QIF 2021/1 Solution to second Exam

Question 1 (6 marks)

(a) $W^{1/2} \parallel W^{1/3}$

	(yes, yes)	(yes, no)	(no, yes)	(no, no)
yes	$6/12 = 1/2$	$3/12 = 1/4$	$2/12 = 1/6$	$1/12$
no	$1/12$	$2/12 = 1/6$	$3/12 = 1/4$	$6/12 = 1/2$

This represents a situation in which the respondant will give his answer through two different instatiations of the protocol, independently from each other. ◀

(b) $W^{1/2} \boxplus_{1/2} W^{1/3} =$

	yes$^{W^{1/2}}$	no$^{W^{1/2}}$	yes$^{W^{1/3}}$	no$^{W^{1/3}}$
yes	$3/8 = 9/24$	$1/8 = 3/24$	$2/6 = 8/24$	$1/6 = 4/24$
no	$1/8 = 3/24$	$3/8 = 9/24$	$1/6 = 4/24$	$2/6 = 8/24$

This represents a scenario in which the respondent will run $W^{1/2}$ or $W^{1/3}$ with equal probability, and reveal the reported answer together with the channel used. ◀

(c) $W^{1/2} \oplus_{1/2} W^{1/3} =$

	yes	no
yes	$17/24$	$7/24$
no	$7/24$	$17/24$

This represents a scenario in which the respondent will run $W^{1/2}$ or $W^{1/3}$ with equal probability, and reveal the reported answer, but not the channel used. ◀

Question 02 (6 marks)

(a) When $C = W^{1/2} \boxplus_{1/2} W^{1/3}$ we have

$$\mathrm{Val}^{\times}_{G^+}(\mathbb{D}, C) = \sum_y \max_x C_{xy} = 9/24 + 9/24 + 8/24 + 8/24$$

$$= 34/24 = 17/12$$

When $C = W^{1/2} \oplus_{1/2} W^{1/3}$ we have

$$\mathrm{Val}^{\times}_{G^+}(\mathbb{D}, C) = \sum_y \max_x C_{xy} = 17/24 + 17/24 = 17/12$$

From the point of view of capacity alone (multiplicative, in this case), both channels are equivalently good or bad, and I could use either of them. (Notice, however, that internal choice refines external choice, so I could prefer the former to the latter.

(b) When $C = W^{1/2} \boxplus_{1/2} W^{1/3}$ we have

$$Ul^{+}_{G^j}(\mathbb{D}, C) = 1 - \sum_y \min_x C_{xy} = 1 - (3+3+4+4)/24$$

$$= 10/24 = 5/12$$

When $C = W^{1/2} \oplus_{1/2} W^{1/3}$ we have

$$Ul^{+}_{G^j}(\mathbb{D}, C) = 1 - \sum_y \min_x C_{xy} = 1 - (7/24 + 7/24) =$$

$$= 10/24 = 5/12$$

From the point of view of capacity alone (multiplicative, in this case), both channels are equivalently good or bad, and I could use either of them. (Notice, however, that internal choice refines external choice, so I could prefer the former to the latter.

Question 03 (6 marks)

Call income Z, real answer X, and reported answer Y.

We can decompose $J : \mathbb{D}(Z \times X)$ into $\rho : \mathbb{D}Z$ and $D : X \to \mathbb{D}Y$ such that $\rho \triangleright D = J$ as follows:

$\rho = (10/15, 5/15) = (2/3, 1/3)$

$D =$

	yes	no
low income	3/5	2/5
high income	1/5	4/5

Then the leakage $W^{1/2}$ causes about Z is

$\mathbb{D}\mathcal{L}^{x}_{1}(J, W^{1/2}) = \mathcal{L}^{x}_{1}(\rho \triangleright D W^{1/2})$

Now we find

$$DW^{1/2} = \begin{pmatrix} 3/5 & 2/5 \\ 1/5 & 4/5 \end{pmatrix} \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix} = \begin{matrix} \text{yes} & \text{no} \\ \begin{pmatrix} 11/20 & 9/20 \\ 7/20 & 13/20 \end{pmatrix} & \begin{matrix} \text{low inc.} \\ \text{high inc.} \end{matrix} \end{matrix}$$

Now $\rho \triangleright D W^{1/2} =$

$$\begin{pmatrix} 2/3 \\ 1/3 \end{pmatrix} \triangleright \begin{pmatrix} 11/20 & 9/20 \\ 7/20 & 13/20 \end{pmatrix} = \begin{matrix} \text{yes} & \text{no} \\ \begin{pmatrix} 22/60 & 18/60 \\ 7/60 & 13/60 \end{pmatrix} & \begin{matrix} \text{low inc.} \\ \text{high inc.} \end{matrix} \end{matrix}$$

and

$D\lambda_j^x (J \triangleright W^{1/2}) =$

$\lambda_i^x (\rho \triangleright D W^{1/2}) =$

$$\sum_y \max_z (\rho \triangleright D W^{1/2})_{zy} \Big/ \max_z f_z =$$

$2/3 \,/\, 2/3 =$

1.

Hence leakage is 1.

Question 04 (7 marks)

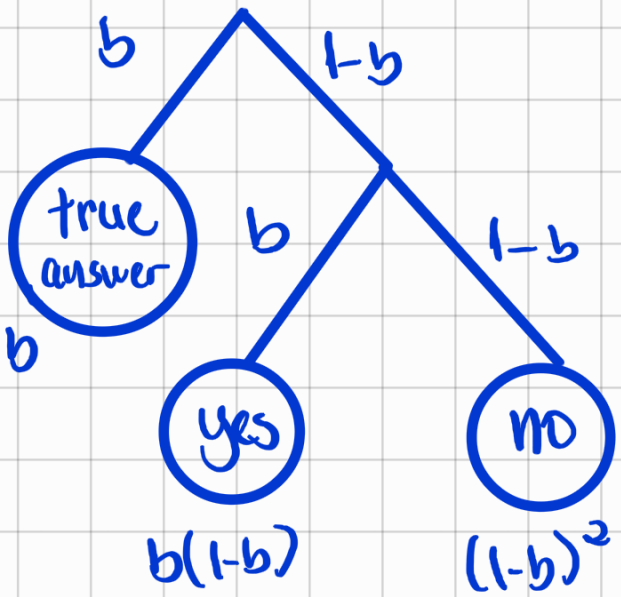
(a) The coder can explain to the respondant that no matter the adversary's prior knowledge and non-negative g-vulnerability, channel $W^{1/3}$ will never leak more than $W^{1/2}$.

I.e., $W^{1/2} \sqsubseteq_G W^{1/3}$.

She can prove that by finding a channel matrix R such that $W^{1/3} = W^{1/2} R$, establishing that $W^{1/2} \sqsubseteq_0 W^{1/3}$.

◀

(b) The protocol's behavior is given by the following tree:



Hence the channel W^b is:

$W^b =$

	yes	no
yes	$b + (1-b)/2$	$(1-b)/2$
no	$(1-b)/2$	$b + (1-b)/2$

$=$

	yes	no
yes	$(1+b)/2$	$(1-b)/2$
no	$(1-b)/2$	$(1+b)/2$

Now if $b_1 \geq b_2$ we can write $b_1 = b_2 + c$ for some $c \geq 0$. We need to find a channel matrix R such that $W^{b_1} R = W^{b_2}$, proving that $W^{b_1} \sqsubseteq W^{b_2}$. So we need:

W^{b_1}	yes	no
yes	$\frac{1+b_2+c}{2}$	$\frac{1-b_2}{2}$
no	$\frac{1-b_2}{2}$	$\frac{1+b_2+c}{2}$

$\cdot$

R	yes	no
yes	m	1-m
no	n	1-n

$=$

W^{b_2}	yes	no
yes	$\frac{1+b_2}{2}$	$\frac{1-b_2}{2}$
no	$\frac{1-b_2}{2}$	$\frac{1+b_2}{2}$

Solving for m, n, we find that R is

R	yes	no
yes	$\frac{2b_2 + c}{2b_2 + 2c}$	$\frac{c}{2b_2 + 2c}$
no	$\frac{c}{2b_2 + 2c}$	$\frac{2b_2 + c}{2b_2 + 2c}$

and we can verify that it's a valid channel matrix (rows add up to 1 and all entries are non-negative). ▲