

# Contents

<b>1</b>	<b>Some notes from which to expand this document</b>	<b>1</b>
<b>2</b>	<b>Definitions</b>	<b>2</b>
<b>3</b>	<b>Coupling proofs of privacy</b>	<b>2</b>
<b>4</b>	<b>Shift-coupling proofs of privacy</b>	<b>2</b>
4.1	Connecting constraints . . . . .	2
4.2	The cost of a shift-coupling . . . . .	4
4.3	Privacy . . . . .	5
4.4	Why the above had to be the way it is. . . . .	5
<b>5</b>	<b>The search for a tight proof as an optimization problem</b>	<b>5</b>
5.1	Stating the problem abstractly . . . . .	5
5.2	Simplifying the problem and introducing segments . . . . .	6
5.3	The problem as a whole . . . . .	6
<b>6</b>	<b>Finite Bounds and Decidability</b>	<b>6</b>
<b>7</b>	<b>Do shift-coupling proofs of privacy have matching lower bounds?</b>	<b>6</b>
7.1	$S^L$ is tight when there is an $L$ -cycle . . . . .	6
7.2	An alternative coupling strategy: $S^J$ . . . . .	7
<b>A</b>	<b>Lemmata</b>	<b>8</b>
A.1	Properties of $f_\varepsilon$ and $F_\varepsilon$ . . . . .	8
A.2	For the proof of Theorem 1 . . . . .	8

## 1 Some notes from which to expand this document

1. An overview of coupling proofs of privacy
2. A tight shift-coupling proof of privacy (segment free)
  - (a) What are the connecting constraints, and why are they there?
  - (b) Proofs have to depend on  $\Delta$ !
  - (c) Proofs have to depend on sequences of segments!
3. Simplifying the problem above in various ways:
  - (a) Separability and the introduction of segments
  - (b) Only inter-segment transitions matter!
    - Given  $\Delta$ , the  $\gamma$  values on inter-segment transitions are easily determined.
    - The  $\Delta$  values on the inter-segment transitions can be determined.
4. Solving the problem.
  - (a) Hardness (incomplete)!!!
  - (b) Solving the easier version, where proofs don't depend on  $\Delta$ .
  - (c) Showing that they are bounded within  $n$  of each other.

$$\exists \text{ finite DP bound} \iff \text{hard system admits a feasible solution}$$

## 2 Definitions

## 3 Coupling proofs of privacy

A coupling proof of privacy

## 4 Shift-coupling proofs of privacy

Consider a path  $\rho = q_0 \rightarrow q_1 \rightarrow \dots \rightarrow q_m$ . Consider inputs  $X\langle 1 \rangle = \langle a_1\langle 1 \rangle, \dots, a_m\langle 1 \rangle \rangle$  and  $X\langle 2 \rangle = \langle a_1\langle 2 \rangle, \dots, a_m\langle 2 \rangle \rangle$  such that  $X\langle 1 \rangle \sim X\langle 2 \rangle$ . We wish to show that there exists  $\varepsilon \in (0, \infty)$  such that

$$\Pr [\rho | X\langle 1 \rangle] \leq \exp(\varepsilon) \cdot \Pr [\rho | X\langle 2 \rangle]$$

**TODO:** Write all of this later after consulting with Sky! ALSO, distinguish between path equivalence and output equivalence.

**Definition 4.1.** Let  $X = \langle a_1, \dots, a_m \rangle$  be an input, and  $\rho = q_0 \rightarrow q_1 \rightarrow \dots \rightarrow q_m$  be a path taken by DiPA  $\mathcal{A}$  on  $X$ . Define  $\tilde{a}_i$  to be the value of **insample** on the  $i$ th transition in  $\rho$  on input  $X$ .

- The above is true if and only if  $\text{path}_A(X) \Psi_\rho^{(\varepsilon, 0)} \text{path}_A(X')$ , where

$$\Psi_\rho = \{(\rho_1, \rho_2) \in P \times P : \rho_1 = \rho \implies \rho_2 = \rho\}$$

Shift-couplings are a technique to show that  $\text{path}_A(X) \Psi_\rho^{(\varepsilon, 0)} \text{path}_A(X')$  by constructing the couplings

$$\tilde{a}_i\langle 1 \rangle + \gamma_i (=)^{\#(\varepsilon_i, 0)} \tilde{a}_i\langle 2 \rangle \quad \forall i \in \{0, \dots, m-1\}$$

and showing that

$$(\tilde{a}\langle 1 \rangle + \gamma = \tilde{a}\langle 2 \rangle) \implies \text{path}_A(X\langle 1 \rangle) \Psi_\rho \text{path}_A(X\langle 2 \rangle)$$

thus showing that  $\text{path}_A(X) \Psi_\rho^{(\varepsilon, 0)} \text{path}_A(X')$  for

$$\varepsilon = \sum_{i=0}^{m-1} \varepsilon_i$$

- A discussion that ends in choosing  $\gamma$  shifts for each segment.
- Maybe: A discussion of the cost of each shift.

### 4.1 Connecting constraints

**Definition 4.2.** Given a fixed path, we say that an assignment of shifts  $\{\gamma_i\}$  is **valid** if

$$(\tilde{a}\langle 1 \rangle + \gamma = \tilde{a}\langle 2 \rangle) \implies \text{path}_A(X\langle 1 \rangle) \Psi_\rho \text{path}_A(X\langle 2 \rangle)$$

**Definition 4.3.** Let  $\rho = q_0 \rightarrow q_1 \rightarrow \dots \rightarrow q_m$  be a path, and let  $i \in \{1, \dots, m\}$ . Define  $\text{at}(i)$  to be the largest index  $a(i) < i$  such that  $\rho[a(i)] \rightarrow \rho[a(i) + 1]$  is an assignment transition.

**Definition 4.4.** Let  $\rho = q_0 \rightarrow q_1 \rightarrow \dots \rightarrow q_m$  be a path. Define  $t_i$  to be the transition  $q_i \rightarrow q_{i+1}$ .

**Definition 4.5.** Let  $X = \langle a_1, \dots, a_m \rangle$  be an input, and let  $\rho = q_0 \rightarrow q_1 \rightarrow \dots \rightarrow q_m$  be a path. Define  $X[i]$  to be the value of  $a_i$ .

Note that such an index must exist due to the initialization condition on DiPA.

**Proposition 4.1.** *Given  $\rho = q_0 \rightarrow q_1 \rightarrow \dots \rightarrow q_m$ , an assignment of shifts  $\{\gamma_i\}$  is valid if and only if it satisfies the following constraints for all  $i \in \{0, \dots, m-1\}$ :*

$$\begin{aligned} \gamma_i &\leq \gamma_{at(i)} && \text{if } t_i \text{ has guard } < \\ \gamma_i &\geq \gamma_{at(i)} && \text{if } t_i \text{ has guard } \geq \end{aligned}$$

*Proof.* (Constraints  $\implies$  valid) Suppose that the above constraints hold. We will show that  $\{\gamma_i\}$  is valid using induction on  $m = |\rho|$ . Construct the couplings  $\tilde{a}_i\langle 1 \rangle + \gamma_i(=)^{(\varepsilon_i, 0)} \tilde{a}_i\langle 2 \rangle$  for all  $i \in \{0, \dots, m-1\}$ .

For a base case, assume  $m = 1$ . Then  $\rho$  consists of an assignment transition  $t_0$  with **true** guard (initialization condition). The constraints are trivially satisfied, and we have that  $path_A(X\langle 1 \rangle)\Psi_\rho^{(0,0)}path_A(X\langle 2 \rangle)$ .

Assume that the constraints hold for all paths of length  $m$ . Let  $\rho = q_0 \rightarrow q_1 \rightarrow \dots \rightarrow q_m \rightarrow q_{m+1}$ . We will show that  $\{\gamma_i\}$  is valid for  $\rho$ . First, by the validity of  $\{\gamma_i\}_{i=0}^{m-1}$  for  $\rho[0:m]$  by the inductive hypothesis, we have that

$$path_A(X\langle 1 \rangle)\Psi_{\rho[0:m]}path_A(X\langle 2 \rangle)$$

by the inductive hypothesis. Now, assume  $path_A(X\langle 1 \rangle) = \rho$ . We have  $path_A(X\langle 2 \rangle)[0:m] = \rho[0:m]$ . Consider the last transition  $t_m$  in  $\rho$ . Since  $path_A(X\langle 1 \rangle) = \rho$ , we know that  $t_m$  is traversed by  $A$  on  $X\langle 1 \rangle$ .

- If  $t_m$  has guard **true**, then we trivially have that  $path_A(X\langle 2 \rangle) = \rho$ .
- If  $t_m$  has guard  $<$ , we have from the constraints that  $\gamma_m \leq \gamma_{at(m)}$ . The value of the state variable  $x\langle 1 \rangle$  is

$$x\langle 1 \rangle = \tilde{a}_{at(m)}\langle 1 \rangle$$

and since  $t_m$  is traversed by  $A$  on  $X\langle 1 \rangle$ , we have

$$\begin{aligned} \tilde{a}_m\langle 1 \rangle &< \tilde{a}_{at(m)}\langle 1 \rangle \\ \tilde{a}_m\langle 2 \rangle - \gamma_m &< \tilde{a}_{at(m)}\langle 2 \rangle - \gamma_{at(m)} \\ \tilde{a}_m\langle 2 \rangle &< \tilde{a}_{at(m)}\langle 2 \rangle - (\gamma_{at(m)} - \gamma_m) < \tilde{a}_{at(m)}\langle 2 \rangle \end{aligned}$$

showing that  $\tilde{a}_m\langle 2 \rangle$  satisfies the guard of  $t_m$ . Thus,  $path_A(X\langle 2 \rangle) = \rho$ .

- If  $t_m$  has guard  $\geq$ , a similar argument as above shows that  $path_A(X\langle 2 \rangle) = \rho$ .

Thus, assuming that  $a\langle 1 \rangle + \gamma = a\langle 2 \rangle$ , we have shown that  $path_A(X\langle 1 \rangle) = \rho \implies path_A(X\langle 2 \rangle) = \rho$ , which shows  $path_A(X\langle 1 \rangle)\Psi_\rho path_A(X\langle 2 \rangle)$ , and so  $\{\gamma_i\}$  is valid.

(Valid  $\implies$  constraints) Suppose that  $\{\gamma_i\}$  is valid. Let  $i \in \{0, \dots, m-1\}$ . We will show that the constraints hold for  $i$ .

We will run the argument above in reverse. Again, we use induction on the length  $m = |\rho|$ . For a base case, assume  $m = 1$ , and so  $\rho$  consists of an assignment transition  $t_0$  with **true** guard. The constraints are trivially satisfied, since there are none.

Assume that the constraints hold for all valid shift assignments on paths of length  $m$ , and let  $\rho = q_0 \rightarrow q_1 \rightarrow \dots \rightarrow q_m \rightarrow q_{m+1}$ . Since  $\{\gamma_i\}$  is valid for  $\rho$ , we have that  $a\langle 1 \rangle + \gamma = a\langle 2 \rangle \implies path_A(X\langle 1 \rangle)\Psi_\rho path_A(X\langle 2 \rangle)$ . Also, we have that  $\{\gamma_i\}_{i=0}^{m-1}$  is valid for  $\rho[0:m]$ , and that constraints on transitions  $t_i \in \rho[0:m]$  hold.

We will now show that the constraints on  $t_m$  hold by cases on the guard of  $t_m$ .

- If  $t_m$  has guard **true**, then there is no constraint on  $\gamma_m$ , and so the constraints hold.

- If  $t_m$  has guard  $<$ , the constraint to be shown is  $\gamma_m \leq \gamma_{at(m)}$ . Recall that we have  $a\langle 1 \rangle + \gamma = a\langle 2 \rangle \implies \text{path}_A(X\langle 1 \rangle) \Psi_\rho \text{path}_A(X\langle 2 \rangle)$ , showing that  $t_m$  being traversed by  $A$  on  $X\langle 1 \rangle$  leads  $t_m$  to be traversed by  $A$  on  $X\langle 2 \rangle$ . Thus, we have

$$\begin{aligned} \tilde{a}_m\langle 1 \rangle < \tilde{a}_{at(m)}\langle 1 \rangle &\implies \tilde{a}_m\langle 2 \rangle < \tilde{a}_{at(m)}\langle 2 \rangle \\ &\iff \tilde{a}_m\langle 1 \rangle + \gamma_m < \tilde{a}_{at(m)}\langle 1 \rangle + \gamma_{at(m)} \\ &\iff \tilde{a}_m\langle 1 \rangle < \tilde{a}_{at(m)}\langle 1 \rangle + (\gamma_{at(m)} - \gamma_m) \end{aligned}$$

which is true if and only if  $\gamma_m \leq \gamma_{at(m)}$ . Thus, the constraint holds.

- A symmetric argument shows that the constraint holds if  $t_m$  has guard  $\geq$ .

Thus, the given constraints on  $\gamma$  hold if and only if it is valid for  $\rho$ . □

**Definition 4.6.** Define  $\mathcal{P}$  to be the set of all paths in  $\mathcal{A}$ .

**Definition 4.7.** Given a DiPA  $\mathcal{A}$ , a **shift-coupling proof of privacy** for  $\mathcal{A}$  is a map

$$\begin{aligned} \Gamma : \mathcal{P} &\rightarrow ([-1, 1]^\rho \rightarrow [-1, 1]^{|\rho|}) \\ \rho &\mapsto (\Delta \mapsto \{\gamma_i\}) \end{aligned}$$

such that for all  $\rho \in \mathcal{P}$  and all  $\Delta \in [-1, 1]^\rho$ , we have that  $\{\gamma_i\}$  is valid for  $\rho$  and  $\Delta$ , and satisfies the output constraints.

Note: we show that this is actually a proof after the next section.

## 4.2 The cost of a shift-coupling

**Proposition 4.2.** Consider a transition  $t_i = q_i \rightarrow q_{i+1}$  which is traversed independently by  $A$  on input  $a_i\langle 1 \rangle$  and  $a_i\langle 2 \rangle$ . Let  $\Delta_i = a_i\langle 2 \rangle - a_i\langle 1 \rangle$ . Let  $q_i$  draw from the distribution  $\text{Lap}(0, \varepsilon_i)$  to noise **insample**. The  $\varepsilon$ -cost of the coupling

$$\tilde{a}_i\langle 1 \rangle + \gamma_i(=)^{(c_i, 0)} \tilde{a}_i\langle 2 \rangle$$

is given by

$$c_i = |\Delta_i - \gamma_i| \varepsilon_i$$

*Proof.* TODO, but easy to see from coupling construction rules. □

**Definition 4.8.** Given a path  $\rho$  and input differences  $\Delta$ , we define the  $\rho$ - $\Delta$ -**cost** of the shifts  $\{\gamma_i\}$  to be

$$\text{cost}_{\rho, \Delta}(\{\gamma_i\}) = \sum_{i=0}^{|\rho|-1} |\Delta_i - \gamma_i| \varepsilon_i$$

**Definition 4.9.** Given a shift-coupling proof of privacy  $\Gamma$ , we define the privacy cost of  $\Gamma$  to be

$$\text{cost}(\Gamma) = \sup_{\rho \in \mathcal{P}} \sup_{\Delta \in [-1, 1]^\rho} \text{cost}_{\rho, \Delta}(\Gamma(\rho, \Delta))$$

### 4.3 Privacy

**Theorem 1.** *Let  $\mathcal{A}$  be a DiPA, and  $\Gamma$  be a shift-coupling proof of privacy for  $\mathcal{A}$ . Then,  $\mathcal{A}$  is  $(\varepsilon, 0)$ -differentially private, where  $\varepsilon = \text{cost}(\Gamma)$ .*

*Proof.* This is a direct consequence of path validity + output constraints.  $\square$

### 4.4 Why the above had to be the way it is.

Since the total validity constraints on  $\{\gamma_i\}$  does not depend on  $X\langle 1 \rangle$  and  $X\langle 2 \rangle$ , one might be tempted to produce a proof of privacy by choosing  $\gamma_i$  to be the same for all  $X\langle 1 \rangle$  and  $X\langle 2 \rangle$ , given a path  $\rho$ . Although this is possible, this does not in general produce a tight proof of privacy.

**Proposition 4.3. (A tight proof must regard input differences)** *There exists a family of DiPA  $\mathcal{F}$  and for  $\mathcal{A} \in \mathcal{F}$ , a shift-coupling proof  $\Gamma^* : \mathcal{P} \rightarrow ([-1, 1]^\rho \rightarrow [-1, 1]^{|\rho|})$  such that for all assignments  $\Pi : \mathcal{P} \rightarrow [-1, 1]^\rho$  of paths to shifts, we have*

$$\text{cost}(\Gamma^*) < \text{cost}(\Pi)$$

*Proof.* The construction is a DiPA with a one-segment path with same number of  $<$  and  $\geq$  transitions.  $\square$

When constructing a shift-coupling proof of privacy, we are actually choosing a shift for each transition. Is it reasonable to ignore paths, and just choose a shift for each transition? The answer is no, as the following proposition shows.

**Proposition 4.4. (A tight proof must regard paths)** *There exists a family of DiPA  $\mathcal{F}$  and for  $\mathcal{A} \in \mathcal{F}$ , a shift-coupling proof  $\Gamma^* : \mathcal{P} \rightarrow ([-1, 1]^\rho \rightarrow [-1, 1]^{|\rho|})$  such that for all assignments  $\Pi : E \rightarrow ([-1, 1]^\rho \rightarrow [-1, 1]^{|\rho|})$  of transitions and differences to shifts, we have*

$$\text{cost}(\Gamma^*) < \text{cost}(\Pi)$$

*Proof.*  $\square$

## 5 The search for a tight proof as an optimization problem

### 5.1 Stating the problem abstractly

Now that we have a characterization of shift-coupling proofs of privacy, the problem of finding a tight proof of privacy can be formulated as finding, given  $\rho$  and  $\Delta$ ,

$$\inf_{\Gamma} \text{cost}(\Gamma) = \inf_{\Gamma} \sup_{\rho} \sup_{\Delta} \text{cost}_{\rho, \Delta}(\Gamma(\rho, \Delta))$$

which is characterized by  $\Gamma^*$  such that for any shift-coupling proof  $\Gamma$ , we have

$$\sup_{\rho} \sup_{\Delta} \text{cost}(\Gamma^*(\rho, \Delta)) \leq \sup_{\rho} \sup_{\Delta} \text{cost}(\Gamma(\rho, \Delta))$$

$$\min_{\gamma \in [-1, 1]^{|\rho|}} \text{cost}_{\rho, \Delta}(\gamma)$$

One such  $\Gamma^*$  is the shift-coupling proof that chooses

$$\Gamma^*(\rho, \Delta) = \inf_{\gamma \in [-1, 1]^{|\rho|}} \text{cost}_{\rho, \Delta}(\gamma)$$

which is the shift-coupling proof that chooses the optimal shift for each input difference and path independently. We will now direct our focus to computing  $\Gamma^*$  given an automaton  $\mathcal{A}$ .

## 5.2 Simplifying the problem and introducing segments

## 5.3 The problem as a whole

# 6 Finite Bounds and Decidability

**Proposition 6.1.**

## 7 Do shift-coupling proofs of privacy have matching lower bounds?

**Last Updated: Wednesday, June 28th, 2023**

The relevant definitions and lemmata for proofs in this section are in the appendix. It is also assumed, for now, that all transition outputs are in the output alphabet.

### 7.1 $S^L$ is tight when there is an $L$ -cycle

**Theorem 2.** ( $S^L$  is tight for segments with  $L$ -cycles) Consider a segment  $s \in \text{seg}(\mathcal{A})$  corresponding to the sequence of states  $q_0 \rightarrow q_1 \rightarrow \dots \rightarrow q_m$ . If  $s$  contains an  $L$ -cycle, then the  $L$ -cost of the segment gives a tight upper bound on the privacy loss of the segment. That is,

$$\text{loss}(s) = \exp \left( 2\varepsilon_0 + \sum_{i>0: \text{guard}(a_i)=\text{insample} \geq x} 2\varepsilon_i \right)$$

given that state  $q_i$  draws from the distribution  $\text{Lap}(0, 1/\varepsilon_i)$  to noise `insample`.

*Proof.* We will prove the result for when  $\varepsilon_i = \varepsilon$  for all  $i \geq 0$ . The proof for the general case goes through in the same fashion. Let  $f, F$  be the probability density function and cumulative distribution function of a random variable  $X$  with  $X \sim \text{Lap}(0, 1/\varepsilon)$  as defined in the appendix.

Since  $s$  has an  $L$ -cycle, there exists a sequence of paths  $\rho_i$  for  $i \in \mathbb{N}$  each with  $l_i$  number of  $L$ -transitions such that  $\lim_{i \rightarrow \infty} l_i = \infty$ . Let  $m$  be the number of  $G$ -transitions in  $\rho_i$ . We will assume that this number is the same across all  $\rho_i$ .<sup>1</sup>

For each  $\rho_i$ , construct the adjacent pair of inputs  $X_i, X'_i$  as follows. Let  $X_i[j] = 0$  for all  $j \in \{1, \dots, |\rho_i|\}$ , where  $|\rho_i|$  is the number of transitions in  $\rho$ . Define  $X_i[j]$  as follows:

$$X_i[j] = \begin{cases} 1 & \text{if } \rho_i[j] \rightarrow \rho_i[j+1] \text{ is an assignment transition or has guard } \text{insample} \geq x \\ -1 & \text{otherwise, in which case } \rho_i[j] \rightarrow \rho_i[j+1] \text{ has guard } \text{insample} < x \end{cases}$$

Let  $\tilde{a}_j$  be the random variable representing the value of `insample` before the  $j$ th transition in  $\rho$  on input  $X_i$ . Let  $\tilde{b}_j$  be the random variable representing the value of `insample` before the  $j$ th transition in  $\rho$  on input  $X'_i$ . Further, let  $\Gamma_L = \{j : \rho_i[j] \rightarrow \rho_i[j+1] \text{ has guard } \text{insample} < x\}$ , and  $\Gamma_G = \{j : \rho_i[j] \rightarrow \rho_i[j+1] \text{ has guard } \text{insample} \geq x\}$ .

Notice that  $\tilde{a}_j = \tilde{b}_j + 1$  for  $j \in \Gamma_L$ , and  $\tilde{a}_j + 1 = \tilde{b}_j$  for  $j \in \{0\} \cup \Gamma_G$ . Since  $\tilde{a}_j$  is distributed as  $\text{Lap}(X_i[j], 1/\varepsilon)$ , we can write its probability density function as  $f(x - X_i[j])$ , and its cumulative distribution function as  $F(x - X_i[j])$ . A similar statement holds for  $\tilde{b}_j$ .

We may now compute and compare  $\Pr(\rho_i | X'_i)$  and  $\Pr(\rho_i | X_i)$  as follows.

<sup>1</sup>Otherwise,  $s$  has a  $G$ -cycle, and  $\mathcal{A}$  is not differentially private. The privacy loss through  $s$  is  $\infty$ , which matches the  $L$ -cost.

$$\begin{aligned}
\Pr(\rho_i|X'_i) &= \int_{-\infty}^{\infty} \Pr(\tilde{b}_0 = x) \prod_{j \in \Gamma_L} \Pr(\tilde{b}_j < x) \prod_{j \in \Gamma_G} \Pr(\tilde{b}_j \geq x) dx \\
&= \int_{-\infty}^{\infty} \Pr(\tilde{b}_0 = x) \prod_{j \in \Gamma_L} \Pr(\tilde{b}_j < x) \prod_{j \in \Gamma_G} \Pr(\tilde{b}_j \geq x) dx \\
&= \int_{-\infty}^{\infty} f_\varepsilon(x - X_i[0]) \prod_{j \in \Gamma_L} F_\varepsilon(x - X_i[j]) \prod_{j \in \Gamma_G} (1 - F_\varepsilon(x - X_i[j])) dx \\
&= \int_{-\infty}^{\infty} f(x - 1)F(x + 1)^{\ell_i}(1 - F(x - 1))^m \\
&= \int_{-\infty}^{\infty} f(x)F(x + 2)^{\ell_i}(1 - F(x))^m \\
&= \exp(2\varepsilon(m + 1)) \left( \int_{(-\infty, -2) \cup (2, \infty)} f(x)F(x)^{\ell_i}(1 - F(x))^m dx + g(\ell_i) \int_{-2}^2 f(x)F(x + 2)^{\ell_i}(1 - F(x))^m \right)
\end{aligned}$$

with  $g(\ell_i) \rightarrow 1$  as  $\ell_i \rightarrow \infty$ . As we take  $\ell_i \rightarrow \infty$ , we see that

$$h(\ell_i) := \frac{\left( \int_{(-\infty, -2) \cup (2, \infty)} f(x)F(x)^{\ell_i}(1 - F(x))^m dx + g(\ell_i) \int_{-2}^2 f(x)F(x + 2)^{\ell_i}(1 - F(x))^m \right)}{\Pr(\rho_i|X_i)} \rightarrow 1$$

and so as we take the supremum over  $\rho_i$  below, we get:

$$\begin{aligned}
\text{loss}(s) &\geq \sup_{\rho_i} \frac{\Pr(\rho_i|X'_i)}{\Pr(\rho_i|X_i)} = \exp(2\varepsilon(m + 1)) \sup_{\rho_i} \{h(\ell_i)\} \\
&= \exp(2\varepsilon(m + 1))
\end{aligned}$$

We know that  $S^L$  is tight, and gives the bound  $\exp(2\varepsilon(m + 1))$ . Thus, we have shown that  $\text{loss}(s) = \exp(2\varepsilon(m + 1))$ , as desired.  $\square$

## 7.2 An alternative coupling strategy: $S^J$

**Definition 7.1.**  $S^J$  is a coupling strategy in which we do not couple the noised threshold, but couple the results of all other transitions with twice the cost. [TODO: Describe in more detail]

**Theorem 3.** Let  $s = q_0 \rightarrow \dots \rightarrow q_m$  be a segment with only L-transitions. If  $S^J$  is the least-cost coupling strategy on  $s$ , then it provides a tight bound on  $\text{loss}(s)$  given by

$$\text{loss}(s) = \sum_{i=1}^m 2\varepsilon_i$$

*Proof.* I have a proof for this, but I will add it into this document soon. [TODO]

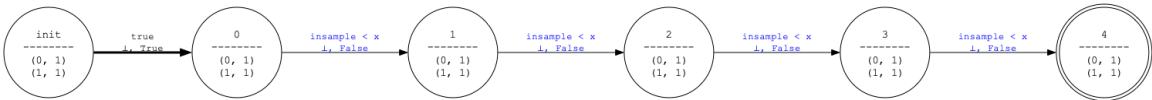


Figure 1: A segment  $s$  with only L-transitions.

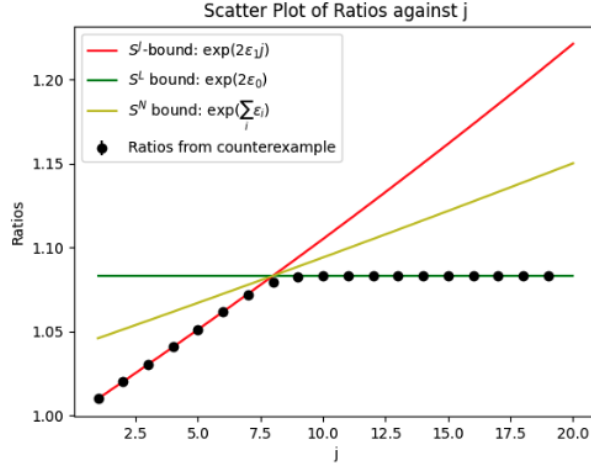


Figure 2:

□

**Hypothesis 7.1.** For segments which contain only  $L$ -transitions and for which the  $J$ -cost exceeds the  $L$ -cost,  $S^L$  is tight.

*Proof.* I think this is true from the graph above, but I need to prove it.

Note June 28 2023: I think this is not true for segments that contain both  $L$ -transitions and  $G$ -transitions.

□

## A Lemmata

### A.1 Properties of $f_\varepsilon$ and $F_\varepsilon$

**Lemma 4.** For  $x \leq 0$ , we have

$$F_\varepsilon(x) = \exp(2\varepsilon)F_\varepsilon(x-2)$$

and equivalently for  $x \leq -2$ , we have

$$F_\varepsilon(x+2) = \exp(2\varepsilon)F_\varepsilon(x)$$

**Lemma 5.** For  $x \geq 0$ , we have

$$1 - F_\varepsilon(x) = \exp(2\varepsilon)(1 - F_\varepsilon(x+2))$$

**Lemma 6.** For  $x \geq 0$ , we have

$$f_\varepsilon(x) = \exp(2\varepsilon)f_\varepsilon(x+2)$$

### A.2 For the proof of Theorem 1

**Lemma 7.**

$$\int_{-\infty}^{-2} f_\varepsilon(x)F_\varepsilon(x+2)^\ell(1-F_\varepsilon(x))^m dx = \exp(2\varepsilon\ell) \int_{-\infty}^{-2} f_\varepsilon(x)F_\varepsilon(x)^\ell(1-F_\varepsilon(x))^m dx$$

*Proof.* From Lemma 4, we have that

$$\begin{aligned} \int_{-\infty}^{-2} f_\varepsilon(x)F_\varepsilon(x+2)^\ell(1-F_\varepsilon(x))^m dx &= \int_{-\infty}^{-2} f_\varepsilon(x)(\exp(2\varepsilon)F_\varepsilon(x))^\ell(1-F_\varepsilon(x))^m dx \\ &= \exp(2\varepsilon\ell) \int_{-\infty}^{-2} f_\varepsilon(x)F_\varepsilon(x)^\ell(1-F_\varepsilon(x))^m dx \end{aligned}$$



□

**Lemma 8.**

$$\int_0^\infty f_\varepsilon(x) F_\varepsilon(x+2)^\ell (1 - F_\varepsilon(x))^m dx = \exp(2\varepsilon m) \int_2^\infty f_\varepsilon(x) F_\varepsilon(x)^\ell (1 - F_\varepsilon(x))^m dx$$

*Proof.* From Lemma 5 and 6, we have that

$$\begin{aligned} \int_0^\infty f_\varepsilon(x) F_\varepsilon(x+2)^\ell (1 - F_\varepsilon(x))^m dx &= \int_0^\infty \exp(2\varepsilon) f_\varepsilon(x+2) F_\varepsilon(x+2)^\ell (\exp(2\varepsilon)(1 - F_\varepsilon(x+2)))^m dx \\ &= \exp(2\varepsilon m) \int_0^\infty f_\varepsilon(x+2) F_\varepsilon(x+2)^\ell (1 - F_\varepsilon(x+2))^m dx \\ &= \exp(2\varepsilon(m+1)) \int_2^\infty f_\varepsilon(x) F_\varepsilon(x)^\ell (1 - F_\varepsilon(x))^m dx \end{aligned}$$

□

**Lemma 9.** *There exists a function  $g : \mathbb{N} \rightarrow \mathbb{R}$  such that*

$$\int_{-2}^0 f_\varepsilon(x) F_\varepsilon(x+2)^\ell (1 - F_\varepsilon(x))^m dx = g(\ell) \exp(2\varepsilon(m+1)) \int_{-2}^2 f_\varepsilon(x) F_\varepsilon(x)^\ell (1 - F_\varepsilon(x))^m dx$$

with  $g(\ell) \rightarrow 1$  as  $\ell \rightarrow \infty$ .

*Proof.* I'm not sure yet how to prove this, although I strongly suspect that the  $(m+1)$  term comes from the fact that  $f_\varepsilon(x)$  is the derivative of  $-(1 - F_\varepsilon(x))$ , and it is taken to the  $m$ th power. Its integral should behave like a polynomial of degree  $m+1$  evaluated at 2, which corresponds to  $\exp(2\varepsilon(m+1))$ . □