Homework 6:

Due: October 28, 2025 at 2:30p.m.

This homework must be typed in LaTeX and submitted via Gradescope.

Please ensure that your solutions are complete, concise, and communicated clearly. Use full sentences and plan your presentation before your write. Except where indicated, consider every problem as asking for a proof.

Problem 1. family $\mathcal{H}$ of hash functions from U to $[0, \ldots, m-1]$ is 2-universal iff for any $x, y \in U$ and h chosen uniformly at random from H

$$Pr(h(x) = h(y)) \leq 1/m.$$

Show that each of the following families of functions is not is not 2-universal.

1. Let $p > m$ be a prime number. Consider the family of functions

   $$H_1 = \{h(x) = ((ax \bmod p) \bmod m) \mid a \in \{1, \ldots, p-1\}\}.$$

   [Hint: try $m = 3$ and $p = 5$.]

2. Let $p > m$ be a prime number. Consider the family of functions

   $$H_1 = \{h(x) = ((x + b \bmod p) \bmod m) \mid b \in \{0, \ldots, p-1\}\}.$$

   [Hint: try $m = 3$ and $p = 5$.]

3. Let q be a multiple of m. Consider the family of functions

   $$H_1 = \{h(x) = ((ax + b \bmod q) \bmod m) \mid a \in \{1, \ldots, q-1\} \text{ and } b \in \{0, \ldots, q-1\}\}.$$

Problem 2. Given an arbitrary undirected graph G, applying DFS on a given vertex will create a tree. The tree can be used to detect the separating edges and vertices of the graph.

(a) Show that the root vertex of a DFS tree is a separating vertex of G if and only if the root vertex has multiple children in the DFS tree.

(b) Show that any non-root vertex v of a DFS tree is a separating vertex of G if and only the exists a child of v, w, such that none of w's descendants in the DFS tree have a back-edge to a proper ancestor of v in the DFS tree.

A **descendant** of a vertex is any vertex reachable from v in the DFS tree.
A **proper ancestor** of a vertex v is a vertex v' such that v is a descendant of v' and $v \neq v'$.
A **child** of a vertex v is a direct descendent of v.

Problem 3. Let $G = (A, B, E)$ be a bipartite graph, $E \subset A \times B$. Let $S \subseteq A$ and $T \subseteq B$. Assume that there is a matching covering S and a matching covering T. Prove that there is a matching covering $S \cup T$