

# MATH 300 Assignment 4

Zeke T. Estes

October 6, 2017

## Problem 1 [Binary Integers]

Write the following unsigned numbers in binary and hexadecimal using 8 bits (8 binary digits).

Problem	$7_{(2^7)}$	$6_{(2^6)}$	$5_{(2^5)}$	$4_{(2^4)}$	$3_{(2^3)}$	$2_{(2^2)}$	$1_{(2^1)}$	$0_{(2^0)}$	Hex
a. 16	0	0	0	1	0	0	0	0	0x10
b. 170	1	0	1	0	1	0	1	0	0xAA
c. 197	1	1	0	0	0	1	0	1	0xC5
d. 255	1	1	1	1	1	1	1	1	0xFF

## Problem 2 [Fixed Point]

You are tasked with determining how many bits are necessary to store some unsigned fixed point numbers. The constraints you are given are as follows:

- The whole portion of the numbers (the part to the left of the decimal point) must be able to store a maximum value of 511.

$$- \frac{\ln(511)}{\ln(2)} \approx 9 \therefore 9 \text{ bits required}$$

- The fractional portion of the numbers (the part to the right of the decimal point) must have a precision of  $\frac{1}{128}$ . In other words, the fractional part must be able to represent any number  $\frac{x}{128}$  where x ranges from 0 to 127.

- To determine the bits required to accomplish precision of  $1/128$ , a representation of  $1/128$  in binary must be found.

$x = \frac{1}{128}$	0.0078125	
$x = x * 2$	0.015625	0
$x = x * 2$	0.03125	0
$x = x * 2$	0.0625	0
$x = x * 2$	0.125	0
$x = x * 2$	0.25	0
$x = x * 2$	0.5	0
$x = x * 2$	1	1
<i>bits</i>		7

- **How many bits are required for a fixed point number that meets these constraints? Explain your reasoning.**
  - In order to represent an unsigned fixed point number  $\leq 511$ , a binary number with 9 bits must be used, as  $0b111111111 == 0d511$ . In order to represent an unsigned fixed point number at a precision of  $\frac{1}{128}$ , then a binary number with 7 bits must be used, as shown above. Therefore, it requires 16 bits to a fixed point number with the supplied specifications.

### Problem 3 [fixed point]

Say you are handed two fixed point numbers A and B, where each of them contain N binary digits for the whole portion and M digits for the fractional portion.

- **How does multiplication affect the number of bits that are required in the result if we multiply A and B if we do not want to lose any information? (If you are stuck and don't know where to begin, work through some examples: let N=2 and M=1, or N=3 and M=2).**
  - If the affects of overflow are ignored, and two fixed point numbers A and B are multiplied, it's important to analyze the extreme cases. Ignoring the fractional portion, if two numbers A and B are multiplied, at their max bit values, this would cause the number of bits to **double**, as shown below.

$A_{N_{max}} * B_{N_{max}}$	<i>Result</i>	<i>bits</i>
$11 * 11$	1001	4
$111 * 111$	110001	6
$1111 * 1111$	11100001	8
$11111 * 11111$	1111000001	10
$111111 * 111111$	111110000001	12
$1111111 * 1111111$	11111100000001	14

- Analyzing the fractional portion of the fixed point numbers is less tangible, as the matter of precision must be defined by the user. when the components of  $A_M$  and  $B_M$  are multiplied, the number of digits present should satisfy the level of precision necessary.
- Knowing this information, it is safe to assume that, although unoptimized, if one wants to ensure that no information is lost, doubling the number of digits, then pruning the leading zeros, would ensure that no information is lost.

### Problem 4

Say Alice and Bob are conducting online financial transactions on the web, and wish to protect their credit card information from malicious parties on the Internet.

- **What protocols will be involved in a secure web transaction? [Hint: there are at least two]. Explain briefly the role that each protocol that you list plays in their transaction.**

- HTTPS and SSL could both be used. HTTPS ensures that the web page a client is accessing is secure and encrypted. SSL also ensures that the data sent over the connection between the web server and client is secure and encrypted, and is responsible for generating the public and private encryption key between these two devices.
- **What piece of information do both Alice and Bob keep secret to ensure that nobody can decode the messages they are sending back and forth? What happens if this secret leaks out?**
  - Alice and Bob must keep their private key *private*, while using public keys to ensure that information sent from said person is actually from the other. If this secret private key is leaked out, then a trained individual could use said key to decrypt encrypted messages sent either over the internet, or even locally.