Theorem 6.9 (Universal hashing)**.** *Let m be prime and $r \in \mathbb{N}$. For $U = [b]^{r+1}$ where $[b] = \{0, \ldots, b-1\}$ and $M = [m]$ with $b \leq m$, $k = (k_0, \ldots, k_r) \in U$ and $a = (a_0, \ldots, a_r) \in [m]^{r+1}$, define*

$$h_a(k_0, \ldots, k_r) = \sum_{i=0}^{r} a_i \cdot k_i \mod m.$$

Then $\mathcal{H} := \{h_a : a \in [m]^{r+1}\}$ is a universal family of hash functions.

Proof. For prime m, any linear function

$$f_\delta(x) := x \cdot \delta \mod m$$

with $x \in [m]$, $\delta \neq 0$ is a bijection $[m] \to [m]$. All $x \in [m]$ have different images under f_δ, and every element of $[m]$ is the image of some $x \in [m]$.

Let $(k_0, \ldots, k_r) = k \neq l = (l_0, \ldots, l_r) \in U$, and consider

$$\begin{aligned} h_a(k) = h_a(l) \Leftrightarrow \quad & \sum_{i=0}^{r} a_i \cdot k_i \equiv \sum_{i=0}^{r} a_i \cdot l_i && \mod m \\ \Leftrightarrow \quad & 0 \equiv \sum_{i=0}^{r} a_i \cdot (l_i - k_i) && \mod m \\ \Leftrightarrow \quad & 0 \equiv \sum_{k_i \neq l_i} a_i \cdot (l_i - k_i) && \mod m \end{aligned}$$

The terms where $k_i = l_i$ are 0 and so we can ignore them. Now define $\delta_i := l_i - k_i$ and we get

$$0 \equiv \sum_{k_i \neq l_i} a_i \cdot \delta_i \mod m$$

Let $S := \{i \in [m] : \delta_i \neq 0\} \neq \emptyset$ be the set of the indices of the non-vanishing terms. There are $m^{|S|}$ possibilities to choose the factors $\{a_j : j \in S\}$. If we choose the first $|S| - 1$ factors, then due to the expression being linear, we have exactly 1 choice left for the last a_j to satisfy the equation. Altogether, we have $m^{|S|-1}$ choices for all a_j to satisfy the equation, and so our chance of picking an a that produces a collision is $\frac{m^{|S|-1}}{m^{|S|}} = \frac{1}{m}$. □