

## SOLUTIONS TO MATH3411 PROBLEMS 48–59

**48.** Define  $A = \{a_1, a_2\}$ ,  $B = \{b_1, b_2\}$ ,  $C = \{c_1, c_2\}$ , where

$a_1$ : student passes  
 $a_2$ : student fails  
 $b_1$ : student owns car  
 $b_2$ : student owns no car  
 $c_1$ : student lives at home  
 $c_2$ : student lives away from home

We are told, and can immediately infer, that

$$\begin{array}{llll} P(a_1) & = & 0.75 & P(b_1|a_1) = 0.10 & P(c_1|b_2 \cap a_1) = 0.40 \\ P(a_2) & = & 0.25 & P(b_2|a_1) = 0.90 & P(c_2|b_2 \cap a_1) = 0.60 \\ & & & P(b_1|a_2) = 0.50 & P(c_1|b_2 \cap a_2) = 0.40 \\ & & & P(b_2|a_2) = 0.50 & P(c_2|b_2 \cap a_2) = 0.60 \end{array}$$

From this, we can calculate

$$\begin{array}{llll} P(a_1 \cap b_1) & = & 0.075 & P(a_1 \cap b_2 \cap c_1) = 0.27 \\ P(a_1 \cap b_2) & = & 0.675 & P(a_1 \cap b_2 \cap c_2) = 0.405 \\ P(a_2 \cap b_1) & = & 0.125 & P(a_2 \cap b_2 \cap c_1) = 0.05 \\ P(a_2 \cap b_2) & = & 0.125 & P(a_2 \cap b_2 \cap c_2) = 0.075 \end{array}$$

and thus

$$\begin{array}{llll} P(b_2 \cap c_1) & = & 0.32 & P(a_1 \cap b_1 \cap c_1) = 0.075 \\ P(b_2 \cap c_2) & = & 0.48 & P(a_1 \cap b_1 \cap c_2) = 0 \\ & & & P(a_2 \cap b_1 \cap c_1) = 0.125 \\ & & & P(a_2 \cap b_1 \cap c_2) = 0 \end{array}$$

and so

$$\begin{array}{llll} P(c_1|b_2) & = & 0.4 & P(a_1 \cap c_1) = 0.345 & P(c_1|a_1) = 0.46 \\ P(c_2|b_2) & = & 0.6 & P(a_1 \cap c_2) = 0.405 & P(c_2|a_1) = 0.54 \\ & & & P(a_2 \cap c_1) = 0.175 & P(c_1|a_2) = 0.7 \\ & & & P(a_2 \cap c_2) = 0.075 & P(c_2|a_2) = 0.3 \end{array}$$

To simplify calculations, we use the function  $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ .

**a.** This is asking to show that  $P(c_i|b_j \cap a_k) = P(c_i|b_j)$  for all  $i, j, k = 1, 2$ .

We could show these 8 equalities explicitly; there is however a short-cut here.

If it is assumed that the student owns a car ( $b_1$ ), then that student lives at home, regardless of course performance:

$$P(c_i|b_1 \cap a_k) = P(c_i|b_1) \quad \text{for all } i, k$$

If the student does not own a car ( $b_2$ ), then that student lives at home ( $c_1$ ) with 40% probability or does not ( $c_2$ ) with 60% probability, regardless of course performance:

$$P(c_i|b_2 \cap a_k) = P(c_i|b_2) \quad \text{for all } i, k$$

b. Here, we are meant to calculate  $I(A, B)$ :

$$\begin{aligned} I(A, B) &= H(B) - H(B|A) \\ &= H(0.2) - (P(a_1)H(B|a_1) + P(a_2)H(B|a_2)) \\ &= H(0.2) - (0.75H(0.1) + 0.25H(0.5)) \\ &\approx 0.120 \end{aligned}$$

c. Here, we are meant to calculate  $I(A, C)$ :

$$\begin{aligned} I(A, C) &= H(C) - H(C|A) \\ &= H(0.52) - (P(a_1)H(C|a_1) + P(a_2)H(C|a_2)) \\ &= H(0.52) - (0.75H(0.46) + 0.25H(0.7)) \\ &\approx 0.032 \end{aligned}$$

d. The information in the first digit is  $H(A) = H(0.75) \approx 0.811$  bits.

The (new) information in the second digit is  $H(B|A) = 0.75H(0.1) + 0.25H(0.5) \approx 0.602$  bits.

The (new or extra) information in the third digit is  $H(C|A \cap B)$ .

By Part a., this equals  $H(C|B) = 0.2H(1) + 0.8H(0.4) \approx 0.777$ .

49.

a.  $P(a_j|b_i) = \frac{P(a_j \cap b_i)}{P(b_i)} = \frac{P(b_i|a_j)P(a_j)}{P(b_i)}$  where

$$\begin{aligned} P(b_1) &= P(b_1|a_1)P(a_1) + P(b_1|a_2)P(a_2) = 0.8 \times \frac{1}{3} + 0.4 \times \frac{2}{3} = \frac{1.6}{3} \\ P(b_2) &= P(b_2|a_1)P(a_1) + P(b_2|a_2)P(a_2) = 0.2 \times \frac{1}{3} + 0.6 \times \frac{2}{3} = \frac{1.4}{3} \end{aligned}$$

so

$$\begin{aligned} P(a_1|b_1) &= \frac{P(b_1|a_1)P(a_1)}{P(b_1)} = \frac{0.8 \times \frac{1}{3}}{\frac{1.6}{3}} = 0.5 \\ P(a_2|b_1) &= \frac{P(b_1|a_2)P(a_2)}{P(b_1)} = \frac{0.4 \times \frac{2}{3}}{\frac{1.6}{3}} = 0.5 \\ P(a_1|b_2) &= \frac{P(b_2|a_1)P(a_1)}{P(b_2)} = \frac{0.2 \times \frac{1}{3}}{\frac{1.4}{3}} \approx \frac{1}{7} \\ P(a_2|b_2) &= \frac{P(b_2|a_2)P(a_2)}{P(b_2)} = \frac{0.6 \times \frac{2}{3}}{\frac{1.4}{3}} \approx \frac{6}{7} \end{aligned}$$

b.

$$\begin{aligned} I(A, B) &= H(B) - H(B|A) \\ &= H(B) - (P(a_1)H(B|a_1) + P(a_2)H(B|a_2)) \\ &= H\left(\frac{1.6}{3}\right) - \left(\frac{1}{3}H(0.8) + \frac{2}{3}H(0.6)\right) \\ &\approx 0.109 \end{aligned}$$

**50.** Let  $P(a_1) = x$  and  $P(a_2) = 1 - x$ . Then

$$\begin{aligned} P(b_1) &= P(b_1|a_1)P(a_1) + P(b_1|a_2)P(a_2) = (1-q)x + 0(1-x) = (1-q)x \\ P(b_2) &= P(b_2|a_1)P(a_1) + P(b_2|a_2)P(a_2) = 0x + (1-q)(1-x) = (1-q)(1-x) \\ P(b_3) &= P(b_3|a_1)P(a_1) + P(b_3|a_2)P(a_2) = qx + q(1-x) = q \end{aligned}$$

so, writing  $p = 1 - q$ ,

$$\begin{aligned} H(B) &= -P(b_1) \log_2 P(b_1) - P(b_2) \log_2 P(b_2) - P(b_3) \log_2 P(b_3) \\ &= -px \log_2 px - p(1-x) \log_2 p(1-x) - q \log_2 q \\ &= -px \log_2 x - p(1-x) \log_2 (1-x) - p \log_2 p - q \log_2 q \\ &= pH(x) + H(q) \\ H(B|a_1) &= -P(b_1|a_1) \log_2 P(b_1|a_1) - P(b_2|a_1) \log_2 P(b_2|a_1) - P(b_3|a_1) \log_2 P(b_3|a_1) \\ &= -p \log_2 p - 0 \log_2 0 - q \log_2 q \\ &= H(q) \\ P(B|a_2) &= -P(b_1|a_2) \log_2 P(b_1|a_2) - P(b_2|a_2) \log_2 P(b_2|a_2) - P(b_3|a_2) \log_2 P(b_3|a_2) \\ &= -0 \log_2 0 - p \log_2 p - q \log_2 q \\ &= H(q) \\ H(B|A) &= H(B|a_1)P(a_1) + H(B|a_2)P(a_2) \\ &= H(q)x + H(q)(1-x) \\ &= H(q) \end{aligned}$$

Therefore,

$$I(A, B) = H(B) - H(B|A) = pH(x) + H(q) - H(q) = pH(x)$$

Then  $\frac{d}{dx} I(A, B) = p \frac{d}{dx} H(x) = \log_2 \left( \frac{1-x}{x} \right)$ .

Solving  $\frac{d}{dx} I(A, B) = 0$ , we get  $x = \frac{1}{2}$ , and so

$$C(A, B) = \max_x I(A, B) = pH\left(\frac{1}{2}\right) = p = 1 - q$$

**51.** We can first calculate, regardless of the probabilities  $P(a_j)$ :

$$H(B|a_j) = \sum_{i=1}^3 (-P(b_i|a_j) \log_2 P(b_i|a_j)) = -\frac{1}{2} \log_2 \frac{1}{2} + 2 \left( -\frac{1}{4} \log_2 \frac{1}{4} \right) = \frac{1}{2} + \frac{1}{2} \log_2 4 = 1.5$$

$$H(B|A) = \sum_{j=1}^3 H(B|a_j)P(a_j) = \frac{3}{2} \times \sum_{j=1}^3 P(a_j) = 1.5$$

**a.**

$$H(A) = 3 \left( -\frac{1}{3} \log_2 \frac{1}{3} \right) = \log_2 3$$

$$P(b_i) = \sum_{j=1}^3 P(b_i|a_j)P(a_j) = \frac{1}{2} \times \frac{1}{3} + 2 \frac{1}{4} \times \frac{1}{3} = \frac{1}{3} = P(a_j) \quad \text{for all } i, j$$

$$H(B) = H(A) = \log_2 3$$

Hence,

$$I(A, B) = H(B) - H(B|A) = \log_2 3 - \frac{3}{2} \approx 0.085$$

$$H(A|B) = H(A) - I(A, B) = \frac{3}{2} = 1.5$$

$$H(A, B) = H(A) + H(B|A) = \log_2 3 + \frac{3}{2} \approx 3.085$$

b.

$$H(A) = -\frac{1}{2} \log_2 \frac{1}{2} - \frac{1}{3} \log_2 \frac{1}{3} - \frac{1}{6} \log_2 \frac{1}{6} \approx 1.459$$

$$P(b_1) = \sum_{j=1}^3 P(b_1|a_j)P(a_j) = \frac{1}{2} \times \frac{1}{2} + \frac{1}{4} \times \frac{1}{3} + \frac{1}{4} \times \frac{1}{6} = \frac{3}{8}$$

$$P(b_2) = \sum_{j=1}^3 P(b_2|a_j)P(a_j) = \frac{1}{4} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{3} + \frac{1}{4} \times \frac{1}{6} = \frac{1}{3}$$

$$P(b_3) = \sum_{j=1}^3 P(b_3|a_j)P(a_j) = \frac{1}{4} \times \frac{1}{2} + \frac{1}{4} \times \frac{1}{3} + \frac{1}{2} \times \frac{1}{6} = \frac{7}{24}$$

$$H(B) = -\frac{3}{8} \log_2 \frac{3}{8} - \frac{1}{3} \log_2 \frac{1}{3} - \frac{7}{24} \log_2 \frac{7}{24} \approx 1.577$$

Hence,

$$I(A, B) = H(B) - H(B|A) \approx 1.577 - 1.5 = 0.077$$

$$H(A|B) = H(A) - I(A, B) \approx 1.459 - 0.077 = 1.382$$

$$H(A, B) = H(A) + H(B|A) \approx 1.459 + 1.5 = 2.959$$

c. Your guess is your guess :)

d. Write  $P(a_1) = x_1$  and  $P(a_2) = x_2$ .

$$P(b_1) = \sum_{j=1}^3 P(b_1|a_j)P(a_j) = \frac{1}{2}x_1 + \frac{1}{4}x_2 + \frac{1}{4}(1 - x_1 - x_2) = \frac{1}{4}(1 + x_1)$$

$$P(b_2) = \sum_{j=1}^3 P(b_2|a_j)P(a_j) = \frac{1}{4}x_1 + \frac{1}{2}x_2 + \frac{1}{4}(1 - x_1 - x_2) = \frac{1}{4}(1 + x_2)$$

$$P(b_3) = \sum_{j=1}^3 P(b_3|a_j)P(a_j) = \frac{1}{4}x_1 + \frac{1}{4}x_2 + \frac{1}{2}(1 - x_1 - x_2) = \frac{1}{4}(2 - x_1 - x_2)$$

$$\begin{aligned} H(B) &= -\frac{1}{4}(1 + x_1) \log_2 \frac{1}{4}(1 + x_1) - \frac{1}{4}(1 + x_2) \log_2 \frac{1}{4}(1 + x_2) - \frac{1}{4}(2 - x_1 - x_2) \log_2 \frac{1}{4}(2 - x_1 - x_2) \\ &= I\left(\frac{1 + x_1}{4}\right) + I\left(\frac{1 + x_2}{4}\right) + I\left(\frac{2 - x_1 - x_2}{4}\right) \end{aligned}$$

where  $I(x) = -x \log_2 x$ . Hence,

$$I(A, B) = H(B) - H(B|A) = I\left(\frac{1 + x_1}{4}\right) + I\left(\frac{1 + x_2}{4}\right) + I\left(\frac{2 - x_1 - x_2}{4}\right) - \frac{3}{2}$$

To find the maximum of this function, we solve the equations  $\frac{d}{dx_1}I(A, B) = 0$  and  $\frac{d}{dx_2}I(A, B) = 0$ . Let us first solve the first equation:

$$0 = \frac{d}{dx_1}I(A, B) = \frac{1}{4} \log_2 \left( \frac{2 - x_1 - x_2}{1 + x_1} \right)$$

$$\text{so } 2 - x_1 - x_2 = 1 + x_1$$

and so  $x_1 = \frac{1}{2}(1 - x_2)$ . Since  $I(A, B)$  is symmetric with respect to  $x_1$  and  $x_2$ , the second equation will imply that  $x_2 = \frac{1}{2}(1 - x_1)$ , so  $x_1 = \frac{1}{2}(1 - \frac{1}{2}(1 - x_1)) = \frac{1}{4} + \frac{1}{4}x_1$  and so  $x_1 = \frac{1}{3}$ . Hence,  $x_2 = 1 - x_1 - x_2 = \frac{1}{3}$ , so we find that  $I(A, B)$  is maximal for the probabilities  $P(a_j) = \frac{1}{3}$  from part **a.**, and that the capacity is

$$C(A, B) = \max_{x_1, x_2} I(A, B) = H(B) - H(B|A) = \log_2 3 - \frac{3}{2} \approx 0.085$$

**52.**

$$P(a_j|b_i) = \frac{P(a_j \cap b_i)}{P(b_i)} = \frac{P(b_i|a_j)P(a_j)}{P(b_i)}$$

where

$$\begin{aligned} P(b_1) &= P(b_1|a_1)P(a_1) + P(b_1|a_2)P(a_2) = \frac{5}{7}x \\ P(b_2) &= P(b_2|a_1)P(a_1) + P(b_2|a_2)P(a_2) = \frac{2}{7}x \\ P(b_3) &= P(b_3|a_1)P(a_1) + P(b_3|a_2)P(a_2) = \frac{1}{10}(1 - x) \\ P(b_4) &= P(b_4|a_1)P(a_1) + P(b_4|a_2)P(a_2) = \frac{9}{10}(1 - x) \end{aligned}$$

so

$$\begin{aligned} P(a_1|b_1) &= \frac{P(b_1|a_1)P(a_1)}{P(b_1)} = 1 \\ P(a_1|b_2) &= \frac{P(b_2|a_1)P(a_1)}{P(b_2)} = 1 \\ P(a_1|b_3) &= \frac{P(b_3|a_1)P(a_1)}{P(b_3)} = 0 \\ P(a_1|b_4) &= \frac{P(b_4|a_1)P(a_1)}{P(b_4)} = 0 \\ P(a_2|b_1) &= \frac{P(b_1|a_2)P(a_2)}{P(b_1)} = 0 \\ P(a_2|b_2) &= \frac{P(b_2|a_2)P(a_2)}{P(b_2)} = 0 \\ P(a_2|b_3) &= \frac{P(b_3|a_2)P(a_2)}{P(b_3)} = 1 \\ P(a_2|b_4) &= \frac{P(b_4|a_2)P(a_2)}{P(b_4)} = 1 \end{aligned}$$

**a.** By the above,  $H(a_j|b_i) = 0$  for all  $i, j$ , so  $H(A|B) = 0$ .

This reflects that the elements of  $B$  imply which elements of  $A$  are given; in other words, there is no

information in  $A$  that is not determined by  $B$ .

In particular, if  $b_1$  or  $b_2$  are received, then  $a_1$  has been sent; otherwise if  $b_3$  or  $b_4$  are received, then  $a_2$  has been sent.

- b.  $I(A, B) = H(A) - H(A|B) = H(A) = H(x)$ , which has maximum

$$C(A, B) = \max_x I(A, B) = H\left(\frac{1}{2}\right) = 1$$

**53.** The block code  $\mathbb{Z}_2^{15}$  contains  $2^{15} = 32768$  which is enough to encode the students, for instance by a binary decision tree.

**54.**

- a) First use the Euclidean Algorithm forwards:

$$3876 = 11 \times 324 + 312$$

$$324 = 1 \times 312 + 12$$

$$312 = 26 \times 12 + 0,$$

so  $d = \gcd(312, 3876) = 12$ . Now use the Euclidean Algorithm backwards:

$$12 = 324 - 312$$

$$= 324 - (3876 - 11 \times 324)$$

$$= 12 \times 324 - 3876$$

Hence,  $12 = \gcd(324, 3876) = 324x + 3876y$  for  $x = 12$  and  $y = -1$ .

- b) First use the Euclidean algorithm forwards:

$$7412 = 4 \times 1513 + 1360$$

$$1513 = 1 \times 1360 + 153$$

$$1360 = 8 \times 153 + 136$$

$$153 = 1 \times 136 + 17$$

$$136 = 8 \times 17 + 0,$$

so  $d = \gcd(7412, 1513) = 17$ . Now use the Euclidean algorithm backwards:

$$17 = 153 - 136$$

$$= 153 - (1360 - 8 \times 153)$$

$$= 9 \times 153 - 1360$$

$$= 9 \times (1513 - 1360) - 1360$$

$$= 9 \times 1513 - 10 \times 1360$$

$$= 9 \times 1513 - 10 \times (7412 - 4 \times 1513)$$

$$= 49 \times 1513 - 10 \times 7412$$

Hence,  $d = \gcd(7412, 1513) = 7412x + 1513y$  for  $x = -10$  and  $y = 49$ .

c) First use the Euclidean algorithm forwards:

$$\begin{aligned}
2187 &= 2 \times 1024 + 139 \\
1024 &= 7 \times 139 + 51 \\
139 &= 2 \times 51 + 37 \\
51 &= 1 \times 37 + 14 \\
37 &= 2 \times 14 + 9 \\
14 &= 1 \times 9 + 5 \\
9 &= 1 \times 5 + 4 \\
5 &= 1 \times 4 + 1
\end{aligned}$$

so  $\gcd(1024, 2187) = 1$ . Now use the Euclidean algorithm backwards:

$$\begin{aligned}
1 &= 5 - 4 \\
&= 5 - (9 - 5) \\
&= 2 \times 5 - 9 \\
&= 2 \times (14 - 9) - 9 \\
&= 2 \times 14 - 3 \times 9 \\
&= 2 \times 14 - 3 \times (37 - 2 \times 14) \\
&= 8 \times 14 - 3 \times 37 \\
&= 8 \times (51 - 37) - 3 \times 37 \\
&= 8 \times 51 - 11 \times 37 \\
&= 8 \times 51 - 11 \times (139 - 2 \times 51) \\
&= 30 \times 51 - 11 \times 139 \\
&= 30 \times (1024 - 7 \times 139) - 11 \times 139 \\
&= 30 \times 1024 - 221 \times 139 \\
&= 30 \times 1024 - 221 \times (2187 - 2 \times 1024) \\
&= 472 \times 1024 - 221 \times 2187
\end{aligned}$$

Hence,  $1 = \gcd(1024, 2187) = 1024x + 2187y$  for  $x = 472$  and  $y = -221$ .

**55.**

$$\begin{array}{lll}
\mathbb{U}_{24} &= \{1, 5, 7, 11, 13, 17, 19, 23\} & \varphi(24) = |\mathbb{U}_{24}| = 8 \\
\mathbb{U}_{36} &= \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\} & \text{so } \varphi(36) = |\mathbb{U}_{24}| = 12 \\
\mathbb{U}_{17} &= \{1, \dots, 16\} & \varphi(17) = |\mathbb{U}_{17}| = 16
\end{array}$$

**56.**

$$\begin{array}{lll}
72 &= 2^3 \cdot 3^2 & \phi(72) = \varphi(2^3)\varphi(3^2) = (2^3 - 2^2)(3^2 - 3^1) = 4 \times 6 = 24 \\
1224 &= 2^3 \cdot 3^2 \cdot 17 = 72 \cdot 17 & \text{so } \phi(1224) = \varphi(72)\varphi(17) = 24 \times 16 = 384 \\
561561 &= 3 \cdot 7 \cdot 11^2 \cdot 13 \cdot 17 & \phi(561561) = \varphi(3)\varphi(7)\varphi(11^2)\varphi(13)\varphi(17) \\
&&= 2 \cdot 6 \cdot (11^2 - 11^1) \cdot 12 \cdot 16 = 253440
\end{array}$$

57.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	3	2
5	0	5	4	3	2	1

Every non-zero element in  $\mathbb{Z}_5$  has an inverse and is therefore a unit, in contrast to the elements 3, 4, and 5 in  $\mathbb{Z}_6$ .

Therefore,  $\mathbb{Z}_5$  is a field and  $\mathbb{Z}_6$  is not.

58.

- a)  $6x \equiv 7 \pmod{17}$   
 $\Leftrightarrow 6x \equiv 24 \pmod{17}$   
 $\Leftrightarrow x \equiv 4 \pmod{17}$  (since  $\gcd(6, 17) = 1$ )
- b)  $6x \equiv 8 \pmod{11}$   
 $\Leftrightarrow 6x \equiv 30 \pmod{11}$   
 $\Leftrightarrow x \equiv 5 \pmod{11}$  (since  $\gcd(6, 11) = 1$ )
- c)  $6x \equiv 9 \pmod{13}$   
 $\Leftrightarrow 2x \equiv 3 \pmod{13}$  (since  $\gcd(3, 13) = 1$ )  
 $\Leftrightarrow 2x \equiv 16 \pmod{13}$   
 $\Leftrightarrow x \equiv 8 \pmod{13}$  (since  $\gcd(2, 13) = 1$ )

59.

- a) In  $\mathbb{Z}_{11}$ ,  $6 \times 2 = 12 = 1$ , so  $6^{-1} = 2$ .
- b)  $\gcd(6, 10) = 2 \neq 1$ , so 6 has no inverse in  $\mathbb{Z}_{10}$ .
- c) In  $\mathbb{Z}_{23}$ ,  $6 \times 4 = 24 = 1$ , so  $6^{-1} = 4$ .