CSL202: Discrete Mathematical Structures
Tutorial/Homework: 10

1. (**Universal Hashing**) Hashing is a technique used to store elements from a large universe $U = \{0, ..., m-1\}$ using a small table $T = \{0, ..., n-1\}$ using a hash function $h : U \to T$ such that the number of collisions are minimized [1].

   Using a fixed hash function might does not work. So, we use a *family* of hash functions H and then pick a hash function randomly from this family. A hash function family H is called 2-universal if

   $$\forall x, y \in U, x \neq y, \mathbf{Pr}_{h \leftarrow H}[h(x) = h(y)] \leq 1/n.$$

   Show how a 2-universal hash function family is useful in hashing and give an example of such a family.

[1] Assume that collisions are resolved using auxiliary data structure