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

SOLUTION OF 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.

   Instructor's solution: Given abstract channels A and B, over the same input $\mathcal{X}$, we say that A is *testing-refined* by B, written $A \sqsubseteq_{\mathbb{G}} B$, if for any prior π and gain function $g{:}\,\mathbb{G}\mathcal{X}$ we have $V_g[\pi \triangleright A] \geq V_g[\pi \triangleright B]$.

   Testing refinement reflects the system customer's point of view: he's interested in that an implementation B of an specification A never leaks more than that specification. Therefore, the customer wants to be assured that B testing-refines A in all contexts defined by possible priors and gain functions yielding non-negative vulnerabilities.

2. Give the definition of *structural refinement*, and explain why it's relevant.

   Instructor's solution: For (probabilistic) channel matrices A and B, we say that A is *structurally refined* by B, again written $\mathsf{A} \sqsubseteq_\circ \mathsf{B}$, just when there exists a –possibly probabilistic– matrix R such that $\mathsf{AR} = \mathsf{B}$.

   Structural refinement reflects the system developers's point of view: she's interested in making sure that her production technique does not introduce undesirable leaks in the process of refinement specifications into implementations. Therefore, the developer can just make sure that an implementation

B structurally-refines an implementation A, meaning that the former can only group together (but never split) outputs of the latter.

3. Explain with your own words the concept of *Dalenius g-vulnerability*, and why it's relevant.

   Instructor's solution: Suppose we are given a channel C on X and a joint distribution $J\colon \mathbb{D}(\mathcal{Z}\times\mathcal{X})$ that represents an adversary's knowledge of a correlation between $\mathcal{Z}$ and $\mathcal{X}$. Let J be a matrix realization of J, and factor it into marginal distribution $\rho\colon \mathbb{D}\mathcal{Z}$ and stochastic matrix $\mathsf{B}\colon \mathcal{Z}\to\!\!\triangleright\mathcal{X}$, i.e. so that $\mathsf{J} = \rho \triangleright \mathsf{B}$. Let C be a concrete realization of C. Then, for any gain function $g\colon \mathbb{G}\mathcal{Z}$, the *Dalenius g-vulnerability* of J and C is defined

$$V_g^D(J,C) \;:=\; V_g[\,\rho \triangleright \mathsf{BC}\,] \quad .$$

   Dalenius g-vulnerability reflects how much information the output of a system C from X to Y reveals about another secret Z correlated with X. This is important because it allows us to model collateral leakage caused by a channel, including secrets the developer was not even aware existed.

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.

   Instructor's solution: Let $\mathsf{A} : \mathcal{X}\to\!\!\triangleright\mathcal{Y}$ and $\mathsf{B} : \mathcal{Y}\to\!\!\triangleright\mathcal{Z}$ be two channel matrices. We want to show that:

   (i) for all $x \in \mathcal{X}, z \in \mathcal{Z}$, we have $(\mathsf{AB})_{x,z} \geq 0$, and
   (ii) for all $x \in \mathcal{X}$, we have $\sum_{z\in\mathcal{Z}}(\mathsf{AB})_{x,z} = 1$.

   Let's prove each one separately.

   (i) Note that for all $x \in \mathcal{X}, z \in \mathcal{Z}$, we have that, by definition of matrix multiplication, $(\mathsf{AB})_{x,z} = \sum_{y\in\mathcal{Y}} \mathsf{A}_{x,y}\mathsf{B}_{y,z}$. Since every term in the sum is non-negative (because it's itself the product of two non-negative factors, coming from two channel matrices A and B), the overall sum is, hence, non-negative.
   (ii) Now, notice that

$$\begin{aligned}
\sum_{z\in\mathcal{Z}}(\mathsf{AB})_{x,z} &= \sum_{z\in\mathcal{Z}}\sum_{y\in\mathcal{Y}}\mathsf{A}_{x,y}\mathsf{B}_{y,z} && \text{(by def. of matrix mult.)}\\
&= \sum_{z\in\mathcal{Z}}\mathsf{B}_{y,z}\sum_{y\in\mathcal{Y}}\mathsf{A}_{x,y} && \text{(reorganizing the summations)}\\
&= \sum_{y\in\mathcal{Y}}\mathsf{B}_{y,z}\cdot 1 && \textstyle(\sum_{y\in\mathcal{Y}}\mathsf{A}_{x,y} = 1)\\
&= 1 && \textstyle(\sum_{y\in\mathcal{Y}}\mathsf{B}_{x,z} = 1)
\end{aligned}$$

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 $\mathsf{CA} \sqsubseteq \mathsf{CB}$?)

Instructor's solution:

First part: Cascading is not monotonic in its left-hand argument. In fact cascading is in general not even well defined if its left-hand argument is refined, since the refinement can change the number of columns on the left, making the matrices no longer conformal. If we avoid that, a simple answer is just to permute 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.

For instance, consider channels A, B and R below, where all that the post-processing matrix R does is to swap columns y_1 and y_2 in the original channel.

A	y_1	y_2	y_3
x_1	$1/2$	0	$1/2$
x_2	0	$1/2$	$1/2$

$\cdot$

R	y_1	y_2	y_3
y_1	1	0	0
y_2	0	0	1
y_3	0	1	0

$=$

B	y_1	y_2	y_3
x_1	$1/2$	$1/2$	0
x_2	0	$1/2$	$1/2$

.

Clearly $\mathsf{A} \sqsubseteq \mathsf{B}$ (since $\mathsf{B} = \mathsf{AR}$).

Now consider channel C below.

C	z_1	z_2
y_1	1	0
y_2	1	0
y_3	0	1

We can compute the cascadings

A	y_1	y_2	y_3
x_1	$1/2$	0	$1/2$
x_2	0	$1/2$	$1/2$

$\cdot$

C	z_1	z_2
y_1	1	0
y_2	1	0
y_3	0	1

$=$

AC	z_1	z_2
x_1	$1/2$	$1/2$
x_2	$1/2$	$1/2$

and

B	y_1	y_2	y_3
x_1	$1/2$	$1/2$	0
x_2	0	$1/2$	$1/2$

$\cdot$

C	z_1	z_2
y_1	1	0
y_2	1	0
y_3	0	1

$=$

BC	z_1	z_2
x_1	1	0
x_2	$1/2$	$1/2$

,

and it's easy to see that $\mathsf{AC} \not\sqsubseteq \mathsf{BC}$, since under the uniform prior $\boldsymbol{\vartheta}$, the multiplicative Bayes leakage of BC is strictly greater than that of AC, as follows

$$\mathcal{L}_1^{\times}(\boldsymbol{\vartheta}, \mathsf{AC}) \;=\; 1/2 + 1/2 \;=\; 1 \;<\; 3/2 \;=\; 1 + 1/2 \;=\; \mathcal{L}_1^{\times}(\boldsymbol{\vartheta}, \mathsf{BC})\ .$$

Second part: Cascading is monotonic in its right-hand argument. Cascading is however monotonic wrt. refinement of its right-hand argument.

To see that, assume that $\mathsf{A} \sqsubseteq \mathsf{B}$. Hence, we know that there is a matrix R such that $\mathsf{B} = \mathsf{AR}$.

Now consider we have a matrix C (of appropriate type). Then

$$\begin{aligned} \mathsf{CB} &= \mathsf{C}(\mathsf{AR}) && (\text{since } `\mathsf{B} = \mathsf{AR}) \\ &= (\mathsf{CA})\mathsf{R} && (\text{assossiativity of matrix multiplication}) \ , \end{aligned}$$

which means that $\mathsf{CA} \sqsubseteq \mathsf{CB}$, since R is a post-processing channel matrix.

6. Suppose that we have a 2-bit secret X and a channel C, expressed concretely as C of type $\mathcal{X} \rightarrowtriangle \{0,1\}$, 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.

Instructor's solution: By marginalization and conditioning, we notice that the joint J^{ZX} can be decomposed into a prior ρ on Z given by

$$\rho = (1/2, 1/2) \ ,$$

and a channel from Z to X given by

B	00	01	10	11
0	$1/5$	$3/10$	$1/2$	0
1	$2/5$	$1/10$	$1/10$	$2/5$

,

such that $\mathsf{J}^{ZX} = \rho \triangleright \mathsf{B}$.

Now, notice that the multiplicative Dalenius Bayes leakage caused by C wrt. Z is given by

$$\mathcal{DL}_1^{\times}(\mathsf{J}^{ZX}, \mathsf{C}) \quad = \quad \frac{V_1[\rho \triangleright \mathsf{BC}]}{V_1(\rho)} \quad = \quad \mathcal{L}_1^{\times}(\rho, \mathsf{BC}) \ .$$

Now, to compute $V_1[\rho \triangleright \mathsf{BC}]$ we first find the channel matrix BC as

B	00	01	10	11
0	$1/5$	$3/10$	$1/2$	0
1	$2/5$	$1/10$	$1/10$	$2/5$

$\cdot$

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

$=$

BC	0	1
0	$8/25$	$17/25$
1	$17/25$	$8/25$

,

and then find the joint $\rho \triangleright \mathsf{BC}$ as

$\rho \triangleright \mathsf{BC}$	0	1
0	$8/50$	$17/50$
1	$17/50$	$8/50$

from which we can compute posterior Bayes vulnerability a the sum of column maxima

$$V_1[\rho \triangleright \mathsf{BC}] = 17/50 + 17/50 = 17/25 \ ,$$

and, since, prior Bayes vulnerability is

$$V_1(\rho) = 1/2 \ ,$$

we get that the multiplicative Dalenius Bayes leakage that C causes about Z is

$$\mathcal{DL}_1^{\times}(\mathsf{J}^{ZX}, \mathsf{C}) \ = \ \mathcal{L}_1^{\times}(\rho, \mathsf{BC}) \ = \ \frac{17/25}{1/2} \ = \ \frac{34}{25} \ .$$

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.

Instructor's solution: We can use Thm. 10.8, which says that for any channel C, non-negative gain function g, anc correlation J, we have

$$\mathcal{DL}_g^{\times}(J, C) \leq \mathcal{ML}_1^{\times}(\mathbb{D}, C) \ .$$

Now notice that, by Thm. 7.2,

$$\begin{aligned} \mathcal{ML}_1^{\times}(\mathbb{D}, \mathsf{C}) &= \sum_{y \in \mathcal{Y}} \max_{x \in \mathcal{X}} \mathsf{C}_{x,y} \\ &= 4/5 + 4/5 \\ &= 8/5 \ , \end{aligned}$$

so the maximum multiplicative leakage C can cause about this secret Z', under any non-negative gain function g is of $8/5$.