Theorem 11.5

The class H_{pm} of hash functions defined by equations (11.3) and (11.4) is universal.

Proof

Consider two distinct keys k and l from Z_p, so that $k \neq l$. Without loss of generality, assume $k > l$.

For a given hash function h_{ab} we let

$$r = (ak + b)\ mod\ p,$$
$$s = (al + b)\ mod\ p.$$

We first prove that $r \neq s$. Assume

$$r = s,$$

We have

$$r - s \equiv (ak + b) - (al + b) \equiv a(k - l) \equiv 0(mod\ p).$$

Then

$$p|a(k - l)$$

On the other hand, because $a \in Z_p^*$,we get $p \nmid a$. Because $(k - l) \in Z_p$,we get $p \nmid (k - l)$.

So

$$p \nmid a(k - l).$$

This is a contradiction.

So we have

$$r \neq s$$

Since $r \equiv s(mod\ m)$

$$r - s \equiv [(ak + b)\ mod\ p] - [(al + b)\ mod\ p] \equiv 0\ (mod\ m)$$
$$[a(k - l)\ mod\ p] \equiv 0\ (mod\ m) \qquad (*)$$

The possible value of $[a(k - l)\ mod\ p]$ is $m, 2 \cdot m, \dots, \lfloor p/m \rfloor \cdot m$. Its value cannot be zero because $r \neq s$.

So the number of different a satisfying formulae $(*)$ is at most $\lfloor p/m \rfloor$. For each value of a, there are p different values of b. So the number of different h_{ab} satisfying $h_{ab}(k) = h_{ab}(l)$ is at most

$$\left\lfloor \frac{p}{m} \right\rfloor \cdot p \leq \frac{(p - 1)p}{m} = \frac{|H_{pm}|}{m}$$

So the class H_{pm} of hash functions is universal.