Math 480A2, Homework 11
Due November 10, 2022

Homework is graded out of a total of 10 points. Collaboration is permitted, but you must list all coauthors on a problem's solution at the top of the page, and your writing must be your own.

Problem 1. (4 points) Suppose that G is a graph with $n = 2^{15}$ vertices and $m = 2^{20}$ edges. Recall that the interactive proof protocol for graph 3-colorability of the graph G has soundness error δ_S at most $1 - 1/m$, meaning that running the protocol will detect a cheating prover with probability at least $1/m$. How many independent repetitions of the protocol are necessary in order to detect a cheating prover at least 99% of the time? How many individual commitments will the prover send to the verifier during this many repetitions? How many of these commitments will be opened?

Problem 2. (4 points) Construct the Merkle tree associated with the vector of messages

$$(m_1, m_2, m_3, m_4) = (0, 3, 1, 2)$$

using the SHA256 cryptographic hash function. When writing down your solution, you may abbreviate the hashes to their first 4 hexadecimal characters (representing the first 16 bits of the output in base-16), but make sure to use the complete hashes when computing successive layers of the tree.

To compute the SHA256 hash evaluations, you may use the following website: `https://emn178.github.io/online-tools/sha256.html`. Make sure to select "Input type: Hex" from the dropdown menu so that your values aren't interpreted as "bytes associated with ASCII characters". If the settings are correct, then `SHA256(0)` should evaluate to "`6e34...`", not "`5fec...`".

Problem 3. (2 points) In the Merkle tree constructed in Problem 2, what is the Merkle path associated with the message m_2? How can you compute the Merkle root using only the values in this Merkle path?