

SOLUTIONS TO MATH3411 PROBLEMS 10–18

10a) We could list the 13 cards of the hand by an (ordered) sequence of 13 6-bit binary numbers $n_1 \cdots n_{13}$, using $13 \times 6 = 78$ bits in all.

b) There are $\binom{52}{13} = 635013559600$, or about $\frac{2}{3}$ of a trillion, different bridge hands, which is more than $2^{39} = 549755813888$. We therefore need at least 40 bits to represent a hand.

To represent a hand, we could for instance list the 52 cards in some order and define the binary 52-bit word $\mathbf{w} = w_1 \cdots w_{52}$ where $w_i = 1$ if card i is in the hand and $w_0 = 0$ if it is not.

c) There are $\frac{52!}{(13!)^4} \approx 5 \times 10^{28}$ different bridge deals, which is more than $2^{95} \approx 4 \times 10^{28}$. We therefore need at least 96 bits to represent a bridge deal.

To represent a deal, we could for instance list the 52 cards in some order and define the binary 104-bit word $\mathbf{x} = x_1 \cdots x_{52}$ where x_i is the hand that card i is in, written in binary (00, 01, 10, 11).

We can improve this a little by deleting x_{52} to get a 102-bit word which tells us how the first 51 cards have been placed in the 4 hands. Just one hand is missing a card which must be card 52.

To further shorten our representation, also delete x_{51} ; we now have the 100-bit word $x_1 \cdots x_{50}$ which tells us how the first 50 cards have been placed in the 4 hands. To reconstruct the hand, we just need to place card 51 and card 52, either into two hands that are missing one card or into one hand that is missing two (we can see which hand(s) this(these) are from the first 50 placements). Suppose that card 51 belongs to hand i and that card 52 belongs to hand j . Now define an extra bit y_{51} by letting $y_{51} = 0$ if $i \leq j$, and $y_{51} = 1$ otherwise. From y_{51} , we can see where cards 51 and 52 belong, so the 101-bit codeword $x_1 \cdots x_{50}y_{51}$ describes the bridge deal completely.

11.

A	0	1	0	0	0	0	0	1
u	1	1	1	1	0	1	0	1
g	1	1	1	0	0	1	1	1
	1	0	1	0	0	0	0	0
2	1	0	1	1	0	0	1	0
0	0	0	1	1	0	0	0	0
1	1	0	1	1	0	0	0	1
2	1	0	1	1	0	0	1	0
r	0	1	1	1	0	0	1	0

We therefore encode **Aug 2012** as **Aug 2012r**.

12a)

$$\begin{array}{cc|cccc} 1 & 1 & 0 & 0 & 0 & 1 \\ 13 & 1 & 1 & 1 & 0 & 1 \\ 2 & 1 & 0 & 0 & 1 & 0 \\ 6 & 0 & 0 & 1 & 1 & 0 \\ \hline 8 & 1 & 1 & 0 & 0 & 0 \end{array}$$

We see that 1,13,2,6 has check integer 8.

b)

$$\begin{array}{cc|cccc} 2 & 1 & 0 & 0 & 1 & 0 \\ 11 & 1 & 1 & 0 & 1 & 1 \\ \mathbf{14} & \mathbf{0} & 1 & 1 & \mathbf{1} & 0 \\ 3 & 0 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 1 & \mathbf{1} & 0 & 0 \end{array}$$

If there were no errors, then the message would be 2,11,**14**,3.

However, the third row and second-last column have incorrect check-bits, so, assuming just a single error, the third row is corrected to **01100**, or 12. The corrected and decoded message is then 2,11,12,3.

13a) We solve $H\mathbf{x} = 0$ (we omit the zero-column in the following matrices):

$$\begin{aligned} \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix} &\xrightarrow{R_3=R_3+R_1} \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix} \xrightarrow[R_3=R_3+R_2]{R_1=R_1+R_2} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \\ &\xrightarrow{R_3=R_3+R_1} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \end{aligned}$$

Writing the solution vectors as $(x_1 \cdots x_5)^T$ and re-naming the non-leading variables $x_4 = \lambda$ and $x_5 = \mu$ where $\lambda, \mu \in \{0, 1\}$, we see that

$$\begin{array}{rcccl} x_1 & & + & \lambda & + & \mu & = & 0 \\ x_2 & & + & \lambda & & & = & 0 \\ x_3 & + & \lambda & + & \mu & = & 0 \end{array}$$

In other words, we find the solutions (working modulo 2) to be

$$\begin{pmatrix} \lambda + \mu \\ \lambda \\ \lambda + \mu \\ \lambda \\ \mu \end{pmatrix} = \lambda \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} + \mu \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \quad \text{where } \lambda, \mu \in \{0, 1\}.$$

In other words, the code \mathcal{C} consists of the codewords

$$\mathbf{x} = 00000, 111110, 10101, 01011$$

b) For instance, columns 1, 2, and 3 (none is the sum of the others).

c) For instance, columns 2, 4, and 5 (column 2 is the sum of the other two).

- d) None of the columns are equal (parallel in \mathbb{Z}_2).
- e) Any four columns form a submatrix of H which must have rank less than or equal to $\text{rank } H = 3$. Therefore, no four columns are linearly independent.

14a) We are looking for a codeword of the form $x_1x_21x_4010$ that satisfies the congruences

$$\begin{array}{cccccccc} x_1 & & + & 1 & & + & 0 & & + & 0 & = & 0 \\ & x_2 & + & 1 & & & & + & 1 & + & 0 & = & 0 \\ & & & & x_4 & + & 0 & + & 1 & + & 0 & = & 0 \end{array}$$

We see that $x_1 = 1$, $x_2 = 0$, and $x_4 = 1$, so the Hamming (7,4) code encodes 1010 as 1011010.

- b) Calculate the syndrome $S(\mathbf{y}) = H\mathbf{y}$ of $\mathbf{y} = (1001111)^T$:

$$S(\mathbf{y}) = H\mathbf{y} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

We see that there is at least one error. Assuming that there is just a single error, the syndrome $S(\mathbf{y})$ tells us that there is an error in bit number 001, i.e. 1, of 1001111. In other words, the correct codeword is 0001111, which decodes to 0111.

15.

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Set $\mathbf{y} = (001010101110110)^T$; then

$$H\mathbf{y} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

so the error is in position 1010, or 10, and the corrected word is 001010101010110. The decoded word is then 11011010110.

16a) We are looking for a codeword of the form $x_1x_21x_4010x_81010101$ that satisfies the congruences

$$\begin{array}{cccccccccccccccc} x_1 & & + & 1 & & + & 0 & & + & 0 & & + & 1 & & + & 1 & & + & 1 & & + & 1 & = & 0 \\ & x_2 & + & 1 & & & & + & 1 & + & 0 & & & + & 0 & + & 1 & & & + & 0 & + & 1 & = & 0 \\ & & & & x_4 & + & 0 & + & 1 & + & 0 & & & & & & + & 0 & + & 1 & + & 0 & + & 1 & = & 0 \\ & & & & & & & & & & & x_8 & + & 1 & + & 0 & + & 1 & + & 0 & + & 1 & + & 0 & + & 1 & = & 0 \end{array}$$

We see that $x_1 = 1$, $x_2 = 0$, $x_4 = 1$, and $x_8 = 0$, so the Hamming (15,11) code encodes 10101010101 as 101101001010101.

b) Calculate the syndrome $S(\mathbf{y}) = H\mathbf{y}$ of $\mathbf{y} = (011100010111110)^T$:

$$S(\mathbf{y}) = H\mathbf{y} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

We see that there is at least one error. Assuming that there is just a single error, the syndrome $S(\mathbf{y})$ tells us that there is an error in bit number 0011, i.e. 3, of \mathbf{y} . In other words, the correct codeword is 010100010111110.

The decoded word is then 00000111110.

17. There are 2^n random sequences of $n = 2^m - 1$ 0s and 1s.

The number of codewords in a Hamming code of length n is $2^k = 2^{n-m} = 2^n/2^m = \frac{2^n}{n+1}$.

Hence, the probability that a random sequence of n 0s and 1s is part of a Hamming code of length n is

$$\left(\frac{2^n}{n+1}\right)/2^n = \frac{1}{n+1}.$$

18. Let X be the number of errors; then X is (n, p) -binomially distributed with $n = 7$ and $p = 0.001$.

a) $P(X = 0) = (1 - p)^7 \approx 0.993021$

b) $P(X = 1) = 7p(1 - p)^6 \approx 0.006958$

c) $P(X = 2) + \dots + P(X = 7) = 1 - P(X = 0) - P(X = 1) \approx 1 - 0.993021 - 0.006958 = 0.000021$

d) Errors will be undetected if $S(\mathbf{y}) = 0$, and this will happen when there are errors in any of the following sets of bits:

123 145 167 246 257 347 356 1247 1256 1346 1357 2345 2367 4567 1234567

For instance, errors in the first three bits of some codeword \mathbf{x} give

$$S(\mathbf{x} + (1110000)^T) = H(\mathbf{x} + e_1 + e_2 + e_3) = H\mathbf{x} + He_1 + He_2 + He_3 = \mathbf{0} + \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \mathbf{0}$$

The probability of any of those fifteen above sets of errors occurring is

$$7p^3(1 - p)^4 + 7p^4(1 - p)^3 + p^7 \approx 7.0 \times 10^{-9}.$$