r] \setminus \{g\}\}$ are deterministic functions of Y and $\mathcal{H}$. Therefore, Lemma 3.4 implies that

$$\left(W_g, \{Z_i\}_{i \in [r] \setminus \{g\}}, \mathcal{H}\right) \approx_{\varepsilon} \left(U_h, \cdot\right).$$

In terms of entropy, by Lemma 2.12, we have that

$$\widetilde{H}_\infty\left(Y \mid \{Z_i\}_{i\in[r]\setminus\{g\}}, \mathcal{H}\right) \geq 0.9k - (r-1)s \geq 2s + \log(1/\varepsilon). \tag{7.1}$$

We apply Lemma 3.3 to the (X, Y)-history $\{Z_i \mid i \in [r] \setminus \{g\}\}$, $\mathcal{H}$ with $P = W_g$, $M = Y$ and the extractor Ext_4. Lemma 3.3 is applicable since W_g is a deterministic function of X and $\mathcal{H}$. Furthermore, Equation (3.2) of Lemma 3.3 follows by Equation (7.1). Since $Z_g = \mathsf{Ext}_4(Y, W_g)$, we have that

$$\left(Z_g, W_g, \{Z_i\}_{i\in[r]\setminus\{g\}}, \mathcal{H}\right) \approx_{3\varepsilon} (U_s, \cdot)\,.$$

In terms of entropy,

$$\begin{aligned}\widetilde{H}_\infty\left(X_g \mid W_g, \{Z_i\}_{i\in[r]\setminus\{g\}}, \mathcal{H}\right) &\geq \widetilde{H}_\infty\left(X_g \mid \{Z_i\}_{i\in[r]\setminus\{g\}}, \mathcal{H}\right) - h \\ &= \widetilde{H}_\infty\left(X_g \mid \mathcal{H}\right) - h \\ &\geq 0.9\ell - h, \end{aligned} \tag{7.2}$$

where the first inequality follows by Lemma 2.12 and the fact that $|W_g| = h$. The second equality follows by Lemma 2.14 and since conditioned on the fixing of $\mathcal{H}$, the random variables $\{Z_i \mid i \in [r] \setminus \{g\}\}$ are all deterministic functions of Y.

Next we apply Lemma 3.4 to the (X, Y)-history W_g, $\{Z_i \mid i \in [r] \setminus \{g\}\}$, $\mathcal{H}$, with $P = Z_g$ and $J = \{T_i \mid i \in [r] \setminus \{g\}\}$. Lemma 3.4 is applicable since Z_g is a deterministic function of Y and W_g, and the latter is contained in the history to which we apply the lemma. On the other hand, $\{T_i \mid i \in [r] \setminus \{g\}\}$ are all deterministic functions of X and $\{Z_i \mid i \in [r] \setminus \{g\}\}$, all of which are contained in the history to which we apply the lemma. Lemma 3.4 implies that

$$\left(Z_g, \{T_i\}_{i\in[r]\setminus\{g\}}, W_g, \{Z_i\}_{i\in[r]\setminus\{g\}}, \mathcal{H}\right) \approx_{3\varepsilon} (U_s, \cdot)\,.$$

Equation (7.2) together with Lemma 2.12 imply that

$$\widetilde{H}_\infty\left(X_g \mid \{T_i\}_{i\in[r]\setminus\{g\}}, W_g, \{Z_i\}_{i\in[r]\setminus\{g\}}, \mathcal{H}\right) \geq 0.9\ell - h - (r-1)m \geq 2m + \log(1/\varepsilon). \tag{7.3}$$

Recall that $T_g = \mathsf{Ext}_5(X_g, Z_g)$. We apply Lemma 3.3 to the (X, Y)-history $\{T_i \mid i \in [r] \setminus \{g\}\}$, W_g, $\{Z_i \mid i \in [r] \setminus \{g\}\}$, $\mathcal{H}$, with $P = Z_g$ and $M = X_g$. The application of Lemma 3.3 is valid since Z_g is a deterministic function of Y and W_g, and the latter is contained in the history to which we apply the lemma. Furthermore, Equation (3.2) of Lemma 3.3 holds by Equation (7.3). Hence, Lemma 3.3 implies that

$$\left(T_g, Z_g, \{T_i\}_{i\in[r]\setminus\{g\}}, W_g, \{Z_i\}_{i\in[r]\setminus\{g\}}, \mathcal{H}\right) \approx_{5\varepsilon} (U_m, \cdot)\,.$$

We apply Lemma 3.4 to the (X, Y)-history Z_g, $\{T_i \mid i \in [r] \setminus \{g\}\}$, W_g, $\{Z_i \mid i \in [r] \setminus \{g\}\}$, $\mathcal{H}$ with $P = T_g$ and $J = Y$. This application of Lemma 3.4 is valid since T_g is a deterministic function of X and Z_g, and the latter is contained in the history to which we apply the lemma. Thus,

$$\left(T_g, Y, Z_g, \{T_i\}_{i\in[r]\setminus\{g\}}, W_g, \{Z_i\}_{i\in[r]\setminus\{g\}}, \mathcal{H}\right) \approx_{5\varepsilon} (U_m, \cdot) .$$

Lemma 2.8 then implies that

$$\left(T_g, \{T_i\}_{i\in[r]\setminus\{g\}}, Y\right) \approx_{5\varepsilon} (U_m, \cdot) .$$

Since $\mathsf{Merg}(X, Y) = \oplus_{i=1}^{r} T_i$, it holds that

$$\left(\mathsf{Merg}(X, Y), \{T_i\}_{i\in[r]\setminus\{g\}}, Y\right) \approx_{5\varepsilon} (U_m, \cdot) .$$

By applying Lemma 2.8 again, one get that

$$(\mathsf{Merg}(X, Y), Y) \approx_{5\varepsilon} (U_m, \cdot) .$$

Note further that the error can be reduced from 5ε to ε without affecting the theorem's hypothesis. This concludes the proof of the theorem. ☐

8 Three-Source Extractors with a Double-Logarithmic Entropy Source

In this section we prove Theorem 1.3. We give a formal restatement of the theorem here that accounts for the dependence in the error ε, as well as the strongness properties of the extractor.

Theorem 8.1. *There exist universal constants $0 < \alpha < 1 < c$ such that the following holds. For any integer n, $\varepsilon > 0$ and for any $\delta > \Omega((\log(n/\varepsilon)/n)^\alpha)$, there exists a* $\mathrm{poly}(n, \log(1/\varepsilon))$*-time computable three-source extractor* $\mathsf{3Ext}\colon (\{0,1\}^n)^3 \to \{0,1\}^m$*, with error ε, that is strong in $\{1,3\}$ and in $\{2,3\}$, for entropies*

$$\begin{aligned} k_1 &= \delta n, \\ k_2 &= \Omega\left((1/\delta)^{3c} \cdot \log(n/\varepsilon)\right), \\ k_3 &= \Omega\left((1/\delta)^{2c} \cdot \log\left(\frac{\log n}{\varepsilon}\right)\right). \end{aligned}$$

The number of output bits is $m = \Omega\left((1/\delta)^c \cdot \log(n/\varepsilon)\right)$.

For the proof of Theorem 8.1, we make use of the following two-source extractor of Raz [Raz05].

Theorem 8.2 ([Raz05]). *For all integers n_1, n_2, b_1, b_2, such that*

$$\begin{aligned} n_1 &\geq 6\log n_1 + 2\log n_2, \\ b_1 &\geq 0.6n_1 + 3\log n_1 + \log n_2, \\ b_2 &\geq 5\log n_1, \\ m &\leq \min\left(n_1/80, b_2/400\right) - 1, \end{aligned}$$

there exists an efficiently-computable function $\mathsf{Raz}\colon \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ *with the following property. For any (n_1, b_1)-weak-source X, and an independent (n_2, b_2)-weak-source Y,*

$$\begin{aligned} (\mathsf{Raz}(X,Y), X) &\approx_\varepsilon (U_m, X), \\ (\mathsf{Raz}(X,Y), Y) &\approx_\varepsilon (U_m, Y), \end{aligned}$$

where $\varepsilon = 2^{-1.5m}$.

We also make use of the following construction of a somewhere-condenser.

Theorem 8.3 ([Raz05, BKS+05, Zuc07]). *There exist universal constants $c_1, c_2 > 0$ such that the following holds. For every $\delta > 0$, there exists an efficiently-computable function* $\mathsf{Cond}\colon \{0,1\}^n \to (\{0,1\}^\ell)^r$, *where the output is interpreted as an $r \times \ell$ matrix, with $r = \Theta((1/\delta)^{c_1})$ rows and $\ell = \Theta(n \cdot \delta^{c_2})$ columns. If X is an $(n, \delta n)$-weak-source, then* $\mathsf{Cond}(X)$ *is $2^{-\Omega(\delta^2 n)}$-close to a convex combination of distributions, each of which has some row with min-entropy rate 0.9.*

Proof of Theorem 8.1. We start by describing the construction of $\mathsf{3Ext}$, and then turn to the analysis. For the construction of $\mathsf{3Ext}$ we need the following building blocks:

- Let $\mathsf{Cond}\colon \{0,1\}^n \to \left(\{0,1\}^\ell\right)^r$ be the somewhere-condenser from Theorem 8.3. By Theorem 8.3, $r = \Theta((1/\delta)^{c_1})$ and $\ell = \Theta(n \cdot \delta^{c_2})$, where $c_1, c_2 > 1$ are the universal constants from Theorem 8.3. We set $c = c_1$.

- Let $\mathsf{Raz}\colon \{0,1\}^\ell \times \{0,1\}^n \to \{0,1\}^t$ be the extractor from Theorem 8.2, set to extract $t = \Theta(r^2 \cdot \log(r) \cdot \log(nr/\varepsilon))$ bits.

- Let $\mathsf{Merg}\colon \left(\{0,1\}^t\right)^r \to \{0,1\}^m$ be the merger with weak-seeds from Theorem 7.2, set with error ε and output length $m = t/(2r) = \Theta(r \cdot \log(r) \cdot \log(nr/\varepsilon))$.

Given these building blocks, the construction of $\mathsf{3Ext}$ is as follows. Let X_1, X_2, X_3 be n-bit sources with entropies k_1, k_2, k_3, respectively. We first compute $\mathsf{Cond}(X_1)$, which is an $r \times \ell$ matrix R. Secondly, for each $i \in [r]$, we compute $S_i = \mathsf{Raz}(R_i, X_2)$. We stack $S_1, \ldots, S_r$ in an $r \times t$ matrix S. The output is then $\mathsf{3Ext}(X_1, X_2, X_3) = \mathsf{Merg}(S, X_3)$.

We now turn to the analysis. We prove that the extractor is strong in $\{2,3\}$. Since Raz is strong in both of its sources, a similar argument can be used to show that the extractor is also strong in $\{1,3\}$. By Theorem 8.3, since X_1 is an $(n, \delta n)$-weak-source, the matrix

R is $2^{-\Omega(\delta^2 n)}$-close to a convex combination of distributions, each of which has some row with min-entropy rate 0.9. Therefore, we may assume that R is $2^{-\Omega(\delta^2 n)}$-close to a random variable R', such that there exists $g \in [r]$ where R'_g has min-entropy rate 0.9. Note that by taking the universal constant α to be smaller than $1/2$, we get that $2^{-\Omega(\delta^2 n)} \le \varepsilon$.

One can easily verify that the hypothesis of Theorem 8.2 is met assuming

$$\delta \ge \Omega\left(\left(\frac{\log(n/\varepsilon)}{n}\right)^{1/(3c_1+c_2)}\right),$$

which holds by taking the universal constant $\alpha = 1/(3c_1 + c_2)$ (note that $\alpha \le 1/2$). By Theorem 8.2, and since $2^{-1.5t} \le \varepsilon$,

$$\big(\mathsf{Raz}(R'_g, X_2), X_2\big) \approx_\varepsilon (U_t, X_2).$$

Since (R_g, R'_g) and X_2 are independent and since $\mathsf{SD}(R, R') \le \varepsilon$, Lemma 2.4 (applied to the random function $f(Z) = (\mathsf{Raz}(Z_g, X_2), X_2)$, where X_2 is the internal randomness of f) implies that

$$(S_g, X_2) = (\mathsf{Raz}(R_g, X_2), X_2) \approx_{2\varepsilon} (U_t, X_2).$$

Thus, by Markov's inequality, with probability at least $1 - \sqrt{\varepsilon}$ over the fixing $X_2 = x_2$, it holds that $(S_g \mid X_2 = x_2)$ is $2\sqrt{\varepsilon}$-close to uniform. We condition on the event $X_2 = x_2$ for such x_2. Lemma 2.10 then implies that $S \approx_{2\sqrt{\varepsilon}} S'$, where S' is a somewhere-random source.

We apply the merger from Theorem 7.2 to S' and the weak-source X_3. By the choice of t, and since $k_3 \ge \Omega(r \cdot \log(r) \cdot \log(r \log(n)/\varepsilon))$, the hypothesis of Theorem 7.2 is met, and so Theorem 7.2 implies that

$$(\mathsf{Merg}(S', X_3), X_3) \approx_\varepsilon (U_m, X_3)\,. \tag{8.1}$$

Since $S \approx_{2\sqrt{\varepsilon}} S'$, and since (S, S') and X_3 are independent, Lemma 2.4 (applied to the random function $f(Z) = (\mathsf{Merg}(Z, X_3), X_3)$, where X_3 is the internal randomness of f), implies that

$$(\mathsf{Merg}(S, X_3), X_3) \approx_{2\sqrt{\varepsilon}} (\mathsf{Merg}(S', X_3), X_3)\,, \tag{8.2}$$

and so by Equation (8.1) and Equation (8.2) we have that

$$(\mathsf{Merg}(S, X_3), X_3) \approx_{3\sqrt{\varepsilon}} (U_m, X_3)\,.$$

By Markov's inequality, with probability at least $1 - \varepsilon^{1/4}$ over the further fixing of $X_3 = x_3$, it holds that $\mathsf{Merg}(S, x_3)$ is $3\varepsilon^{1/4}$-close to uniform. Thus, we have that

$$(\mathsf{3Ext}(X_1, X_2, X_3), X_2, X_3) = (\mathsf{Merg}(S, X_3), X_2, X_3) \approx_{O(\varepsilon^{1/4})} (U_m, X_2, X_3)\,.$$

Note that the error can be reduced from $O(\varepsilon^{1/4})$ to ε without affecting the theorem statement. This concludes the proof of the theorem.

□

Acknowledgement

This work began while the author was hosted as an intern of Guy Rothblum at the Microsoft Research Silicon Valley lab. The author wish to thank Guy for his warm hospitality and guidance, for many insightful discussions regarding this work, and for his suggestions that improved the presentation of this paper. During the internship we had many interesting discussions with Raghu Meka and Omer Reingold for whom we wish to thank.

We thank Oded Goldreich for assisting us in choosing an appropriate name for our object of interest – a local correlation breaker (which was initially called a "wiser"). We thank Roei Tell for his suggestions which improved the presentation of this paper. The author would like to thank his advisor Ran Raz for his continues encouragement.

References

[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.

[Bou05] J. Bourgain. More on the sum-product phenomenon in prime fields and its applications. *International Journal of Number Theory*, 1(01):1–32, 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.

[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.

[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.

[DR08] Z. Dvir and R. Raz. Analyzing linear mergers. *Random Structures & Algorithms*, 32(3):334–345, 2008.

[DS07] Z. Dvir and A. Shpilka. An improved analysis of linear mergers. *computational complexity*, 16(1):34–59, 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.

[DW11] Z. Dvir and A. Wigderson. Kakeya sets, new mergers, and old extractors. *SIAM Journal on Computing*, 40(3):778–792, 2011.

[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.

[Li12] X. Li. Non-malleable condensers for arbitrary min-entropy, and almost optimal protocols for privacy amplification. *arXiv preprint arXiv:1211.0651*, 2012.

[Li13] 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.

[Li15] X. Li. Three-source extractors for polylogarithmic min-entropy. *Electronic Colloquium on Computational Complexity (ECCC)*, 2015.

[LRVW03] C.J. Lu, O. Reingold, S. Vadhan, and A. Wigderson. Extractors: Optimal up to constant factors. In *Proceedings of the thirty-fifth annual ACM Symposium on Theory of Computing*, pages 602–611. ACM, 2003.

[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.

[TS96] A. Ta-Shma. On extracting randomness from weak random sources. In *Proceedings of the twenty-eighth annual ACM Symposium on Theory of Computing*, pages 276–285, 1996.

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

A Proof of Lemma 4.1

For the proof of Lemma 4.1 we use the following simple lemma.

Lemma A.1. *Let X, Y be two random variable over a common domain D. Let $E \subseteq D$ be an event. Then,*

$$\mathsf{SD}\left(X \mid E, Y \mid E\right) \le \frac{1}{\mathbf{Pr}[E]} \cdot \mathsf{SD}\left(X, Y\right).$$

We start by proving the following lemma.

Lemma A.2. *Let L, R be two independent random variables, and let $\mathcal{H}$ be an (L, R)-history. Let M be a random variable over $\{0,1\}^m$ which is a deterministic function of $\mathcal{H}, L$ such that*

$$(M, \mathcal{H}) \approx_{\delta_M} (U_m, \mathcal{H}). \tag{A.1}$$

Let J be a random variable over $\{0,1\}^j$ which is a deterministic function of $\mathcal{H}, L$. Let P be a random variable over $\{0,1\}^p$ which is a deterministic function of $\mathcal{H}, R, J$, such that

$$(P, J, \mathcal{H}) \approx_{\delta_P} (U_p, J, \mathcal{H}). \tag{A.2}$$

Let $\mathsf{Ext}\colon \{0,1\}^m \times \{0,1\}^p \to \{0,1\}^f$ be a strong seeded extractor for entropy $m - j - \log(1/\varepsilon)$, with error ε. Define $F = \mathsf{Ext}(M, P)$. Then, $P, J, \mathcal{H}$ is an (L, R)-history, and

$$(F, P, J, \mathcal{H}) \approx_{\delta_P + \delta_M + 2\varepsilon} (U_f, P, J, \mathcal{H}).$$

Proof of Lemma A.2. For $h \in \mathsf{supp}(\mathcal{H})$ denote by J_h the random variable $(J \mid \mathcal{H} = h)$. For $j \in \mathsf{supp}(J_h)$ let $E_{h,j}$ be the event $\mathcal{H} = h,\ J_h = j$. For the sake of readability, we let $M_{h,j}$ denote the random variable $(M \mid E_{h,j})$. Similarly, we define $P_{h,j}$, $L_{h,j}$, $R_{h,j}$ to be $(P \mid E_{h,j})$, $(L \mid E_{h,j})$ and $(R \mid E_{h,j})$, respectively.

Since J is a deterministic function of $\mathcal{H}, L$, the random variable J_h is a deterministic function of L. Thus, even after further conditioning on the event $J_h = j$, the random variables L, R remain independent. That is, the random variables $L_{h,j}$ and $R_{h,j}$ are independent. Furthermore, since P is a deterministic function of $\mathcal{H}, R, J$ and M is a deterministic function of $\mathcal{H}, L$, we have that $M_{h,j}$ and $P_{h,j}$ are independent.

Let $\delta_{P;h,j} = \mathsf{SD}\left(P_{h,j}, U_p\right)$. By Equation (A.2) and Lemma 2.5 we have that

$$\mathop{\mathbf{E}}_{h \sim \mathcal{H}} \mathop{\mathbf{E}}_{j \sim J_h} \left[\delta_{P;h,j}\right] \le \delta_P.$$

Since $M_{h,j}$ and $P_{h,j}$ are independent, Lemma 2.5 implies that

$$\mathsf{SD}\left(\left(\mathsf{Ext}\left(M_{h,j}, P_{h,j}\right), P_{h,j}\right)\left(U_f, P_{h,j}\right)\right) = \mathop{\mathbf{E}}_{s \sim P_{h,j}} \left[\mathsf{SD}\left(\mathsf{Ext}\left(M_{h,j}, s\right), U_f\right)\right].$$

As the function $g(s) = \mathsf{SD}\left(\mathsf{Ext}\left(M_{h,j}, s\right), U_f\right)$ attains values in the interval $[0,1]$, Lemma 2.9 yields

$$\mathop{\mathbf{E}}_{s \sim P_{h,j}} \left[\mathsf{SD}\left(\mathsf{Ext}\left(M_{h,j}, s\right), U_f\right)\right] \le \mathop{\mathbf{E}}_{s \sim U_p} \left[\mathsf{SD}\left(\mathsf{Ext}\left(M_{h,j}, s\right), U_f\right)\right] + \delta_{P;h,j}.$$

Thus,

$$\begin{aligned}\mathsf{SD}\left((F,P,J,\mathcal{H}),(U_f,P,J,\mathcal{H})\right) &= \mathop{\mathbf{E}}_{h\sim\mathcal{H}}\mathop{\mathbf{E}}_{j\sim J_h}\mathop{\mathbf{E}}_{s\sim P_{h,j}}\left[\mathsf{SD}\left(\mathsf{Ext}\left(M_{h,j},s\right),U_f\right)\right] \\ &\le \mathop{\mathbf{E}}_{h\sim\mathcal{H}}\mathop{\mathbf{E}}_{j\sim J_h}\left(\mathop{\mathbf{E}}_{s\sim U_p}\left[\mathsf{SD}\left(\mathsf{Ext}\left(M_{h,j},s\right),U_f\right)\right]+\delta_{P;h,j}\right) \\ &\le \mathop{\mathbf{E}}_{h\sim\mathcal{H}}\mathop{\mathbf{E}}_{j\sim J_h}\mathop{\mathbf{E}}_{s\sim U_p}\left[\mathsf{SD}\left(\mathsf{Ext}\left(M_{h,j},s\right),U_f\right)\right]\ +\delta_P.\end{aligned}$$

Let $\delta_{M;h} = \mathsf{SD}\left((M \mid \mathcal{H}=h), M'\right)$, where M' is a random variable that is uniformly distributed over $\{0,1\}^m$ and is independent of $\mathcal{H}$. By Equation (A.1) and Lemma 2.5,

$$\mathop{\mathbf{E}}_{h\sim\mathcal{H}}\left[\delta_{M;h}\right] \le \delta_M.$$

Lemma A.1 implies that for every $j \in \mathsf{supp}(J_h)$, the distribution of the random variable $M_{h,j}$ is $\delta_{M;h,j}$-close to the distribution $(M' \mid J_h = j)$, where

$$\delta_{M;h,j} = \frac{\delta_{M;h}}{\mathbf{Pr}[J_h = j]}.$$

Let $M'_{h,j}$ be a random variable with distribution $(M' \mid J_h = j)$. By the triangle inequality and Lemma 2.4, it holds that

$$\begin{aligned}\mathsf{SD}\left(\mathsf{Ext}\left(M_{h,j},s\right),U_f\right) &\le \mathsf{SD}\left(\mathsf{Ext}\left(M_{h,j},s\right),\mathsf{Ext}\left(M'_{h,j},s\right)\right)+\mathsf{SD}\left(\mathsf{Ext}\left(M'_{h,j},s\right),U_f\right) \\ &\le \mathsf{SD}\left(M_{h,j},M'_{h,j}\right)+\mathsf{SD}\left(\mathsf{Ext}\left(M'_{h,j},s\right),U_f\right) \\ &= \delta_{M;h,j}+\mathsf{SD}\left(\mathsf{Ext}\left(M'_{h,j},s\right),U_f\right),\end{aligned}$$

and so,

$$\begin{aligned}\mathsf{SD}\left((F,P,J,\mathcal{H}),(U_f,P,J,\mathcal{H})\right) &\le \mathop{\mathbf{E}}_{h\sim\mathcal{H}}\mathop{\mathbf{E}}_{j\sim J_h}\mathop{\mathbf{E}}_{s\sim U_p}\left[\mathsf{SD}\left(\mathsf{Ext}\left(M'_{h,j},s\right),U_f\right)+\delta_{M;h,j}\right]+\delta_P \\ &\le \mathop{\mathbf{E}}_{h\sim\mathcal{H}}\mathop{\mathbf{E}}_{j\sim J_h}\mathop{\mathbf{E}}_{s\sim U_p}\left[\mathsf{SD}\left(\mathsf{Ext}\left(M'_{h,j},s\right),U_f\right)\right]+\delta_M+\delta_P. \qquad \text{(A.3)}\end{aligned}$$

By Lemma 2.12, for any $h \in \mathsf{supp}(\mathcal{H})$, $\widetilde{H}_\infty(M'_{h,j}) = \widetilde{H}_\infty(M' \mid J_h = j) \ge m - j$. Thus, by Lemma 2.13, for any $h \in \mathsf{supp}(\mathcal{H})$,

$$\mathop{\mathbf{Pr}}_{j\sim J_h}\left[H_\infty(M'_{h,j}) \ge m - j - \log(1/\varepsilon)\right] \ge 1-\varepsilon.$$

We say that a pair h,j, where $h \in \mathsf{supp}(\mathcal{H})$ and $j \in \mathsf{supp}(J_h)$, is *good* if $H_\infty(M'_{h,j}) \ge m-j-\log(1/\varepsilon)$. By the above, for every $h \in \mathsf{supp}(\mathcal{H})$, with probability $1-\varepsilon$ over $j \sim J_h$ it holds that the pair h,j is good. Since Ext is a strong seeded extractor for entropy $m-j-\log(1/\varepsilon)$ and error ε, we have that the contribution of any good pair h,j to the expectation in Equation (A.3) is at most ε. Since $1-\varepsilon$ fraction of the pairs are good, and since any pair contributes at most 1 to the expectation, we get that

$$\mathsf{SD}\left((F,P,J,\mathcal{H}),(U_f,P,J,\mathcal{H})\right) \le 2\varepsilon+\delta_M+\delta_P,$$

as stated. To conclude the proof of the lemma, note that $P, J, \mathcal{H}$ is an (L, R)-history since $\mathcal{H}$ is an (L, R)-history, J is a deterministic function of $\mathcal{H}, L$, and P is a deterministic function of R and $J, \mathcal{H}$ (note that J precede P in the history and so P is allowed to depend on J). $\square$

Proof of Lemma 4.1. We apply Lemma 3.3 to the (X, Y)-history $\mathcal{H}$ with $P = (W_g)|_s$, $M = Y$ and the extractor Ext_1. The hypothesis of Lemma 3.3 is met since the random variable $P = (W_g)|_s$ is a deterministic function of $X, \mathcal{H}$. Moreover, by the Equation (4.1), $\widetilde{H}_\infty(Y \mid \mathcal{H}) \geq 2a + \log(1/\varepsilon)$. Since Ext_1 is a strong seeded extractor for entropy $2a$, Equation (3.2) of Lemma 3.3 holds. Since $A_g = \mathsf{Ext}_1(Y, (W_g)|_s)$, Lemma 3.3 together with Equation (4.3) imply that

$$(A_g, (W_g)|_s, \mathcal{H}) \approx_{\delta+2\varepsilon} (U_a, \cdot).$$

Moreover, $(W_g)|_s, \mathcal{H}$ is an (X, Y)-history.

Note that A_g is a deterministic function of Y and $(W_g)|_s$, whereas the joint distribution of $\{(W_i)|_s\}_{i \in [r] \setminus \{g\}}$ is a deterministic function of X and $\mathcal{H}$. Thus, Lemma 3.4 applied with $P = A_g$, $J = \{(W_i)|_s\}_{i \in [r] \setminus \{g\}}$ and the (X, Y)-history $(W_g)|_s, \mathcal{H}$, implies that

$$(A_g, W|_s, \mathcal{H}) \approx_{\delta+2\varepsilon} (U_a, \cdot). \tag{A.4}$$

Furthermore, $W|_s, \mathcal{H}$ is an (X, Y)-history.

We apply Lemma A.2 to the (X, Y)-history $\mathcal{H}$, with $M = W_g$, $P = A_g$, $J = W|_s$ and the extractor Ext_2. The hypothesis of Lemma A.2 is met since $W|_s, W_g$ are deterministic functions of $\mathcal{H}, X$, and A_g is a deterministic function of $Y, W|_s$. Moreover, Equation (4.2) implies that

$$|W_g| - |(W|_s)| - \log(1/\varepsilon) = h - rs - \log(1/\varepsilon) \geq 2s.$$

Since Ext_2 is a strong seeded extractor for entropy $2s$ with error ε, Lemma A.2 together with Equation (4.3) and Equation (A.4) imply that

$$(Z_g, A_g, W|_s, \mathcal{H}) \approx_{2\delta+4\varepsilon} (U_s, \cdot). \tag{A.5}$$

Furthermore, $A_g, W|_s, \mathcal{H}$ is an (X, Y)-history.

We apply Lemma 3.4 with $P = Z_g$, the (X, Y)-history $A_g, W|_s, \mathcal{H}$ and $J = \{A_i\}_{i \in [r] \setminus \{g\}}$, and conclude that

$$(Z_g, \{A_i\}_{i=1}^r, W|_s, \mathcal{H}) \approx_{2\delta+4\varepsilon} (U_s, \cdot). \tag{A.6}$$

This application of Lemma 3.4 is valid since $Z_g = \mathsf{Ext}_2(W_g, A_g)$ is a deterministic function of A_g, which is contained in the (X, Y)-history to which we apply the lemma, and W_g which, by assumption, is a deterministic function of $X, \mathcal{H}$ (and $\mathcal{H}$ is also contained in (X, Y)-history above). On the other hand, the joint distribution of $\{A_i\}_{i \in [r] \setminus \{g\}}$ is a deterministic function of $Y, W|_s$, and $W|_s$ is contained in the (X, Y)-history to which we apply the lemma. Lemma 3.4 further implies that $\{A_i\}_{i=1}^r, W|_s, \mathcal{H}$ is an (X, Y)-history.

Next, we apply Lemma 3.3 to the (X, Y)-history $\{A_i\}_{i=1}^r, W|_s, \mathcal{H}$ with $P = Z_g$, $M = Y$ and the extractor Ext_1. The hypothesis of Lemma 3.3 is met since the random variable

$Z_g = \mathsf{Ext}_2(W_g, A_g)$ is a deterministic function of $X, \mathcal{H}, A_g$, and $\mathcal{H}, A_g$ are contained in the (X,Y)-history to which we apply the lemma. In terms of entropy,

$$\begin{aligned}\widetilde{H}_\infty\left(Y \mid \{A_i\}_{i=1}^r, W|_s, \mathcal{H}\right) &\ge \widetilde{H}_\infty\left(Y \mid (W|_s), \mathcal{H}\right) - ra \\ &= \widetilde{H}_\infty\left(Y \mid \mathcal{H}\right) - ra \\ &\ge 2a + \log(1/\varepsilon), \end{aligned} \tag{A.7}$$

where the first inequality follows by Lemma 2.12 and the fact that $\{A_i\}_{i=1}^r$ consists of ra bits. The second equality follows by Lemma 2.14, which is applicable in this case as conditioned on any fixing of $\mathcal{H}$, the random variables $W|_s, Y$ are independent. The last inequality follows by Equation (4.1). Since Ext_1 is a strong seeded extractor for entropy $2a$, Equation (3.2) of Lemma 3.3 holds. As $B_g = \mathsf{Ext}_1\left(Y, Z_g\right)$, Lemma 3.3 together with Equation (A.6) imply that

$$\left(B_g, Z_g, \{A_i\}_{i=1}^r, W|_s, \mathcal{H}\right) \approx_{2\delta+6\varepsilon} \left(U_a, \cdot\right).$$

Moreover, $Z_g, \{A_i\}_{i=1}^r, W|_s, \mathcal{H}$ is an (X,Y)-history.

Note that B_g is a deterministic function of Y, Z_g whereas W is a deterministic function of $X, \mathcal{H}$. Thus, we can apply Lemma 3.4 with $P = B_g$ and $J = W$ to the (X,Y)-history $Z_g, \{A_i\}_{i=1}^r, W|_s, \mathcal{H}$ and conclude that

$$\left(B_g, \mathcal{H}'\right) \approx_{2\delta+6\varepsilon} \left(U_a, \cdot\right),$$

where $\mathcal{H}' = (W, Z_g, \{A_i\}_{i=1}^r, W|_s, \mathcal{H})$ is an (X,Y)-history. This proves the first and second items of the lemma.

As for the third item, since W and Y are independent conditioned on any fixing of $Z_g, \{A_i\}_{i=1}^r, W|_s, \mathcal{H}$, Lemma 2.14 implies that

$$\widetilde{H}_\infty\left(Y \mid \mathcal{H}'\right) = \widetilde{H}_\infty\left(Y \mid Z_g, \{A_i\}_{i=1}^r, W|_s, \mathcal{H}\right).$$

Similarly, conditioned on any fixing of $\{A_i\}_{i=1}^r, W|_s, \mathcal{H}$, the random variables Y and Z_g are independent, and so

$$\widetilde{H}_\infty\left(Y \mid \mathcal{H}'\right) = \widetilde{H}_\infty\left(Y \mid \{A_i\}_{i=1}^r, W|_s, \mathcal{H}\right).$$

By Equation (A.7), the right hand side of the equation above is bounded below by $\widetilde{H}_\infty\left(Y \mid \mathcal{H}\right) - ra$, which proves the third item of the lemma.

As for the fourth item, note that Z_g is a deterministic function of W, A_g, and $W|_s$ is a deterministic function of W, and so

$$\widetilde{H}_\infty\left(N \mid \mathcal{H}'\right) = \widetilde{H}_\infty\left(N \mid W, \{A_i\}_{i=1}^r, \mathcal{H}\right).$$

Note that conditioned on any fixing of $W, \mathcal{H}$, the random variables $\{A_i\}_{i=1}^r$ are deterministic functions of Y. Since N is a deterministic function of $X, \mathcal{H}$, Lemma 2.14 further implies that

$$\widetilde{H}_\infty\left(N \mid \mathcal{H}'\right) = \widetilde{H}_\infty\left(N \mid W, \mathcal{H}\right) \ge \widetilde{H}_\infty\left(N \mid \mathcal{H}\right) - rh,$$

where the last inequality follows by Lemma 2.12. □

ECCC ISSN 1433-8092
http://eccc.hpi-web.de