COMPSCI 314 S1C 05 Assignment 2

Sample Answers

Department of Computer Science
The University of Auckland
Due Thursday 28 April 2005, 4pm

This assignment will contribute 40/300 = 13.3% to your coursework mark, and 4% to your overall course mark.

1. Using the applet at http://falstad.com/fourier/, compute the analogue signals

   a. $A(t) = \sin(t)$

   b. $A(t) = \sin(t) + 0.33 \sin(3t)$

   c. $A(t) = \sin(t) + 0.33 \sin(3t) + 0.20 \sin(5t)$

   d. $A(t) = \sin(t) + 0.33 \sin(3t) + 0.20 \sin(5t) + 0.14 \sin(7t)$

   e. $A(t) = \sin(t) + 0.33 \sin(3t) + 0.20 \sin(5t) + 0.14 \sin(7t) + 0.11 \sin(9t)$.

   What is the title of the lecture slide that best illustrates this series of signals? Do your signals have the same phase as the signals in this lecture slide? If not, what is the difference in phase? Note that you may use the "Phase Shift" button in the Java applet to see what happens to the Fourier components and the analogue waveform, as a result of a phase shift. (**2 marks**)

The "Fourier synthesis of a square wave" slide (#8 of 80_PhysicalComm.pdf) is very similar to these waveforms. However the t=0 point on these waveforms is not clearly indicated. If we assume that thee waveforms on the slide are drawn starting from t=0 (at the left), then they are compositions of sine waves and are thus identical to the ones drawn in the applet. Note that the x=0 line in the applet must be in its middle, not at its left-hand side, because its display of "1.0 sin(x)" would be incorrect if the x=0 line were at the left-hand side.

Marking guidelines: 1 mark for identifying the lecture slide, and 1 mark for any understandable discussion of phase. No deduction if the student assumes the applet waveforms are drawn with x=0 at the left (because the instructor made this mistake in the first draft of the answer key -- congratulations to the sharp-eyed student who pointed out this mistake!

2. Using the applet at http://falstad.com/fourier/, compute the analogue signal $A(t) = 0.3 \sin(5t) + \sin(6t) + 0.3 \sin(7t)$. Describe this signal in your own words, using terms from your lecture notes and textbook. To receive full credit, you must make

appropriate use of the terms “sideband”, “carrier”, “modulation”, and “bandwidth”. (**4 marks**)

This signal is a sine wave of frequency *6t*, with an amplitude modulation by a sine wave of frequency *t*. The Fourier Transform of this signal has a carrier at frequency *6t* of amplitude 1, a lower sideband at frequency *5t* of amplitude 0.3, and an upper sideband at frequency *7t* of amplitude 0.3. The bandwidth of this signal is *2t*.

Marking guidelines: 1 mark for using each of the terms “sideband”, “carrier”, “modulation”, and “bandwidth” correctly. No penalty for grammatical mistakes, however if any of the technical terms are incorrectly spelled then no credit should be given for this usage.

3. Compute the channel capacity, in bits per second, of a signal with a 20 kHz bandwidth and a S/N ratio of 60 dB. (**2 marks**)

Using Shannon’s formula, the channel capacity $C = W \log_2(1 + S/N_{power}) = 20000 \log_2(1 + 10^{(60/10)}) = 20000 \log_2(1000001) = 20000(20) = 400$ kb/s.

Marking guidelines: 1 mark for correctly computing 10^6 as the S/N power ratio corresponding to 60 dB, and 1 mark for the correct final answer.

4. Repeat your calculation of problem #3 for S/N = −10 dB. (**1 mark**)

The capacity is now $C = W \log_2(1 + S/N_{power}) = 20000 \log_2(1 + 10^{(-10/10)}) = 20000 \log_2(1.1) = 20000(0.14) = 2.8$ kb/s

Marking guidelines: 1 mark for the correct answer, which may be rounded to 3 kb/s. No penalty for an answer that has many digits of precision (e.g. 2750.07 b/s), even though this is technically incorrect because the input parameters 20 kHz and -10 dB are given only to one or two digits of precision.

5. Consider the STM-1 frame definition given in the lecture slide entitled “Synchronous Digital Hierarchy: SDH, or SONET”, taking care to note the corrections posted to the web at http://www.cs.auckland.ac.nz/compsci314s1c/lectures/85_Physical2.pdf. As noted in the lecture slides, an STM-1 channel has a raw data rate of 150.336 Mbps. What fraction of this raw data rate is available to carry user data, assuming that the protocol overheads shown in the lecture slide are the only overheads? (**1 mark**)

The lecture slides were corrected again, after this question was posed, to show the correct data rate for the STM-1 channel: 155.52 Mb/s. So it should be marked generously.

The raw bitrate of an STM-1 channel is (270 columns / STM-1 frame)(9 bytes/column)(8 bits/byte)(8000 STM-1 frames/second) = 155.52 Mb/s. The payload or user-data rate is (260 payload columns / STS-1 frame)(9 bytes/column)(8 bits/byte)(8000 STM-1 frames/second) = 149.76 Mb/s. The fraction of raw data rate available to carry user data is 149.76 Mb/s / 155.52 Mb/s = 260/270 = 96.23%.

Marking guidelines: 1 mark for correctly calculating 96.23%, or for any answer that indicates the student understands that an STM-1 frame has 9 bytes of path overhead as well as 81 bytes of section and line overheads.

6. What is parity bit? Give an example of odd parity (1 mark)

   An extra bit appended to a (binary) message to make sum of all the bits odd, or even, depending on whether it is odd or even parity.

   For example, for odd parity:
   01000101 = 010001010
   01011100 = 010111001

7. Name the three key steps that occur during compression of bzip2 (1/2 mark)

   A permutation (The Burrows-Wheeler Transform)
   A Transformation (The Move-To-Front Algorithm)
   The compression (A Huffman compression scheme)

8. Hamming codes were used to transmit the following messages. For both part 3.a and 3.b draw up a Hamming code table. For each message was there an error, and if so, at which position did the error occur? (Assume odd-parity)
   What was the original message? (6 marks)

   a. 110011001101

	1	**1**	0	**0**	1	1	0	**0**	1	1	0	1	Count	Syndrome
Group 1	**X**		X		X		X		X		X		3	0
Group 2		**X**	X			X	X			X	X		3	0
Group 3				**X**	X	X	X					X	3	0
Group 4								**X**	X	X	X	X	3	0

   No Error
   Original Message: 01101101

   b. 001001011001

	0	**0**	1	**0**	0	1	0	**1**	1	0	0	1	Count	Syndrome
Group 1	**X**		X		X		X		X		X		2	1
Group 2		**X**	X			X	X			X	X		2	1
Group 3				**X**	X	X	X					X	2	1
Group 4								**X**	X	X	X	X	3	0

$0111_2 = 7$
Error at position 7: 001001011001->00100111001
Original Message: 10111001

9. Solve the following modulo 2 polynomial division (2 marks)

$$x^3 + x + 1 \;\overline{)\; x^7 + x^5 + x^4 + x^3 + x + 1}$$

$$\begin{array}{r} x^4 + 1 \\ x^3 + x + 1 \;\overline{)\; x^7 + x^5 + x^4 + x^3 + x + 1} \\ \underline{x^7 + x^5 + x^4} \\ x^3 + x + 1 \end{array}$$

10. Why is 1 + 1 = 0 using modulo 2 arithmetic? (1/2 mark)
*It is binary-base arithmetic, so we carry the 1. Same as 9+1 = 1**0** decimal arithmetic*

11. The following message was received using a CRC: 0101101101. The generator polynomial was $(x^4 + x^3 + x^2 + 1)$. Was there an error in the message? If not, what was the original message? Show your working (4 marks)

```
     11111
   ----------
11101 | 010110110
      | 1
        11101
        -----
        010111
         11101
         -----
         010101
          11101
          -----
          010000
           11101
           -----
           011011
            11101
            -----
            00111
              111
            -----
```

There is a remainder. There was an error.

12. Encode the following message, using a Huffman tree: “the meaning of life” (2 marks)

There will be multiple solutions to this. Check that the codes are Huffman codes!

{e=110, _=111, i=010, n=011, f=1011, l=1010, o=1001, g=1000, a=0011, m=0010, T=0000, h=0001}

T h e _ m e a n…
0000-0001-110-111-0010-110-0011-011…

13. Huffman codes have a unique property that makes them ideal to use under conditions where chunks of data may get corrupted or lost. What is this? (1 mark)

Huffman codes are self-synchronizing.

Or,

They are prefix free, i.e. no one code is a prefix of another – making it easy to determine an error due to loss of synchronization, and then recover from it.

14. Encode the following message using LZW: “think this is history”. Use a table. (4 marks)

Pass	Input string	Test string	Emit	Make entry	index	Contents
1	T	T			256	TH
2	H	TH	T	TH	257	HI
3	I	HI	H	HI	258	IN
4	N	IN	I	IN	259	NK
5	K	NK	N	NK	260	K_
6	_	K_	K	K_	261	_T
7	T	_T	_	_T	262	THI
8	H	TH			263	IS
9	I	THI	256 (TH)	THI	264	S_
10	S	IS	I	IS	265	_I
11	_	S_	S	S_	266	IS_
12	I	_I	_	_I	267	_H
13	S	IS			268	HIS
14	_	IS_	263 (IS)	IS_	269	ST
15	H	_H	_	_H	270	TO
16	I	HI			271	OR
17	S	HIS	257 (HI)	HIS	272	RY
18	T	ST	S	ST	273	
19	O	TO	T	TO		
20	R	OR	O	OR		
21	Y	RY	R	RY		
			Y			

15. Why is it secure to use RSA encryption if the cryptographic key is known (1 mark)

Each node/station/computer has both a public and private key. The private key is never given out, instead, the public key is transmitted. To transmit a message the sender and receiver exchange public keys, and encrypt the message using each other's public keys. The message can then only be decrypted using the corresponding private key.

Even if an outside party obtains the public key, they cannot decrypt the message without calculating the private key which involves factoring of large numbers and is computationally infeasible.

16. What are two differences between gzip and bzip2? (1 mark)

Any of:

- *gzip gives better compression than bzip2*
- *gzip use LZW algorithm, gzip2 uses the Burrows-Wheeler Transform*
- *gzip is a dictionary-based compression scheme, bzip2 is statistical based (Huffman-end compressor)*

- *gzip is most commonly used in data communications*

17. Explain how ssh-based authentication would work (2 marks)
    - *Initialization:*
        - *User generates a pair of public and private keys.*
        - *User copies the public key across to the host, where it is stored in a special file (e.g. /home/user/.ssh/authorized_keys2)*
    - *Upon authentication request:*
        - *Host sends user a random string encrypted with the user's public key, obtained from the file*
        - *User decrypts the message using their private key and sends it back to the host*
        - *Host determines if message was correct, and if so can authenticate user, and grant access*

18. What are the differences between DES, RSA and DSA (3 marks)
    DES: Digital Encryption Standard – An encryption standard that does not use public key based encryption, instead, it performs a series of complex substitutions, transpositions, XOR operations, and finally encryption. It is a symmetric encryption algorithm

    RSA: The name of a commonly used public-key encryption algorithm, named after its creators Rivest, Shamir and Adelman. An asymmetric encryption algorithm

    DSA: Digital Signature Algorithm - A public-key algorithm, that is part of the digital signature standard. Unlike RSA, it cannot be used for encryption, and only for digital signatures.

19. Why are repeaters necessary in some networks? (1 mark)
    In large networks, a signal may degrade and a repeater is required to regenerate the signal before retransmitting it.

20. What type of LAN is most commonly used today? (1 mark)

Switched Ethernet