Quantitative Information Flow (QIF) **DCC/ICEx/UFMG**
Prof. Mário S. Alvim **2021/1**

PROBLEM SET

Refinement / The Dalenius perspective
(Chapters 09 / 10)

Necessary reading for this assignment:

- *The Science of Quantitative Information Flow* (Alvim, Chatzikokolakis, McIver, Morgan, Palamidessi, and Smith):
  - Chapter 9: *Refinement*
    - Chapter 9.1: *Refinement: for the customer; for the developer*
    - Chapter 9.2: *Structural refinement: the developer's point of view*
    - Chapter 9.3: *Testing refinement: the customer's point of view*
    - Chapter 9.4: *Soundness of structural refinement*
    - Chapter 9.5: *Completeness of structural refinement: the Coriaceous theorem*
    - Chapter 9.6: *The structure of abstract channels under refinement*
    - Chapter 9.7: *Refinement and monotonicity*
    - Chapter 9.9: *Capacity is unsuitable as a criterion for refinement*
  - Chapter 10: *The Dalenius perspective*
    - Chapter 10.1: *Dalenius scenarios*
    - Chapter 10.2: *Compositional closure for Dalenius contexts*
    - Chapter 10.3: *Bounding Dalenius leakage*

Review questions.

1. Give the definition of *testing refinement*, and explain why it's relevant.
2. Give the definition of *structural refinement*, and explain why it's relevant.
3. Explain with your own words the concept of *Dalenius g-vulnerability*, and why it's relevant.

Exercises.

4. Recall that in our proof that structural refinement is transitive, we used the fact that the product of two stochastic matrices (or, equivalently, two channels, in which there are only non-negative entries and in which all rows add up to 1) is also a stochastic matrix — as long as, of course, the inner dimensions of the matrices are compatible. Prove here that this fact is indeed true.
5. (Exercise 9.2) Give an example to show that cascading (of channel matrices) is not refinement-monotonic in its left-hand argument. (That is, show that there are two conforming channel matrices A, B for which there exists a channel matrix C of appropriate type s.t. $\mathsf{A} \sqsubseteq \mathsf{B}$ but $\mathsf{AC} \not\sqsubseteq \mathsf{BC}$. *Hint: Create a post-processing matrix* C *that just permutes the columns of the left-hand argument: the resulting matrix is equal to the original as far as its leakage properties are concerned, but its columns connect potentially to completely different rows of the right-hand argument.*)

   Is it monotonic in its right-hand argument? (That is, is it true that for all channel matrices A, B and a channel matrix C of appropriate type, we have that $\mathsf{A} \sqsubseteq \mathsf{B}$ implies $\mathsf{CA} \sqsubseteq \mathsf{CB}$?)

6. Suppose that we have a 2-bit secret X and a channel C, expressed concretely as C of type $\mathcal{X} \to \{0,1\}$, that leaks the binary sum of the bits in X with probability $4/5$, and its complement with probability $1/5$:

C	0	1
00	$4/5$	$1/5$
01	$1/5$	$4/5$
10	$1/5$	$4/5$
11	$4/5$	$1/5$

.

a) Suppose further that there is a 1-bit secret Z that is correlated with X according to the joint-distribution matrix J^{ZX}:

J^{ZX}	00	01	10	11
0	$1/10$	$3/20$	$1/4$	0
1	$1/5$	$1/20$	$1/20$	$1/5$

.

Compute the multiplicative Dalenius Bayes leakage that channel C causes about Z.

b) Suppose now that there is a different secret Z' correlated with X in an unknown way. Estimate the maximum multiplicative leakage C can cause about this secret Z', under any non-negative gain function g.