Theoretical Limitations of multi-layer Transformer

Paper by: Lijie Chen, Binghui Peng, Hongxun Wu

PALMS Group Lunch, 3/25

Result

Main result:

For any constant L, there exists an input on n tokens for which any L layer decoder-only transformer needs polynomial model dimension, $n^{\Omega(1)}$, to solve.

(Benefits of Chain-of-Thought)

The function from **Main Result** can be computed by an $L + 1$ layer decoder-only transformer with poly$(\log(n))$ model dimension.

"there exists a task exponentially harder for L layer transformers than for $(L + 1)$ layer transformers"

Notable omissions: Everything in the appendix – some complexity theoretic results.

Talk Outline

- Discuss *decoder-only transformer*
- Discuss hard function – sequential composition
- Autoregressive Communication Game
- Reducing transformer to communication model
- Lower-bound on the game

Talk Outline

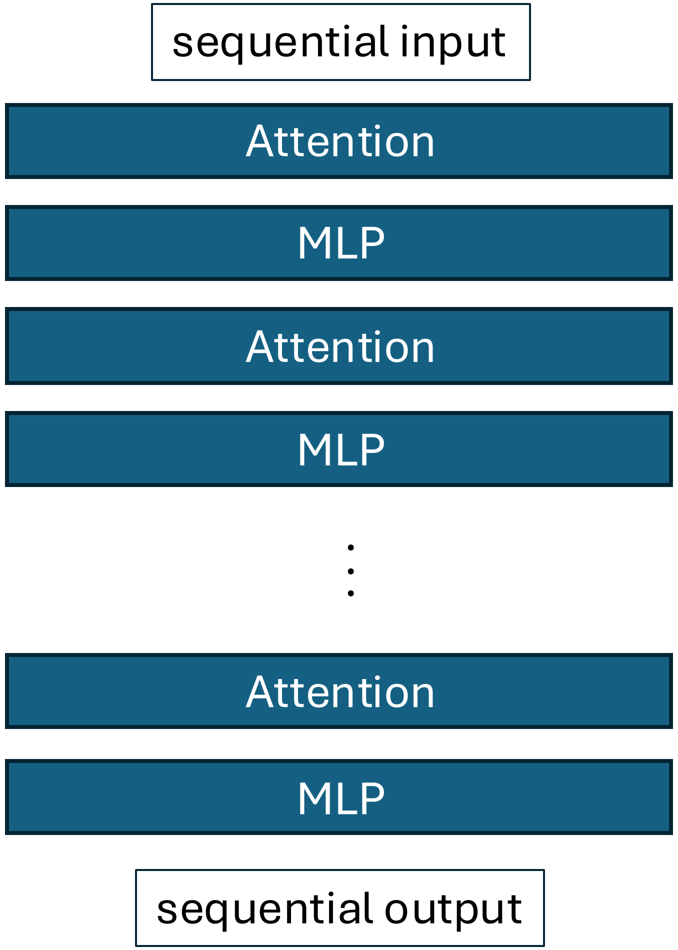
- **Discuss *decoder-only transformer***
- Discuss hard function – sequential composition
- Autoregressive Communication Game
- Reducing transformer to communication model
- Lower-bound on the game

High-level Architecture

$$f_{\text{tran}} = f^{(L)}_{\text{mlp}} \circ f^{(L)}_{\text{attn}} \circ \cdots \circ f^{(1)}_{\text{mlp}} \circ f^{(1)}_{\text{attn}}$$

Each layer has several *heads* which assist with computation

Transformer Jargon	Symbol
Number of layers/ "depth"	L
Number of heads	H
Embedding Dimension	d
Precision per entry in embedding	p
Model dimension / "width"	dHp



sequential input

Attention

MLP

Attention

MLP

⋮

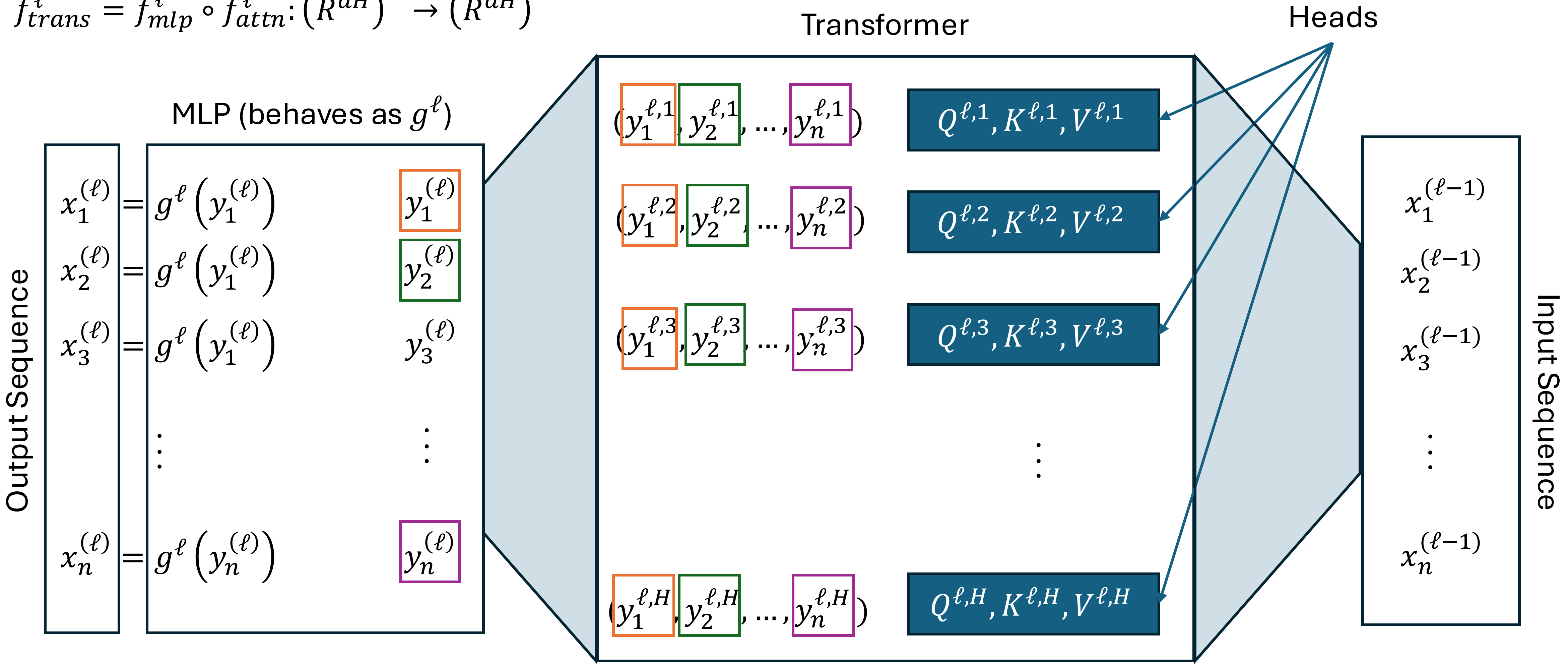
Attention

MLP

sequential output

View within a level, ℓ

$$f_{trans}^{\ell} = f_{mlp}^{\ell} \circ f_{attn}^{\ell} \colon \left(R^{dH}\right)^{n} \to \left(R^{dH}\right)^{n}$$

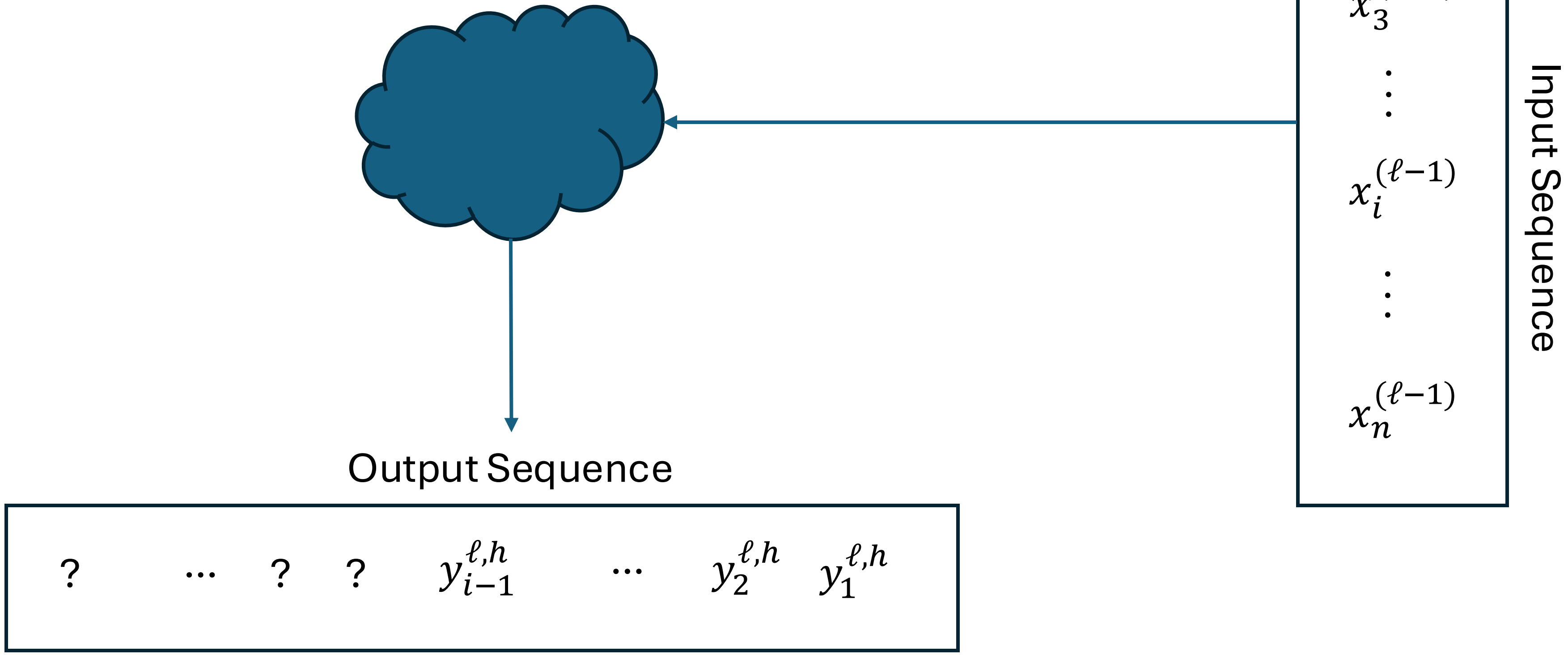

Transformer
Heads
MLP (behaves as g^{ℓ})
Output Sequence
$x_1^{(\ell)} = g^{\ell}\left(y_1^{(\ell)}\right)$
$x_2^{(\ell)} = g^{\ell}\left(y_1^{(\ell)}\right)$
$x_3^{(\ell)} = g^{\ell}\left(y_1^{(\ell)}\right)$
$\vdots$
$x_n^{(\ell)} = g^{\ell}\left(y_n^{(\ell)}\right)$
$y_1^{(\ell)}$
$y_2^{(\ell)}$
$y_3^{(\ell)}$
$\vdots$
$y_n^{(\ell)}$
$(y_1^{\ell,1}, y_2^{\ell,1}, \ldots, y_n^{\ell,1})$
$Q^{\ell,1}, K^{\ell,1}, V^{\ell,1}$
$(y_1^{\ell,2}, y_2^{\ell,2}, \ldots, y_n^{\ell,2})$
$Q^{\ell,2}, K^{\ell,2}, V^{\ell,2}$
$(y_1^{\ell,3}, y_2^{\ell,3}, \ldots, y_n^{\ell,3})$
$Q^{\ell,3}, K^{\ell,3}, V^{\ell,3}$
$\vdots$
$(y_1^{\ell,H}, y_2^{\ell,H}, \ldots, y_n^{\ell,H})$
$Q^{\ell,H}, K^{\ell,H}, V^{\ell,H}$
$x_1^{(\ell-1)}$
$x_2^{(\ell-1)}$
$x_3^{(\ell-1)}$
$\vdots$
$x_n^{(\ell-1)}$
Input Sequence

View within a head, (ℓ, h)

The function f_{attn}^{ℓ} is made up of H heads, each responsible for a sequence $(y_1^{\ell,h}, y_2^{\ell,h}, \ldots, y_n^{\ell,h})$

Computation is parametrized by $\mathrm{Q}^{\ell,h}, \mathrm{K}^{\ell,h}, \mathrm{V}^{\ell,h} \in R^{d \times dH}$

Below: Generating $y_i^{\ell,h}$



Input Sequence

$x_1^{(\ell-1)}$

$x_2^{(\ell-1)}$

$x_3^{(\ell-1)}$

$\vdots$

$x_i^{(\ell-1)}$

$\vdots$

$x_n^{(\ell-1)}$

Output Sequence

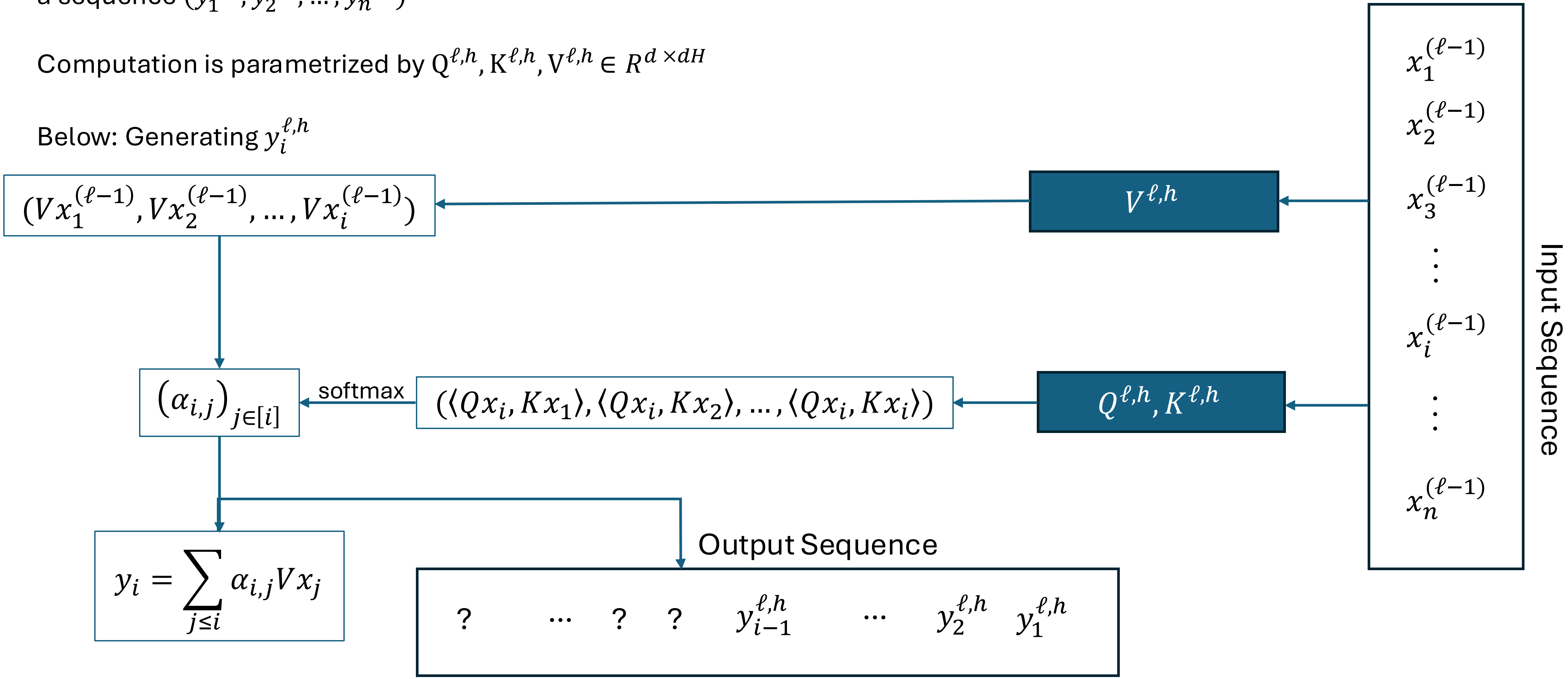
? … ? ? $y_{i-1}^{\ell,h}$ … $y_2^{\ell,h}$ $y_1^{\ell,h}$

View within a head, (ℓ, h)

The function f_{attn}^{ℓ} is made up of H heads, each responsible for a sequence $(y_1^{\ell,h}, y_2^{\ell,h}, \dots, y_n^{\ell,h})$

Computation is parametrized by $\mathrm{Q}^{\ell,h}, \mathrm{K}^{\ell,h}, \mathrm{V}^{\ell,h} \in R^{d \times dH}$

Below: Generating $y_i^{\ell,h}$



$(Vx_1^{(\ell-1)}, Vx_2^{(\ell-1)}, \dots, Vx_i^{(\ell-1)})$

$V^{\ell,h}$

$x_1^{(\ell-1)}$

$x_2^{(\ell-1)}$

$x_3^{(\ell-1)}$

$\vdots$

$x_i^{(\ell-1)}$

$\vdots$

$x_n^{(\ell-1)}$

Input Sequence

$(\alpha_{i,j})_{j\in[i]}$

softmax

$(\langle Qx_i, Kx_1\rangle, \langle Qx_i, Kx_2\rangle, \dots, \langle Qx_i, Kx_i\rangle)$

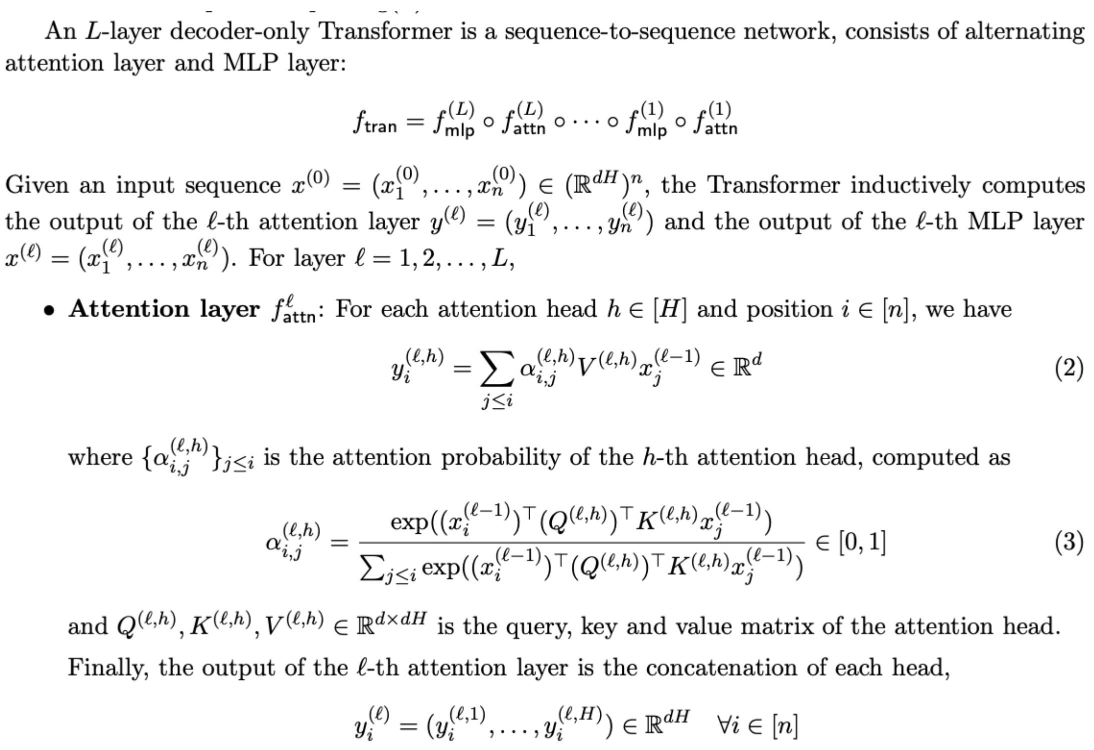
$Q^{\ell,h}, K^{\ell,h}$

$y_i = \sum_{j\leq i} \alpha_{i,j} V x_j$

Output Sequence

? … ? ? $y_{i-1}^{\ell,h}$ … $y_2^{\ell,h}$ $y_1^{\ell,h}$

Formalisms



An L-layer decoder-only Transformer is a sequence-to-sequence network, consists of alternating attention layer and MLP layer:

$$f_{\mathsf{tran}} = f_{\mathsf{mlp}}^{(L)} \circ f_{\mathsf{attn}}^{(L)} \circ \cdots \circ f_{\mathsf{mlp}}^{(1)} \circ f_{\mathsf{attn}}^{(1)}$$

Given an input sequence $x^{(0)} = (x_1^{(0)}, \ldots, x_n^{(0)}) \in (\mathbb{R}^{dH})^n$, the Transformer inductively computes the output of the ℓ-th attention layer $y^{(\ell)} = (y_1^{(\ell)}, \ldots, y_n^{(\ell)})$ and the output of the ℓ-th MLP layer $x^{(\ell)} = (x_1^{(\ell)}, \ldots, x_n^{(\ell)})$. For layer $\ell = 1, 2, \ldots, L$,

- **Attention layer** f_{attn}^{ℓ}: For each attention head $h \in [H]$ and position $i \in [n]$, we have

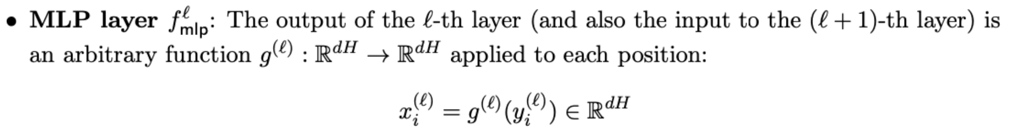
$$y_i^{(\ell,h)} = \sum_{j \le i} \alpha_{i,j}^{(\ell,h)} V^{(\ell,h)} x_j^{(\ell-1)} \in \mathbb{R}^d \tag{2}$$

where $\{\alpha_{i,j}^{(\ell,h)}\}_{j \le i}$ is the attention probability of the h-th attention head, computed as

$$\alpha_{i,j}^{(\ell,h)} = \frac{\exp((x_i^{(\ell-1)})^\top (Q^{(\ell,h)})^\top K^{(\ell,h)} x_j^{(\ell-1)})}{\sum_{j \le i} \exp((x_i^{(\ell-1)})^\top (Q^{(\ell,h)})^\top K^{(\ell,h)} x_j^{(\ell-1)})} \in [0,1] \tag{3}$$

and $Q^{(\ell,h)}, K^{(\ell,h)}, V^{(\ell,h)} \in \mathbb{R}^{d \times dH}$ is the query, key and value matrix of the attention head. Finally, the output of the ℓ-th attention layer is the concatenation of each head,

$$y_i^{(\ell)} = (y_i^{(\ell,1)}, \ldots, y_i^{(\ell,H)}) \in \mathbb{R}^{dH} \quad \forall i \in [n]$$



- **MLP layer** f_{mlp}^{ℓ}: The output of the ℓ-th layer (and also the input to the $(\ell+1)$-th layer) is an arbitrary function $g^{(\ell)} : \mathbb{R}^{dH} \to \mathbb{R}^{dH}$ applied to each position:

$$x_i^{(\ell)} = g^{(\ell)}(y_i^{(\ell)}) \in \mathbb{R}^{dH}$$

Takeaways

Within each head, computing $y_i^{\ell,h}$ has no (direct) dependence previous or future outputs in the sequence. Given the input sequence, one can think of these being computed “in parallel”

$y_i^{\ell,h}$ depends only on $(x_1^{(\ell-1)}, x_2^{(\ell-1)}, \dots, x_i^{(\ell-1)})$

There are succinct linear forms for most computation! Sadly, this will be ignored in this talk.

Talk Outline

- Discuss *decoder-only transformer*
- **Discuss hard function – sequential composition**
- Autoregressive Communication Game
- Reducing transformer to communication model
- Lower-bound on the game

Intuition

Consider input that *reverses* natural order of computation: earlier tokens have to “process” later tokens

Input sequence: $(z_L, z_{L-1}, \dots, z_0, w)$

Output (roughly): $z_L\left(z_{L-1}\left(\cdots\left(z_0(w)\right)\right)\right)$

We formalize the notion with a more ”granular” w.

L-sequential function composition

z_0 z_1 z_2 z_3 $\cdots$ z_{L-1} z_L

w_1

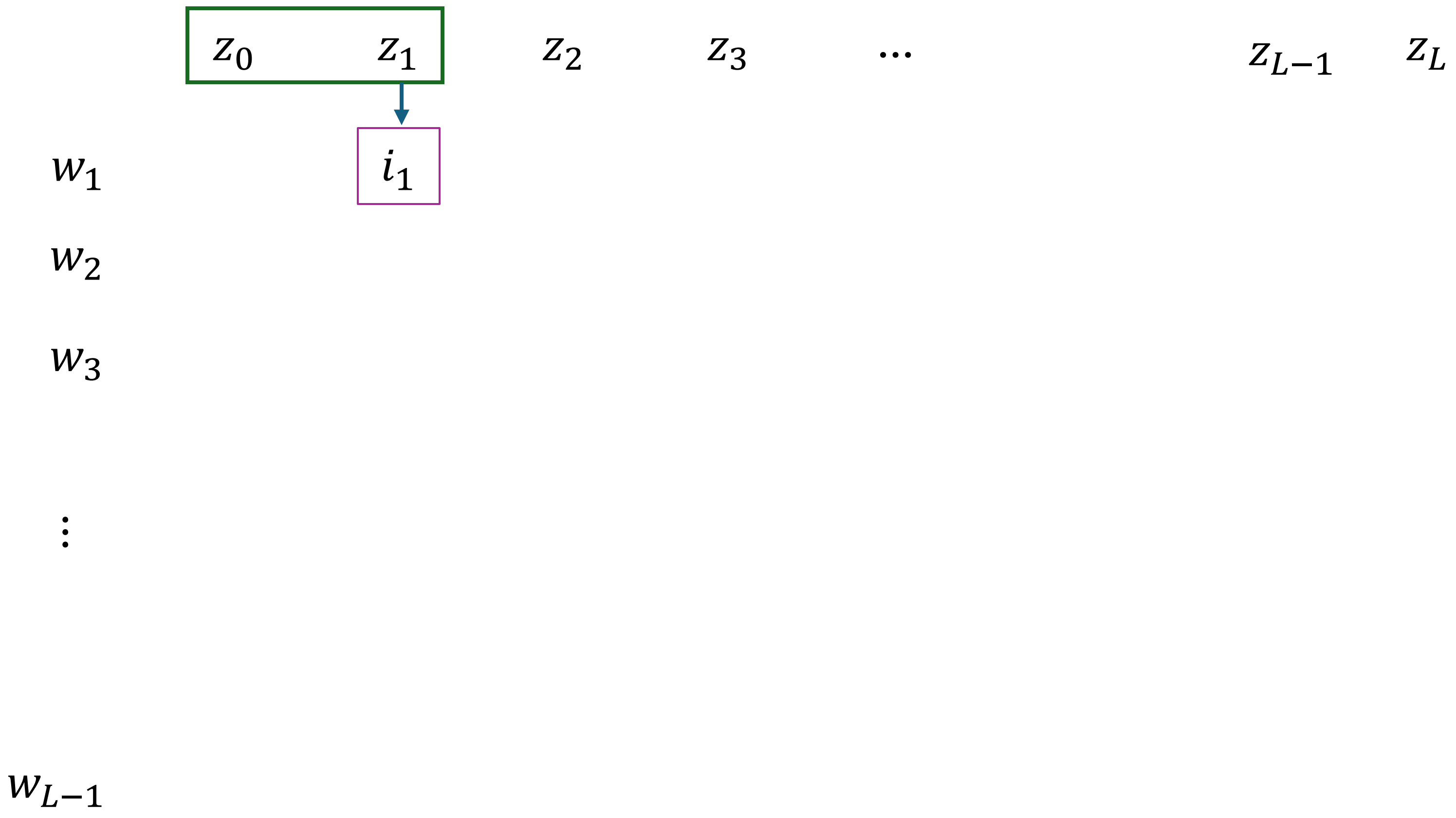
w_2

w_3

$\vdots$

w_{L-1}

L-sequential function composition



z_0 z_1 z_2 z_3 $\cdots$ z_{L-1} z_L

w_1 i_1

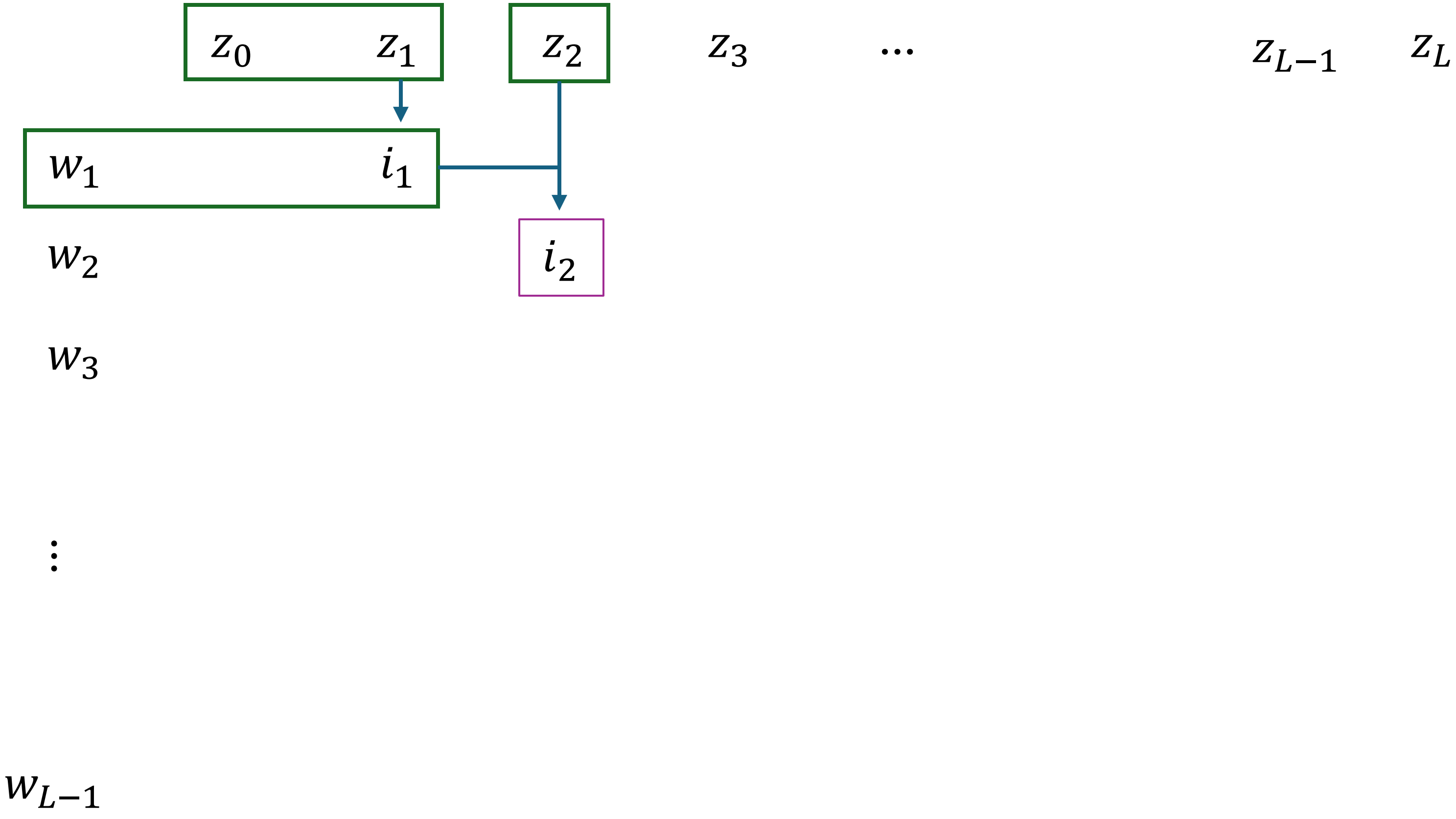
w_2

w_3

$\vdots$

w_{L-1}

L-sequential function composition



z_0 z_1 z_2 z_3 $\cdots$ z_{L-1} z_L

w_1 i_1

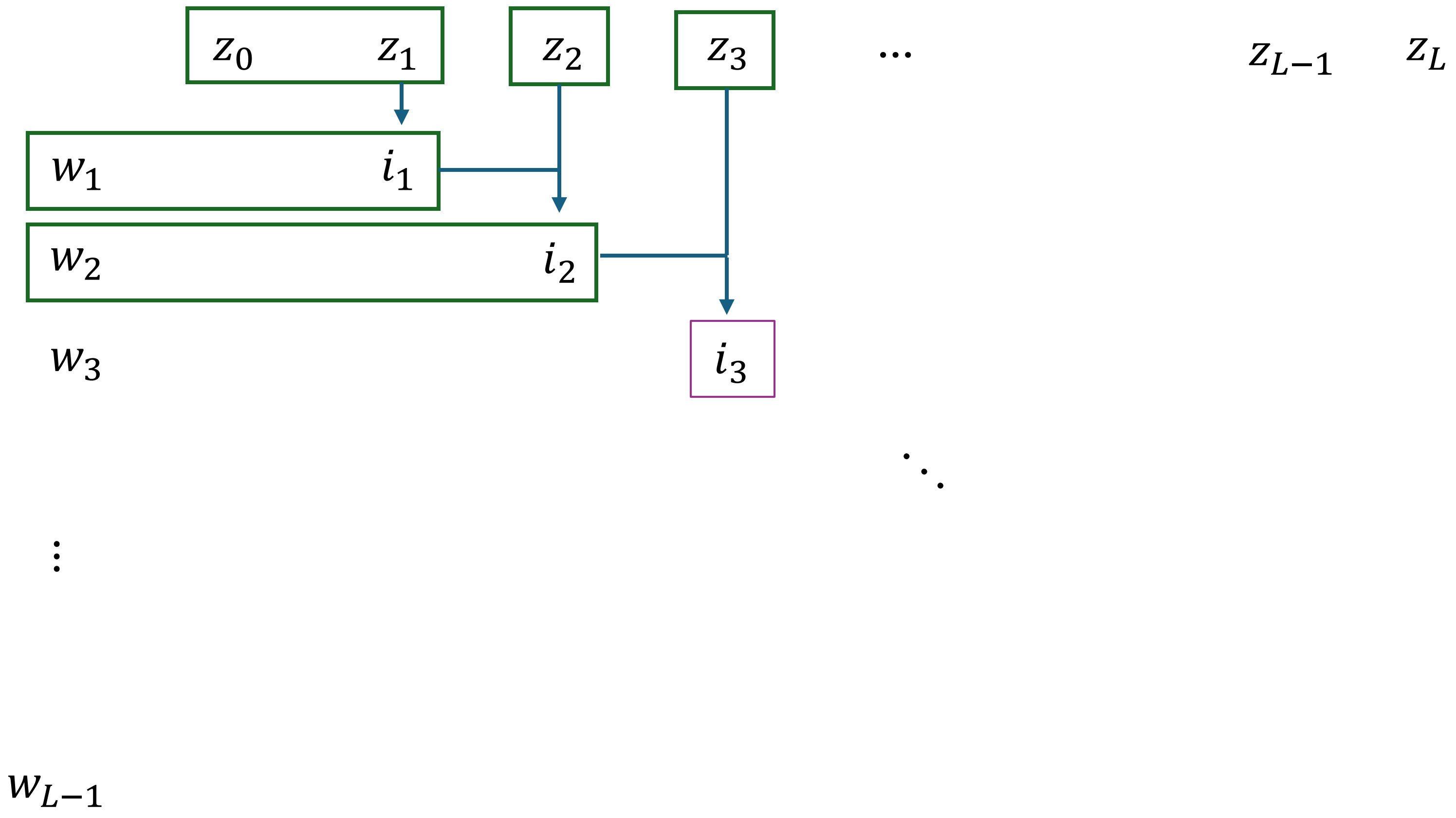
w_2 i_2

w_3

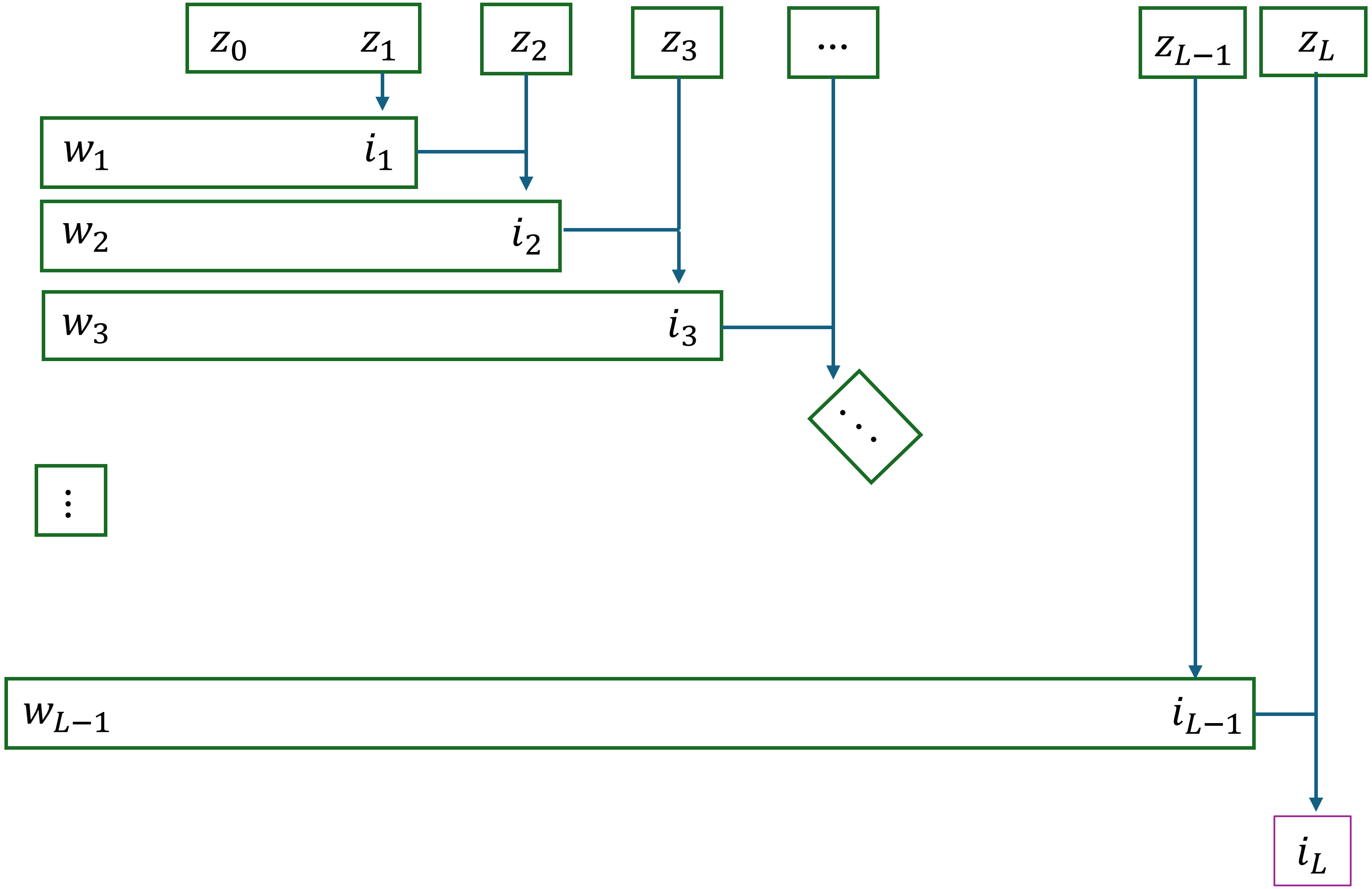
$\vdots$

w_{L-1}

L-sequential function composition

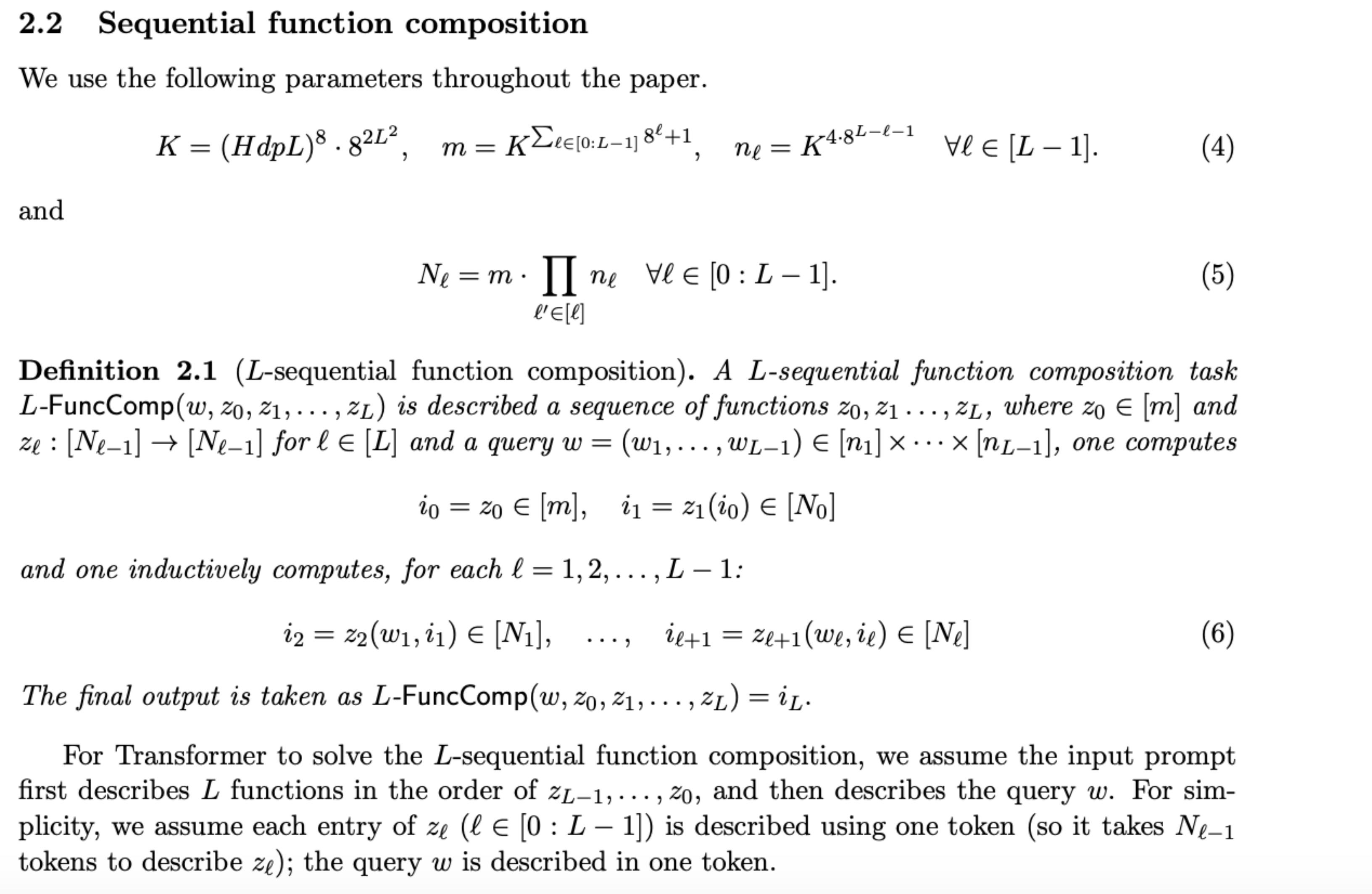


L-sequential function composition



Desired output!

Formalisms



2.2 Sequential function composition

We use the following parameters throughout the paper.

$$K = (HdpL)^8 \cdot 8^{2L^2}, \quad m = K^{\sum_{\ell \in [0:L-1]} 8^{\ell} + 1}, \quad n_\ell = K^{4 \cdot 8^{L-\ell-1}} \quad \forall \ell \in [L-1]. \tag{4}$$

and

$$N_\ell = m \cdot \prod_{\ell' \in [\ell]} n_\ell \quad \forall \ell \in [0 : L-1]. \tag{5}$$

Definition 2.1 (L-sequential function composition). *A L-sequential function composition task L-$\mathsf{FuncComp}(w, z_0, z_1, \ldots, z_L)$ is described a sequence of functions $z_0, z_1 \ldots, z_L$, where $z_0 \in [m]$ and $z_\ell : [N_{\ell-1}] \to [N_{\ell-1}]$ for $\ell \in [L]$ and a query $w = (w_1, \ldots, w_{L-1}) \in [n_1] \times \cdots \times [n_{L-1}]$, one computes*

$$i_0 = z_0 \in [m], \quad i_1 = z_1(i_0) \in [N_0]$$

and one inductively computes, for each $\ell = 1, 2, \ldots, L-1$:

$$i_2 = z_2(w_1, i_1) \in [N_1], \quad \ldots, \quad i_{\ell+1} = z_{\ell+1}(w_\ell, i_\ell) \in [N_\ell] \tag{6}$$

The final output is taken as L-$\mathsf{FuncComp}(w, z_0, z_1, \ldots, z_L) = i_L$.

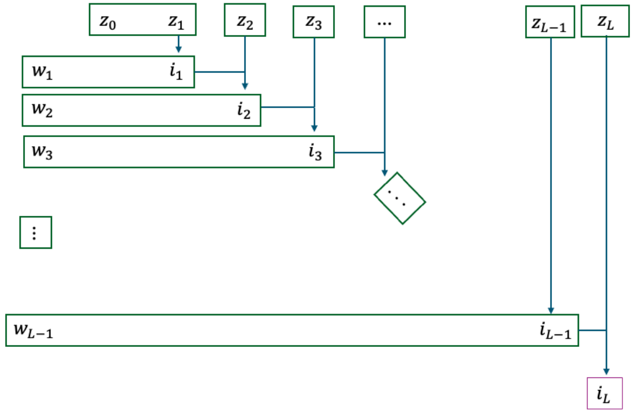
For Transformer to solve the L-sequential function composition, we assume the input prompt first describes L functions in the order of $z_{L-1}, \ldots, z_0$, and then describes the query w. For simplicity, we assume each entry of z_ℓ ($\ell \in [0 : L-1]$) is described using one token (so it takes $N_{\ell-1}$ tokens to describe z_ℓ); the query w is described in one token.

Some more observations…

It's natural to think about $z_\ell: [N_{\ell-1}] \to [N_{\ell-1}]$ as $z_\ell \in A_\ell$ where $A_\ell = [N_{\ell-1}^{N_{\ell-1}}]$ and the special case $A_0 = [m]$.

For the rest of the talk, we'll use $\mathrm{w} = \mathrm{z}_{-1}$ interchangeably. Thus, $A_{-1} = [n_1] \times [n_2] \times \cdots \times [n_{L-1}]$

After fixing $\widetilde{z_0}, \widetilde{z_1}, \ldots, \widetilde{z_\ell}$ reason that i_ℓ dependent only on $(w_1, w_2, \ldots, w_{l-1})$ and **independent** of w_l. This is the 🗝 for induction!



Talk Outline

- Discuss *decoder-only transformer*
- Discuss hard function – sequential composition
- **Autoregressive Communication Game**
- Reducing transformer to communication model
- Lower-bound on the game

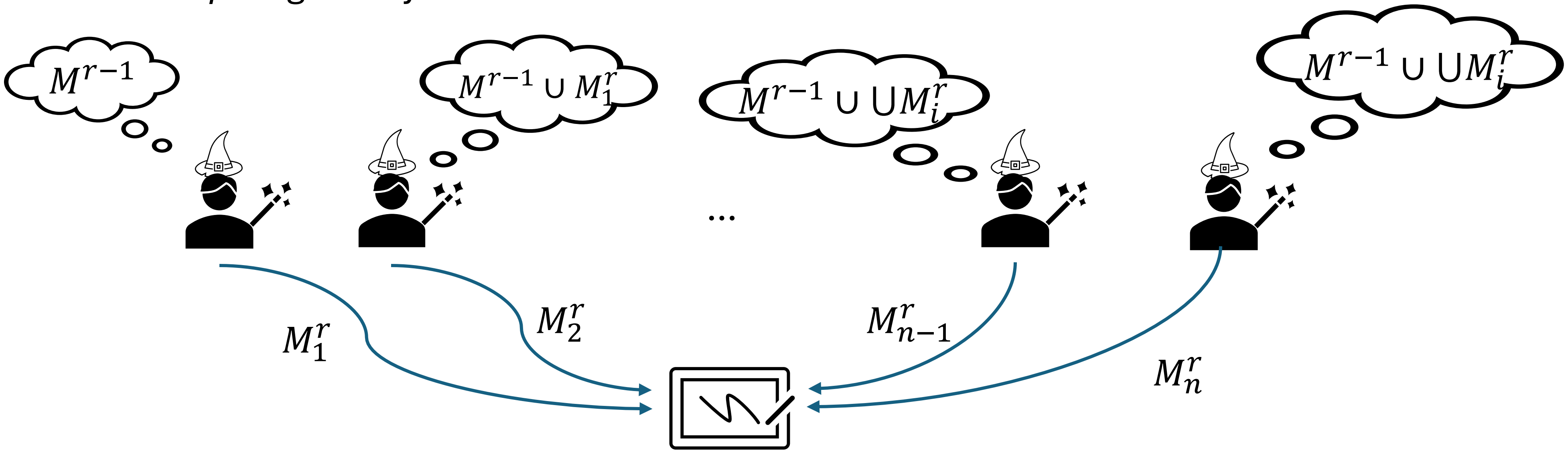
Multiparty Communication

Suppose there is some function $f\colon X_1 \times X_2 \times \cdots \times X_n \to Y$, and player i receives $x_i \in X_i$
How much *information* (bits) do they have to share in order to compute f?

Multiparty Communication

Suppose there is some function $f: X_1 \times X_2 \times \cdots \times X_n \to Y$, and player i receives $x_i \in X_i$
How much *information* (bits) do they have to share in order to compute f?

In the “blackboard” model, each round $r = 1, 2, \ldots r$, player $i = 1, 2, \ldots n$ writes $\Pi_{r,i}$ visible to everyone
The *transcript* is given by the contents of the blackboard at termination!



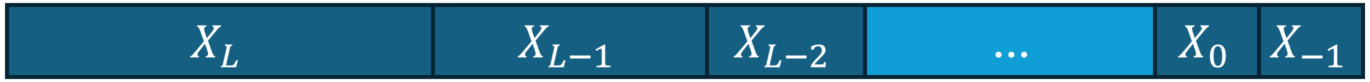
Output: f(M^R)

Many “memory” lower bounds follow from a reduction to this game, where one argues that a transcript of small size can’t compute f too well…

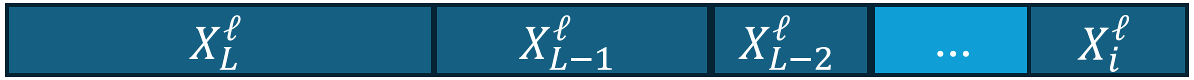
Autoregressive Game

To prove the sharper lower bounds, one should reduce to the *weakest* possible communication game

Input: $L+2$ players, $i \in [-1\colon L]$ each receiving z_i in m_i “tokens”



Game: At epoch $\ell = 0$, nothing has happened. For epoch $\ell \in [1\colon L]$ and for player $i \in [-1\colon L]$, execute the *game rooted at player i*

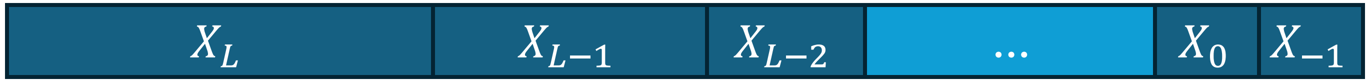


1. *player* i sends its information to all players $j \in [i+1\colon L]$
2. *player* j sends $\Pi_{j,i}^\ell$ of size at most $2B \cdot m_i$ back, depending on X_j^ℓ and X_i^ℓ

Autoregressive Game

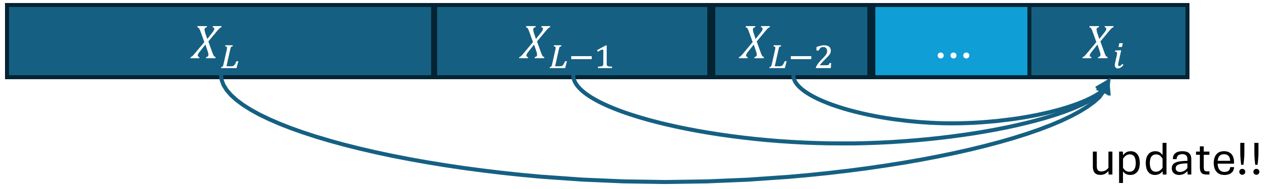
To prove the sharper lower bounds, one should reduce to the *weakest* possible communication game

Input: $L + 2$ players, $i \in [-1{:}\,L]$ each receiving z_i in m_i "tokens", message bits B



X_L X_{L-1} X_{L-2} … X_0 X_{-1}

Game: At epoch $\ell = 0$, nothing has happened. For epoch $\ell \in [1{:}\,L]$ and for player $i \in [-1{:}\,L]$, execute the *game rooted at player i*



X_L X_{L-1} X_{L-2} … X_i

update!!

1. *player* i sends its information to all players $j \in [i+1{:}\,L]$
2. *player* j sends $\Pi_{j,i}^{\ell}$ of size at most $2B \cdot m_i$ back, depending on X_j^{ℓ} and X_i^{ℓ}
3. *player* i accumulates responses: $X_i^{\ell+1} = X_i^{\ell} \cup \bigcup_{j>i} \Pi_{j,i}^{\ell}$

At the end of L epochs, player -1 computes a function on its information, and outputs a response!

Takeaways

Important to remember that player j does not “remember” its responses to $\mathrm{i} < j$
⇒ the game rooted at j is oblivious to the game rooted at i,
⇒ think about the games executing “in parallel” (familiar?)

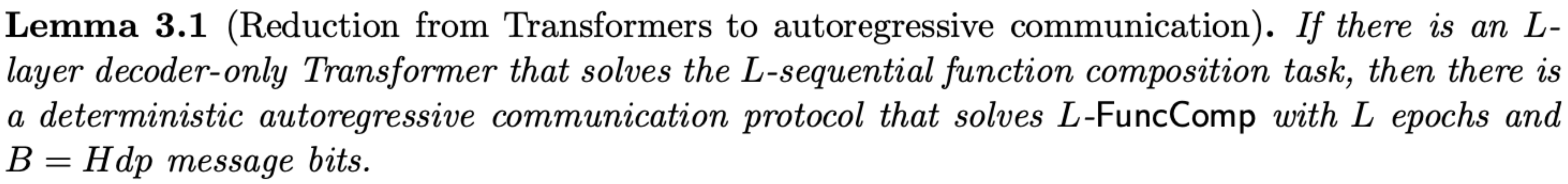
The player at the end of the line has the “strongest” communication power (familiar?), so it’s necessary to limit its input size

To avoid “short-circuit,” however, the first input should be *important* for the task.

Talk Outline

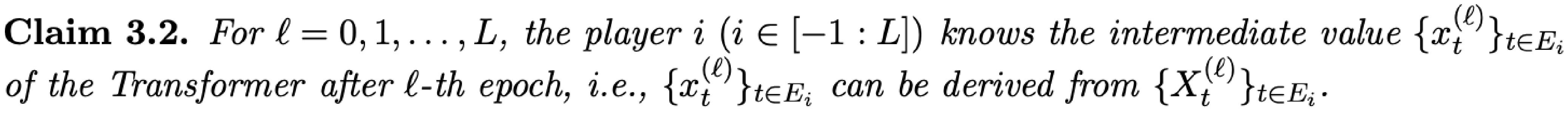
- Discuss *decoder-only transformer*
- Discuss hard function – sequential composition
- Autoregressive Communication Game
- **Reducing transformer to communication model**
- Lower-bound on the game

Main Lemma



Lemma 3.1 (Reduction from Transformers to autoregressive communication)**.** *If there is an L-layer decoder-only Transformer that solves the L-sequential function composition task, then there is a deterministic autoregressive communication protocol that solves L-*FuncComp *with L epochs and $B = Hdp$ message bits.*

In fact, we can go further: *any* transformer $\Gamma = \left(K^{\ell,h}, Q^{\ell,h}, V^{\ell,h}\right)_{\ell\in[L],h\in[H]}$ can be simulated in L epochs by an autoregressive communication protocol

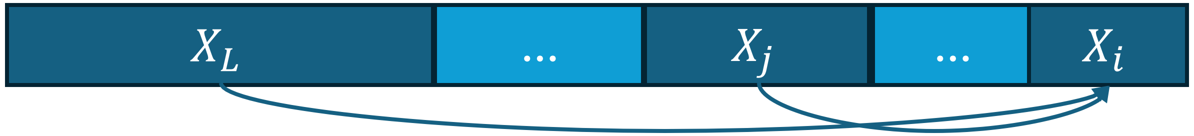


Claim 3.2. *For $\ell = 0, 1, \dots, L$, the player i ($i \in [-1 : L]$) knows the intermediate value $\{x_t^{(\ell)}\}_{t\in E_i}$ of the Transformer after ℓ-th epoch, i.e., $\{x_t^{(\ell)}\}_{t\in E_i}$ can be derived from $\{X_t^{(\ell)}\}_{t\in E_i}$.*

Main Lemma’s Main Claim

Claim 3.2. *For $\ell = 0, 1, \dots, L$, the player i ($i \in [-1 : L]$) knows the intermediate value $\{x_t^{(\ell)}\}_{t \in E_i}$ of the Transformer after ℓ-th epoch, i.e., $\{x_t^{(\ell)}\}_{t \in E_i}$ can be derived from $\{X_t^{(\ell)}\}_{t \in E_i}$.*

sketch Let E_j be the set of tokens making up input X_j. Clearly, at $\ell = 0$, the claim holds. We show by induction if it will hold at $\ell + 1$. Consider the game rooted at X_i



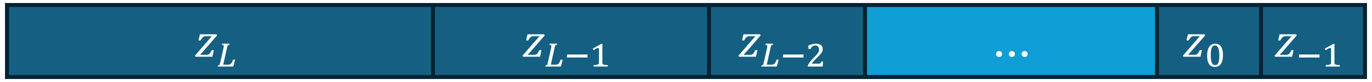
$$\Pi_{j,i}^{(\ell)} = \left\{ \sum_{t \in E_j} \exp((x_r^{(\ell-1)})^\top (Q^{(\ell,h)})^\top K^{(\ell,h)} x_t^{(\ell-1)}) V^{(\ell,h)} x_t^{(\ell-1)} \right\}_{h \in [H], r \in E_i}$$
$$\bigcup \left\{ \sum_{t \in E_j} \exp((x_r^{(\ell-1)})^\top (Q^{(\ell,h)})^\top K^{(\ell,h)} x_t^{(\ell-1)}) \right\}_{h \in [H], r \in E_i}$$

Using the first set from $\Pi_{j,i}^{(\ell)}$ we can compute external *values* and the second *set* to collect external key-query products.

Putting it together with local computation, (using internal values, key-query products, and g^{ℓ}), the update to X_i^{ℓ} contains enough information to compute $X_i^{\ell+1}$. This completes the induction.

Sequential Function Protocol

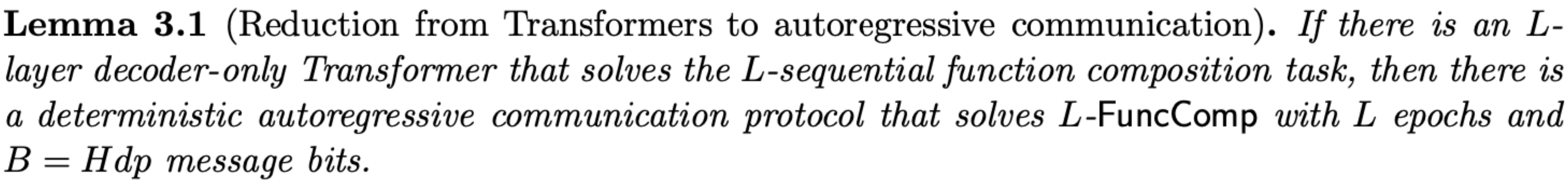
Suppose that the following input is given (read from left-to-right) to a transformer, who computes sequential function composition:



z_L z_{L-1} z_{L-2} … z_0 z_{-1}

where z_i is defined using N_i tokens (one for each input) whenever $i \geq 1$, and z_0, z_{-1} are defined in 1 token each.

By the previous claim, a transformer on this token sequence “solving” the sequential function problem can be turned into a communication protocol



Lemma 3.1 (Reduction from Transformers to autoregressive communication). *If there is an L-layer decoder-only Transformer that solves the L-sequential function composition task, then there is a deterministic autoregressive communication protocol that solves L-*FuncComp *with L epochs and $B = Hdp$ message bits.*

Talk Outline

- Discuss *decoder-only transformer*
- Discuss hard function – sequential composition
- Autoregressive Communication Game
- Reducing transformer to communication model
- **Lower-bound on the game**

Remaining Work

Lemma (Reduction): If there is an L layer decoder only transformer solving sequential composition, then there is a deterministic autoregressive communication protocol using at most L epochs and $B = Hdp$ message bits.

Lemma (Lower Bound): There is no autoregressive communication protocol solving sequential composition with L epochs and $B = Hdp$ message bits.

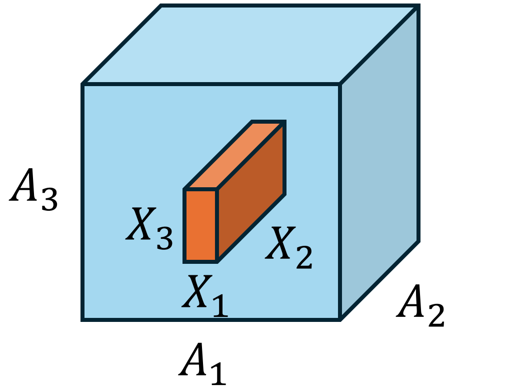
Main Thm follows after examining parameters (not in this talk!)

Communication Rectangles

Rectangles are a tool for combinatorial analysis of communication protocols

Often, when players are restricted to a *subset* of their input, the protocol has some shared behavior across *all* inputs in this subset

Note: Rectangles are *not* arbitrary subsets of $A_1 \times A_2 \times A_3$, but have to follow the ”product” nature which gives them this name!



$X_1 \subset A_1, X_2 \subset A_2, X_3 \subset A_3$

Players $[\ell, L]$

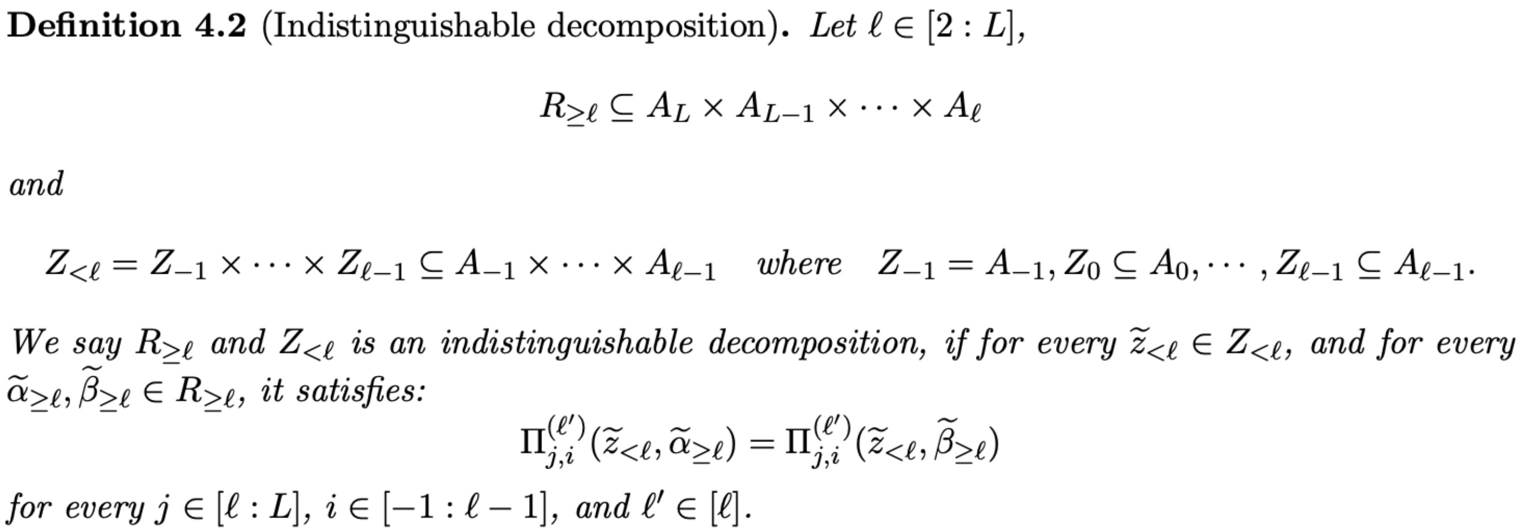
$$R_{\geq \ell} = Z_\ell \times Z_{\ell+1} \times \cdots \times Z_L$$

Players $[-1, \ell - 1]$

$$Z_{<\ell} = A_{-1} \times Z_0 \times \cdots \times Z_{\ell-1}$$

A pair of rectangles $(Z_{<\ell}, R_{\geq \ell})$ is called *indistinguishable* if, fixing any $\widetilde{Z_{<\ell}} \in Z_{<\ell}$, each $\widetilde{R_{\geq \ell}} \in R_{\geq \ell}$ produces the same *transcript* after ℓ epochs (round of communication)

Formalisms



Definition 4.2 (Indistinguishable decomposition)**.** *Let $\ell \in [2 : L]$,*

$$R_{\geq \ell} \subseteq A_L \times A_{L-1} \times \cdots \times A_\ell$$

and

$$Z_{<\ell} = Z_{-1} \times \cdots \times Z_{\ell-1} \subseteq A_{-1} \times \cdots \times A_{\ell-1} \quad \textit{where} \quad Z_{-1} = A_{-1}, Z_0 \subseteq A_0, \cdots, Z_{\ell-1} \subseteq A_{\ell-1}.$$

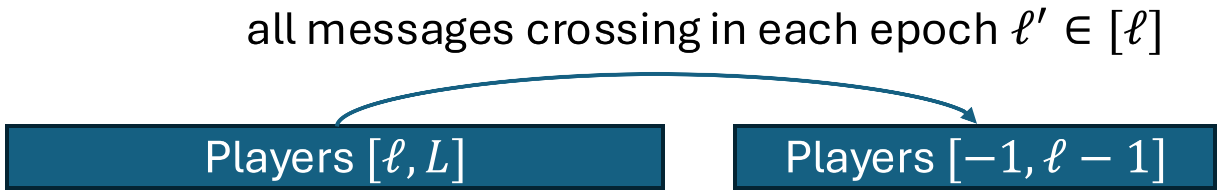
We say $R_{\geq \ell}$ and $Z_{<\ell}$ is an indistinguishable decomposition, if for every $\widetilde{z}_{<\ell} \in Z_{<\ell}$, and for every $\widetilde{\alpha}_{\geq \ell}, \widetilde{\beta}_{\geq \ell} \in R_{\geq \ell}$, it satisfies:

$$\Pi_{j,i}^{(\ell')}(\widetilde{z}_{<\ell}, \widetilde{\alpha}_{\geq \ell}) = \Pi_{j,i}^{(\ell')}(\widetilde{z}_{<\ell}, \widetilde{\beta}_{\geq \ell})$$

for every $j \in [\ell : L]$, $i \in [-1 : \ell - 1]$, and $\ell' \in [\ell]$.

Transcript

It’s worth formalizing a little further what we mean by “transcript” Λ^{ℓ} on $(Z_{<\ell}, R_{\geq \ell})$.



all messages crossing in each epoch $\ell' \in [\ell]$

Players $[\ell, L]$

Players $[-1, \ell - 1]$

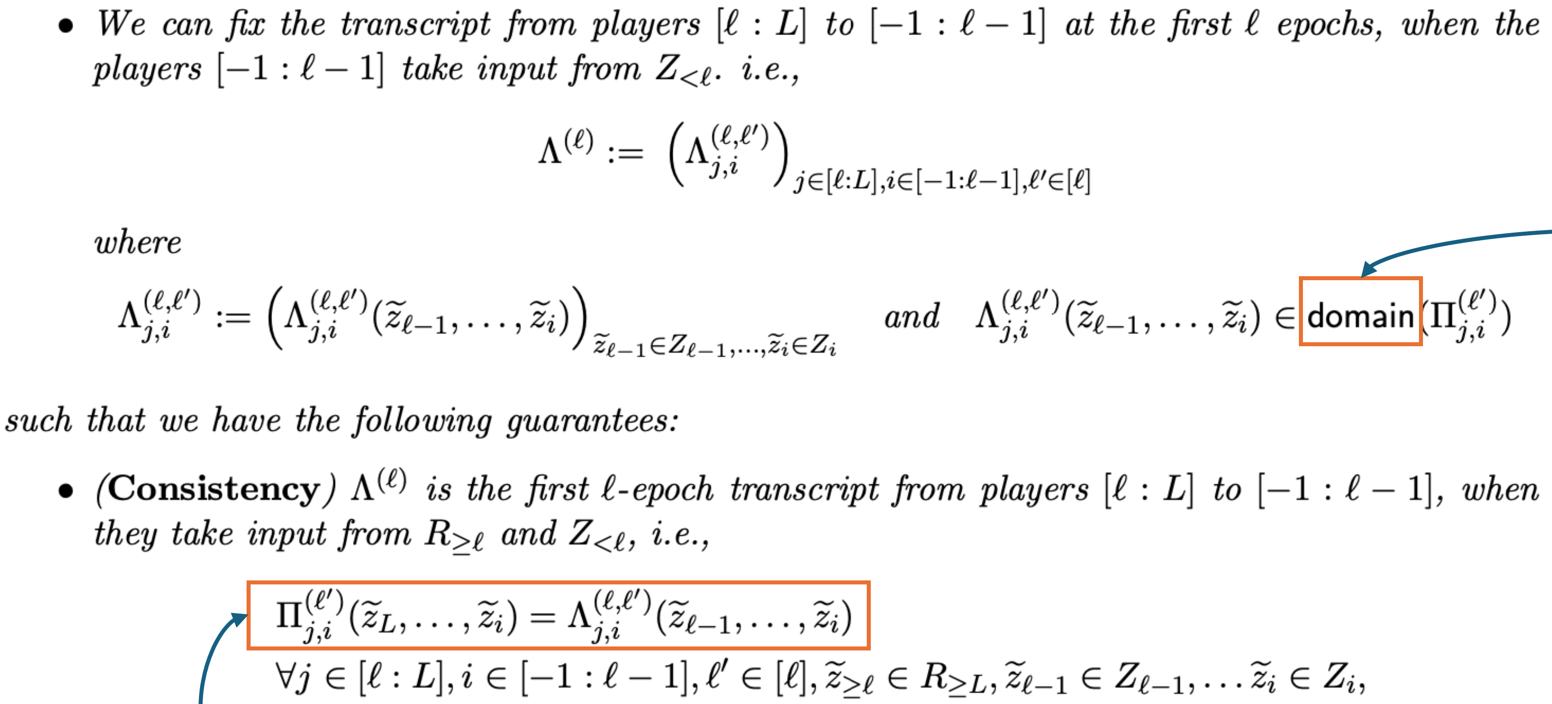
$R_{\geq \ell} = Z_{\ell} \times Z_{\ell+1} \times \cdots \times Z_L$ $\qquad$ $Z_{<\ell} = A_{-1} \times Z_0 \times \cdots \times Z_{\ell-1}$

In other words, Λ^{ℓ} is indexed by $\widetilde{Z_{<\ell}} \in Z_{<\ell}, \widetilde{R_{\geq \ell}} \in R_{\geq \ell}, \ell' \in [\ell], j \in [\ell, L], i \in [-1, \ell - 1\,]$

Key: If the decomposition is *indistinguishable*, what gets “sent back” is **independent** of $\widetilde{R_{\geq \ell}}$, thus we can index Λ^{ℓ} without it!

Formalism

The information from the previous slide is densely stuffed into formalisms here…



- *We can fix the transcript from players $[\ell : L]$ to $[-1 : \ell - 1]$ at the first ℓ epochs, when the players $[-1 : \ell - 1]$ take input from $Z_{<\ell}$. i.e.,*

$$\Lambda^{(\ell)} := \left(\Lambda_{j,i}^{(\ell,\ell')}\right)_{j\in[\ell:L],i\in[-1:\ell-1],\ell'\in[\ell]}$$

where

$$\Lambda_{j,i}^{(\ell,\ell')} := \left(\Lambda_{j,i}^{(\ell,\ell')}(\widetilde{z}_{\ell-1},\dots,\widetilde{z}_i)\right)_{\widetilde{z}_{\ell-1}\in Z_{\ell-1},\dots,\widetilde{z}_i\in Z_i} \quad \textit{and} \quad \Lambda_{j,i}^{(\ell,\ell')}(\widetilde{z}_{\ell-1},\dots,\widetilde{z}_i) \in \boxed{\text{domain}}(\Pi_{j,i}^{(\ell')})$$

such that we have the following guarantees:

- *(**Consistency**) $\Lambda^{(\ell)}$ is the first ℓ-epoch transcript from players $[\ell : L]$ to $[-1 : \ell - 1]$, when they take input from $R_{\geq\ell}$ and $Z_{<\ell}$, i.e.,*

$$\boxed{\Pi_{j,i}^{(\ell')}(\widetilde{z}_L,\dots,\widetilde{z}_i) = \Lambda_{j,i}^{(\ell,\ell')}(\widetilde{z}_{\ell-1},\dots,\widetilde{z}_i)}$$
$$\forall j \in [\ell : L], i \in [-1 : \ell - 1], \ell' \in [\ell], \widetilde{z}_{\geq\ell} \in R_{\geq L}, \widetilde{z}_{\ell-1} \in Z_{\ell-1}, \dots \widetilde{z}_i \in Z_i,$$

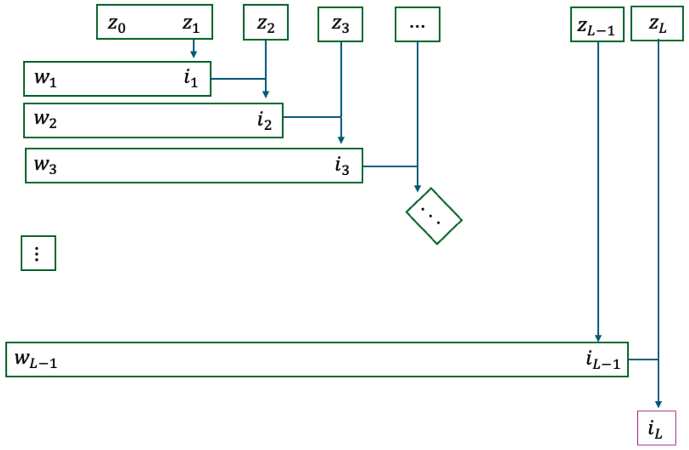
should this be range lol?

Here, we are “indexing” Λ^{ℓ} without $R_{\geq\ell}$ on all epochs $\ell' \in [\ell]$

Contradiction

Player L | Players $[-1, L-1]$

$R_{\geq L}$ | $Z_{<L}$



Suppose a successful protocol admits *indistinguishable* $(R_{\geq L}, Z_{<L})$

Then, for all $\widetilde{z_L} \in R_{\geq L}$, the output $\widetilde{z_L}\ (w_{L-1}, i_{L-1})$ should be the same!

Clearly, there are n_{L-1} possibilities for w_{L-1} (recall $Z_{-1} = A_{-1}$).

$$\mathcal{I}_{\ell-1}(Z_{<\ell}) := \{\widetilde{i}_{\ell-1} : \widetilde{i}_{\ell-1} = i_{\ell-1}(\widetilde{z}_{-1}, \widetilde{z}_0, \ldots, \widetilde{z}_{\ell-1}) \text{ for some } (\widetilde{z}_{-1}, \widetilde{z}_0, \ldots, \widetilde{z}_{\ell-1}) \in Z_{<\ell}\}.$$

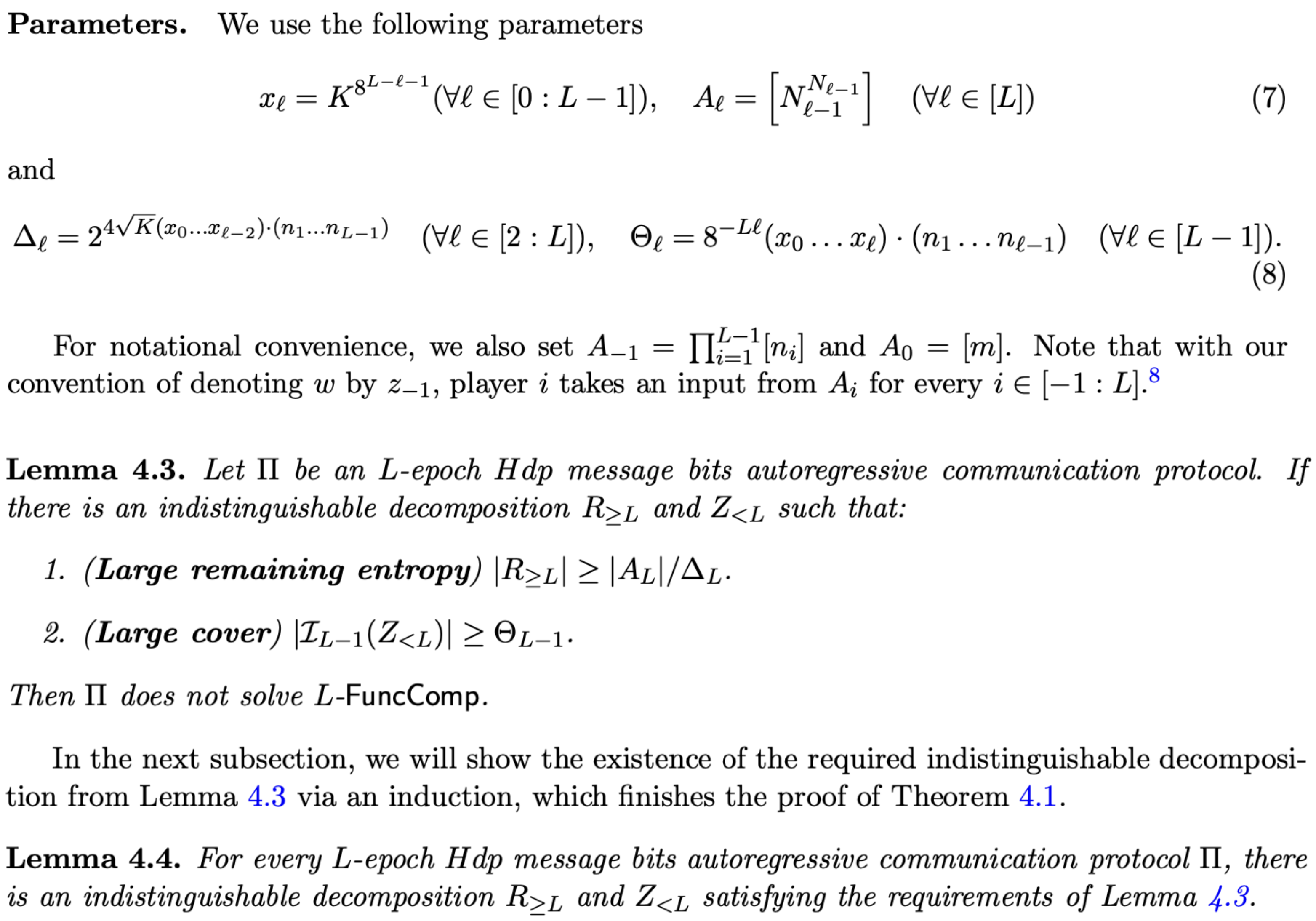
Thus, $\widetilde{z_L}$ is a function from $[N_{L-1}] \rightarrow [N_{L-1}]$ fixed on $n_{L-1}|\mathcal{J}_{L-1}|$ input values, so we have the following bound:

$$|R_{\geq L}| \leq \frac{|A_L|}{N_{L-1}^{|\mathcal{I}_{L-1}| \cdot n_{L-1}}}.$$

why can we get away with multiplying?

Sufficient for contradiction: There exists $(R_{\geq L}, Z_{<L})$ such that both $|R_{\geq L}|$ and $|\mathcal{J}_{L-1}|$ large!

Formalisms



Parameters. We use the following parameters

$$x_\ell = K^{8^{L-\ell-1}} (\forall \ell \in [0:L-1]), \quad A_\ell = \left[N_{\ell-1}^{N_{\ell-1}}\right] \quad (\forall \ell \in [L]) \tag{7}$$

and

$$\Delta_\ell = 2^{4\sqrt{K}(x_0 \ldots x_{\ell-2})\cdot(n_1 \ldots n_{L-1})} \quad (\forall \ell \in [2:L]), \quad \Theta_\ell = 8^{-L\ell}(x_0 \ldots x_\ell)\cdot(n_1 \ldots n_{\ell-1}) \quad (\forall \ell \in [L-1]). \tag{8}$$

For notational convenience, we also set $A_{-1} = \prod_{i=1}^{L-1}[n_i]$ and $A_0 = [m]$. Note that with our convention of denoting w by z_{-1}, player i takes an input from A_i for every $i \in [-1:L]$.[8]

Lemma 4.3. *Let Π be an L-epoch Hdp message bits autoregressive communication protocol. If there is an indistinguishable decomposition $R_{\geq L}$ and $Z_{<L}$ such that:*

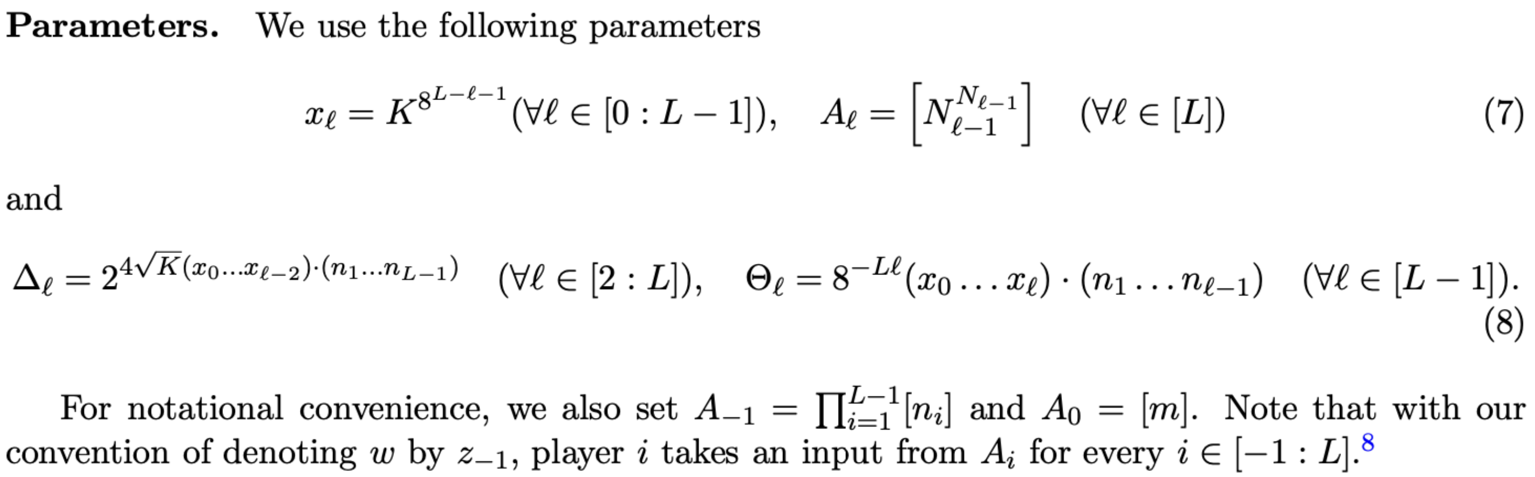
1. *(**Large remaining entropy**) $|R_{\geq L}| \geq |A_L|/\Delta_L$.*
2. *(**Large cover**) $|\mathcal{I}_{L-1}(Z_{<L})| \geq \Theta_{L-1}$.*

*Then Π does not solve L-*FuncComp.

In the next subsection, we will show the existence of the required indistinguishable decomposition from Lemma 4.3 via an induction, which finishes the proof of Theorem 4.1.

Lemma 4.4. *For every L-epoch Hdp message bits autoregressive communication protocol Π, there is an indistinguishable decomposition $R_{\geq L}$ and $Z_{<L}$ satisfying the requirements of Lemma 4.3.*

Formalisms



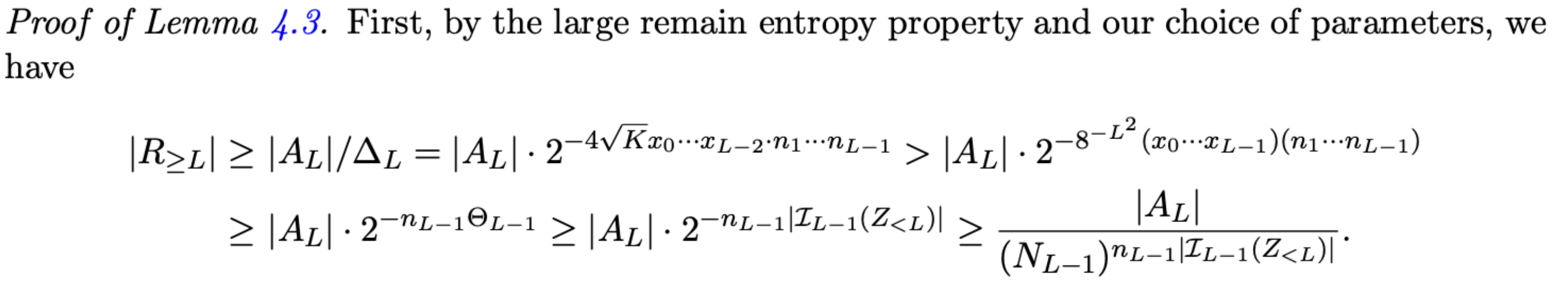
Parameters. We use the following parameters

$$x_\ell = K^{8^{L-\ell-1}} (\forall \ell \in [0 : L-1]), \quad A_\ell = \left[N_{\ell-1}^{N_{\ell-1}}\right] \quad (\forall \ell \in [L]) \tag{7}$$

and

$$\Delta_\ell = 2^{4\sqrt{K}(x_0 \ldots x_{\ell-2})\cdot(n_1 \ldots n_{L-1})} \quad (\forall \ell \in [2 : L]), \quad \Theta_\ell = 8^{-L\ell}(x_0 \ldots x_\ell) \cdot (n_1 \ldots n_{\ell-1}) \quad (\forall \ell \in [L-1]). \tag{8}$$

For notational convenience, we also set $A_{-1} = \prod_{i=1}^{L-1}[n_i]$ and $A_0 = [m]$. Note that with our convention of denoting w by z_{-1}, player i takes an input from A_i for every $i \in [-1 : L]$.[8]



Proof of Lemma 4.3. First, by the large remain entropy property and our choice of parameters, we have

$$\begin{aligned} |R_{\geq L}| &\geq |A_L|/\Delta_L = |A_L| \cdot 2^{-4\sqrt{K}x_0 \cdots x_{L-2} \cdot n_1 \cdots n_{L-1}} > |A_L| \cdot 2^{-8^{-L^2}(x_0 \cdots x_{L-1})(n_1 \cdots n_{L-1})} \\ &\geq |A_L| \cdot 2^{-n_{L-1}\Theta_{L-1}} \geq |A_L| \cdot 2^{-n_{L-1}|\mathcal{I}_{L-1}(Z_{<L})|} \geq \frac{|A_L|}{(N_{L-1})^{n_{L-1}|\mathcal{I}_{L-1}(Z_{<L})|}}. \end{aligned}$$

Remaining Objective

It suffices to show that there exists a large *indistinguishable* separation for the final player.

This is shown inductively at each level $\ell \in [2 : L - 1]$

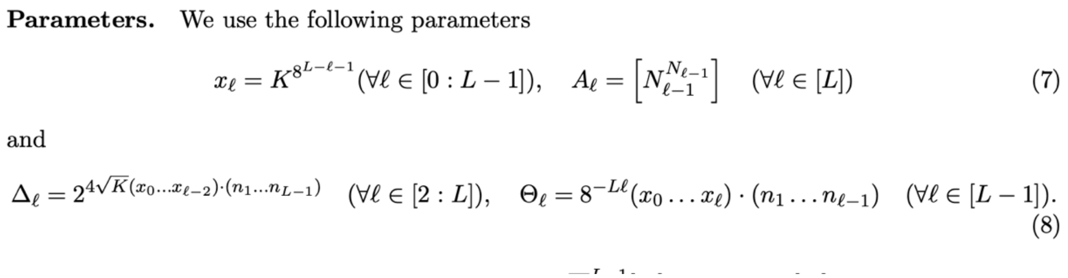
Base Case: For $\ell = 2$, one can construct $(Z_{<2}, R_{\geq 2})$ such that messages to players $-1, 0, 1$ are the same for all $\widetilde{R_{\geq 2}} \in R_{\geq 2}$ in the first 2 epochs. [The transcripts are determined entirely through $\widetilde{Z_{<2}} \in Z_{<2}$]

Inductive Hypothesis: Suppose one can find $(Z_{<\ell}, R_{\geq \ell})$ such that messages to players $[-1, \ell - 1]$ are the same for all $\widetilde{R_{\geq \ell}} \in R_{\geq \ell}$ through each epoch $\ell' \in [\ell]$.

Inductive Step: There exists $(Z_{<\ell+1}, R_{\geq \ell+1})$ such that messages to players $[-1, \ell]$ are the same for all $\widetilde{R_{\geq \ell+1}} \in R_{\geq \ell+1}$ through each epoch $\ell' \in [\ell + 1]$.

Each of these decomposition must be "large enough" so that we fail at L!

Formalisms

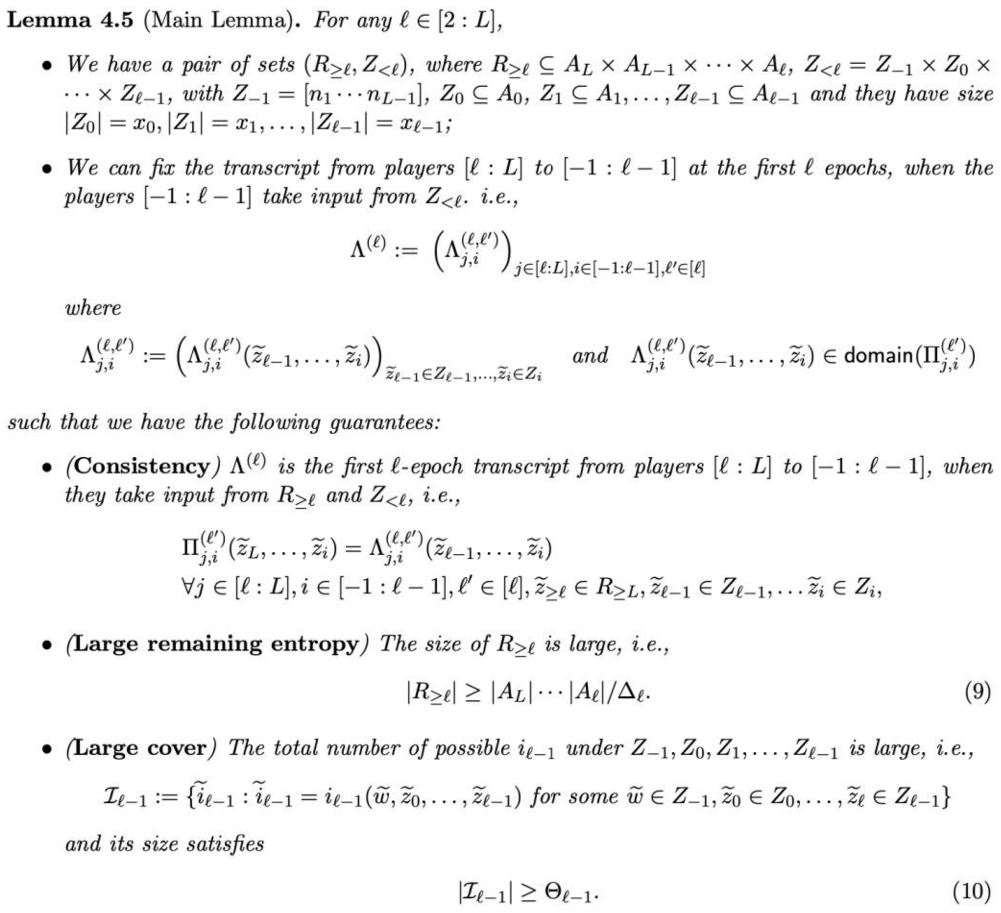


Parameters. We use the following parameters

$$x_\ell = K^{8^{L-\ell-1}} (\forall \ell \in [0 : L-1]), \quad A_\ell = \left[N_{\ell-1}^{N_{\ell-1}}\right] \quad (\forall \ell \in [L]) \tag{7}$$

and

$$\Delta_\ell = 2^{4\sqrt{K}(x_0 \ldots x_{\ell-2}) \cdot (n_1 \ldots n_{L-1})} \quad (\forall \ell \in [2 : L]), \quad \Theta_\ell = 8^{-L\ell}(x_0 \ldots x_\ell) \cdot (n_1 \ldots n_{\ell-1}) \quad (\forall \ell \in [L-1]). \tag{8}$$



Lemma 4.5 (Main Lemma)**.** *For any $\ell \in [2 : L]$,*

- *We have a pair of sets $(R_{\geq \ell}, Z_{<\ell})$, where $R_{\geq \ell} \subseteq A_L \times A_{L-1} \times \cdots \times A_\ell$, $Z_{<\ell} = Z_{-1} \times Z_0 \times \cdots \times Z_{\ell-1}$, with $Z_{-1} = [n_1 \cdots n_{L-1}]$, $Z_0 \subseteq A_0$, $Z_1 \subseteq A_1, \ldots, Z_{\ell-1} \subseteq A_{\ell-1}$ and they have size $|Z_0| = x_0, |Z_1| = x_1, \ldots, |Z_{\ell-1}| = x_{\ell-1}$;*
- *We can fix the transcript from players $[\ell : L]$ to $[-1 : \ell-1]$ at the first ℓ epochs, when the players $[-1 : \ell-1]$ take input from $Z_{<\ell}$. i.e.,*

  $$\Lambda^{(\ell)} := \left(\Lambda_{j,i}^{(\ell,\ell')}\right)_{j \in [\ell:L], i \in [-1:\ell-1], \ell' \in [\ell]}$$

  where

  $$\Lambda_{j,i}^{(\ell,\ell')} := \left(\Lambda_{j,i}^{(\ell,\ell')}(\widetilde{z}_{\ell-1}, \ldots, \widetilde{z}_i)\right)_{\widetilde{z}_{\ell-1} \in Z_{\ell-1}, \ldots, \widetilde{z}_i \in Z_i} \quad \text{and} \quad \Lambda_{j,i}^{(\ell,\ell')}(\widetilde{z}_{\ell-1}, \ldots, \widetilde{z}_i) \in \mathsf{domain}(\Pi_{j,i}^{(\ell')})$$

such that we have the following guarantees:

- *(**Consistency**) $\Lambda^{(\ell)}$ is the first ℓ-epoch transcript from players $[\ell : L]$ to $[-1 : \ell-1]$, when they take input from $R_{\geq \ell}$ and $Z_{<\ell}$, i.e.,*

  $$\Pi_{j,i}^{(\ell')}(\widetilde{z}_L, \ldots, \widetilde{z}_i) = \Lambda_{j,i}^{(\ell,\ell')}(\widetilde{z}_{\ell-1}, \ldots, \widetilde{z}_i)$$
  $$\forall j \in [\ell : L], i \in [-1 : \ell-1], \ell' \in [\ell], \widetilde{z}_{\geq \ell} \in R_{\geq L}, \widetilde{z}_{\ell-1} \in Z_{\ell-1}, \ldots \widetilde{z}_i \in Z_i,$$

- *(**Large remaining entropy**) The size of $R_{\geq \ell}$ is large, i.e.,*

  $$|R_{\geq \ell}| \geq |A_L| \cdots |A_\ell| / \Delta_\ell. \tag{9}$$

- *(**Large cover**) The total number of possible $i_{\ell-1}$ under $Z_{-1}, Z_0, Z_1, \ldots, Z_{\ell-1}$ is large, i.e.,*

  $$\mathcal{I}_{\ell-1} := \{\widetilde{i}_{\ell-1} : \widetilde{i}_{\ell-1} = i_{\ell-1}(\widetilde{w}, \widetilde{z}_0, \ldots, \widetilde{z}_{\ell-1}) \text{ for some } \widetilde{w} \in Z_{-1}, \widetilde{z}_0 \in Z_0, \ldots, \widetilde{z}_\ell \in Z_{\ell-1}\}$$

  and its size satisfies

  $$|\mathcal{I}_{\ell-1}| \geq \Theta_{\ell-1}. \tag{10}$$

Base Case

The first order of business it to select $Z_{<2} = Z_{-1} \times Z_0 \times Z_1$

Z_{-1} is fixed (why?) and since $|Z_0| \subset [m]$ has size x_0, we can take $Z_0 = [x_0]$ without loss of generality (why?)

So, we only have to select $Z_1 \subseteq A_1$. Consider the set of first epoch messages from player 1 to -1:

$$\Psi^{(1)}_{1,-1} = \left(\Psi^{(1)}_{1,-1}(\widetilde{z}_{-1})\right)_{\widetilde{z}_{-1} \in Z_{-1}} \quad \text{where} \quad \Psi^{(1)}_{1,-1}(\widetilde{z}_{-1}) \in \{0,1\}^{2Hdp}.$$

Each $\mathrm{z} \in A_1$ realizes a *particular* tuple above. There are $2^{2Hdp|Z_{-1}|} = 2^{2Hdpn_1 \cdots n_{L-1}}$ total possible tuples, so there is some $S \subseteq A_1$ that produces the same tuple (possible transcripts) of size at least $|\mathrm{A}_1| 2^{-2Hdpn_1 \cdots n_{L-1}}$.

$$\boxed{S := \{\widetilde{z}_1 \in A_1 : \Pi^{(1)}_{1,-1}(\widetilde{z}_1, \widetilde{z}_{-1}) = \Psi^{(1)}_{1,-1}(\widetilde{z}_{-1}) \ \forall \widetilde{z}_{-1} \in Z_{-1}\} \subseteq A_1}$$

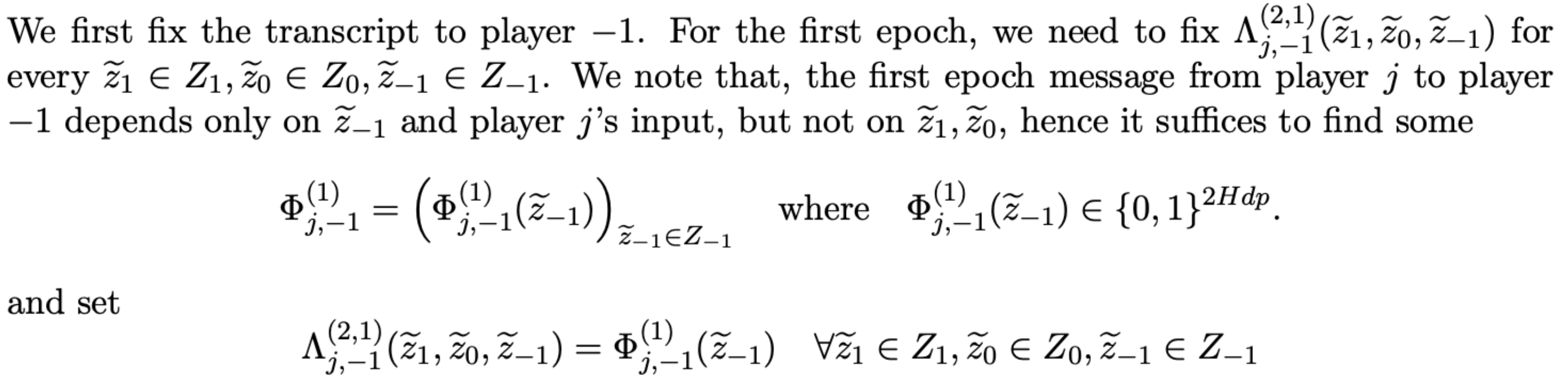
The upshot is as follows:

Lemma 4.6. *There exists a subset $Z_1 \subseteq S$ with size $|Z_1| = x_1$, such that it satisfies*

$$|\{\widetilde{z}_1(i_0) : \widetilde{z}_1 \in Z_1, i_0 \in Z_0\}| \geq 8^{-L} x_0 x_1 = \Theta_1. \tag{12}$$

Fixing Transcripts: Player -1

Now that we’ve ”determined” $Z_{<2}$, it remains to select $R_{\geq 2}$, which we do by “fixing transcripts” (i.e., repeatedly applying the consistency property). We start with the first player on the first epoch.



We first fix the transcript to player -1. For the first epoch, we need to fix $\Lambda^{(2,1)}_{j,-1}(\widetilde{z}_1, \widetilde{z}_0, \widetilde{z}_{-1})$ for every $\widetilde{z}_1 \in Z_1, \widetilde{z}_0 \in Z_0, \widetilde{z}_{-1} \in Z_{-1}$. We note that, the first epoch message from player j to player -1 depends only on $\widetilde{z}_{-1}$ and player j’s input, but not on $\widetilde{z}_1, \widetilde{z}_0$, hence it suffices to find some

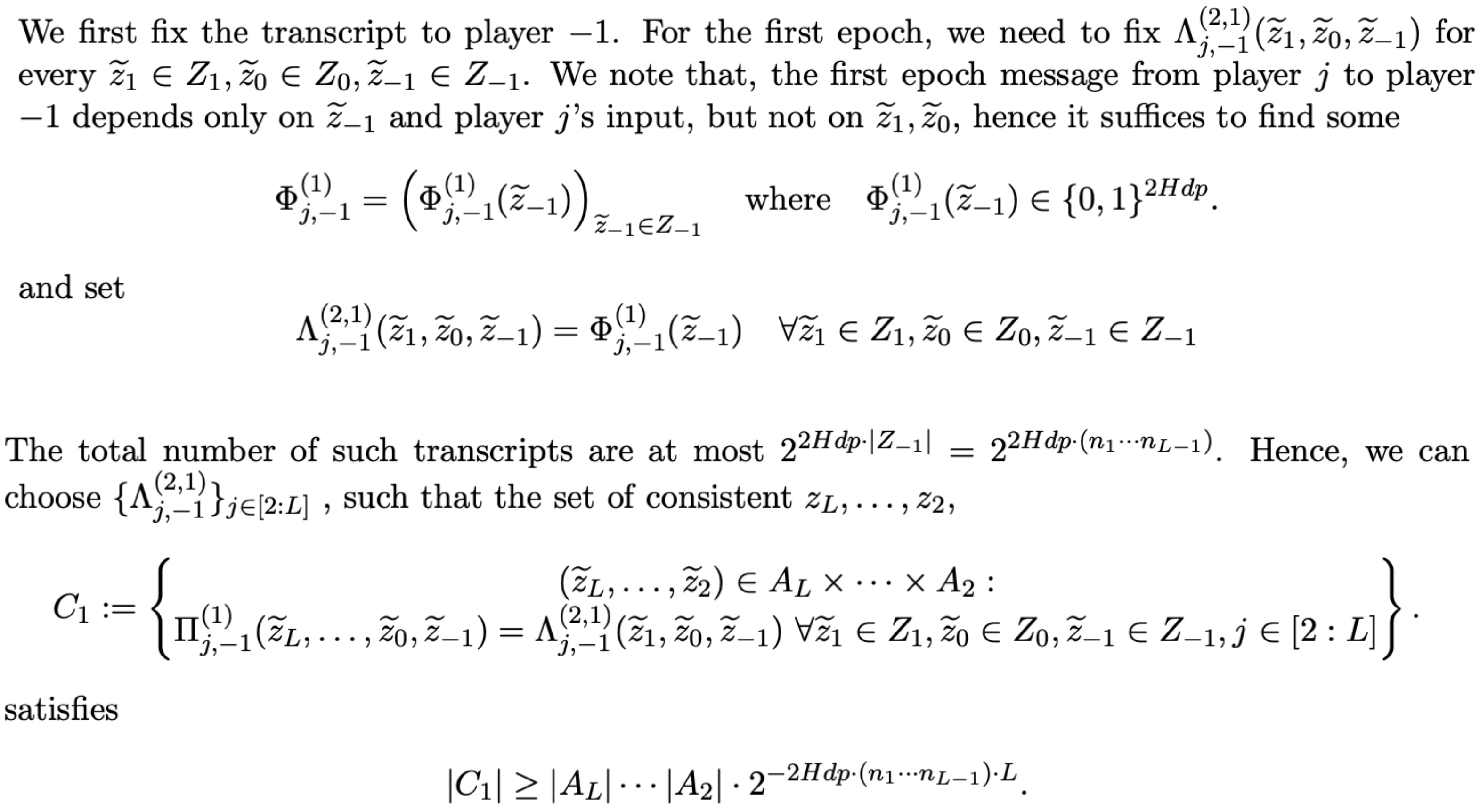
$$\Phi^{(1)}_{j,-1} = \left(\Phi^{(1)}_{j,-1}(\widetilde{z}_{-1})\right)_{\widetilde{z}_{-1} \in Z_{-1}} \quad \text{where} \quad \Phi^{(1)}_{j,-1}(\widetilde{z}_{-1}) \in \{0,1\}^{2Hdp}.$$

and set

$$\Lambda^{(2,1)}_{j,-1}(\widetilde{z}_1, \widetilde{z}_0, \widetilde{z}_{-1}) = \Phi^{(1)}_{j,-1}(\widetilde{z}_{-1}) \quad \forall \widetilde{z}_1 \in Z_1, \widetilde{z}_0 \in Z_0, \widetilde{z}_{-1} \in Z_{-1}$$

Fixing Transcripts: Player -1

Now that we've ”determined” $Z_{<2}$, it remains to select $R_{\geq 2}$, which we do by “fixing transcripts” (i.e., repeatedly applying the consistency property). We start with the first player on the first epoch.



We first fix the transcript to player -1. For the first epoch, we need to fix $\Lambda^{(2,1)}_{j,-1}(\widetilde{z}_1, \widetilde{z}_0, \widetilde{z}_{-1})$ for every $\widetilde{z}_1 \in Z_1, \widetilde{z}_0 \in Z_0, \widetilde{z}_{-1} \in Z_{-1}$. We note that, the first epoch message from player j to player -1 depends only on $\widetilde{z}_{-1}$ and player j's input, but not on $\widetilde{z}_1, \widetilde{z}_0$, hence it suffices to find some

$$\Phi^{(1)}_{j,-1} = \left(\Phi^{(1)}_{j,-1}(\widetilde{z}_{-1})\right)_{\widetilde{z}_{-1} \in Z_{-1}} \quad \text{where} \quad \Phi^{(1)}_{j,-1}(\widetilde{z}_{-1}) \in \{0,1\}^{2Hdp}.$$

and set

$$\Lambda^{(2,1)}_{j,-1}(\widetilde{z}_1, \widetilde{z}_0, \widetilde{z}_{-1}) = \Phi^{(1)}_{j,-1}(\widetilde{z}_{-1}) \quad \forall \widetilde{z}_1 \in Z_1, \widetilde{z}_0 \in Z_0, \widetilde{z}_{-1} \in Z_{-1}$$

The total number of such transcripts are at most $2^{2Hdp \cdot |Z_{-1}|} = 2^{2Hdp \cdot (n_1 \cdots n_{L-1})}$. Hence, we can choose $\{\Lambda^{(2,1)}_{j,-1}\}_{j \in [2:L]}$, such that the set of consistent $z_L, \ldots, z_2$,

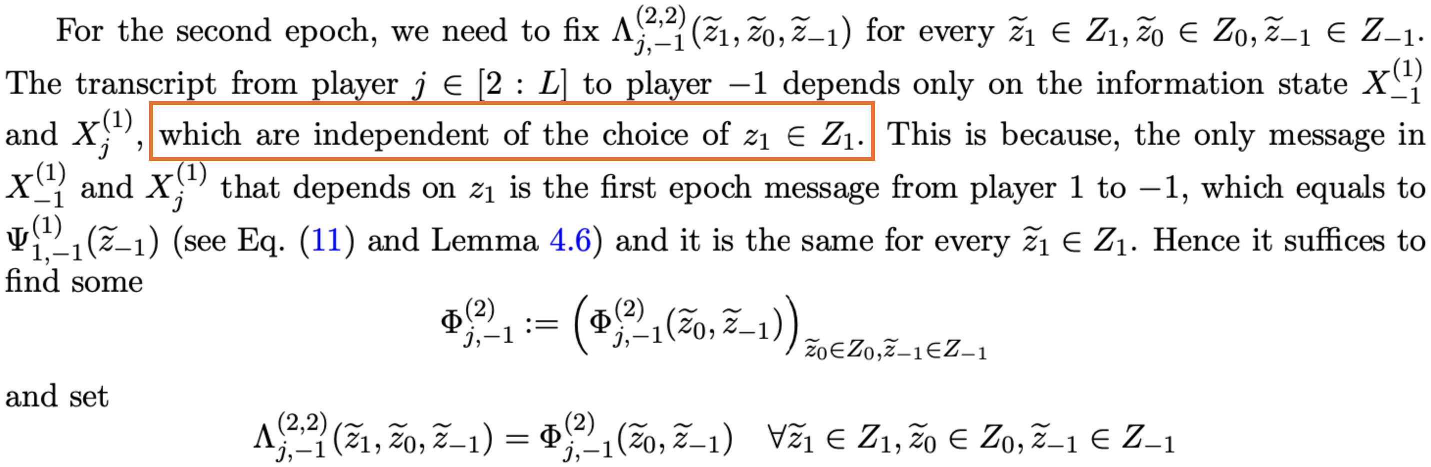
$$C_1 := \left\{ \begin{array}{c} (\widetilde{z}_L, \ldots, \widetilde{z}_2) \in A_L \times \cdots \times A_2 : \\ \Pi^{(1)}_{j,-1}(\widetilde{z}_L, \ldots, \widetilde{z}_0, \widetilde{z}_{-1}) = \Lambda^{(2,1)}_{j,-1}(\widetilde{z}_1, \widetilde{z}_0, \widetilde{z}_{-1}) \ \forall \widetilde{z}_1 \in Z_1, \widetilde{z}_0 \in Z_0, \widetilde{z}_{-1} \in Z_{-1}, j \in [2:L] \end{array} \right\}.$$

satisfies

$$|C_1| \geq |A_L| \cdots |A_2| \cdot 2^{-2Hdp \cdot (n_1 \cdots n_{L-1}) \cdot L}.$$

Fixing Transcripts: Player -1

We continue examining player 1, but on the second epoch. The way we selected $Z_1 \subset S$ becomes *essential* in this part!



For the second epoch, we need to fix $\Lambda^{(2,2)}_{j,-1}(\widetilde{z}_1, \widetilde{z}_0, \widetilde{z}_{-1})$ for every $\widetilde{z}_1 \in Z_1, \widetilde{z}_0 \in Z_0, \widetilde{z}_{-1} \in Z_{-1}$. The transcript from player $j \in [2 : L]$ to player -1 depends only on the information state $X^{(1)}_{-1}$ and $X^{(1)}_{j}$, which are independent of the choice of $z_1 \in Z_1$. This is because, the only message in $X^{(1)}_{-1}$ and $X^{(1)}_{j}$ that depends on z_1 is the first epoch message from player 1 to -1, which equals to $\Psi^{(1)}_{1,-1}(\widetilde{z}_{-1})$ (see Eq. (11) and Lemma 4.6) and it is the same for every $\widetilde{z}_1 \in Z_1$. Hence it suffices to find some

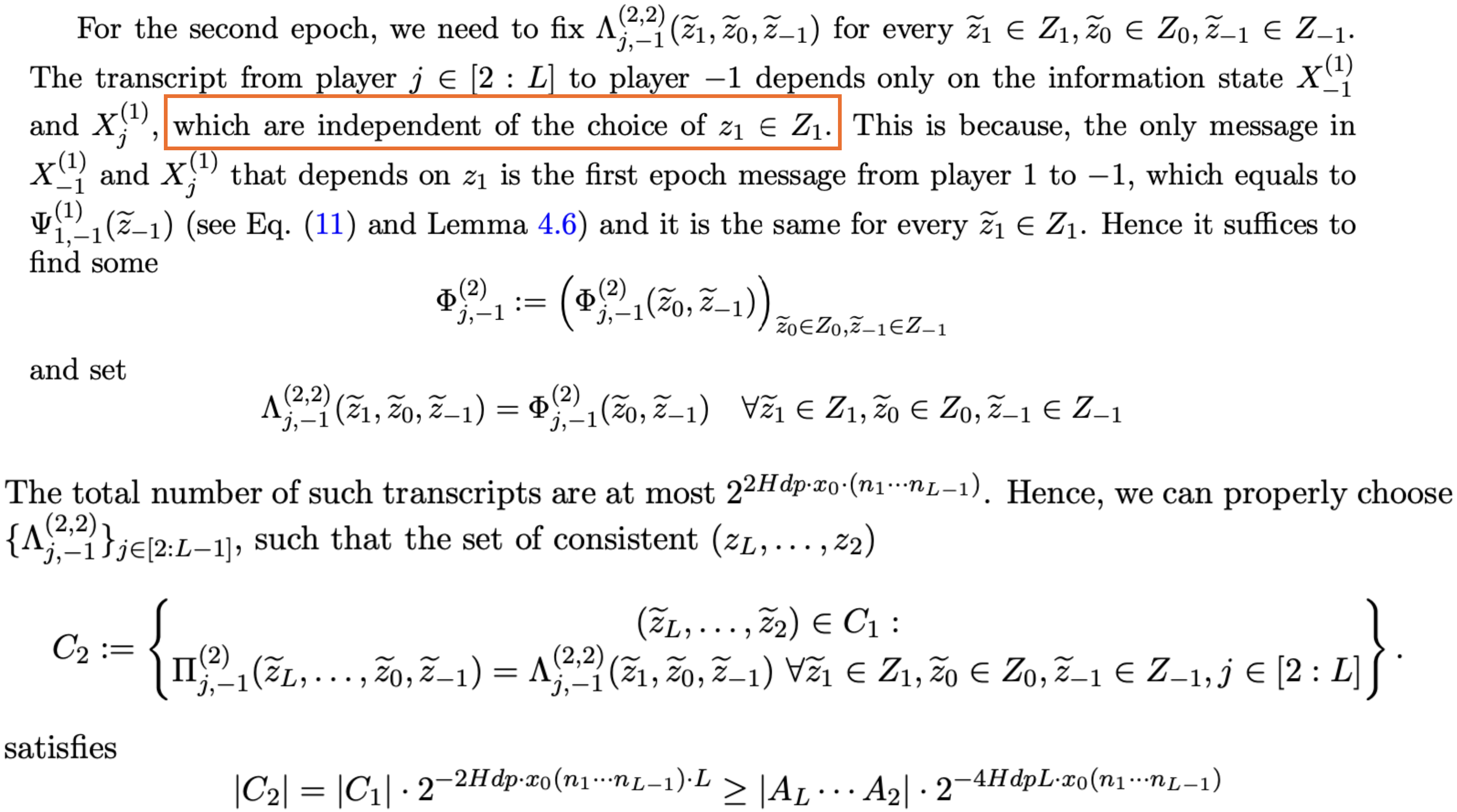
$$\Phi^{(2)}_{j,-1} := \left(\Phi^{(2)}_{j,-1}(\widetilde{z}_0, \widetilde{z}_{-1})\right)_{\widetilde{z}_0 \in Z_0, \widetilde{z}_{-1} \in Z_{-1}}$$

and set

$$\Lambda^{(2,2)}_{j,-1}(\widetilde{z}_1, \widetilde{z}_0, \widetilde{z}_{-1}) = \Phi^{(2)}_{j,-1}(\widetilde{z}_0, \widetilde{z}_{-1}) \quad \forall \widetilde{z}_1 \in Z_1, \widetilde{z}_0 \in Z_0, \widetilde{z}_{-1} \in Z_{-1}$$

Fixing Transcripts: Player -1

We continue examining player 1, but on the second epoch. The way we selected $Z_1 \subset S$ becomes *essential* in this part!



For the second epoch, we need to fix $\Lambda^{(2,2)}_{j,-1}(\widetilde{z}_1, \widetilde{z}_0, \widetilde{z}_{-1})$ for every $\widetilde{z}_1 \in Z_1, \widetilde{z}_0 \in Z_0, \widetilde{z}_{-1} \in Z_{-1}$. The transcript from player $j \in [2:L]$ to player -1 depends only on the information state $X^{(1)}_{-1}$ and $X^{(1)}_j$, which are independent of the choice of $z_1 \in Z_1$. This is because, the only message in $X^{(1)}_{-1}$ and $X^{(1)}_j$ that depends on z_1 is the first epoch message from player 1 to -1, which equals to $\Psi^{(1)}_{1,-1}(\widetilde{z}_{-1})$ (see Eq. (11) and Lemma 4.6) and it is the same for every $\widetilde{z}_1 \in Z_1$. Hence it suffices to find some

$$\Phi^{(2)}_{j,-1} := \left(\Phi^{(2)}_{j,-1}(\widetilde{z}_0, \widetilde{z}_{-1})\right)_{\widetilde{z}_0 \in Z_0, \widetilde{z}_{-1} \in Z_{-1}}$$

and set

$$\Lambda^{(2,2)}_{j,-1}(\widetilde{z}_1, \widetilde{z}_0, \widetilde{z}_{-1}) = \Phi^{(2)}_{j,-1}(\widetilde{z}_0, \widetilde{z}_{-1}) \quad \forall \widetilde{z}_1 \in Z_1, \widetilde{z}_0 \in Z_0, \widetilde{z}_{-1} \in Z_{-1}$$

The total number of such transcripts are at most $2^{2Hdp \cdot x_0 \cdot (n_1 \cdots n_{L-1})}$. Hence, we can properly choose $\{\Lambda^{(2,2)}_{j,-1}\}_{j \in [2:L-1]}$, such that the set of consistent $(z_L, \ldots, z_2)$

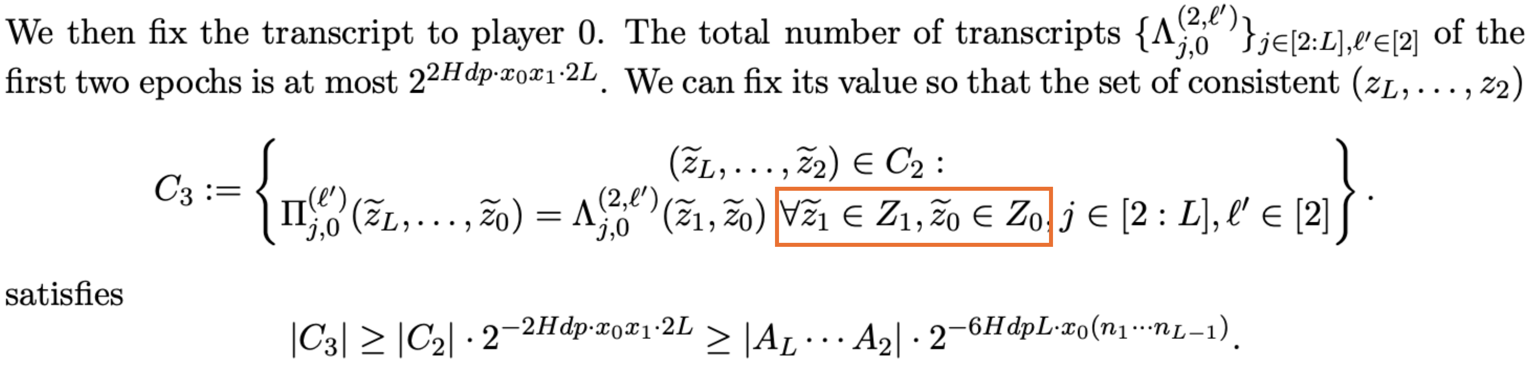
$$C_2 := \left\{ \begin{array}{c} (\widetilde{z}_L, \ldots, \widetilde{z}_2) \in C_1 : \\ \Pi^{(2)}_{j,-1}(\widetilde{z}_L, \ldots, \widetilde{z}_0, \widetilde{z}_{-1}) = \Lambda^{(2,2)}_{j,-1}(\widetilde{z}_1, \widetilde{z}_0, \widetilde{z}_{-1}) \; \forall \widetilde{z}_1 \in Z_1, \widetilde{z}_0 \in Z_0, \widetilde{z}_{-1} \in Z_{-1}, j \in [2:L] \end{array} \right\}.$$

satisfies

$$|C_2| = |C_1| \cdot 2^{-2Hdp \cdot x_0 (n_1 \cdots n_{L-1}) \cdot L} \geq |A_L \cdots A_2| \cdot 2^{-4HdpL \cdot x_0 (n_1 \cdots n_{L-1})}$$

Fixing Transcripts: Players 0, 1

We are more crude with players 0 and 1 (why can we afford this?)

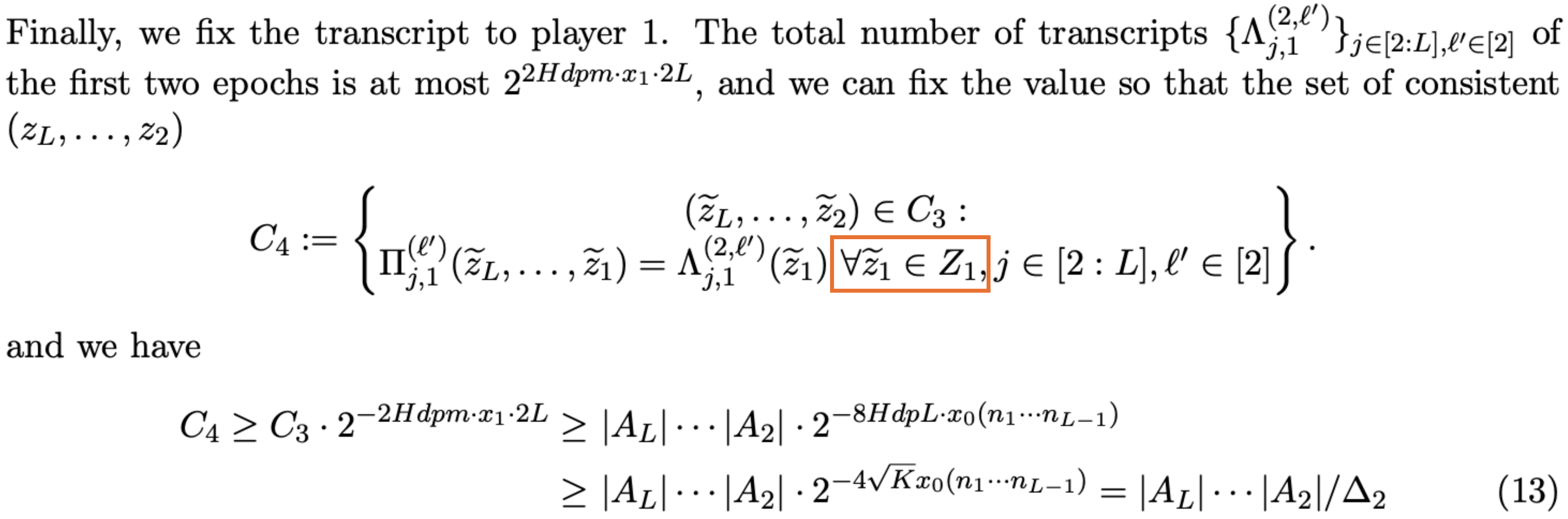


We then fix the transcript to player 0. The total number of transcripts $\{\Lambda_{j,0}^{(2,\ell')}\}_{j\in[2:L],\ell'\in[2]}$ of the first two epochs is at most $2^{2Hdp\cdot x_0x_1\cdot 2L}$. We can fix its value so that the set of consistent $(z_L,\ldots,z_2)$

$$C_3 := \left\{ \begin{array}{c} (\widetilde{z}_L,\ldots,\widetilde{z}_2) \in C_2 : \\ \Pi_{j,0}^{(\ell')}(\widetilde{z}_L,\ldots,\widetilde{z}_0) = \Lambda_{j,0}^{(2,\ell')}(\widetilde{z}_1,\widetilde{z}_0)\ \boxed{\forall \widetilde{z}_1 \in Z_1, \widetilde{z}_0 \in Z_0,}\ j \in [2:L], \ell' \in [2] \end{array} \right\}.$$

satisfies

$$|C_3| \geq |C_2| \cdot 2^{-2Hdp\cdot x_0x_1\cdot 2L} \geq |A_L \cdots A_2| \cdot 2^{-6HdpL\cdot x_0(n_1\cdots n_{L-1})}.$$



Finally, we fix the transcript to player 1. The total number of transcripts $\{\Lambda_{j,1}^{(2,\ell')}\}_{j\in[2:L],\ell'\in[2]}$ of the first two epochs is at most $2^{2Hdpm\cdot x_1\cdot 2L}$, and we can fix the value so that the set of consistent $(z_L,\ldots,z_2)$

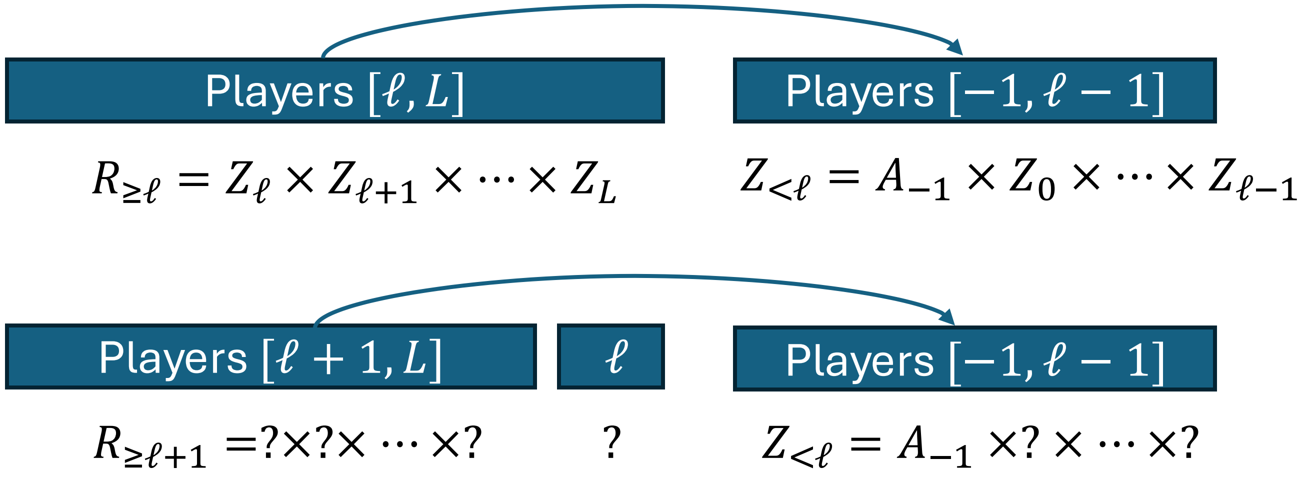
$$C_4 := \left\{ \begin{array}{c} (\widetilde{z}_L,\ldots,\widetilde{z}_2) \in C_3 : \\ \Pi_{j,1}^{(\ell')}(\widetilde{z}_L,\ldots,\widetilde{z}_1) = \Lambda_{j,1}^{(2,\ell')}(\widetilde{z}_1)\ \boxed{\forall \widetilde{z}_1 \in Z_1,}\ j \in [2:L], \ell' \in [2] \end{array} \right\}.$$

and we have

$$\begin{aligned} C_4 \geq C_3 \cdot 2^{-2Hdpm\cdot x_1\cdot 2L} &\geq |A_L| \cdots |A_2| \cdot 2^{-8HdpL\cdot x_0(n_1\cdots n_{L-1})} \\ &\geq |A_L| \cdots |A_2| \cdot 2^{-4\sqrt{K}x_0(n_1\cdots n_{L-1})} = |A_L| \cdots |A_2|/\Delta_2 \qquad (13) \end{aligned}$$

Inductive Step

We have a decomposition $(Z_{<\ell}, R_{\geq \ell})$ which is indistinguishable through ℓ epochs, we'd like to distill $(Z_{<\ell+1}, R_{\geq \ell+1})$ which holds through $\ell + 1$ epochs



Players $[\ell, L]$

Players $[-1, \ell - 1]$

holds for $\ell' \in [\ell]$

$R_{\geq \ell} = Z_\ell \times Z_{\ell+1} \times \cdots \times Z_L$

$Z_{<\ell} = A_{-1} \times Z_0 \times \cdots \times Z_{\ell-1}$

Players $[\ell + 1, L]$

ℓ

Players $[-1, \ell - 1]$

holds for $\ell' \in [\ell + 1]$

$R_{\geq \ell+1} = ? \times ? \times \cdots \times ?$

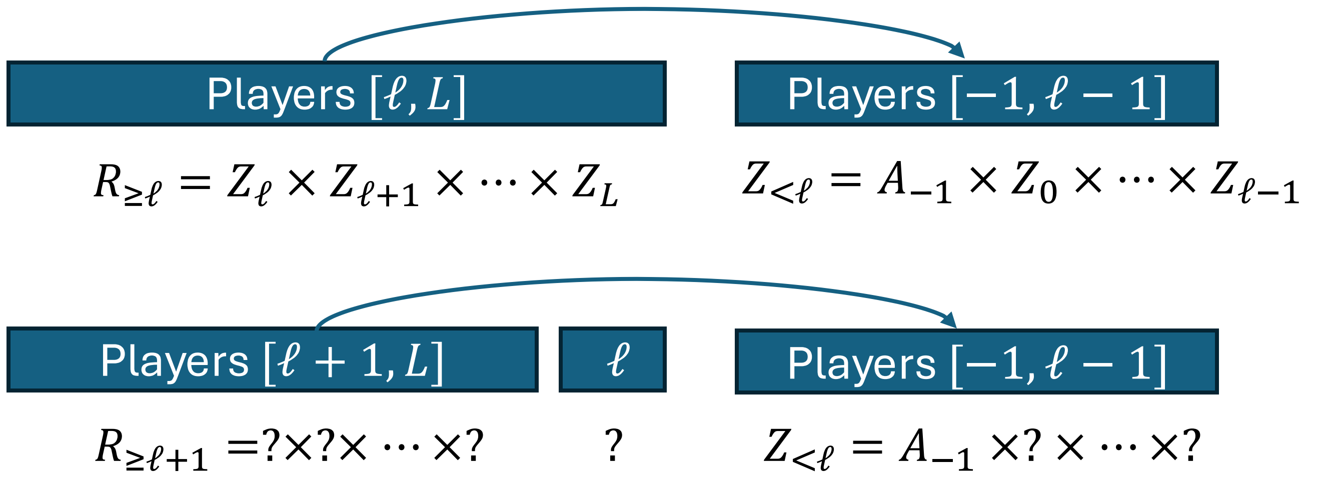
$?$

$Z_{<\ell} = A_{-1} \times ? \times \cdots \times ?$

Is there an easy way to fill in the ? above?

Inductive Step

We have a decomposition $(Z_{<\ell}, R_{\geq \ell})$ which is indistinguishable through ℓ epochs, we'd like to distill $(Z_{<\ell+1}, R_{\geq \ell+1})$ which holds through $\ell + 1$ epochs



Players $[\ell, L]$

Players $[-1, \ell - 1]$

$R_{\geq \ell} = Z_\ell \times Z_{\ell+1} \times \cdots \times Z_L$

$Z_{<\ell} = A_{-1} \times Z_0 \times \cdots \times Z_{\ell-1}$

holds for $\ell' \in [\ell]$

Players $[\ell + 1, L]$

ℓ

Players $[-1, \ell - 1]$

$R_{\geq \ell+1} = ? \times ? \times \cdots \times ?$

$?$

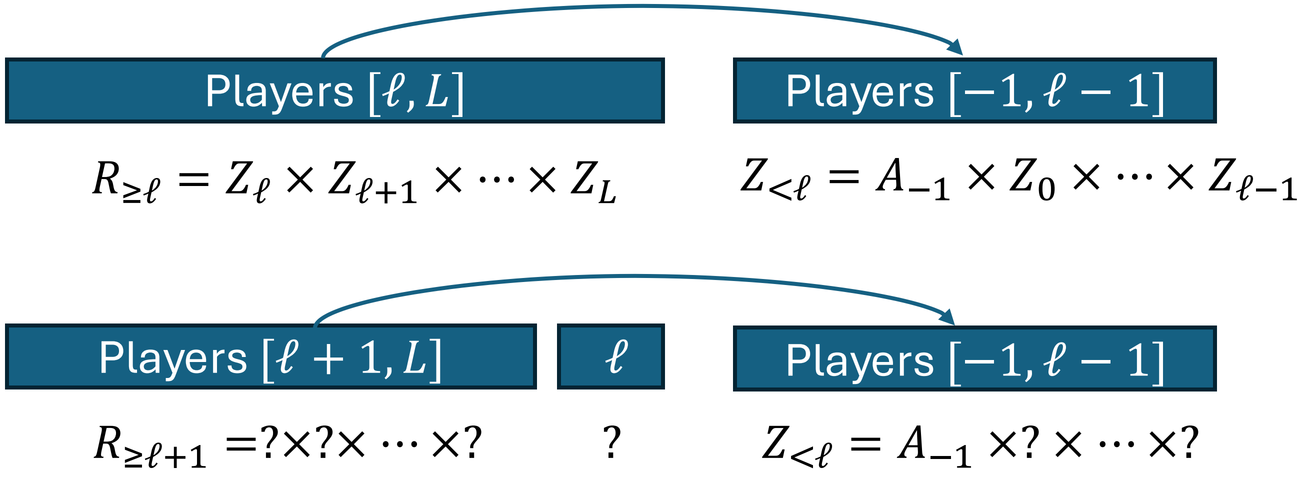
$Z_{<\ell} = A_{-1} \times ? \times \cdots \times ?$

holds for $\ell' \in [\ell + 1]$

Is there an easy way to fill in the ? above? **No ☹, too many moving parts!**

Inductive Step

We have a decomposition $(Z_{<\ell}, R_{\geq \ell})$ which is indistinguishable through ℓ epochs, we'd like to distill $(Z_{<\ell+1}, R_{\geq \ell+1})$ which holds through $\ell+1$ epochs



Players $[\ell, L]$ Players $[-1, \ell-1]$

$R_{\geq \ell} = Z_\ell \times Z_{\ell+1} \times \cdots \times Z_L$ $Z_{<\ell} = A_{-1} \times Z_0 \times \cdots \times Z_{\ell-1}$

holds for $\ell' \in [\ell]$

Players $[\ell+1, L]$ ℓ Players $[-1, \ell-1]$

$R_{\geq \ell+1} = ? \times ? \times \cdots \times ?$? $Z_{<\ell} = A_{-1} \times ? \times \cdots \times ?$

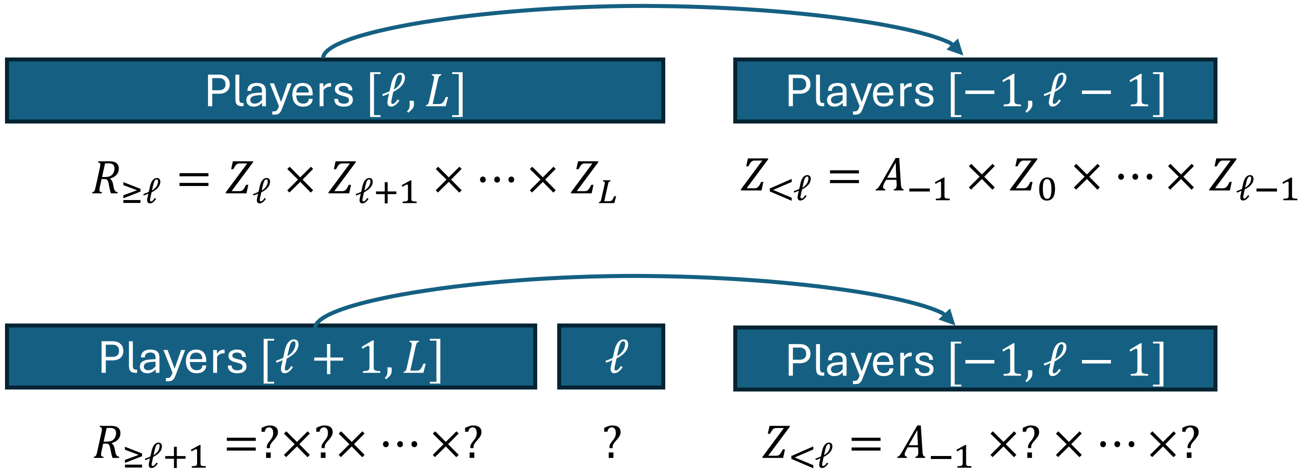
holds for $\ell' \in [\ell+1]$

Order of attack:

1. Determine the new Z_ℓ and a superset of the new $R_{\geq \ell}$ (yet subset of old)
2. "Fix the transcripts" between $[\ell+1, L]$ and $[-1, \ell-1]$ on just the first ℓ epochs
3. "Fix the transcripts" between $[\ell+1, L]$ and $[-1, \ell-1]$ on the $\ell+1$ epoch
4. "Fix the transcript" for player ℓ over all $\ell+1$ epochs

Inductive Step

We have a decomposition $(Z_{<\ell}, R_{\geq \ell})$ which is indistinguishable through ℓ epochs, we'd like to distill $(Z_{<\ell+1}, R_{\geq \ell+1})$ which holds through $\ell + 1$ epochs



Players $[\ell, L]$

Players $[-1, \ell - 1]$

$R_{\geq \ell} = Z_\ell \times Z_{\ell+1} \times \cdots \times Z_L$

$Z_{<\ell} = A_{-1} \times Z_0 \times \cdots \times Z_{\ell-1}$

holds for $\ell' \in [\ell]$

Players $[\ell + 1, L]$

ℓ

Players $[-1, \ell - 1]$

$R_{\geq \ell+1} = ? \times ? \times \cdots \times ?$

$?$

$Z_{<\ell} = A_{-1} \times ? \times \cdots \times ?$

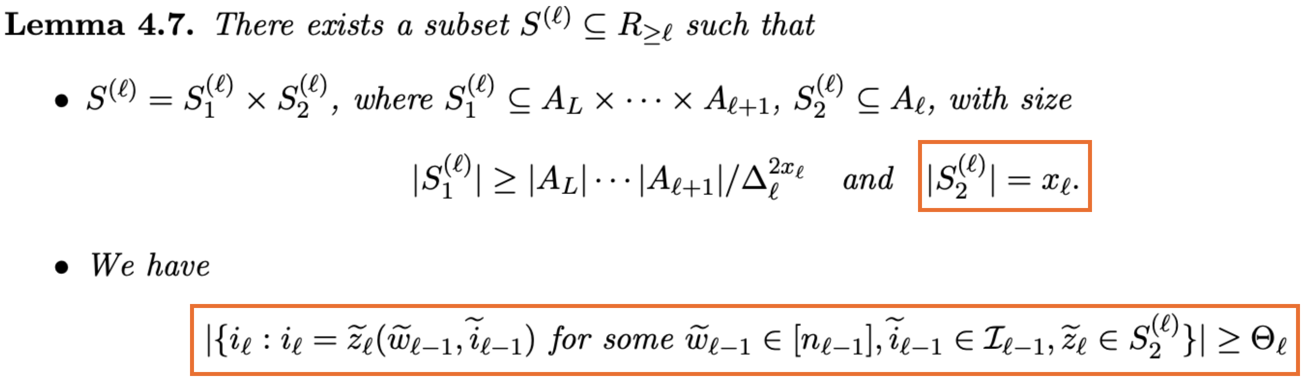
holds for $\ell' \in [\ell + 1]$

Order of attack:

1. **Determine the new Z_ℓ and a superset of the new $R_{\geq \ell}$ (yet subset of old)**
2. "Fix the transcripts" between $[\ell + 1, L]$ and $[-1, \ell - 1]$ on just the first ℓ epochs
3. "Fix the transcripts" between $[\ell + 1, L]$ and $[-1, \ell - 1]$ on the $\ell + 1$ epoch
4. "Fix the transcript" for player ℓ over all $\ell + 1$ epochs

Building the new $Z_{<\ell+1}$

The following technical lemma essentially one-shots picking $Z_{<\ell}$



Lemma 4.7. *There exists a subset* $S^{(\ell)} \subseteq R_{\geq \ell}$ *such that*

- $S^{(\ell)} = S_1^{(\ell)} \times S_2^{(\ell)}$, *where* $S_1^{(\ell)} \subseteq A_L \times \cdots \times A_{\ell+1}$, $S_2^{(\ell)} \subseteq A_\ell$, *with size*

$$|S_1^{(\ell)}| \geq |A_L| \cdots |A_{\ell+1}| / \Delta_\ell^{2x_\ell} \quad \textit{and} \quad \boxed{|S_2^{(\ell)}| = x_\ell.}$$

- *We have*

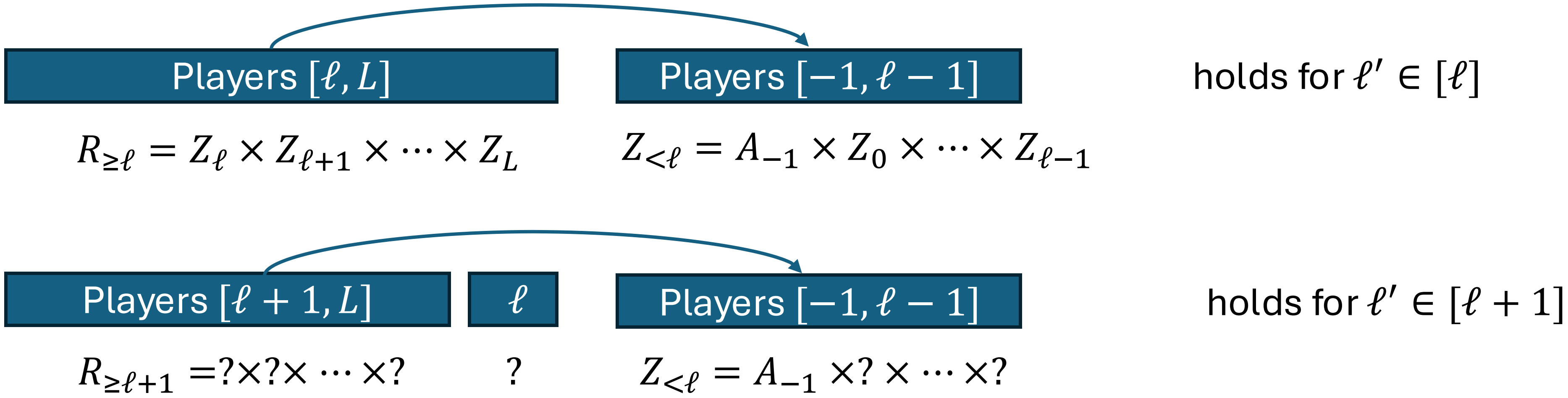
$$\boxed{|\{i_\ell : i_\ell = \widetilde{z}_\ell(\widetilde{w}_{\ell-1}, \widetilde{i}_{\ell-1}) \textit{ for some } \widetilde{w}_{\ell-1} \in [n_{\ell-1}], \widetilde{i}_{\ell-1} \in \mathcal{I}_{\ell-1}, \widetilde{z}_\ell \in S_2^{(\ell)}\}| \geq \Theta_\ell}$$

We get all the properties we dreamed about $Z_{<\ell+1} = Z_\ell \times Z_{<\ell}$, besides consistency

As with the base case, we'll whittle down S_1^ℓ in the following steps until we get an indistinguishable rectangle.

Inductive Step

We have a decomposition $(Z_{<\ell}, R_{\geq \ell})$ which is indistinguishable through ℓ epochs, we'd like to distill $(Z_{<\ell+1}, R_{\geq \ell+1})$ which holds through $\ell + 1$ epochs


Players $[\ell, L]$
Players $[-1, \ell - 1]$
holds for $\ell' \in [\ell]$
$R_{\geq \ell} = Z_\ell \times Z_{\ell+1} \times \cdots \times Z_L$
$Z_{<\ell} = A_{-1} \times Z_0 \times \cdots \times Z_{\ell-1}$
Players $[\ell + 1, L]$
ℓ
Players $[-1, \ell - 1]$
holds for $\ell' \in [\ell + 1]$
$R_{\geq \ell+1} = ? \times ? \times \cdots \times ?$
?
$Z_{<\ell} = A_{-1} \times ? \times \cdots \times ?$

Order of attack:

1. Determine the new Z_ℓ and a superset of the new $R_{\geq \ell}$ (yet subset of old)
2. **"Fix the transcripts" between $[\ell + 1, L]$ and $[-1, \ell - 1]$ on just the first ℓ epochs**
3. "Fix the transcripts" between $[\ell + 1, L]$ and $[-1, \ell - 1]$ on the $\ell + 1$ epoch
4. "Fix the transcript" for player ℓ over all $\ell + 1$ epochs

”Fixing the transcript” I

Recall we have constructed a decomposition $(\mathrm{Z}_{<\ell+1}, S_1)$ which is not necessarily indistinguishable.

In this step, we consider the transcripts only between players $[\ell + 1, L]$ and $[-1, \ell - 1]$ in just the first ℓ epochs…

Question: Does $(\mathrm{Z}_{<\ell+1}, S_1)$ behave indistinguishably? If so, what transcript does it adopt?

”Fixing the transcript” I

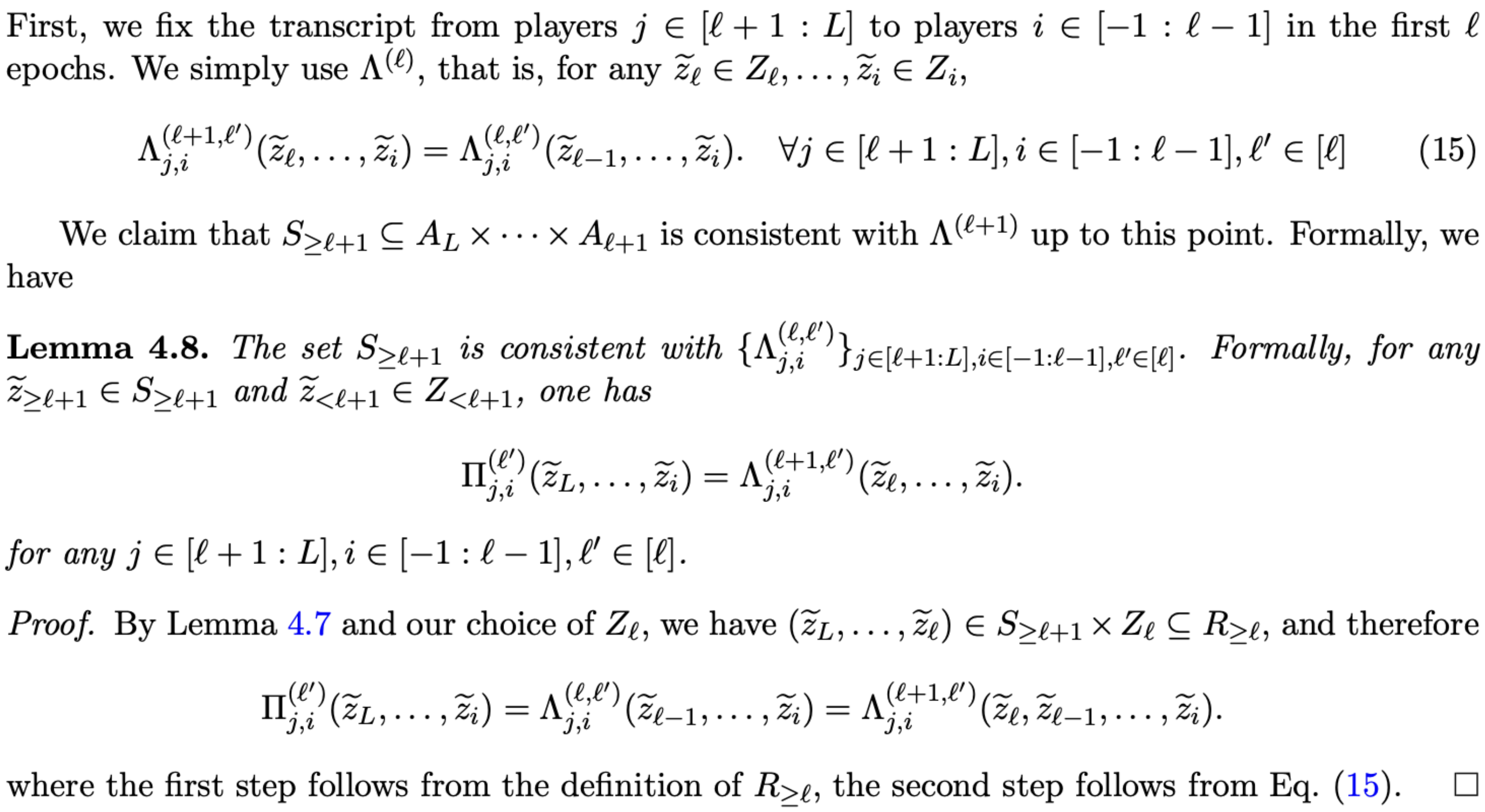
Recall we have constructed a decomposition $(\mathrm{Z}_{<\ell+1}, S_1)$ which is not necessarily indistinguishable.

In this step, we consider the transcripts only between players $[\ell + 1, L]$ and $[-1, \ell - 1]$ in just the first ℓ epochs…

Question: Does $(\mathrm{Z}_{<\ell+1}, S_1)$ behave indistinguishably? If so, what transcript does it adopt?

Answer: Yes!! Note that $S_1 \subset R_{\geq\ell}$ and we consider assignments in $\mathrm{Z}_{<\ell}$ up to ℓ epochs … sub-rectangles of indistinguishable rectangles remain indistinguishable! We adopt the transcript of the inductive hypothesis.

”Fixing the transcript” I



First, we fix the transcript from players $j \in [\ell + 1 : L]$ to players $i \in [-1 : \ell - 1]$ in the first ℓ epochs. We simply use $\Lambda^{(\ell)}$, that is, for any $\widetilde{z}_\ell \in Z_\ell, \dots, \widetilde{z}_i \in Z_i$,

$$\Lambda_{j,i}^{(\ell+1,\ell')}(\widetilde{z}_\ell, \dots, \widetilde{z}_i) = \Lambda_{j,i}^{(\ell,\ell')}(\widetilde{z}_{\ell-1}, \dots, \widetilde{z}_i). \quad \forall j \in [\ell+1 : L], i \in [-1 : \ell-1], \ell' \in [\ell] \tag{15}$$

We claim that $S_{\geq \ell+1} \subseteq A_L \times \cdots \times A_{\ell+1}$ is consistent with $\Lambda^{(\ell+1)}$ up to this point. Formally, we have

Lemma 4.8. *The set $S_{\geq \ell+1}$ is consistent with $\{\Lambda_{j,i}^{(\ell,\ell')}\}_{j\in[\ell+1:L], i\in[-1:\ell-1], \ell'\in[\ell]}$. Formally, for any $\widetilde{z}_{\geq \ell+1} \in S_{\geq \ell+1}$ and $\widetilde{z}_{<\ell+1} \in Z_{<\ell+1}$, one has*

$$\Pi_{j,i}^{(\ell')}(\widetilde{z}_L, \dots, \widetilde{z}_i) = \Lambda_{j,i}^{(\ell+1,\ell')}(\widetilde{z}_\ell, \dots, \widetilde{z}_i).$$

for any $j \in [\ell+1 : L], i \in [-1 : \ell-1], \ell' \in [\ell]$.

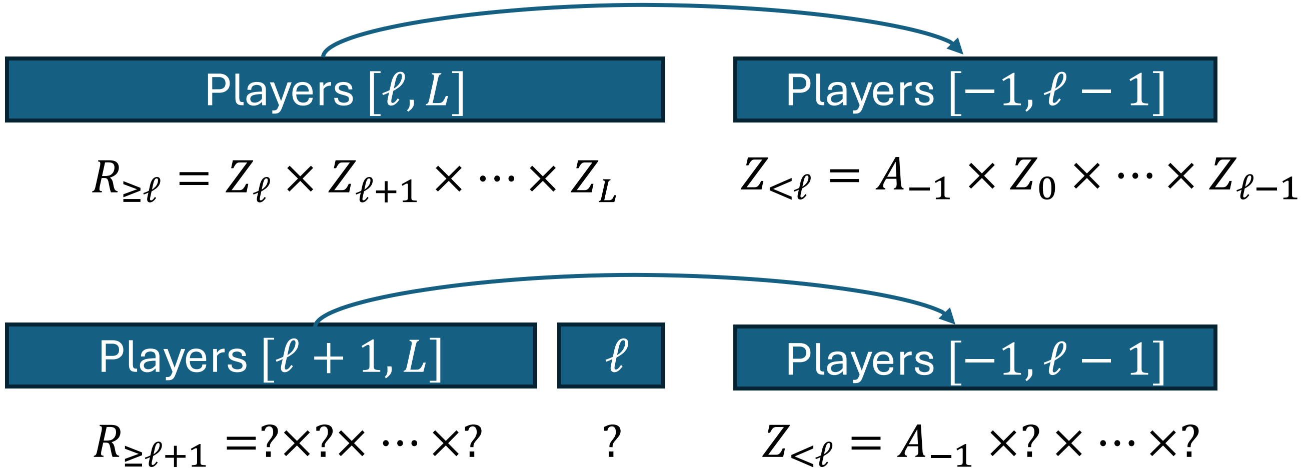
Proof. By Lemma 4.7 and our choice of Z_ℓ, we have $(\widetilde{z}_L, \dots, \widetilde{z}_\ell) \in S_{\geq \ell+1} \times Z_\ell \subseteq R_{\geq \ell}$, and therefore

$$\Pi_{j,i}^{(\ell')}(\widetilde{z}_L, \dots, \widetilde{z}_i) = \Lambda_{j,i}^{(\ell,\ell')}(\widetilde{z}_{\ell-1}, \dots, \widetilde{z}_i) = \Lambda_{j,i}^{(\ell+1,\ell')}(\widetilde{z}_\ell, \widetilde{z}_{\ell-1}, \dots, \widetilde{z}_i).$$

where the first step follows from the definition of $R_{\geq \ell}$, the second step follows from Eq. (15). □

Inductive Step

We have a decomposition $(Z_{<\ell}, R_{\geq \ell})$ which is indistinguishable through ℓ epochs, we'd like to distill $(Z_{<\ell+1}, R_{\geq \ell+1})$ which holds through $\ell + 1$ epochs



Players $[\ell, L]$ | Players $[-1, \ell - 1]$

$R_{\geq \ell} = Z_\ell \times Z_{\ell+1} \times \cdots \times Z_L$ | $Z_{<\ell} = A_{-1} \times Z_0 \times \cdots \times Z_{\ell-1}$

holds for $\ell' \in [\ell]$

Players $[\ell + 1, L]$ | ℓ | Players $[-1, \ell - 1]$

$R_{\geq \ell+1} = ? \times ? \times \cdots \times ?$ | $?$ | $Z_{<\ell} = A_{-1} \times ? \times \cdots \times ?$

holds for $\ell' \in [\ell + 1]$

Order of attack:

1. Determine the new Z_ℓ and a superset of the new $R_{\geq \ell}$ (yet subset of old)
2. "Fix the transcripts" between $[\ell + 1, L]$ and $[-1, \ell - 1]$ on just the first ℓ epochs
3. **"Fix the transcripts" between $[\ell + 1, L]$ and $[-1, \ell - 1]$ on the $\ell + 1$ epoch**
4. "Fix the transcript" for player ℓ over all $\ell + 1$ epochs

“Fixing the transcript” II

The first *nontrivial* step, where we finally see a distillation of $S_{\geq \ell+1}$!

In this step, we consider the transcripts only between players $[\ell + 1, L]$ and $[-1, \ell - 1]$ on the $\ell + 1$ epoch

Observation: Using the previous “fixing the transcript,” players $[-1, \ell - 1]$ receive the same transcript on all $\ell' \in [\ell]$ of which $z_\ell \in Z_\ell$ we select

Conclusion: The message sent at the $\ell + 1$ epoch is **independent** of Z_ℓ!

“Fixing the transcript” II

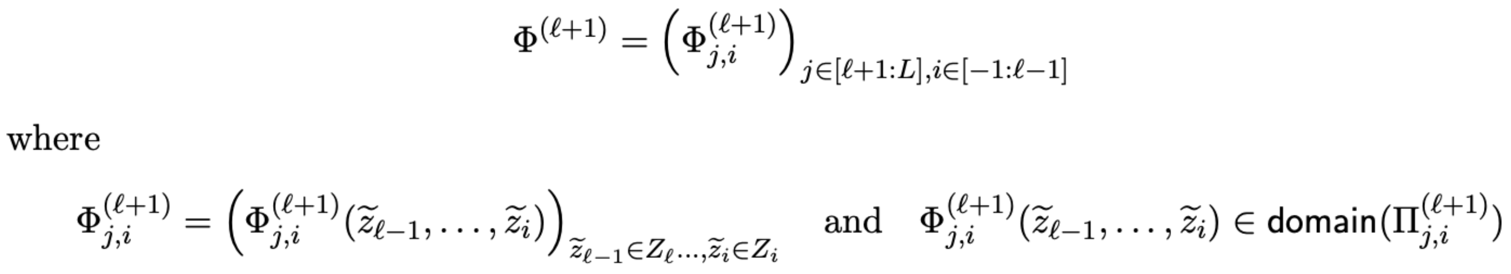
The first *nontrivial* step, where we finally see a distillation of $S_{\geq \ell+1}$!

In this step, we consider the transcripts only between players $[\ell + 1, L]$ and $[-1, \ell - 1]$ on the $\ell + 1$ epoch

Observation: Using the previous “fixing the transcript,” players $[-1, \ell - 1]$ receive the same transcript on all $\ell' \in [\ell]$ of which $z_\ell \in Z_\ell$ we select

Conclusion: The message sent at the $\ell + 1$ epoch is **independent** of Z_ℓ!

Therefore, we can write the transcript tuple *without indexing* z_ℓ



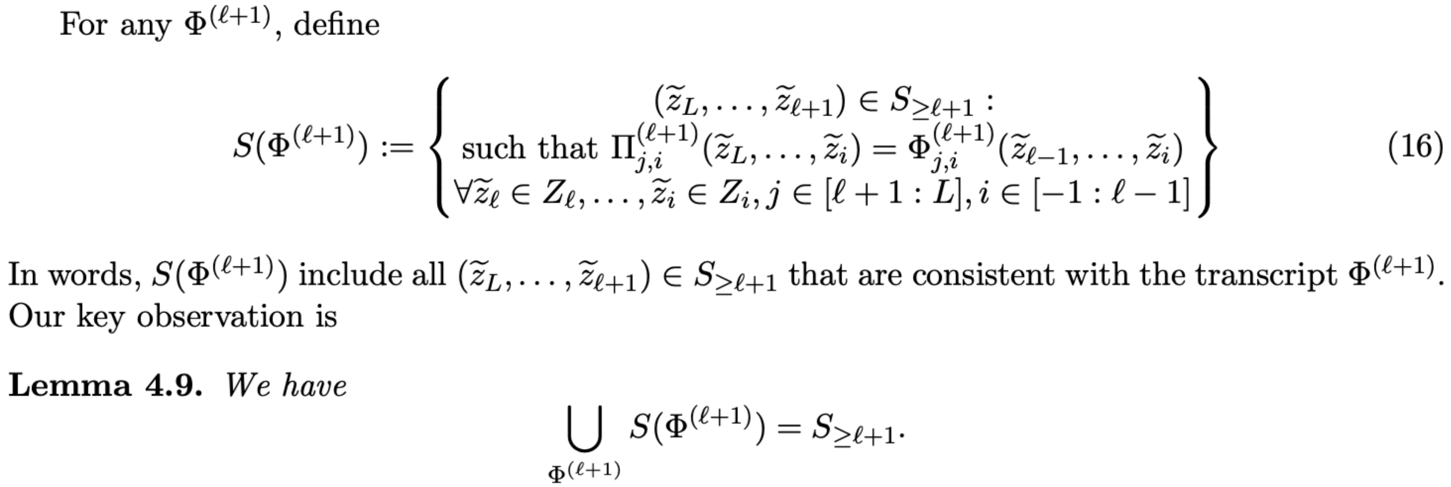
$$\Phi^{(\ell+1)} = \left(\Phi^{(\ell+1)}_{j,i}\right)_{j\in[\ell+1:L],i\in[-1:\ell-1]}$$

where

$$\Phi^{(\ell+1)}_{j,i} = \left(\Phi^{(\ell+1)}_{j,i}(\widetilde{z}_{\ell-1}, \ldots, \widetilde{z}_i)\right)_{\widetilde{z}_{\ell-1}\in Z_\ell \ldots, \widetilde{z}_i \in Z_i} \quad \text{and} \quad \Phi^{(\ell+1)}_{j,i}(\widetilde{z}_{\ell-1}, \ldots, \widetilde{z}_i) \in \mathsf{domain}(\Pi^{(\ell+1)}_{j,i})$$

“Fixing the transcript” II

With some more thought, the following lemma follows from **observation**



For any $\Phi^{(\ell+1)}$, define

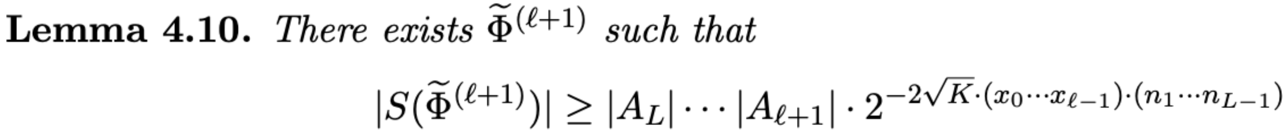
$$S(\Phi^{(\ell+1)}) := \left\{ \begin{array}{c} (\widetilde{z}_L, \ldots, \widetilde{z}_{\ell+1}) \in S_{\geq \ell+1} : \\ \text{such that } \Pi^{(\ell+1)}_{j,i}(\widetilde{z}_L, \ldots, \widetilde{z}_i) = \Phi^{(\ell+1)}_{j,i}(\widetilde{z}_{\ell-1}, \ldots, \widetilde{z}_i) \\ \forall \widetilde{z}_\ell \in Z_\ell, \ldots, \widetilde{z}_i \in Z_i, j \in [\ell+1 : L], i \in [-1 : \ell-1] \end{array} \right\} \tag{16}$$

In words, $S(\Phi^{(\ell+1)})$ include all $(\widetilde{z}_L, \ldots, \widetilde{z}_{\ell+1}) \in S_{\geq \ell+1}$ that are consistent with the transcript $\Phi^{(\ell+1)}$. Our key observation is

Lemma 4.9. *We have*

$$\bigcup_{\Phi^{(\ell+1)}} S(\Phi^{(\ell+1)}) = S_{\geq \ell+1}.$$

By counting transcripts $\Phi^{\ell+1}$ and again using pigeonhole, we find:



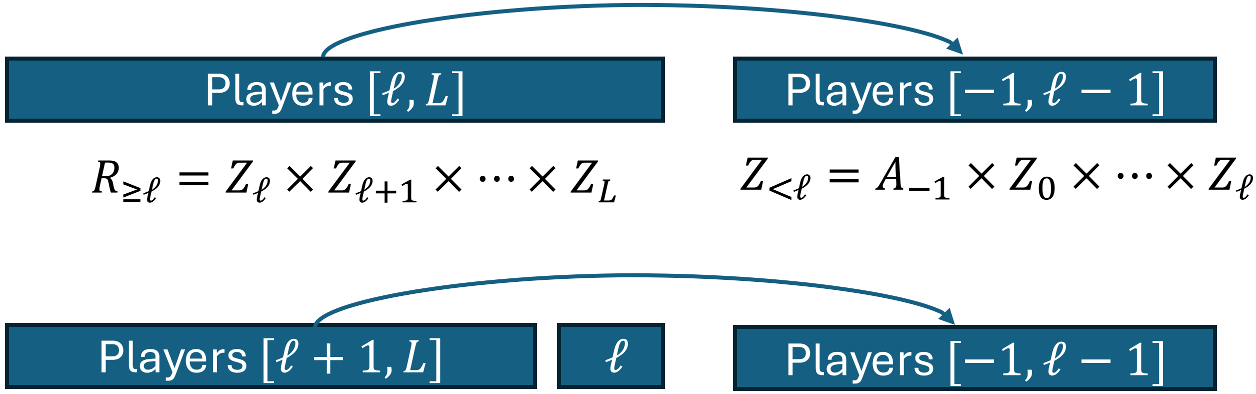
Lemma 4.10. *There exists* $\widetilde{\Phi}^{(\ell+1)}$ *such that*

$$|S(\widetilde{\Phi}^{(\ell+1)})| \geq |A_L| \cdots |A_{\ell+1}| \cdot 2^{-2\sqrt{K} \cdot (x_0 \cdots x_{\ell-1}) \cdot (n_1 \cdots n_{L-1})}$$

We set $T_{\geq \ell+1} = S\left(\widetilde{\Phi}^{\ell+1}\right) \subset S_{\geq \ell+1}$ to be our *first* refinement!!

Inductive Step

We have a decomposition $(Z_{<\ell}, R_{\geq \ell})$ which is indistinguishable through ℓ epochs, we'd like to distill $(Z_{<\ell+1}, R_{\geq \ell+1})$ which holds through $\ell+1$ epochs



Players $[\ell, L]$

Players $[-1, \ell-1]$

holds for $\ell' \in [\ell]$

$$R_{\geq \ell} = Z_\ell \times Z_{\ell+1} \times \cdots \times Z_L \qquad Z_{<\ell} = A_{-1} \times Z_0 \times \cdots \times Z_{\ell-1}$$

Players $[\ell+1, L]$

ℓ

Players $[-1, \ell-1]$

holds for $\ell' \in [\ell+1]$

$$R_{\geq \ell+1} = ?\times ?\times \cdots \times ? \qquad ? \qquad Z_{<\ell} = A_{-1} \times ? \times \cdots \times ?$$

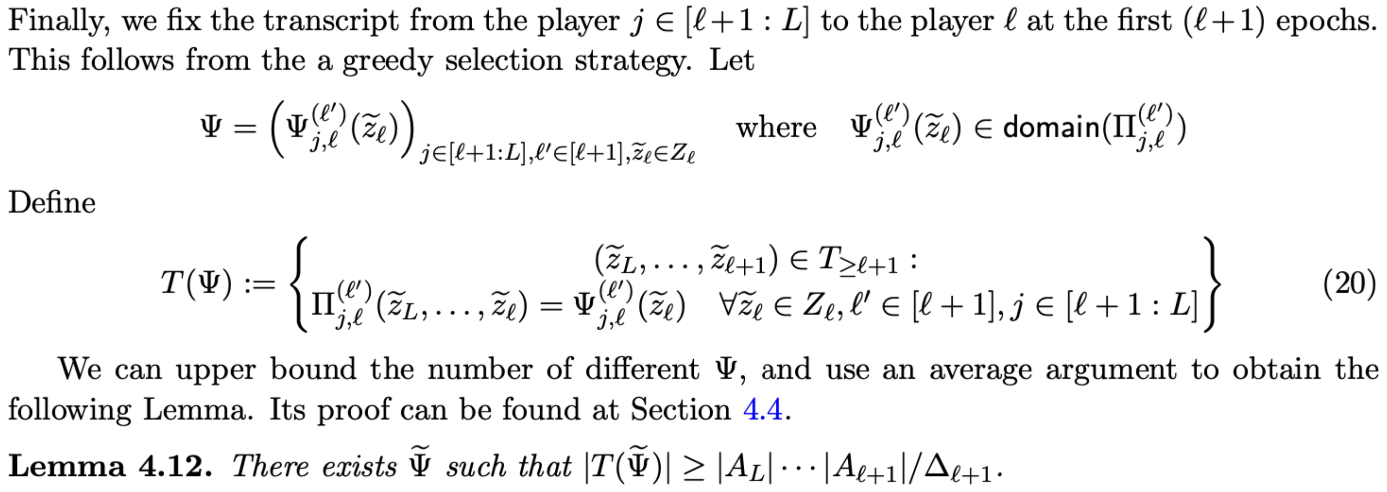
Order of attack:

1. Determine the new Z_ℓ and a superset of the new $R_{\geq \ell}$ (yet subset of old)
2. "Fix the transcripts" between $[\ell+1, L]$ and $[-1, \ell-1]$ on just the first ℓ epochs
3. "Fix the transcripts" between $[\ell+1, L]$ and $[-1, \ell-1]$ on the $\ell+1$ epoch
4. **"Fix the transcript" for player ℓ over all $\ell+1$ epochs**

“Fixing the transcript” III

The final step is to “fix the transcript” sent to player ℓ by players $[\ell+1, L]$ in all $\ell+1$ epochs.

Doing this will complete the induction, so the distillation of $T_{\geq \ell+1}$ we retrieve will be the output $R_{\geq \ell+1}$!



Finally, we fix the transcript from the player $j \in [\ell+1 : L]$ to the player ℓ at the first $(\ell+1)$ epochs. This follows from the a greedy selection strategy. Let

$$\Psi = \left(\Psi^{(\ell')}_{j,\ell}(\widetilde{z}_\ell)\right)_{j\in[\ell+1:L],\ell'\in[\ell+1],\widetilde{z}_\ell\in Z_\ell} \quad \text{where} \quad \Psi^{(\ell')}_{j,\ell}(\widetilde{z}_\ell) \in \mathsf{domain}(\Pi^{(\ell')}_{j,\ell})$$

Define

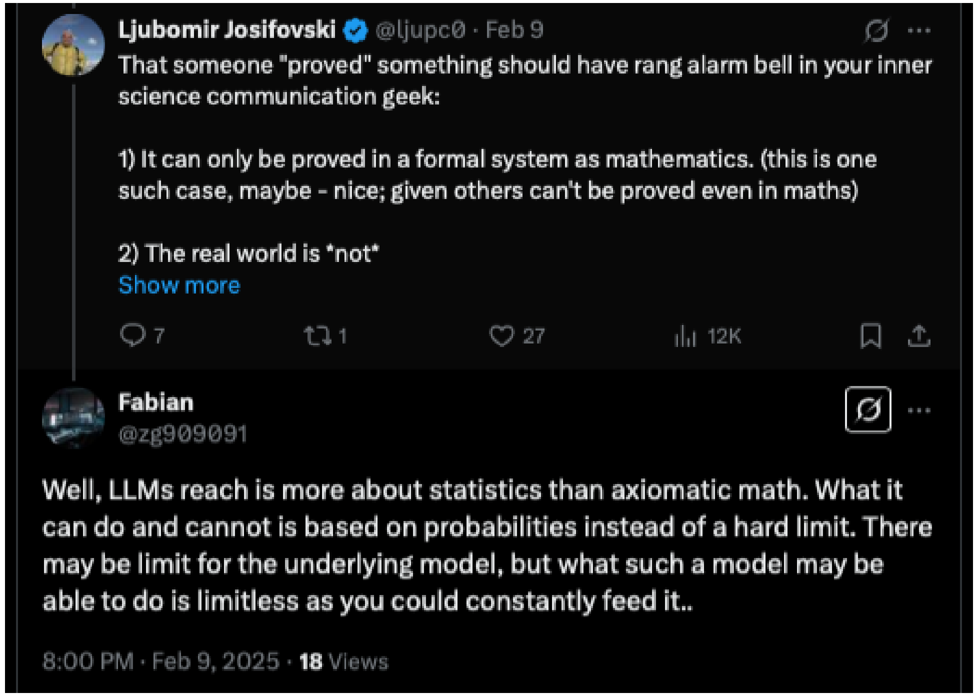
$$T(\Psi) := \left\{ \begin{array}{c} (\widetilde{z}_L, \ldots, \widetilde{z}_{\ell+1}) \in T_{\geq \ell+1} : \\ \Pi^{(\ell')}_{j,\ell}(\widetilde{z}_L, \ldots, \widetilde{z}_\ell) = \Psi^{(\ell')}_{j,\ell}(\widetilde{z}_\ell) \quad \forall \widetilde{z}_\ell \in Z_\ell, \ell' \in [\ell+1], j \in [\ell+1 : L] \end{array} \right\} \tag{20}$$

We can upper bound the number of different Ψ, and use an average argument to obtain the following Lemma. Its proof can be found at Section 4.4.

Lemma 4.12. *There exists* $\widetilde{\Psi}$ *such that* $|T(\widetilde{\Psi})| \geq |A_L| \cdots |A_{\ell+1}| / \Delta_{\ell+1}$.

Thus, we set $R_{\geq \ell+1} = T(\widetilde{\Psi})$ and note that it satisfies all the desired properties. The induction is complete!

Thanks for listening!! ☺



Ljubomir Josifovski @ljupc0 · Feb 9

That someone "proved" something should have rang alarm bell in your inner science communication geek:

1) It can only be proved in a formal system as mathematics. (this is one such case, maybe - nice; given others can't be proved even in maths)

2) The real world is *not*

Show more

Fabian
@zg909091

Well, LLMs reach is more about statistics than axiomatic math. What it can do and cannot is based on probabilities instead of a hard limit. There may be limit for the underlying model, but what such a model may be able to do is limitless as you could constantly feed it..

8:00 PM · Feb 9, 2025 · 18 Views

Via X/Twitter