

## Questions

1. As mentioned in Lemma 13,  $T$  is any valid transformation of size  $t$ . A  $T$  is valid for  $x$  and  $y$  only if the number of *delete* and *replace* operations in  $T \leq |x|$  and the number of *insert* and *replace* operations in  $T \leq |y|$ . In the proof, it is mentioned that *if  $g(x, y, \rho) \in G_T$  and  $g(x, y, \rho)$  is complete, then  $T$  is a prefix of  $\mathcal{T}(x, y, \rho)$* . If we are given  $x$ ,  $y$ , and  $\rho$ , then we can have only one gridwalk  $g(x, y, \rho)$  which gives rise to only one transformation  $\mathcal{T}(x, y, \rho)$ , but we can have multiple valid  $T$ . How does the above statement hold true?
2. In Lemma 13, while defining  $g''$ , the proof mentions:  *$g''$  consists of loop and match operations concatenated onto the end of  $g' \cdot \sigma$ , ending with a match operation*. Consider a simple case where  $h_\rho(x) = h_\rho(y)$ , the last element in transcript would process \$ and have same value of  $|s|$ , hence the transcript could be hash-replace - hash-replace, in which case the Edit Distance operation would be replace, in this case  $\sigma$  i.e., the gridwalk would be of the form  $g' \cdot \sigma$  and would not have the *match* operation mentioned above.
3. The proof of Lemma 14 mentions: *By Lemma 13,  $h$  induces  $T$  on  $x$  and  $y$  (which is sufficient for  $h(x) = h(y)$  by Lemma 12) with probability  $p^r - 2/n^2$* . Lemma 12 mentions the case where  $T$  **solves**  $x$  and  $y$  and the probability is derived from Lemma 13 which mentions  $T$  of length  $t$  that is **valid** for  $x$  and  $y$ .