Contents

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 Δ!
   (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 Δ, the γ values on inter-segment transitions are easily determined.
      - The Δ 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 Δ.
   (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

Definition 4.1. *Let $X = \langle a_1, \ldots, a_m \rangle$ 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.*

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

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

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

- The above is true if and only if $path_A(X) \Psi_\rho^{(\varepsilon,0)} path_A(X')$, 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 $path_A(X) \Psi_\rho^{(\varepsilon,0)} path_A(X')$ by constructing the couplings

  $$\tilde{a_i}\langle 1 \rangle + \gamma_i (=)^{\#(\varepsilon_i, 0)} \tilde{a_i}\langle 2 \rangle \qquad \forall i \in \{0, \ldots, m-1\}$$

  and showing that

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

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

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

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

4.1 Constraints

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

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

Definition 4.3. *Let $\rho = q_0 \to q_1 \to \cdots \to q_m$ be a path, and let $i \in \{1, \ldots, m\}$. 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.*

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

Definition 4.5. *Let $X = \langle a_1, \ldots, a_m \rangle$ be an input, and let $\rho = q_0 \to q_1 \to \cdots \to q_m$ 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 $\rho = q_0 \to q_1 \to \cdots \to q_m$, an assignment of shifts $\{\gamma_i\}$ is valid if and only if it satisfies the following constraints for all $i \in \{0, \ldots, m-1\}$:*

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

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 $i \in \{0, \ldots, m-1\}$.

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 $path_A(X\langle 1\rangle)\Psi_\rho^{(0,0)} path_A(X\langle 2\rangle)$.

Assume that the constraints hold for all paths of length m. Let $\rho = q_0 \to q_1 \to \cdots \to q_m \to q_{m+1}$. We will show that $\{\gamma_i\}$ is valid for ρ. 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 ρ. 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 $i \in \{0, \ldots, m-1\}$. 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 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 valid for ρ, 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 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 $a\langle 1\rangle + \gamma = a\langle 2\rangle \implies path_A(X\langle 1\rangle)\Psi_\rho path_A(X\langle 2\rangle)$, 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 γ hold if and only if it is valid for ρ. □

We can now reduce checking path-validity to checking the above constraints.

Definition 4.6. *We say that γ is output-valid for ρ and Δ if we have*

$$(\tilde{a}\langle 1\rangle + \gamma = \tilde{a}\langle 2\rangle) \implies output_A(X\langle 1\rangle)\Psi_o output_A(X\langle 2\rangle)$$

where

$$\Psi_o = \{(o_1, o_2) \in \mathcal{O}_\rho : o_1 = o \implies o_2 = o\}$$

where $\mathcal{O}_\rho$ is the set of all outputs that can be produced by the path ρ.

Definition 4.7. *Define $\mathcal{P}$ to be the set of all paths in $\mathcal{A}$.*

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

Definition 4.8. *Given a DiPA $\mathcal{A}$, a **shift-coupling proof of privacy** for $\mathcal{A}$ is a map*

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

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

4.2 The cost of a shift-coupling

Proposition 4.2. *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 ε-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 4.9. *Given a path ρ and input differences Δ, we define the ρ-Δ-**cost** of the shifts $\{\gamma_i\}$ to be*

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

Definition 4.10. *Given a shift-coupling proof of privacy Γ, we define the privacy cost of Γ to be*

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

4.3 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. □

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

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

Proof. The construction is a DiPA with a one-segment path with 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 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 $\Gamma^* : \mathcal{P} \to ([-1,1]^\rho \to [-1,1]^{|\rho|})$ 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. I have the counterexample written down, I found it by computer. Will write it up soon. □

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 ρ and Δ,

$$\inf_\Gamma cost(\Gamma) = \inf_\Gamma \sup_\rho \sup_\Delta cost_\rho(\Delta, \Gamma(\rho, \Delta))$$

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

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

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

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

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

5.2 Simplifying the problem with fixed ρ, Δ

Proposition 5.1. *Let ρ, Δ be given, and let*

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

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

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

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. □

5.3 Simplifying the problem with fixed ρ

Proposition 5.2. *Let ρ be given. Let*

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

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*

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

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

As a consequence of Propositions 5.1 and 5.2, 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!

5.3.1 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 5.1. *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 5.2. *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 5.3. *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 5.3. *Given a path $\rho \in segF(s)$, we define the **ρ-segment cost of** s given γ, Δ to be*

$$\rho\text{-}segcost_s(\Delta, \gamma) = \sum_{t_j \in \rho, t_j \in s} cost_\rho(\Delta, \gamma_j)$$

Definition 5.4. *Let $s \in seg(q_i, q_j)$ be a segment, and let Δ and γ be input differences and shifts for all reachable transitions from s. Define the **segment cost of** s to be*

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

Now, we can begin to formulate finding optimal Δ and γ for a path ρ as an optimization problem over segments.

Proposition 5.4. *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*

$$segcost_s(\Delta, \gamma) < \infty \iff \gamma = 1$$

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

$$segcost_s(\Delta, \gamma) < \infty \iff \gamma = -1$$

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 in $segF(s)$ which make $\rho\text{-}segcost_s(\Delta, \gamma)$ arbitrarily large if these cyclic transitions are traversed with non-zero coupling cost. □

5.4 The optimization problem over segments

By Proposition 5.3, 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

$$b = \sup_{\rho} \sup_{\Delta} \inf_{\gamma} cost(\Gamma^*(\rho, \Delta))$$

can be formulated as

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

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 constraints on γ given by the segments in s^*. In particular:

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

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

5.5 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

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

Proposition 5.5. *As a function of Δ, the inner problem*

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

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

$$\gamma^* = \arg\inf_{\gamma} \sum_i segcost_{s_i}(\Delta, \gamma) \qquad G_{s^*}(\gamma) \geq 0$$

  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 equi-finiteness results for solutions to this optimization problem and solutions to a relaxed version of the problem.

6 Relaxations, Finite DP bounds, and Linear-Time Decidability

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 3. *(S^L is tight for segments with L-cycles) Consider 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. 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.[1]

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:

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

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

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.

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

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:

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

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

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 4. *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* $\text{loss}(s)$ *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]

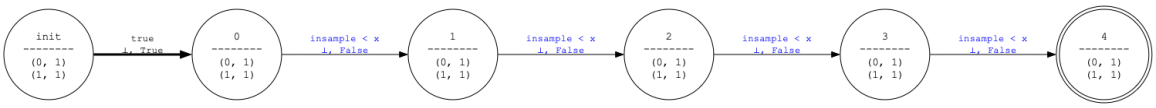

Figure 1: A segment s with only L-transitions.

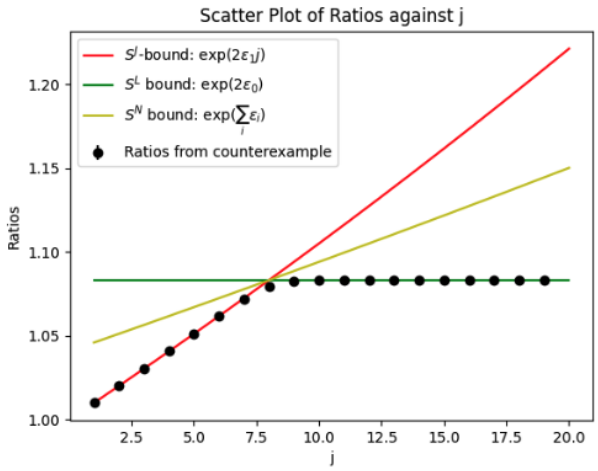

Figure 2:

□

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_ε and F_ε

Lemma 5. *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 6. *For $x \geq 0$, we have*

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

Lemma 7. *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 8.

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

Proof. From Lemma 5, 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 9.

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

Proof. From Lemma 6 and 7, 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 10. *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 $\exp(2\varepsilon(m+1))$. □