Optimizing shift-coupling proofs of privacy for DiPA

Vishnu Nittoor

Summer Research: May – August 2023

Summary

This document is a summary of the work done this summer on finding tight privacy bounds for DiPA using probabilistic couplings. We restrict ourselves to shift-couplings, which are couplings on the noise of neighbouring inputs on transitions. We find necessary and sufficient conditions on shift-couplings to show ε-differential privacy, and show that finding a tight shift-coupling proof of privacy can be formulated as an optimization problem. We show that tight shift-coupling proofs must necessarily depend on the differences between neighbouring inputs, and the paths taken by the automaton on those inputs.

We present the notion of a segment, which allows us to optimize over finitely many families of paths. Although the search for a tight proof is a convex maximization problem, a relaxation can be formulated as linear programs over segment sequences. We bound the cost of a tight proof of privacy in terms of the cost of the tight relaxated shift-coupling proof, and show that differential privacy can be decided in linear-time for DiPA using the model of shift-couplings. An open problem is whether there exist privacy bounds for DiPA that cannot be shown using shift-couplings.

Contents

1 Coupling proofs of privacy

In order to set up shift-coupling proofs of privacy, we first need to define the notion of a coupling proof of privacy.

Definition 1.1. *Let $\mathcal{A}$ be a randomized mechanism taking outputs in B. A **coupling proof of privacy** with cost ε for $\mathcal{A}$ constructs for every two adjacent inputs $X\langle 1\rangle \sim X\langle 2\rangle$ and output $b \in B$ of $\mathcal{A}$ the coupling*

$$\mathcal{A}(X\langle 1\rangle)\Phi_b^{\#(\varepsilon,0)}A(X\langle 2\rangle)$$

where

$$\Phi_b = \{(x_1, x_2) \in B \times B : x_1 = b \implies x_2 = b\}$$

Proposition 1.1. *A randomized mechanism $\mathcal{A}$ is ε-differentially private if there exists a coupling proof of privacy for $\mathcal{A}$ with cost ε.*

Proof. From "Proving Differential Privacy via Probabilistic Couplings" by Barthe et al. □

2 Shift-coupling proofs of privacy

Shift-coupling proofs of privacy attempt to couple the neighbouring noised inputs read by a DiPA $\mathcal{A}$ on $X\langle 1\rangle \sim X\langle 2\rangle$ using shifts in order to construct a coupling proof of privacy. In order to do this, we need to understand the correspondence between paths and outputs in a DiPA.

Let $path_{\mathcal{A}}(X)$ be a random variable representing the path taken by $\mathcal{A}$ on X, and $output_{\mathcal{A}}(X)$ be a random variable representing the output produced by $\mathcal{A}$ on X.

Proposition 2.1. *Let $\mathcal{A}$ be a DiPA, and $X\langle 1\rangle \sim X\langle 2\rangle$ be two neighbouring inputs. We have*

$$path_{\mathcal{A}}(X\langle 1\rangle) = path_{\mathcal{A}}(X\langle 2\rangle) \text{ with same real-valued outputs} \iff output_{\mathcal{A}}(X\langle 1\rangle) = output_{\mathcal{A}}(X\langle 2\rangle)$$

and

$$path_{\mathcal{A}}(X\langle 1\rangle)\Psi_\rho path_{\mathcal{A}}(X\langle 2\rangle) \text{ with same real-valued outputs} \iff \forall o \in [o]_\rho : output_{\mathcal{A}}(X\langle 1\rangle)\Phi_o output_{\mathcal{A}}(X\langle 2\rangle)$$

where $[o]_\rho$ is the class of all possible outputs that can be produced by the path ρ.

Proof. This directly follows from the output determinism conditions in DiPA. □

Proposition 2.2. *If we have for all $X\langle 1\rangle \sim X\langle 2\rangle$ and paths ρ taken by $\mathcal{A}$ that*

$$output_{\mathcal{A}}(X\langle 1\rangle)\Psi_\rho^{\#(\varepsilon,0)} output_{\mathcal{A}}(X\langle 2\rangle)$$

$$\Psi_\rho = \{(o_1, o_2) \in B \times B : o_1 \in [o]_\rho \implies o_1 = o_2\}$$

then $\mathcal{A}$ is $(\varepsilon, 0)$-differentially private.

Proof. For any output $o \in B$, find the path ρ for which $o \in [o]_\rho$. Then we can construct the coupling

$$output_{\mathcal{A}}(X\langle 1\rangle)\Phi_o^{\#} output_{\mathcal{A}}(X\langle 2\rangle)$$

where

$$\Phi_o = \{(o_1, o_2) \in B \times B : o_1 = o \implies o_2 = o\}$$

which shows $(\varepsilon, 0)$-privacy. □

The goal of shift-coupling proofs of privacy is to construct the lifting in Proposition 2.2 by the relation Ψ_ρ. This is because working with paths is more amenable to shift-couplings than working with outputs.

Definition 2.1. *Let $X = \langle a_1, \dots, a_m \rangle$ be an input, and $\rho = q_0 \to q_1 \to \cdots \to q_m$ be a path taken by DiPA $\mathcal{A}$ on X. Define $\tilde{a_i}$ to be the value of* `insample` *on the ith transition in ρ on input X.*

A shift-coupling proof of privacy attempts to construct the couplings in Proposition 2.2 by constructing the couplings for $X\langle 1 \rangle = \langle a_1\langle 1 \rangle, \dots, a_m\langle 1 \rangle \rangle$ and $X\langle 2 \rangle = \langle a_1\langle 2 \rangle, \dots, a_m\langle 2 \rangle \rangle$ for all $a_i\langle 1 \rangle, a_i\langle 2 \rangle \in [-1, 1]$. Let us use the notation

$$\tilde{a}\langle 1 \rangle + \boldsymbol{\gamma} = \tilde{a}\langle 2 \rangle$$

to denote the couplings

$$\tilde{a}_i\langle 1 \rangle + \gamma_i =^{\#} \tilde{a}_i\langle 2 \rangle \qquad \forall i$$

We call $\boldsymbol{\gamma}$ an assignment of shifts.

Definition 2.2. *Given a fixed path, we say that an assignment of shifts $\boldsymbol{\gamma} = \{\gamma_i\}$ is **path-valid** if*

$$(\tilde{a}\langle 1 \rangle + \gamma = \tilde{a}\langle 2 \rangle) \implies \big(path_{\mathcal{A}}(X\langle 1 \rangle) = \rho \implies path_{\mathcal{A}}(X\langle 2 \rangle) = \rho\big)$$

Definition 2.3. *Given a fixed path, we say that an assignment of shifts $\boldsymbol{\gamma} = \{\gamma_i\}$ is **valid** if*

$$(\tilde{a}\langle 1 \rangle + \gamma = \tilde{a}\langle 2 \rangle) \implies \big(output_{\mathcal{A}}(X\langle 1 \rangle) \Psi_\rho output_{\mathcal{A}}(X\langle 2 \rangle)\big)$$

where Ψ_ρ is the relation on outputs defined by

$$\Psi_\rho = \{(o_1, o_2) \in B \times B : o_1 \in [o]_\rho \implies o_1 = o_2\}$$

Definition 2.4. *Given a DiPA $\mathcal{A}$, a **shift-coupling proof of privacy** for $\mathcal{A}$ is a map*

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

such that for all $\rho \in paths(\mathcal{A})$ and all $\Delta \in [-1, 1]^{|\rho|}$, we have that $\{\gamma_i\}$ is valid for ρ.

We choose $\gamma \in [-1, 1]$ as any choice of $\gamma \in \mathbb{R}$ can be projected to $[-1, 1]$ to construct a valid shift-coupling proof of privacy without increasing 'cost', as defined below.

2.1 Constraints

We now wish to find necessary and sufficient conditions on $\boldsymbol{\gamma}$ that ensure that it is valid.

Definition 2.5. *Let $\rho = q_0 \to q_1 \to \cdots \to q_m$ be a path, and let $i \in \{1, \dots, m\}$. Define $at(i)$ to be the largest index $a(i) < i$ such that $\rho[a(i)] \to \rho[a(i) + 1]$ is an assignment transition.*

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

Proposition 2.3. *Given $\rho = q_0 \to q_1 \to \cdots \to q_m$, an assignment of shifts $\boldsymbol{\gamma} = \{\gamma_i\}$ is path-valid if and only if it satisfies the following constraints for all $i \in \{0, \dots, m - 1\}$:*

$$\gamma_i \le \gamma_{at(i)} \qquad \text{if } t_i \text{ has guard } < \tag{1}$$

$$\gamma_i \ge \gamma_{at(i)} \qquad \text{if } t_i \text{ has guard } \ge \tag{2}$$

where $t_i = q_i \to q_{i+1}$ is the ith transition in ρ.

Proof. (Constraints $\implies$ path-valid) Suppose that the above constraints hold. We will show that $\{\gamma_i\}$ is path-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 $i \in \{0, \ldots, m-1\}$.

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

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

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

by the inductive hypothesis. Now, assume $path_{\mathcal{A}}(X\langle 1\rangle) = \rho$. We have $path_{\mathcal{A}}(X\langle 2\rangle)[0:m] = \rho[0:m]$. Consider the last transition t_m in ρ. Since $path_{\mathcal{A}}(X\langle 1\rangle) = \rho$, 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 $path_{\mathcal{A}}(X\langle 2\rangle) = \rho$.
- 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, $path_{\mathcal{A}}(X\langle 2\rangle) = \rho$.
- If t_m has guard $\geq$, a similar argument as above shows that $path_{\mathcal{A}}(X\langle 2\rangle) = \rho$.

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

(Path-valid $\implies$ constraints) Suppose that $\{\gamma_i\}$ is path-valid. Let $i \in \{0, \ldots, m-1\}$. 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 ρ 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 path-valid shift assignments on paths of length m, and let $\rho = q_0 \to q_1 \to \cdots \to q_m \to q_{m+1}$. Since $\{\gamma_i\}$ is path-valid for ρ, we have that $a\langle 1\rangle + \gamma = a\langle 2\rangle \implies path_{\mathcal{A}}(X\langle 1\rangle)\Psi_{\rho} path_{\mathcal{A}}(X\langle 2\rangle)$. Also, we have that $\{\gamma_i\}_{i=0}^{m-1}$ is path-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 γ_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 $a\langle 1\rangle + \gamma = a\langle 2\rangle \implies path_{\mathcal{A}}(X\langle 1\rangle)\Psi_{\rho} path_{\mathcal{A}}(X\langle 2\rangle)$, 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 γ hold if and only if it is path-valid for ρ. □

Proposition 2.4. *A shift assignment $\boldsymbol{\gamma} = \{\gamma_i\}$ is valid for ρ if and only if it is path-valid for ρ and satisfies the following output determinism constraint:*

$$\gamma_i = 0 \qquad \text{if } t_i \text{ outputs } \texttt{insample} \text{ or } \texttt{insample}'$$

Proof. To obtain path validity and the output determinism constraint from validity and vice versa, one applies Proposition 2.1. □

2.2 The cost of a shift-coupling

Proposition 2.5. *Consider a transition $t_i = q_i \to q_{i+1}$ 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 $Lap(0, \varepsilon_i)$ to noise* `insample`*. The 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. This is seen from coupling construction rules. □

Definition 2.6. *Given a path ρ and input differences Δ, we define the ρ-Δ-**cost** of the shifts $\gamma = \{\gamma_i\}$ to be*

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

Definition 2.7. *Given a path ρ and a shift-coupling proof of privacy Γ define the ρ-**cost** of Γ*

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

Definition 2.8. *Given a shift-coupling proof of privacy Γ, we define the privacy cost of Γ to be*

$$cost(\Gamma) = \sup_{\rho \in paths(\mathcal{A})} \rho\text{-}cost(\Gamma)$$

2.3 Tight proofs of privacy

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

Proof. This is a direct consequence of output validity. □

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 γ_i to be the same for all $X\langle 1\rangle$ and $X\langle 2\rangle$, given a path ρ. Although this is possible, this does not in general produce a tight proof of privacy.

Proposition 2.6. ***(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 $\Gamma^* : paths(\mathcal{A}) \to ([-1,1]^\rho \to [-1,1]^{|\rho|})$ such that for all assignments $\Pi : paths(\mathcal{A}) \to [-1,1]^\rho$ of paths to shifts, we have*

$$cost(\Gamma^*) < cost(\Pi)$$

Proof. The construction is a DiPA with a path with one assignment transition, and the same number of $<$ and $\geq$ transitions. □

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 2.7. ***(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 $\Gamma^* : paths(\mathcal{A}) \to ([-1,1]^\rho \to [-1,1]^{|\rho|})$ such that for all assignments $\Pi : E \to ([-1,1]^\rho \to [-1,1]^\rho)$ of transitions and differences to shifts, we have*

$$cost(\Gamma^*) < cost(\Pi)$$

Proof. In the construction, we have a DiPA for which there are two constraints on three assignment transitions, but also the assignment transition followed by γ_1 has a cycle of $<$ transitions before reaching the γ_3 assignment transition. For finite cost, this forces $\gamma_1 = 1$.

$$\gamma_1 \leq \gamma_3$$
$$\gamma_2 \leq \gamma_3$$

Then satisfying this constraint system also requires $\gamma_3 = 1$, which forces a high cost on paths that pass through the γ_2 and γ_3 transitions. We can achieve a lower maximum cost by assigning shifts independently to paths. □

3 The search for a tight proof as an optimization problem

3.1 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 ρ and Δ,

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

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

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

One such Γ^* is the shift-coupling proof that chooses

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

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 Γ^* given an automaton $\mathcal{A}$.

3.2 Simplifying the problem with fixed ρ, Δ

Proposition 3.1. *Let ρ, Δ be given, and let*

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

For non-assignment transitions $t_i \in \rho$, we have that

$$\gamma_i^* = \min(\Delta_i, \gamma_{at(i)}) \qquad \text{if } t_i \text{ has guard } <$$
$$\gamma_i^* = \max(\Delta_i, \gamma_{at(i)}) \qquad \text{if } t_i \text{ has guard } \geq$$

Proof. Missing, but I have notes for it. The proof comes from noting that shifts non-assignment transitions have only one linear constraint, and so we can solve for them optimally in terms of the shift on the previous assignment transition. □

3.3 Simplifying the problem with fixed ρ

Proposition 3.2. *Let ρ be given. Let*

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

For non-assignment transitions $t_i \in \rho$, we have that

$$\Delta_i^* = \begin{cases} 1 & \text{if } t_i \text{ has guard } < \\ -1 & \text{if } t_i \text{ has guard } \geq \end{cases}$$

Proof. Missing, but I have notes for it. The proof goes by showing that the solution to the inner problem is at least as much as the solution to the inner problem with $\Delta_i = 1$ or $\Delta_i = -1$ respectively. □

Corollary 1.1. *Let ρ be given. Let*

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

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

As a consequence of Propositions 3.1 and 3.2, if $t_i \in \rho$ is a non-assignment transition, then

$$\gamma_i^* = \gamma_{at(i)}^*$$

.

The corollary above is important: it reveals that the only transitions that matter are assignment transitions!

3.3.1 Identifying segments

Corollary 1.1 allows us to formulate the problem of finding cost-minimal shifts γ over maximal input differences $\Delta \in [-1,1]^{|\rho|}$ given ρ to the problem of finding γ and Δ for only the assignment transitions in ρ. This motivates the definition of a *segment* – a way of identifying paths in order to consider finitely many classes of paths.

Definition 3.1. *Consider a DiPA $\mathcal{A}$. Let $q_i, q_j \in Q$ be such that there is a path $\rho = a_1 \to \cdots \to a_m$ such that:*

- *$a_1 = q_i$ and $a_m = q_j$*
- *$a_1 \to a_2$ is the only assignment transition in ρ*
- *There exists an assignment transition out of q_j or it is a terminal state*

*Then we define $seg(q_i, q_j)$ to be the set of all paths from q_i to q_j that are acyclic with their first transition being their only assignment transition. We call such a path $s \in seg(q_i, q_j)$ a **segment**.*

Definition 3.2. *Given a segment $s \in seg(q_i, q_j)$, define the **segment family** $segF(s)$ to be the set of all paths ρ from q_i to q_j such that the only assignment transition in ρ is from q_i and $acyclic(\rho) = s$.*

Proposition 3.3. *Consider a path ρ with assignment transitions from states $a_0, a_2, \ldots, a_{n-1}$, and terminal state a_n. There exists a unique sequence of segments $s_1 \hookrightarrow s_2 \hookrightarrow \cdots \hookrightarrow s_n$ such we can write $\rho = \rho_1 \circ \rho_2 \circ \cdots \circ \rho_n$ where $\rho_i \in segF(s_i)$ for all $i \in \{1, \ldots, n\}$.*

Proof. This is straightforward. □

Since we know from Corollary 1.1 that shifts on a segment are equal to the shift on the assignment transition of the segment, we need only consider pairs of $\Delta, \gamma \in \mathbb{R}$ for the assignment transition of the segment. From this, we can deduce the γ-minimal cost with respect to maximal Δ for any path in the segment family.

Definition 3.3. *Let $s \in seg(q_i, q_j)$ be a segment, and let $\Delta, \gamma \in \mathbb{R}$ be the input difference and shift for the assignment transition of s. Define the **s-segment cost** of Δ and γ to be*

$$s\text{-}segcost(\Delta, \gamma) = \sup_{\rho \in segF(s)} \rho\text{-}cost(\Gamma)$$

where Γ is a coupling strategy that chooses shift γ for all transitions in s given maximal non-assignment transition input differences with assignment input difference Δ.

The above is well-defined since the maximizing input differences for non-assignment transitions are determined independently of Δ, and the optimal shifts on those transitions with respect to the differences depend only on γ. Now, we can begin to formulate finding optimal Δ and γ for a path ρ as an optimization problem over segments.

Proposition 3.4. *If a segment $s \in seg(q_i, q_j)$ has a cycle with a transition with guard $<$, then for $\Delta, \gamma \in \mathbb{R}$, we have*

$$s\text{-}segcost(\Delta, \gamma) < \infty \iff \gamma = 1$$

Similarly, if s has a cycle with a transition with guard $\geq$, then for $\Delta, \gamma \in \mathbb{R}$, we have

$$s\text{-}segcost(\Delta, \gamma) < \infty \iff \gamma = -1$$

Proof. This follows from the fact that the $<$ transitions in a cycle have cost $|1 - \gamma|$, and $\geq$ transitions in a cycle have cost $|(-1) - \gamma|$. There are paths $\rho \in segF(s)$ which make $\rho\text{-}cost(\Gamma)$ arbitrarily large if these cyclic transitions are traversed with non-zero coupling cost. □

3.4 The optimization problem over segments

By Proposition 3.3, we can write any path ρ as a concatenation of paths each belonging to a segment family. Thus, our search for the tight shift-coupling bound

$$b = \sup_{\rho} \sup_{\Delta} \inf_{\gamma} \rho\text{-}\Delta\text{-}cost(\gamma); \qquad \gamma \text{ is valid for } \rho$$

can be formulated as

$$\max_{s^*} \max_{\Delta \in [-1,1]^n} \inf_{\gamma \in [-1,1]^n} \sum_{i=1}^{n} s_i\text{-}segcost(\Delta, \gamma)$$
$$\text{subject to } G_{s^*}(\gamma) \geq 0$$

where s^* varies over all sequences of segments $s_1 \hookrightarrow s_2 \hookrightarrow \cdots \hookrightarrow s_n$, and $G_{s^*} : \mathbb{R}^n \to \mathbb{R}^m$ encodes the set of validity constraints on γ given by the segments in s^*. In particular:

$$
\begin{aligned}
G_{s^*}(\gamma) = (\\
&\gamma_i - \gamma_{i+1}, && \text{if } s_{i+1} \text{ has guard } < && \forall i\\
&\gamma_{i+1} - \gamma_i, && \text{if } s_{i+1} \text{ has guard } \geq && \forall i\\
&\gamma_i, && \text{if } s_i \text{ has a transition that outputs insample or insample'} && \forall i\\
&\gamma_i - 1, && \text{if } s_i \text{ has a cycle with a transition with guard } < && \forall i\\
&-\gamma_i - 1 && \text{if } s_i \text{ has a cycle with a transition with guard } \geq && \forall i\\
)
\end{aligned}
$$

The first two constraints correspond to path validity, the third to output validity, and the last two to finiteness of the segment cost.

3.5 Solving the optimization problem over segments

Given a sequence of segments $s_1 \hookrightarrow s_2 \hookrightarrow \cdots \hookrightarrow s_n$, we note certain properties about the optimization problem

$$
\begin{aligned}
&\max_{\Delta \in [-1,1]^n} \inf_{\gamma \in [-1,1]^n} \sum_{i=1}^{n} s_i\text{-}segcost(\Delta, \gamma)\\
&\text{subject to } G_{s^*}(\gamma) \geq 0
\end{aligned}
$$

Proposition 3.5. *As a function of Δ, the inner problem*

$$
\Delta \mapsto \inf_{\gamma \in [-1,1]^n} \sum_{i=1}^{n} s_i\text{-}segcost(\Delta, \gamma)
$$

is strongly convex.

Proof. Segment costs are sums of absolute value functions and so are strongly convex, whose sum is convex. The pointwise infimum of convex functions is convex. □

This shows that the optimization problem as stated is a convex maximization problem, which is NP-hard in general. Several attempts were made to solving this problem efficiently:

- Brute-force search over all $\Delta \in \{-1, 1\}^n$ and solving a linear program for $\gamma \in [-1, 1]^n$, which is computationally infeasible for large n. We can search for $\Delta \in \{-1, 1\}^n$ since convex functions take maxima at the vertices of their domain.
- Linear program sensitivity analysis – finding conditions on Δ that do not change optimal shifts for those Δ. Given $\gamma^* \in \{-1, 0, 1\}^n$ with $G_{s^*}(\gamma) \geq 0$, we use sensitivity analysis to find linear constraints on Δ for which

  $$
  \gamma^* = \arg\inf_{\gamma} \sum_{i} s_i\text{-}segcost(\Delta, \gamma) \qquad G_{s^*}(\gamma) \geq 0
  $$

  This does not work in general as the number of feasible γ satisfying constraints given by G_{s^*} could be exponential in n, as shown by the following lemma:

  Lemma 2. *For the constraints on γ of the form*

  $$
  \gamma_1 \leq \gamma_2 \geq \gamma_3 \leq \cdots \geq \gamma_n
  $$

  there are $f(n-1)$ feasible γ satisfying the constraints, where $f(n)$ is the nth Fibonacci number.

No efficient solutions were found, and I suspect that the problem of finding maximal input differences with respect to minimal coupling shifts is NP-hard.

We will now present some bounds with respect to solutions to this optimization problem and solutions to a relaxed version of the problem.

4 A Relaxation and Linear-Time Decidability

4.1 Relaxing the optimization problem

Despite Proposition 2.6, we will now consider shift-coupling proofs of privacy that do not regard input differences, and investigate the tightness of such proofs.

Recall that a shift-coupling proof of privacy is a map

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

that assigns a shift to each path and sequence of input differences. We will consider shifts for which $\Gamma(\rho, \Delta)$ is constant for all Δ. We will call such a shift-coupling proof a **relaxed shift-coupling proof of privacy**.[1]

The privacy bound afforded by such a proof is given by

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

We will now see what the search for a relaxed shift-coupling proof of privacy looks like.

Proposition 4.1. *Let ρ be given. Let*

$$\begin{gathered}\gamma^* = \arg \inf_{\gamma \in [-1,1]^{|\rho|}} \sup_{\Delta \in [-1,1]^{|\rho|}} \rho\text{-}\Delta\text{-}\mathit{cost}(\gamma) \\ \textit{subject to } G_\rho(\gamma) \geq 0\end{gathered}$$

and define $\Gamma^*(\rho, \Delta) = \gamma^*$ for all Δ. Then, for all relaxed shift-coupling proofs of privacy Γ, we have $\mathit{cost}(\Gamma^*) \leq \mathit{cost}(\Gamma)$.

Proof. For fixed path ρ, we see that Γ^* has at most the cost of Γ on that path. This remains true when we take the supremum over all paths ρ. □

Proposition 4.2. *(Relaxed shift-coupling proofs over segments) The search for a relaxed shift-coupling proof of privacy can be formulated as*

$$\begin{gathered}\max_{s^*} \inf_{\gamma \in [-1,1]^n} \sup_{\Delta \in [-1,1]^n} \sum_{i=1}^{n} s_i\text{-}\mathit{segcost}(\Delta, \gamma) \\ \textit{subject to } G_{s^*}(\gamma) \geq 0\end{gathered}$$

where s^* varies over all sequences of segments $s_1 \hookrightarrow s_2 \hookrightarrow \cdots \hookrightarrow s_n$, and $G_{s^*} : \mathbb{R}^n \to \mathbb{R}^m$ encodes the set of constraints on γ given by the segments in s^*.

[1] I'm open to suggestions for a better name.

Proof. Writing the problem over segments requires exactly the same steps as the formulation of the non-relaxed optimization problem over segments. The only difference is that we have switched γ and Δ. □

Lemma 3. *For $\gamma \in [-1, 1]$, we have that*

$$\sup_{\Delta \in [-1,1]} |\gamma - \Delta| = 1 + |\gamma|$$

Proof. Choosing $\Delta = -1 \cdot \text{sgn}(\gamma)$ shows that the supremum is at least $1 + |\gamma|$. To see that the supremum does not exceed $1 + |\gamma|$, use the triangle inequality. □

Proposition 4.3. *For sequence of segments $s_1 \hookrightarrow s_2 \hookrightarrow \cdots \hookrightarrow s_n$ and $\gamma \in [-1, 1]^n$, we have that*

$$\arg \sup_{\Delta \in [-1,1]^n} \sum_{i=1}^{n} s_i\text{-}segcost(\Delta, \gamma) = -1 \cdot \text{sgn}(\gamma)$$

where $\text{sgn}(\gamma)$ *is the vector with ith entry* $\text{sgn}(\gamma_i)$*, for which*

$$\sum_{i=1}^{n} s_i\text{-}segcost(-1 \cdot \text{sgn}(\gamma), \gamma) = \sum_{i=1}^{n} \left((1 + |\gamma_i|)\varepsilon_i^0 + \sum_{t_j \in s_i, guard(t_j) = <} (1 - \gamma_i)\varepsilon_i^j + \sum_{t_j \in s_i, guard(t_j) = <} (1 + \gamma_i)\varepsilon_i^j \right)$$

where ε_i^j is the scale factor of the Laplace noise added to `insample` *at transition t_j in segment s_i.*

Proof. The main idea in the proof is that Δ is unconstrained, and each component Δ_i can be dealt with separately using Lemma 3. □

We then see that we can find the minimum cost relaxed coupling shifts for a sequence of segments $s_1 \hookrightarrow s_2 \hookrightarrow \cdots \hookrightarrow s_n$ by solving the following linear program with absolute values:

$$\begin{aligned} &\min_{\gamma \in [-1,1]^n} \sum_{i=1}^{n} s_i\text{-}segcost(-1 \cdot sgn(\gamma), \gamma) \\ &\text{subject to } G_{s^*}(\gamma) \geq 0 \end{aligned}$$

since the objective function is linear in γ and $|\gamma|$. Further, the number of constraints is linear in n. Such programs can be solved using the simplex or ellipsoid methods. [2]

4.2 Closeness of relaxed shift-coupling proofs to tight shift-coupling proofs

We will now show that the cost of a relaxed shift-coupling proof of privacy is can be bounded in terms of the cost of a tight shift-coupling proof of privacy on a sequence of segments, and vice versa.

Theorem 4. *Let $\mathcal{A}$ be a DiPA, and let Γ^* be an optimal shift-coupling proof of privacy. Let β^* be a relaxed shift-coupling proof of privacy with minimal cost. Consider a sequence of segments $s^* = s_1 \hookrightarrow s_2 \hookrightarrow \cdots \hookrightarrow s_n$. Then, for any path ρ with $acyclic(\rho) = s^*$, we have*

$$\rho\text{-}cost(\Gamma^*) \leq \rho\text{-}cost(\beta^*) \leq \rho\text{-}cost(\Gamma^*) + \sum_{i=1}^{n} \varepsilon_{i,0}$$

[2] I am yet verifying that it meets the conditions for strongly polynomial solvability.

Proof. We immediately have $\rho\text{-}cost(\Gamma^*) \leq \rho\text{-}cost(\beta^*)$ since Γ^* is the optimal shift-coupling proof of privacy. We will now show that $\rho\text{-}(cost\beta^*) \leq \rho\text{-}cost(\Gamma^*) + \sum_{i=1}^{n} \varepsilon_{i,0}$.

We can write

$$\begin{aligned}
\rho\text{-}cost(\Gamma^*) &= \sup_{\Delta} \inf_{\gamma} \sum_{i=1}^{n} s_i\text{-}segcost(\Delta, \gamma) \qquad \text{with } G_{s^*}(\gamma) \geq 0 \\
&= \sup_{\Delta} \inf_{\gamma} \sum_{i=1}^{n} \left(|\gamma_i - \Delta_i| \varepsilon_{i,0} + m_i \gamma_i + c_i \right) \qquad \text{with } G_{s^*}(\gamma) \geq 0
\end{aligned}$$

for some $m_i, c_i \in \mathbb{R}$. Similarly,

$$\begin{aligned}
\rho\text{-}cost(\beta^*) &= \inf_{\gamma} \sup_{\Delta} \sum_{i=1}^{n} s_i\text{-}segcost(\Delta, \gamma) \qquad \text{with } G_{s^*}(\gamma) \geq 0 \\
&= \inf_{\gamma} \sum_{i=1}^{n} \left((1 + |\gamma_i|) \varepsilon_{i,0} + m_i \gamma_i + c_i \right) \qquad \text{with } G_{s^*}(\gamma) \geq 0
\end{aligned}$$

for the same $m_i, c_i \in \mathbb{R}$. Now, applying the reverse triangle inequality, we get that

$$\begin{aligned}
\sum_{i=1}^{n} \left(|\gamma_i - \Delta_i| \varepsilon_{i,0} + m_i \gamma_i + c_i \right) &\geq \sum_{i=1}^{n} \left((|\gamma_i| - |\Delta_i|) \varepsilon_{i,0} + m_i \gamma_i + c_i \right) \\
&= \sum_{i=1}^{n} \left((|\gamma_i|) \varepsilon_{i,0} + m_i \gamma_i + c_i \right) - \sum_{i=1}^{n} |\Delta_i| \varepsilon_{i,0} \\
&= \sum_{i=1}^{n} \left((1 + |\gamma_i|) \varepsilon_{i,0} + m_i \gamma_i + c_i \right) - \sum_{i=1}^{n} (1 + |\Delta_i|) \varepsilon_{i,0}
\end{aligned}$$

$$\inf_{\gamma} \sum_{i=1}^{n} \left(|\gamma_i - \Delta_i| \varepsilon_{i,0} + m_i \gamma_i + c_i \right) \geq \inf_{\gamma} \sum_{i=1}^{n} \left((1 + |\gamma_i|) \varepsilon_{i,0} + m_i \gamma_i + c_i \right) - \sum_{i=1}^{n} (1 + |\Delta_i|) \varepsilon_{i,0} \qquad \text{with } G_{s^*}(\gamma) \geq 0$$

$$\sup_{\Delta} \inf_{\gamma} \sum_{i=1}^{n} \left(|\gamma_i - \Delta_i| \varepsilon_{i,0} + m_i \gamma_i + c_i \right) \geq \sup_{\Delta} \left[\inf_{\gamma} \sum_{i=1}^{n} \left((1 + |\gamma_i|) \varepsilon_{i,0} + m_i \gamma_i + c_i \right) - \sum_{i=1}^{n} (1 + |\Delta_i|) \varepsilon_{i,0} \right] \qquad \text{with } G_{s^*}(\gamma) \geq 0$$

$$= \inf_{\gamma} \sum_{i=1}^{n} \left((1 + |\gamma_i|) \varepsilon_{i,0} + m_i \gamma_i + c_i \right) - \sum_{i=1}^{n} \varepsilon_{i,0} \qquad \text{with } G_{s^*}(\gamma) \geq 0$$

$$= \rho\text{-}cost(\beta^*) - \sum_{i=1}^{n} \varepsilon_{i,0}$$

finally showing that

$$\rho\text{-}cost(\beta^*) \leq \rho\text{-}cost(\Gamma^*) + \sum_{i=1}^{n} \varepsilon_{i,0}$$

□

This is a result that shows that the cost of a relaxed shift-coupling proof of privacy is close to the cost of a tight shift-coupling proof of privacy on a sequence of segments. This result is important because it allows us to bound the optimal shift-coupling cost in terms of the optimal relaxed shift-coupling cost, which is relatively easy to compute given a sequence of segments.

It also allows us to decide privacy by solving a simpler optimization problem. However, the next section shows that we can decide privacy in linear time without solving any optimization problems.

4.3 Deciding privacy in linear time

Theorem 5. *A DiPA $\mathcal{A}$ is differentially private if and only if there exists a shift-coupling proof of privacy Γ with finite cost.*

Proof. This is one of Sky's theorems. □

Definition 4.1. *Define the **segment shift graph** of a DiPA $\mathcal{A}$ to be the directed graph $G = (V, E)$ where:*

- *For every segment $s_i \in seg(\mathcal{A})$, there is a vertex $v_i \in V$ representing the coupling shift on the assignment transition of s_i.*
- *For every pair of segments (s_i, s_j) which have the connecting constraint $\gamma_i \leq \gamma_j$, there is an edge $(v_i, v_j) \in E$.*
- *There are nodes $\mathbf{1}, -\mathbf{1} \in V$ such that:*
  - *The only edge incident to $-\mathbf{1}$ is $(-\mathbf{1}, u)$ where u is the segment that initializes $\mathcal{A}$.*
  - *All terminal segments s_i have an edge $(v_i, \mathbf{1})$.*

Lemma 6. *Let there exist a path $v_1 \to \cdots \to v_k$ in the segment shift graph of $\mathcal{A}$, and let the corresponding segments be $s_{i_1}, \ldots, s_{i_k}$. Then we either have that*

$$s_{i_1} \hookrightarrow s_{i_2} \hookrightarrow \cdots \hookrightarrow s_{i_k} \qquad \text{and} \qquad guard(s_{i_k}) = <$$

or

$$s_{i_k} \hookrightarrow s_{i_{k-1}} \hookrightarrow \cdots \hookrightarrow s_{i_1} \qquad \text{and} \qquad guard(s_{i_k}) = \geq$$

Proof. We will use induction on k with base case $k = 2$. If we have $v_1 \to v_2$ in the segment shift graph, then we either have that $s_{i_1} \hookrightarrow s_{i_2}$ with $guard(s_{i_2}) = <$, or that $s_{i_2} \hookrightarrow s_{i_1}$ with $guard(s_{i_2}) = \geq$. For a path with length $k+1$ in the segment shift graph, let us assume the desired result. Then apply the base case on $s_{i_k} \to s_{i_{k+1}}$ to conclude. □

Theorem 7. *A DiPA $\mathcal{A}$ is differentially private if and only if there does not exist a path from $\mathbf{1}$ to $-\mathbf{1}$ in the segment shift graph of $\mathcal{A}$.*

Proof. ($\implies$) Suppose that $\mathcal{A}$ is differentially private. Then there exists a shift-coupling proof of privacy Γ with finite cost. Assume that there exists a path $\mathbf{1} \to v_1 \to \cdots \to v_k \to -\mathbf{1}$ in the segment shift graph of $\mathcal{A}$. Without loss of generality, we have the sequence of segments $s_{i_1} \hookrightarrow \cdots \hookrightarrow s_{i_k}$ corresponding to the path by Lemma 6. We can then extend this to a sequence of segments $s_1 \to \cdots \to s_{i_1} \to \cdots \to s_{i_k} \to \cdots \to s_n$ that begins with the initialization segment and ends with a terminal segment.

If we restrict the segment-shift graph to only these segments, we find that any assignment of shifts γ would not be valid, as we would be able to construct a sequence of inequalities to conclude that $1 \leq -1$, which is false. Thus, there is no valid assignment of shifts γ for this sequence of segments with finite cost, and so Γ is not a shift-coupling proof of privacy with finite cost. This is a contradiction.

($\impliedby$) This direction follows from the fact that there is *some* valid assignment of shifts γ with finite cost on each segment, and so we can construct a shift-coupling proof of privacy Γ with finite cost. □

We can construct the segment shift graph of a DiPA in linear time, and check for a path from $\mathbf{1}$ to $-\mathbf{1}$ in linear time using a breadth-first search. Thus, we can decide privacy in linear time.

4.4 A comparison of the naive and relaxed shift-coupling proofs

Definition 4.2. *Define a **naive** shift-coupling proof of privacy to be a collection of shifts $\{\gamma_i\}$ on segments s_i that adheres to the segment shift graph inequalities of $\mathcal{A}$.*

Theorem 7 shows that a naive shift-coupling proof of privacy exists if and only if $\mathcal{A}$ is differentially private. The cost of a naive shift-coupling proof of privacy is the cost of its most expensive sequence of segments, and Proposition 2.7 shows that it is not tight in general.

Here, we will show that there exists a family of automata $\mathfrak{F}$ for which the cost of a naive shift-coupling proof of privacy grows arbitrarily large while the cost of a relaxed shift-coupling proof of privacy remains bounded.

Theorem 8. *There exists a family of automata $\mathfrak{F} = \{\mathcal{A}_n\}$, $n \in \mathbb{N}$ such that the cost of the tight relaxed shift-coupling proof of privacy is in $O(n)$, but the cost of any naive shift-coupling proof of privacy is in $\Omega(n^2)$.*

Proof. Define $\mathcal{A}_n$ as shown below in Figure 4.4. It consists of segments q_i and p_i for $i \in \{1, \ldots, n\}$. The identical segments p_i have L-cycles, and are such that $p_i \hookrightarrow q_i$. The segments q_i are in sequence but separated by *true* transition segments so that their shifts do not constrain each other. We also have $guard(q_i) = <$.

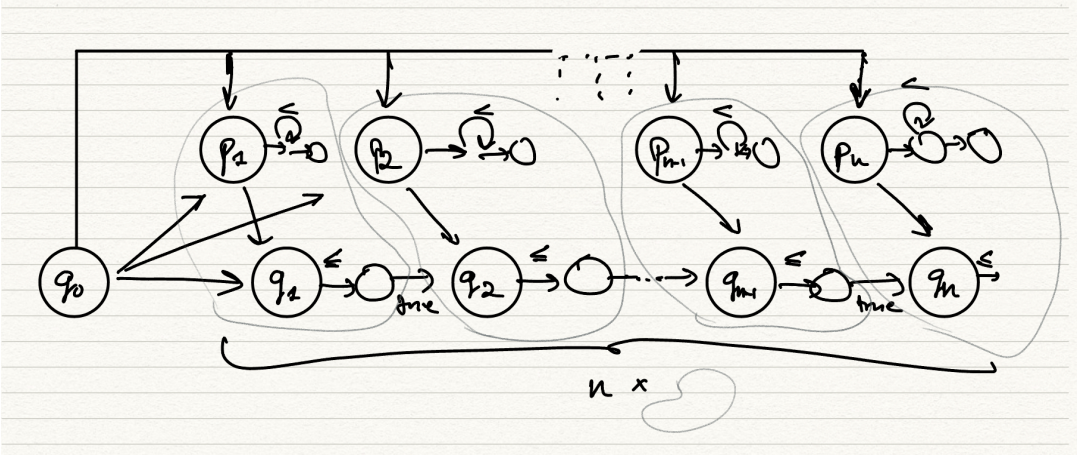

Figure 1: An illustration of $\mathcal{A}_n$

Let the states p_i have only one $\geq$ transition, and let the states q_i have m transitions with guard $\geq$ and no $<$ transitions.

All other transitions not shown in this diagram are to a designated terminal state, which is also not shown as they are not relevant to the proof. Let us denote the shift assigned to a segment s by γ_s.

Any naive shift-coupling proof of privacy assigns a shift of $\gamma_{p_i} = 1$ since p_i has an L-cycle. Since $p_i \hookrightarrow q_i$, we have that $\gamma_{p_i} \leq \gamma_{q_i}$, which forces $\gamma_{q_i} = 1$. Let q_0 be the initial segment with some coupling cost c_0. Let c_1 bound the cost of the segment p_i if we choose $\gamma_{p_i} = 1$.

The cost of constructing the naive shift-coupling proof of privacy is then the maximum cost over all segments, which is $q_0 \to p_1 \to q_1 \to \cdots \to q_n$. This has cost at least $c_0 + c_1 + n \cdot (2 + 2m)$, or

$$\text{naive cost } \geq c_0 + c_1 + 2n + 2mn$$

However, the cost of the relaxed shift-coupling proof of privacy is at most $c_0 + c_1 + 2 + 2m + 2n$, since only one of the q_i segments would have a shift of 1 for any given sequence of segments. This is because paths traverse through at most one p_i, and the shifts on q_i do not constrain each other.

$$\text{relaxed cost } \leq c_0 + c_1 + 2 + 2m + 2n$$

If we let $m = n$, then we get that the naive cost is in $\Omega(n^2)$ while the relaxed cost is in $O(n)$.

□

5 Is the tight shift-coupling proof also a tight coupling proof?

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.

5.1 Conjecture: S^L is tight when there is an L-cycle

Conjecture 5.1. *(S^L is tight for segments with L-cycles) onsider a segment $s \in seg(\mathcal{A})$ corresponding to the sequence of states $q_0 \to q_1 \to \cdots \to q_m$. 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,*

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

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

Proof. Note: the proof of this conjecture can be reduced to showing Lemma 15. 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 $X \sim Lap(0, 1/\varepsilon)$ as defined in the appendix.

Since s has an L-cycle, there exists a sequence of paths ρ_i for $i \in \mathbb{N}$ each with l_i number of L-transitions such that $\lim_{i\to\infty} l_i = \infty$. Let m be the number of G-transitions in ρ_i. We will assume that this number is the same across all ρ_i.[3]

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

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

Let $\tilde{a_j}$ be the random variable representing the value of `insample` before the jth transition in ρ on input X_i. Let $\tilde{b_j}$ be the random variable representing the value of `insample` before the jth transition in ρ on input X_i'. Further, let $\Gamma_L = \{j : \rho_i[j] \to \rho_i[j+1] \text{ has guard } \texttt{insample}<\texttt{x}\}$, and $\Gamma_G = \{j : \rho_i[j] \to \rho_i[j+1] \text{ has guard } \texttt{insample}\geq\texttt{x}\}$.

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 $Lap(X_i[j], 1/\varepsilon)$, 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.

[3] Otherwise, s has a G-cycle, and $\mathcal{A}$ is not differentially private. The privacy loss through s is ∞, which matches the L-cost.

$$
\begin{aligned}
\Pr(\rho_i|X_i') &= \int_{-\infty}^{\infty} \Pr(\tilde{b_0} = x) \prod_{j\in\Gamma_L} \Pr(\tilde{b_j} < x) \prod_{j\in\Gamma_G} \Pr(\tilde{b_j} \geq x)\,\mathrm{d}x \\
&= \int_{-\infty}^{\infty} \Pr(\tilde{b_0} = x) \prod_{j\in\Gamma_L} \Pr(\tilde{b_j} < x) \prod_{j\in\Gamma_G} \Pr(\tilde{b_j} \geq x)\,\mathrm{d}x \\
&= \int_{-\infty}^{\infty} f_\varepsilon(x - X_i[0]) \prod_{j\in\Gamma_L} F_\varepsilon(x - X_i[j]) \prod_{j\in\Gamma_G} (1 - F_\varepsilon(x - X_i[j]))\,\mathrm{d}x \\
&= \int_{-\infty}^{\infty} f(x-1)F(x+1)^{\ell_i}(1-F(x-1))^m \\
&= \int_{-\infty}^{\infty} f(x)F(x+2)^{\ell_i}(1-F(x))^m \\
&= \exp(2\varepsilon(m+1)) \left(\int_{(-\infty,-2)\cup(2,\infty)} f(x)F(x)^{\ell_i}(1-F(x))^m\,\mathrm{d}x + g(\ell_i) \int_{-2}^{2} f(x)F(x+2)^{\ell_i}(1-F(x))^m \right)
\end{aligned}
$$

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

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

and so as we take the supremum over ρ_i below, we get:

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

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

5.2 Investigating costs of alternative coupling strategies

Definition 5.1. *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.*

Theorem 9. *Let $s = q_0 \to \cdots \to q_m$ 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* $\mathrm{loss}(s)$ *given by*

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

Proof. Follows from some algebra.

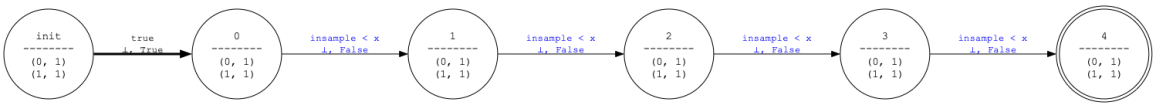

Figure 2: A segment s with only L-transitions.

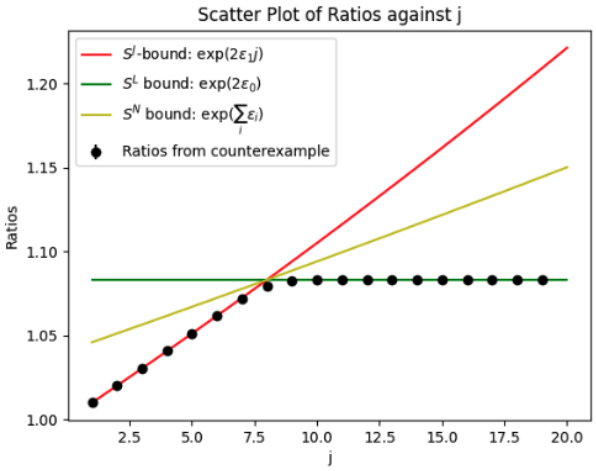

Figure 3:

□

Conjecture 5.2. *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. □

Lemmata

Properties of f_ε and F_ε

Lemma 10. *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 11. *For $x \geq 0$, we have*

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

Lemma 12. *For $x \geq 0$, we have*

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

For the proof of Theorem 1

Lemma 13.

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

Proof. From Lemma 10, we have that

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

□

Lemma 14.

$$\int_0^\infty f_\varepsilon(x)F_\varepsilon(x+2)^\ell(1-F_\varepsilon(x))^m\,\mathrm{d}x = \exp(2\varepsilon m)\int_2^\infty f_\varepsilon(x)F_\varepsilon(x)^\ell(1-F_\varepsilon(x))^m\,\mathrm{d}x$$

Proof. From Lemma 11 and 12, we have that

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

□

Lemma 15. *There exists a function $g:\mathbb{N}\to\mathbb{R}$ such that*

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

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

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 mth power. Its integral should behave like a polynomial of degree $m+1$ evaluated at 2, which corresponds to $\exp(2\varepsilon(m+1))$. □