Expander Graphs and their Applications*
Lecture 11: Lossless Conductors and Expanders

Notes taken by Ariel Elbaz, Yuval Filmus and Michal Igell

July 2002

Summary: In this lecture we define conductors, a generalization of expanders. Extractors, dispersers and condensers are all types of conductors. We use the new structures to explicitly construct lossless expanders.

1 Min-entropy

Min-entropy measures the rarity of the most probable event. If all events occur at probability at most 2^{-k}, then the min-entropy is at most k, and vice versa. For a random variable X (or a distribution) over some finite set S, let

$$\mathrm{Supp}(X) = \{x \in S : \Pr[X = x] > 0\}.$$

Definition 1. The min-entropy of a distribution X

$$H_\infty(X) = \min_x \left\{ \log \frac{1}{\Pr[X = x]} \right\} = -\max_x \left\{ \log \left(\Pr[X = x] \right) \right\}$$

where minimum and maximum are taken over $x \in \mathrm{Supp}(X)$.

Note: throughout this work, $\log$ is always taken to base 2.

Definition 2. The Rényi entropy of a distribution X is

$$H_2(X) = -\log \sum_x (\Pr[X = x])^2 = -\log \mathbb{E}\Big[\Pr[X = x] \Big].$$

Lemma 3. *The min-entropy and Rényi entropy of a distribution X obey the following inequality:*

$$H_\infty(X) \le H_2(X) \le 2H_\infty(X)$$

The left inequality is tight iff X is uniformly distributed on some set S.

* Lecture Notes for a course given by Nati Linial and Avi Wigderson at the Hebrew University, Israel.

Proof. Since $\log$ is a monotone increasing function, we have

$$\begin{aligned} H_2(X) &= -\log \mathbb{E}[\ \Pr[X = x]] \\ &\geq -\log \max_{x \in \mathrm{Supp}(X)} \Pr[X = x] = H_\infty(X) \end{aligned}$$

and equality holds iff X is uniformly distributed over $\mathrm{Supp}(X)$.
On the other hand, let $x_M = \mathrm{argmax}_x \Pr[X = x]$. We have

$$\begin{aligned} H_2(X) &= -\log\Big(\sum_x (\Pr[X = x])^2\Big) \\ &= -\log\Big(\sum_{x \neq x_M} (\Pr[X = x])^2 + (\Pr[X = x_M])^2\Big) \\ &\leq -\log\Big((\Pr[X = x_M])^2\Big) \\ &= -2\log\Big(\ \Pr[X = x_M]\Big) = 2H_\infty(X) \end{aligned}$$

□

A distribution which is uniformly distributed on some set S is called a flat distribution, and both its min-entropy and its Rényi entropy are $\log|S|$. These are maximal among distributions with support S.

Flat distributions combine to make the most general distributions:

Lemma 4. *Every distribution over a finite set is a convex combination of a finite number of flat distributions. In other words, if X is a distribution then $X = \sum p_i U(S_i)$, where $S_i \subset \mathrm{Supp}(X)$, $p_i \geq 0$ and $\sum p_i = 1$.*

Proof. The proof goes by induction on $|\,\mathrm{Supp}(X)|$. If $\mathrm{Supp}(X) = \{x\}$ then $X = U(x)$. Otherwise, let $x_m = \mathrm{argmin} \Pr[X = x]$, and let $p_m = \Pr[X = x_m]$. We have $X = p_m U(\mathrm{Supp}(X)) + (1 - p_m)Y$, where $\mathrm{Supp}(Y) \subsetneq \mathrm{Supp}(X)$ since $x_m \notin \mathrm{Supp}(Y)$. □

If we combine a distribution Y with a flat distribution X, the joint distribution has min-entropy equal to $H_\infty(Y) + H_\infty(X)$:

Lemma 5. *Suppose X is a flat distribution, with $H_\infty(X) = c$, and let Y be another distribution. Then $H_\infty(X, Y) \leq k$ iff for every $x \in \mathrm{Supp}(X)$, we have $H_\infty(Y|X = x) \leq k - c$.*

Proof. Suppose first that $H_\infty(X, Y) \leq k$. If $H_\infty(Y|X = x) \geq k - c$ for some $x \in \mathrm{Supp}(X)$, then $\Pr[Y = y|X = x] \leq 2^{c-k}$ for some $y \in \mathrm{Supp}(Y)$. Since X is flat, $\Pr[X = x, Y = y] \leq 2^{c-k}2^{-c} = 2^{-k}$, contradicting the promise $H_\infty(X, Y) \leq k$.

Next, suppose that $H_\infty(Y|X = x) \leq k - c$ for all $x \in \mathrm{Supp}(X)$. Then for all $y \in \mathrm{Supp}(Y)$, we have $\Pr[Y = y|X = x] \geq 2^{c-k}$. Since X is flat, $\Pr[Y = y] \geq 2^{c-k}2^{-c} = 2^{-k}$. Therefore, $H_\infty(Y) \leq k$.

□

We complete this section with a technical lemma, showing how to divide a joint distribution according to conditional min-entropy.

Definition 6. Two distributions X and Y over the same set S are said to be ϵ-close if $|\Pr[X \in P] - \Pr[Y \in P]| \leq \epsilon$ for every subset $P \subset S$. Alternatively, X and Y are ϵ-close if $\sum_s |\Pr[X = s] - \Pr[Y = s]| \leq 2\epsilon$. We leave the reader to show that the two definitions are equivalent.

Lemma 7. *Let X_1 and X_2 be two distributions. Given $\epsilon > 0$ and a, there exist distributions Y_1 and Y_2 such that*

- *The joint distributions (X_1, X_2) and (Y_1, Y_2) are ϵ-close;*
- *The joint distribution (Y_1, Y_2) is a convex combination of two other joint distributions $(\hat{Y}_1, \hat{Y}_2)$ and $(\check{Y}_1, \check{Y}_2)$, both having min-entropy at least $H_\infty(X_1, X_2) - \log \frac{1}{\epsilon}$;*
- *For all $x \in \mathrm{Supp}(\hat{Y}_1)$ we have $H_\infty(\hat{Y}_2 | \hat{Y}_1 = x) \geq a$;*
- *For all $x \in \mathrm{Supp}(\check{Y}_1)$ we have $H_\infty(\check{Y}_2 | \check{Y}_1 = x) \leq a$;*

Proof. We begin by constructing $(\hat{Y}_1, \hat{Y}_2)$ and $(\check{Y}_1, \check{Y}_2)$. We split $\mathrm{Supp}(X_1)$ according to $H_\infty(X_2 | X_1 = x)$:

$$\begin{aligned}\hat{X} &= \{x : H_\infty(X_2 | X_1 = x) \geq a\},\\ \check{X} &= \{x : H_\infty(X_2 | X_1 = x) < a\}.\end{aligned}$$

Now we can define

$$\begin{aligned}\Pr[\hat{Y}_1 = y_1, \hat{Y}_2 = y_2] &= \Pr[X_1 = x_1, X_2 = x_2 | x_1 \in \hat{X}],\\ \Pr[\check{Y}_1 = y_1, \check{Y}_2 = y_2] &= \Pr[X_1 = x_1, X_2 = x_2 | x_1 \in \check{X}].\end{aligned}$$

In other words, $\hat{Y}_1$ gets only values in $\hat{X}$, and $\check{Y}_1$ is restricted to $\check{X}$.

If $p = \Pr[X_1 \in \hat{X}]$, then the probability of each event in $(\hat{Y}_1, \hat{Y}_2)$ is multiplied by $1/p$, and the probability of each event in $(\check{Y}_1, \check{Y}_2)$ is multiplied by $1/(1-p)$. Therefore, if $\epsilon \leq p \leq 1 - \epsilon$ then the min-entropy of $(\hat{Y}_1, \hat{Y}_2)$ and $(\check{Y}_1, \check{Y}_2)$ is reduced by at most $\log 1/\epsilon$. Since $(X_1, X_2) = p(\hat{Y}_1, \hat{Y}_2) + (1-p)(\check{Y}_1, \check{Y}_2)$ we can take $(Y_1, Y_2) = (X_1, X_2)$.

If, for example $p < \epsilon$, $(\check{Y}_1, \check{Y}_2)$ still has high enough min-entropy, and so we take $(Y_1, Y_2) = (\check{Y}_1, \check{Y}_2)$. This distribution is ϵ-close to (X_1, X_2):

$$\begin{aligned}&\sum_{x_1 \in \hat{X}, x_2} \big| \Pr[X_1 = x_1, X_2 = x_2] - \Pr[\check{Y}_1 = x_1, \check{Y}_2 = x_2] \big| +\\ &\sum_{x_1 \in \check{X}, x_2} \big| \Pr[X_1 = x_1, X_2 = x_2] - \Pr[\check{Y}_1 = x_1, \check{Y}_2 = x_2] \big| =\\ &p + \left(\frac{1}{1-p} - 1\right)(1-p) = 2p < 2\epsilon.\end{aligned}$$

$\square$

2 Conductors and lossless expanders

2.1 Conductors

Loosely speaking, a conductor is a function that transfers entropy from its inputs to its output. In other words, if the input distributions have high min-entropy, then the output distribution will have high min-entropy.

Definition 8 (conductors). A function $E\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a $(k_{\max}, a, \epsilon)$-conductor if for any distribution X on $\{0,1\}^n$ satisfying $H_\infty(X) = k \leq k_{\max}$, the distribution $E(X, U_d)$ is ϵ-close to a distribution Y whose min-entropy is at least $k + a$.

Remark: In this text we identify a distribution with a random variable sampled from it.

In other words, E gets two inputs: a distribution X with min-entropy $k \leq k_{\max}$, and the uniform distribution U_d (with min-entropy d). The output is ϵ-close to a distribution with min-entropy at least $k + a$.

The following definitions (definitions 3.4 to 3.7 from [1]) are several special cases of conductors, which we will later use.

Definition 9 (extracting conductors). A function $E\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is an (ϵ, a) extracting conductor if for any $0 \leq k \leq m - a$, and any k-source X over $\{0,1\}^n$, the distribution $E(X, U_d)$ is a $(k + a, \epsilon)$-source.

Note that if $E\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is an (ϵ, a) extracting conductor, it is also an $(m - a, \epsilon)$ extractor.

Definition 10 (lossless conductors). A function $E\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is an $(k_{\max}, \epsilon)$ lossless conductor if for any $0 \leq k \leq k_{\max}$, and any k-source X over $\{0,1\}^n$, the distribution $E(X, U_d)$ is a $(k + d, \epsilon)$-source.

The next two definitions require that the prefix of the output is an extracting conductor:

Definition 11 (buffer conductors). A pair of functions $\langle E, C\rangle\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m \times \{0,1\}^b$ is an $(k_{\max}, a, \epsilon)$ buffer conductor if E is an (ϵ, a) extracting conductor, and $\langle E, C\rangle$ is an $(k_{\max}, \epsilon)$-lossless conductor.

Definition 12 (permutation conductors). A pair of functions $\langle E, C\rangle\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m \times \{0,1\}^b$, where $n + d = m + b$ is an (ϵ, a) permutation conductor if E is an (ϵ, a) extracting conductor, and $\langle E, C\rangle$ is a permutation over $\{0,1\}^{n+d}$.

2.2 Lossless expanders

Having defined conductors, we define lossless expanders and reveal the connection.

Definition 13. A d-regular bipartite graph is a $(k_{\max}, \epsilon)$-lossless expander if every set of $k \leq k_{\max}$ vertices on the left side has at least $(1 - \epsilon)d \cdot k$ neighbors.

That is, a lossless expander has almost the maximal expansion possible for a d-regular graph, for small enough subsets. An alternative view is that for every subset on the left side, most neighbors will be unique neighbors, i.e. neighboring a single vertex of the set. Naturally, $k_{\max}$ should be somewhat smaller than m/d for this to be possible, where m is the number of vertices on the right side.

Expanders, condensers and dispersers (which we don't define here) can be viewed as special cases of conductors. For example, a lossless conductor E can be viewed as a 2^d-regular bipartite graph with 2^n vertices on the left side and 2^m vertices on the right side, where each set of $2^k \leq 2^{k_{\max}}$ vertices has at least $(1-\epsilon)2^{k+d}$ neighbors on the right side. In other words, we get a $(2^{k_{\max}}, \epsilon)$-lossless expander.

We can explicitly construct constant-degree lossless expanders which losslessly expand sets of size $O(M/D)$, where $M = 2^m$ is the number of right vertices, and $D = 2^d$ is the left degree.

Theorem 14. *For any $\epsilon > 0$, there is an explicit family of $D = (N/\epsilon M)^c$-regular bipartite graphs which are $(O(\epsilon M/D), \epsilon)$-lossless expanders, where N is the number of vertices on the left side, $M < N$ is the number of vertices on the right side, $N = O(M)$ and c is a constant. Note that since $N = O(M)$, the degree itself is bounded by a constant depending only on ϵ.*

We will prove the theorem by constructing an explicit family of $(\log \frac{\epsilon M}{D}, \log D, \epsilon)$-conductors.

3 The Construction

The required lossless conductors will be constructed using a zigzag product. Let us recall the zigzag product for expanders:

Definition 15 (The zigzag product of two regular bipartite graphs). Let H be a d-regular bipartite graph with s vertices on each side, and let G be an s-regular bipartite graph with n vertices on each side.

The zigzag product $G \circledz H$ is a d^2-regular bipartite graph with sn vertices on each side, which we may conceive as n copies of H, one per each vertex of G. Pick a left vertex $(x, y) \in [n] \times [s]$. The edges emanating from (x, y) are labeled using labels from $[d] \times [d]$. The edge labeled (a, b) is determined as follows:

1. Take a left to right step in the local copy of H (use a to choose an edge).
2. Take a left to right step on G, that is between copies of H.
3. Take a left to right step in the new local copy of H (use b to choose an edge).

We expand on the second step. Suppose after the first step we are at (x, y'). Let $x' \in G$ be the y'-th neighbor of x, and let x be the z-th neighbor of x'. Then the second step takes us from (x, y') to (x', z).

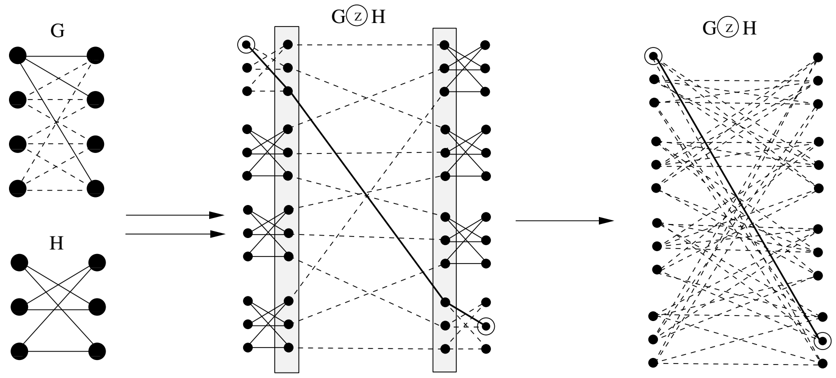

Figure 1: Zigzag product of bipartite graphs

3.1 The zigzag product for conductors

We now define the zigzag product for conductors, and show that composing conductors with carefully selected parameters, we get constant degree lossless expanders, as in theorem 14.

Recall that the zigzag theorem, proved in a previous lecture, shows that $G \,ⓩ\, H$ is an expander if both G and H are such. Moreover, the degree of $G \,ⓩ\, H$ is related to H, while its size and expansion are related to both G and H. Unfortunately, while $\deg(G ⓩ H) = \deg^2(H)$, the expansion of $G ⓩ H$ is the minimum between the expansion of H and the expansion of G. That is, the expansion of $G ⓩ H$ is at most the square root of $deg(G ⓩ H)$ (this can be seen by considering a set consisting of a single copy of H). This expansion is too low for lossless expanders, which require expansion almost as big as the degree.

Recall also that in the proof of the zigzag theorem, of the two random steps (steps 1 and 3 in definition 15), only one is "used" and contributes to the output entropy. That is, out of d^2 choices, only d are surely increasing the entropy.

Here we try to avoid this loss of entropy by buffering the random choices made at each step, and then using a lossless conductor, together with some fresh truly random bits, to condense the leftovers of entropy.

The name "conductor" suggests an analogy to electricity or water conductors. Another analogy to water is to think of the lossless conductor construction as putting a bucket beneath each object, so that when we pour randomness (water) into it, the leftovers (unused randomness, beyond the $k_{\max}$ bound), are stored for later use.

In the zigzag product for conductors we make use of several objects. We remark that they can be explicitly constructed using lemmas from [1].

Let us then assume that we have in our hands the following objects:

1. $\langle E_1, C_1\rangle \colon \{0,1\}^{n_1} \times \{0,1\}^{d_1} \to \{0,1\}^{m_1} \times \{0,1\}^{b_1}$, a permutation conductor that can be taken from lemma 4.4 in [1];
2. $\langle E_2, C_2\rangle \colon \{0,1\}^{n_2} \times \{0,1\}^{d_2} \to \{0,1\}^{d_1} \times \{0,1\}^{b_2}$, a buffer conductor;

3. $E_3\colon \{0,1\}^{b_1+b_2} \times \{0,1\}^{d_3} \to \{0,1\}^{m_3}$, a lossless conductor.

Both E_2 and E_3 can be taken from lemma 4.13 in [1].

We describe the zigzag product for conductors.

Set $n = n_1+n_2$, $d = d_2+d_3$ and $m = m_1+m_3$. For $x_1 \in \{0,1\}^{n_1}$, $x_2 \in \{0,1\}^{n_2}$, $r_2 \in \{0,1\}^{d_2}$ and $r_3 \in \{0,1\}^{d_3}$, define

$$E\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$$

by $E(x_1x_2, r_2r_3) \stackrel{def}{=} y_1y_3$, where

- $(y_2, z_2) = \langle E_2, C_2\rangle(x_2, r_2)$
- $(y_1, z_1) = \langle E_1, C_1\rangle(x_1, y_2)$
- $y_3 = E_3(z_1z_2, r_3)$

z_1 and z_2 are buffers of $\langle E_1, C_1\rangle$ and $\langle E_2, C_2\rangle$.

Figure 2 shows an example of this construction.

Our notation in figure 2 is that (y_i, z_i) are the output of $\langle E_i, C_i\rangle$ on the inputs (x_i, r_i) (except for E_3 which has only one output). As $\langle E_1, C_1\rangle$ gets it's seed from $\langle E_2, C_2\rangle$, we get that $r_1 = y_2$, and since E_3 gets it's input from $\langle E_1, C_1\rangle$ and $\langle E_2, C_2\rangle$, we get that $x_3 = z_1z_2$.

Recall that the zigzag product for bipartite graphs, $G \circledz H$, uses H twice. In the new construction, the first use is replaced with E_2. This ensures that when x_2 has high min-entropy, y_2 is close to uniform, and is a good seed for E_1. The second use of H is replaced with E_3, which is a lossless conductor. The role of E_3 is to transfer entropy lost in E_1 and E_2 to the output.

3.2 A specific example of a lossless conductor

It will be constructive for the sake of explanation to look at a concrete example of the construction.

Set $a = 1000\log(\frac{1}{\epsilon})$ and $d = 2a$. Then we have

- $\langle E_1, C_1\rangle\colon \{0,1\}^{n-20a}\times\{0,1\}^{14a} \to \{0,1\}^{n-20a}\times\{0,1\}^{14a}$, an $(n-30a, 6a, \epsilon)$ permutation conductor;
- $\langle E_2, C_2\rangle\colon \{0,1\}^{20a} \times \{0,1\}^{a} \to \{0,1\}^{14a} \times \{0,1\}^{21a}$, a $(14a, 0, \epsilon)$-buffer conductor;
- $E_3\colon \{0,1\}^{35a} \times \{0,1\}^{a} \to \{0,1\}^{17a}$, a $(15a, a, \epsilon)$ lossless conductor.

The result is

$$E\colon \{0,1\}^n \times \{0,1\}^{2a} \to \{0,1\}^{n-3a}$$

which is a $(n-30a, 2a, 4\epsilon)$-lossless conductor.

Let us try and follow the entropy flow from the input (x_1x_2, r_2r_3) to the output y_1y_3.

Let $k = H_\infty(X_1, X_2)$, then we show that if we start with min-entropy k, we end up with min-entropy of $k + 2a$. Two main ideas for this example are emphasized:

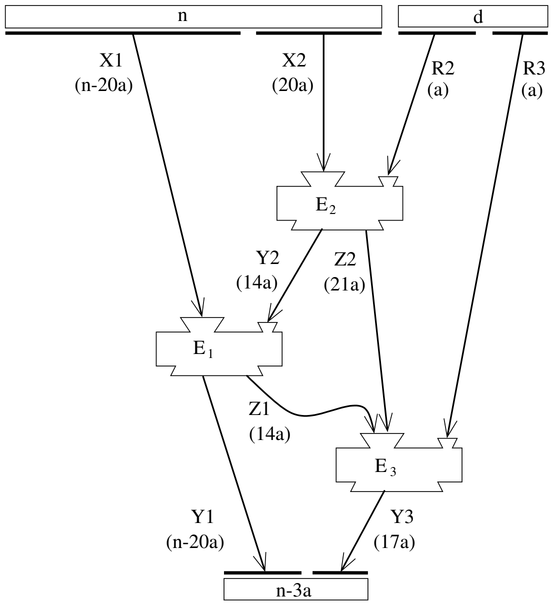

Figure 2: Entropy flow in a lossless conductor

1. The entropy is conserved by $\langle E_1, C_1\rangle, \langle E_2, C_2\rangle$, because $\langle E_1, C_1\rangle$ is a permutation conductor, and $\langle E_2, C_2\rangle$ is a buffer conductor. Therefore, we get

$$k + a = H_\infty(X_1, X_2, R_2) = H_\infty(X1, Y_2, Z_2) = H_\infty(Y_1, Z_1, Z_2)$$

2. We want to verify that enough entropy is transferred, using E_1 and E_2, to Y_1. We know that $H_\infty(Y_1, Z_1, Z_2) = k + a$, and if we prove that $H_\infty(Y_1) \geq k - 14a$, then $H_\infty(Z_1, Z_2|Y_1) \leq 15a$. In that case E_3, which is a $(15a, a, \epsilon)$-conductor will conduct a bits of entropy from R_3 to Y_3. That is, all the entropy of Z_1, Z_2 will be transferred to the output Y_3, without any entropy loss, as we want.

To prove that $H_\infty(Y_1) \geq k - 14a$, we look at the two cases, which lemma 7 essentially shows that are sufficient to prove the general case.

Case 1 For all $x_1 \in \mathrm{Supp}(X_1)$, we have $H_\infty(X_2|X_1 = x_1) \geq 14a$.

In this case, $H_\infty(Y_2|X_1 = x_1) = 14a$, for any $x_1 \in \mathrm{Supp}(X_1)$. Therefore Y_2 can be used as a seed for $\langle E_1, C_1\rangle$ for any $x_1 \in \mathrm{Supp}(X_1)$. We know that $H_\infty(X_1) \geq k - 20a$, and therefore E_1 conducts $6a$ bits of entropy from the seed into Y_1, and we get that $H_\infty(Y_1) \geq k - 14a$.

Case 2 For all $x_1 \in \mathrm{Supp}(X_1)$, we have $H_\infty(X_2|X_1 = x_1) \leq 14a$.

Since $H_\infty(X_1, X2) = k$, it follows that $H_\infty(X_1) \geq k - 14a$. Therefore, since E_2 is a lossless extractor, $H_\infty(Y_2|X_1 = x_1) \geq H_\infty(X_2|X_1 = x_1)$ for any $x_1 \in$

$\mathrm{Supp}(X_1)$. It follows that $H_\infty(X_1, Y_2) \geq H_\infty(X_1, X_2) = k$. Since $\langle E_1, C_1\rangle$ is a permutation, also $H_\infty(Y_1, Z_1) \geq k$, and again we get that $H_\infty(Y_1) \geq k - 14a$.

To complete the example, for any $y_1 \in \mathrm{Supp}(Y_1)$,

$$H_\infty(Z_1, Z_2|Y_1 = y_1) \leq H_\infty(Y_1, Z_1, Z_2) - H_\infty(Y_1) \leq (k + a) - (k - 14a) = 15a.$$

Therefore, the lossless extractor E_3 transfers a bits of entropy from R_3 to Y_3, and we get that $H_\infty(Y_3|Y_1 = y_1) \geq H_\infty(Z_1, Z_2|Y_1 = y_1) + a$. This implies that, $H_\infty(Y_1, Y_3) \geq k + 2a$, as needed.

References

[1] M. Capalbo, O. Reingold, S. Vadhan and A. Wigderson, *Randomness Conductors and Constant-Degree Lossless Expanders*, Extended Abstract, STOC 2002.