7. LOSSLESS CONDUCTOR

Vertex isoperimetric parameter $\Psi_V(G,k)$ are difficult. We know that this can't be more than $d-2+o(1)$ as if $G[U]$ is connected, then $E(U,\overline{U}]$ has at most $(d-2)|U|+2$ edges, hence $N(U)\setminus U$ also has size at most $(d-2+o(1))|U|$. Also, as we have seen d-regular Ramanujan graphs are guaranteed to have vertex expansion about $d/2$ for small sets. Constructing (n,d)-graphs in which every vertex set of size εn expands by at least $d/2$ is a challenging problem. This also has some applications for many fields, including construction of expander-based linear codes, routing algorithms etc. (Recall the error correcting code application in section 1, which requires expansion by more than $d/2$.)

For bipartite graphs, there exists an explicit constructin of families of bipartite expanders whose left degree is d and every small set of linear size on the left expands by $(1-\delta)d$. This can play the role of magical graph in the application of error correcting code construction we saw in Section 1. The construction is based on the zig-zag product to conductors.

So far we have used spectral gap. However, it seems that spectral gap is not strong to obtain $(1-o(1))d$-expansion. Hence we consider min-entropy H_∞. Recall that $H_\infty(p)\geq k$ implies that no point has probability bigger than 2^{-k}. As this seems very strong, we consider a weaker condition.

Definition 7.1. *A k-source is a distribution with min-entropy at least k. A distribution is called a (k,ε)-source if there is a k-source at ℓ_1 distance at most ε from it.*

Consider a bipartite graph with bipartition (L,R). Consider a function associating a given Left vertex x and and edge label i, the right vertex that is the i-th neighbor of x. We name the vertices and edge labels using bit strings. For given distribution on L with known entropy, take a random step along an edge to the right. This induces a distribution on the right vertices. Given a bound on the incoming entropy, we seek a lower bound on the amount of entropy coming out (up to a small ℓ_1 distance). We consider the choice of an edge to be taken in the next step as the randomness injected into the process or as the 'seed' being used. Let U_d be the uniform distribution over $\{0,1\}^d$.

Definition 7.2. *A function $E:\{0,1\}^n\times\{0,1\}^d\to\{0,1\}^m$ is a $(k_{\max},a,\varepsilon)$-conductor if for any $k\leq k_{\max}$ and any k-source X over $\{0,1\}^n$, the distribution $E(X,U_d)$ is a $(k+a,\varepsilon)$-source.*

Note that for the above $(k_{\max},a,\varepsilon)$-conductor E, if (X',U') is ε-away from (X,U_d) in ℓ_1 norm, then $E(X,U_d)$ is also ε-away from $E(X,U_d)$ in ℓ_1 norm, hence $E(X',U')$ is a $(k+a,2\varepsilon)$-source. Like this, we can still get some conclusion with a larger error term even if the input is not as pure as given above, i.e. the second coordinate U_d does not have to have the absolutely uniform distribution.

The following are tools we need.

Definition 7.3. *A function $E:\{0,1\}^n\times\{0,1\}^d\to\{0,1\}^m$ is an (a,ε)-extracting conductor if it is an $(m-a,a,\varepsilon)$-conductor.*

Definition 7.4. *A function $E:\{0,1\}^n\times\{0,1\}^d\to\{0,1\}^m$ is a $(k_{\max},\varepsilon)$-lossless conductor if it is a $(k_{\max},d,\varepsilon)$-conductor.*

In other words, almost none of the injected randomess are lost in lossless conductor.

Definition 7.5. *A pair of function $\langle E,C\rangle:\{0,1\}^n\times\{0,1\}^d\to\{0,1\}^m\times\{0,1\}^b$ is a $(k_{\max},a,\varepsilon)$-buffer conductor if E is an $(k_{\max},a,\varepsilon)$-conductor and $\langle E,C\rangle$ is an $(k_{\max},\varepsilon)$-lossless conductor.*

In other words, E saves most of the entropy from $\{0,1\}^d$, and whatever entropy lost there is saved completely by the second function C. The second function may be viewed as an overflow buffer or bucket.

Definition 7.6. *A pair of function* $\langle E, C\rangle : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m \times \{0,1\}^b$ *where* $n + d = m + b$ *is an* $(k_{\max}, a, \varepsilon)$*-permutation conductor if* E *is an* $(k_{\max}, a, \varepsilon)$*-conductor and* $\langle E, C\rangle$ *is a permutation over* $\{0,1\}^{n+d}$.

Why we care about these, is that this lossless conductor is same as the bipartite graph we seek for.

Definition 7.7. *A bipartite graph* G *on bipartition* (L, R) *such that every vertex on* L *has degree* D *is a* $(K_{\max}, \varepsilon)$*-lossless expander if every set of* $K \leq K_{\max}$ *left vertices has at least* $(1-\varepsilon)DK$ *neighbors.*

If we view this as a conductor with $N = 2^n, D = 2^d$ and $M = 2^m$, then $(k_{\max}, \varepsilon)$-lossless conductor is $(K_{\max}, \varepsilon)$-lossless expander where $K_{\max} = 2^{k_{\max}}$. To see this, for each set $A \subseteq L$ of size at most $K_{\max}$, consider a distribution uniform on A and 0 outside. This has entropy $\log|A|$. As it is $(k_{\max}, \varepsilon)$-loseless conductor, the resulting distribution on the right vertices has entropy at least $\log|A| + d$ up to ℓ_1-distance ε. If the neighborhood has size less than $(1-\varepsilon)DK$, then we get min-entropy less than $\log(D|A|) = \log|A| + d$, a contradiction.

Now, we consider the definition of zig-zag product for bipartite graphs.

Definition 7.8. *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 zig-zag product* $G \textcircled{z} H$ *is a* d^2*-regular bipartite graph with* sn *vertices on each side, where the left and right sides are arranged as* n *copies of* H*, one per each vertex of* G*. The edges emanating from a left vertex* $(x, y) \in [n] \times [s]$ *are labeled by* $[d] \times [d]$*. The edge labeled* (a, b) *is determined as follows:*

(1) Take a left to right step in the local copy of H*, using* a *to choose an edge.*
(2) Take a left to right step along and edge of G*, between copies of* H*. More precisely, suppose we are at* (x, y')*. Let* $x' \in G$ *bet the* y'*-th neighbor of* x*. And* x *is the* z*-th neighbor of* x'*. Then we take from* (x, y') *to* (x', z)*.*
(3) Take a left to right step in the new local copy of H*, using* b *to choose an edge.*

However, the vertex expansion of this $G \textcircled{z} H$ cannot be better than the expansion of H or the expansion of G while its degree is d^2. While taking a random walk, the random choice of a neighbor of a vertex provides the randomness. This can be seen as the injected randomness (second coordinate of the conductor). However, in this example, if the initial distribution was uniform over each copy of H (possibly with different constants for different copies), then the injected entropy is wasted. In order to save this injected entropy, we use buffer.

We define three conductor $\langle E_1, C_1\rangle, \langle E_2, C_2\rangle$ and E each of which plays the role of G, H, H in the original zig-zag product.

(1) $\langle E_1, C_1\rangle : \{0,1\}^{n_1} \times \{0,1\}^{d_1} \to \{0,1\}^{m_1} \times \{0,1\}^{b_1}$, a permutation conductor
(2) $\langle E_2, C_2\rangle : \{0,1\}^{n_2} \times \{0,1\}^{d_2} \to \{0,1\}^{d_1} \times \{0,1\}^{b_2}$, a buffer conductor
(3) $E_3 : \{0,1\}^{b_1+b_2} \times \{0,1\}^{d_3} \to \{0,1\}^{m_3}$, a lossless conductor.

The zig-zag product for conductors produces the conductor $E : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ where $n = n_1 + n_2$ and $d = d_2 + d_3$ and $m = m_1 + m_3$. Let $x_1, x_2, r_2, r_3, y_1, y_2, y_3$ be binary strings of respective lengths $n_1, n_2, d_2, d_3, m_1, d_1, m_3$. We evaluate by

(1) $(y_2, z_2) = \langle E_2, C_2\rangle(x_2, r_2)$
(2) $(y_1, z_1) = \langle E_1, C_1\rangle(x_1, y_2)$
(3) $y_3 = E_3(z_1 z_2, r_3)$.

and let $y_1 y_3 = E(x_1 x_2, r_2 r_3)$. Let $X_1, X_2, X_3, Y_1, Y_2, Y_3, R_2, R_3$ be the random variables, and $x_1, \ldots, r_3$ be the actual string we get from the random variables.

The first $\langle E_2, C_2\rangle$ ensures that Y_2 is close to uniform when X_2 has high min-entropy, thus Y_2 is a good seed for $\langle E_1, C_1\rangle$ up to small error term. (This is like the first use of H

in the zig-zag product $G \textcircled{z} H$ for bipartite graphs) The second use of H is replaced with E_3 that transfers entropy lost in $\langle E_1, C_1\rangle$ and $\langle E_2, C_2\rangle$ to the output. The deterministic step of the zig-zag product using the graph G is replaced with $\langle E_1, C_1\rangle$, which as before doesn't use any new random bits and whose output is just a permutation of its input (which moves entropy about to allow more to come in later).

By constructing lossless conductor, we can prove the following theorem.

Theorem 7.9. *For any $\varepsilon > 0$ and $M \le N$, there is an explicit family of left D-regular bipartite graphs that are $(\Omega(\varepsilon M/D), \varepsilon)$-lossless expanders, where $D \le (N/\varepsilon M)^c$ for some constant c.*

Note that if $\varepsilon, M/N$ are bounded from below, then D is a constant. For this, we instead prove the following. When $D = 2^d$, the condition $D \le (N/(\varepsilon M))^c$ is equivalent to $d \le c(\log(1/\varepsilon) + \log(N/M))$. So, the following condition $a = 1000\log(1/\varepsilon)$ and $d = 2a$ is good for us to deduce the above theorem.

Theorem 7.10. *We can construct $E : \{0,1\}^n \times \{0,1\}^{2a} \to \{0,1\}^{n-3a}$, which is an $(n - 30a, 4\varepsilon)$-lossless conductor, where $a = 1000\log(1/\varepsilon)$.*

Before this, one thing to note is the following. In order to estimate $H_\infty(X, Y)$, we need to measure $\max_{x,y} \mathbb{P}[(X, Y) = (x, y)]$. In order to compare this with $H_\infty(X)$, what we need is a way to compare $\mathbb{P}[X = x]$ with $\mathbb{P}[(X, Y) = (x, y)]$. Hence, it would be useful if we have some information about the conditional probability $\mathbb{P}[Y = y \mid X = x]$. The following lemma will ensures that we can decomposed a probability distribution (X_1, X_2) into two types up to small error term, where each type will be easier for us to analyze in terms of their min-entropy.

Lemma 7.11. *Let (X_1, X_2) be a probability distribution on a finite product space. Given $\varepsilon > 0$ and a, there exists a distribution (Y_1, Y_2) on the same space such that*

1. *The distributions (X_1, X_2) and (Y_1, Y_2) are ε-close*
2. *The distribution (Y_1, Y_2) is a convex combination of two other distributions $(\hat{Y}_1, \hat{Y}_2)$ and $(\check{Y}_1, \check{Y}_2)$ each having min-entropy at least $H_\infty(X_1, X_2) - \log(1/\varepsilon)$.*
3. *For all $x \in Supp(\hat{Y}_1)$, we have $H_\infty(\hat{Y}_2 \mid \hat{Y}_1 = x) \ge a$.*
4. *For all $x \in Supp(\check{Y}_1)$, we have $H_\infty(\check{Y}_2 \mid \check{Y}_1 = x) < a$.*

Proof. We split $Supp(X_1)$ according to $H_\infty(X_2 \mid X_1 = x)$:

$$\hat{S} = \{z : H_\infty(X_2 \mid X_1 = z) \ge a\}, \check{S} = \{z : H_\infty(X_2 \mid X_1 = z) < a\}.$$

Then we define

$$\mathbb{P}[(\hat{Y}_1, \hat{Y}_2) = (z_1, z_2)] = \mathbb{P}[(X_1, X_2) = (z_1, z_2) \mid X_1 \in \hat{S}]$$
$$\mathbb{P}[(\check{Y}_1, \check{Y}_2) = (z_1, z_2)] = \mathbb{P}[(X_1, X_2) = (z_1, z_2) \mid X_1 \in \check{S}]$$

Let $p = \mathbb{P}[X_1 \in \hat{S}]$. Then the probability of each value in $(\hat{Y}_1, \hat{Y}_2)$ is multiplied by $1/p$ and the probability of each value in $(\check{Y}_1, \check{Y}_2)$ is multiplied by $1/(1-p)$. Hence, if $\varepsilon \le p \le 1 - \varepsilon$, then the min-entropy of $(\hat{Y}_1, \hat{Y}_2)$ and $(\check{Y}_1, \check{Y}_2)$ is reduced by at most $\log(1/\varepsilon)$. In this case, we let $(Y_1, Y_2) = (X_1, X_2)$ and we are done, as it is a convex cobination $(Y_1, Y_2) = p(\hat{Y}_1, \hat{Y}_2) + (1-p)(\check{Y}_1, \check{Y}_2)$.

Otherwise, assume $p < \varepsilon$ (the other case is similar). In this case, we take $(Y_1, Y_2) = (\check{Y}_1, \check{Y}_2)$. This distribution is ε-close to (X_1, X_2) since

$$\sum_{z_1 \in \hat{S}, z_2} |\mathbb{P}[(X_1, X_2) = (z_1, z_2)] - \mathbb{P}[(\check{Y}_1, \check{Y}_2) = (z_1, z_2)| \le p \le \varepsilon$$

$$\sum_{z_1 \in \check{S}, z_2} |\mathbb{P}[(X_1, X_2) = (z_1, z_2)] - \mathbb{P}[(\check{Y}_1, \check{Y}_2) = (z_1, z_2)| \le (\frac{1}{1-p} - 1)(1-p) = p < \varepsilon.$$

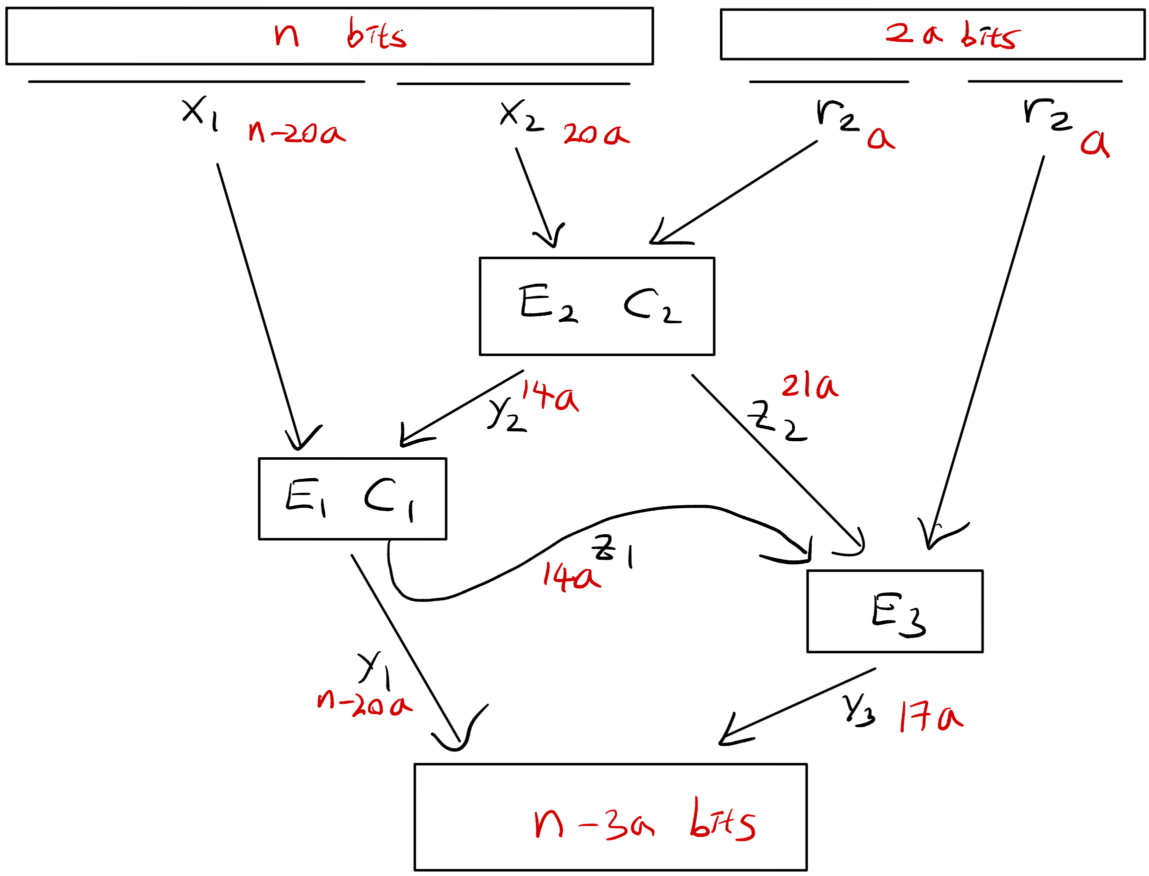

FIGURE 1. Conductor E.

□

Proof. We now prove the main theorem. Assume we have the following.

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

The binary strings $X_1, X_2, X_3, Y_1, Y_2, Y_3, R_2, R_3$ are as explained before.

As a is a constant, exhaustive search yields $\langle E_2, C_2\rangle$ and E_3.

$\langle E_1, C_1\rangle$ has big size, so constructing this requires something other than exhaustive search. Simply take a graph G which is close to be a 2^d-regular Ramanujan graph, and make it bipartite by taking vertex set $V(G) \times \{1,2\}$ and edges $(u,1)(v,2)$ for each $uv \in E(G)$. This yields the desired E_1 where X_1 is the given probability distribution on $V(G) \times \{1\}$ and Y_2 is the choice of its neighbor on each vertex. And Y_1 is the distribution on the vertex set $V(G) \times \{2\}$ which we reach after taking a random step, and Z_1 is the edge we took to reach to the right vertex, which is the distribution on the edges incident to the vertex on $V(G) \times \{2\}$.

As we saw at the end of Section 3, $\lambda(G)$ being very small implies that the 2-entropy of Y_1 is guaranteed to be increased from the 2-entropy of X_1.

One thing we can easily show is that if the 2-entropy of X is b, then X is as $(b - \log(1/\varepsilon), \varepsilon)$-source. By using this rough equivalence of the 2-entropy and the min-entropy, we can also show that the min-entropy of Y_1 is also bigger than the min-entropy of X_1 by the desired amount with small error. Thus we obtain the desired permutation conductor.

We would like to prove that if $H_\infty(X_1, X_2) = k$, then $Y_1 Y_3$ is a $(k + 2a, 4\varepsilon)$-source as long as $k \leq n - 30a$. For ease of discussion, we first ignore the small ℓ_1-errors in the outputs of all conductors. These errors will simply be added at the end to give the final error of the lossless conductor E.

Claim 5. $H_\infty(Y_1) \geq k - 14a$.

Proof. Note that if a probability distribution Z is a convex combination $pZ_1 + (1-p)Z_2$ of two probability distribution where Z_1, Z_2 both have min-entropy at least b, then $H_\infty(Z)$ is also at least b.[1] By Lemma 7.11, this shows that we only have to prove this bound for the extreme cases when $H_\infty(X_2 \mid X_1 = x_1)$ are all large or all small for all attainable values for x_1.

As we assume $H_\infty(X_1, X_2) \geq k$, we know that for any (x_1, x_2), we have

$$\mathbb{P}[X_1 = x_1]\mathbb{P}[X_2 = x_2 \mid X_1 = x_1] = \mathbb{P}[(X_1, X_2) = (x_1, x_2)] \leq 2^{-k}.$$

Hence if we know $H_\infty(X_2 \mid X_1 = x_1) \leq b$, meaning that $\max_{x_2} \mathbb{P}[X_2 = x_2 \mid X_1 = x_1] \geq 2^{-b}$, then we have $\mathbb{P}[X_1 = x_1] \leq 2^{-k+b}$ and this yields $H_\infty(X_1) \geq k - b$.

In order for us to estimate min-entropies of product distribution, we fix one part and consider conditional min-entropy.

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

In this case, as E_2 is an $(0, \varepsilon)$-extracting conductor, $H_\infty(Y_2 \mid X_1 = x_1) = 14a$, for any $x_1 \in \mathit{Supp}(X_1)$. Hence Y_2 is uniform (up to ε-error in ℓ_1 norm which we ignore for now) and can be used as a seed for $\langle E_1, C_1 \rangle$ for any $x_1 \in \mathit{Supp}(X_1)$. As $\max_{x_2}[X_2 = x_2 \mid X_1 = x_1] \leq 2^{-20a}$, we know $H_\infty(X_1) \geq k - 20a$. As E_1 is a $(6a, \varepsilon)$-extracting conductor, E_1 conducts $6a$ bits of entropy from the seed into Y_1 and we obtain $H_\infty(Y_1) \geq k - 14a$.

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

Since $H_\infty(X_1, X_2) = k$, it follows that $H_\infty(X_1) \geq k - 14a$. As E_2 is a $(0, \varepsilon)$-extractor, $H_\infty(Y_2 \mid X_1 = x_1) \geq H_\infty(X_2 | X_1 = x_1)$ for any $x_1 \in \mathit{Supp}(X_1)$. 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 $H_\infty(Y_1) \geq k - 14a$.

□

[1] Recall that min-entropy of a distribution Z is same as $-\log(\max_z \mathbb{P}[Z = z])$. then we have $\mathbb{P}[E(Z) = z] = p\mathbb{P}[E(Z_1) = z] + (1-p)\mathbb{P}[E(Z_2) = z]$. By taking $-\log \max_z()$ on both side, we have

$$\begin{aligned} H_\infty(Z) &= -\log(\max_z(p\mathbb{P}[E(Z_1) = z] + (1-p)\mathbb{P}[E(Z_2) = z])) \\ &\geq -\log\left(p \max_z \mathbb{P}[E(Z_1) = z] + (1-p) \max_{z'} \mathbb{P}[E(Z_2) = z']\right) \\ &\geq -\log(p2^{-b} + (1-p)2^{-b}) = b. \end{aligned}$$

Both $\langle E_1, C_1\rangle$ and $\langle E_2, C_2\rangle$ conserve entropy (as they are permutation conductor and buffer conductor). Hence

$$k + a = H_\infty(X_1, X_2, R_2) = H_\infty(X_1, Y_2, Z_2) = H_\infty(Y_1, Z_1, Z_2). \tag{7.1}$$

We now aim to show that $\mathbb{P}[(Y_1, Y_3) = (y_1, y_3)] \le 2^{-k-2a}$ for any y_1, y_3, which will show $H_\infty(Y_1, Y_3) \ge k + 2a$. For this, consider a string $y_1 \in Supp(Y_1)$.

If $H_\infty(Z_1, Z_2 \mid Y_1 = y_1) \ge 15a$, then as E_3 is a $(15a, a, \varepsilon)$-conductor, we have $H_\infty(Y_3 \mid Y_1 = y_1) \ge 16a$. Hence, for any y_3, we have

$$\mathbb{P}[Y_3 = y_3 \mid Y_1 = y_1] \le 2^{-16a}.$$

Hence, for such y_1 and any y_3, we have

$$\mathbb{P}[(Y_1, Y_3) = (y_1, y_3)] \le 2^{-16a}\mathbb{P}[Y_1 = y_1] \le 2^{-16a}2^{-k+14a} \le 2^{-k-2a}.$$

If $H_\infty(Z_1, Z_2 \mid Y_1 = y_1) \le 15a$, then as E_3 which is $(15a, a, \varepsilon)$-conductor, conducts a bits of entropy from R_3 to Y_3. That is, all the entropy of Z_1, Z_2 is transferred to the output Y_3 without any entropy loss, $H_\infty(Y_3 \mid Y_1 = y_1) = H_\infty(Z_1, Z_2 \mid Y_1 = y_1) + a$. Together with Claim 5 and (7.1), for any y_3, we have

$$\mathbb{P}[Y_3 = y_3 \mid Y_1 = y_1] \le 2^{-H_\infty(Z_1,Z_2|Y_1=y_1)-a} \le 2^{-a} \max_{z_1,z_2} \mathbb{P}[Z_1 = z_1, Z_2 = z_2 \mid Y_1 = y_1].$$

Hence,

$$\begin{aligned}\mathbb{P}[(Y_1, Y_3) = (y_1, y_3)] &= \mathbb{P}[Y = y_1] \cdot 2^{-a} \max_{z_1,z_2} \mathbb{P}[Z_1 = z_1, Z_2 = z_2 \mid Y_1 = y_1] \\ &\le 2^{-a} \max_{z_1,z_2,y} \mathbb{P}[Z_1 = z_1, Z_2 = z_2, Y_1 = y] \\ &\le 2^{-a}2^{-H_\infty(Y_1,Z_1,Z_2)} = 2^{-k-2a}.\end{aligned}$$

Therefore, for any y_1, y_3, we have $\mathbb{P}[(Y_1, Y_3) = (y_1, y_3)] \le 2^{-k-2a}$, so we have $H_\infty(Y_1, Y_3) = k + 2a$ as claimed.

To see the dependence on ε, note that these ℓ_1 errors on the extractor outputs add up. In the above analysis, we make four moves from a variable to its ε-close counterpart, one for each $\langle E_1, C_1\rangle, \langle E_2, C_2\rangle, E_3$ and one in the use of the Lemma 7.11. Hence we conclude that E is an $(n - 30a, 2a, 4\varepsilon)$-lossless conductor. □

References

[1] S. Hoory, N. Linial, and A. Wigderson, *Expander graphs and their applications*, Bulletin of the Amererican Mathematical Society 43(4), 2006.