Algorithms, February 2021 at CIS

Homework 1

1. Let $U = 2^u$ and $M = 2^m$. Prove that the family of hash functions $A \cdot x + b \bmod 2$, where $A \in \{0,1\}^{m \times u}$ is a random binary matrix, and $b \in \{0,1\}^m$ is a random binary vector, is a 2-universal family.

2. A k-universal family $\mathcal{H}$ of hash functions, each mapping to $\{0, 1, \ldots, M-1\}$ is such that for all k distinct keys $x_1, \ldots, x_k$ in a universe $\mathcal{U}$, and all k possible values $v_1, \ldots, v_k$ in $\{0, 1, \ldots, M-1\}$, we have $\mathbf{Pr}_h[h(x_1) = v_1 \text{ and } h(x_2) = v_2 \text{ and } \ldots h(x_k) = v_k] = \frac{1}{M^k}$. Suppose $\mathcal{H}$ is a 3-universal family of hash functions. Show that $\mathcal{H}$ is also a 2-universal family of hash functions.

3. Show that the universal hash function family we studied in class, namely, $h(x) = A \cdot x \bmod 2$, where A is a random binary matrix, is not a 2-universal family of hash functions.