

CECS 329, Homework Assignment 1, Fall 2025, Dr. Ebert

Directions: Please review the Homework section on pages 5 and 6 of the syllabus including a list of all rules and guidelines for writing and submitting solutions.

Due Date: Saturday September 6th as a PDF file upload to the HW1 Canvas dropbox.

Problem

This problem is a spinoff of Additional Exercise A from the Turing Reducibility lecture. That exercise indicates that the multiplication algorithm provided in Example 3.1 is very inefficient in that the number of steps it requires for two unsigned n -bit integer inputs is $\Omega(2^n)$, and thus has exponential growth. The objective of this problem is to provide a more efficient multiplication algorithm. The pseudocode that you write may only use loops, conditional statements, variable assignments, queries to an **add** oracle, and logical operations (including bit shift and other bitwise operations). To receive full credit, your algorithm must make nontrivial use of the **add** oracle. In other words, it should not solely rely on logical operations. It should also be as efficient as possible.

1. Write a short paragraph that describes how your algorithm works. (15 pts)
2. Provide pseudocode for your algorithm in a mannner similar to what was provided in Example 3.1. (15 pts)
3. Use big-O notation to provide an upper bound on the number of steps required by your algorithm, assuming that inputs a and b are two unsigned n -bit integers. Also, assume that the execution of a logic operation counts as one step, as does each query to the **add** oracle. (10 pts)