CS253 HW12

Suppose S = (T1, . . . , T9) . Explain how Alice computes a commitment to S using a ternary Merkle tree (i.e., k = 3). How does Alice later prove to Bob that T4 is in S ? What values are provided in the proof?

Alice would compute a commitment to S using a ternary Merkle tree by hashing the values of T1, T2, and T3 together to form the root node. She would then prove to Bob that T4 is in S by providing the values of the root node and the two child nodes of T4.

For large n , if we want to minimise the proof size, is it better to use a binary or a ternary tree? Why?

For large n, it is better to use a binary tree because the proof size is   . This is because a binary tree can store twice as many elements as a ternary tree of the same size.