

(a)

It is **not** universal.

Counter example: Since $M \gg p$, we can simply let $u = p$ and $v = 2p$. Then $h_a(u) = (pa \bmod p) = 0$, $h_a(v) = (2pa \bmod p) = 0$. The probability is now 1 (much higher than $1/|T|$). Hence this is not a universal case.

(b)

It is **not** universal.

Counter example: Suppose $u = (0, 0, 0)$ and $v = (n/2, 0, 0)$ (since n is not a prime we assume it can be divided by 2, other divisor would be the same). Then $h_a(u) = 0$, $h_a(v) = a_1 n/2 \bmod p \bmod n$. Since $n \leq p$, if $a_1 = 0$ or $a_1 = 2$, $h_a(v) = n \bmod p \bmod n = 0 = h_a(u)$. There might be other cases, but we do not care, since at least two cases make $h_a(u) = h_a(v)$. So the probability that u and v collide is greater or equal to:

$$Pr \geq \frac{2}{p} > \frac{1}{p} \quad (1)$$

Hence, this is not a universal case.

(c)

This one is **universal**.

Proof: Let $u = (u_1, \dots, u_k)$ and $v = (v_1, \dots, v_k)$ be 2 distinct elements. We know that there must be an index j such that $u_j \neq v_j$. We first choose all a_i where $i \neq j$, and finally choose a_j . No matter how other coordinates are chosen, the probability of $h_a(u) = h_a(v)$ is exactly $1/p$. Hence, we conclude that $h_a(u) = h_a(v)$ iff:

$$a_j(v_j - u_j) = \sum_{i \neq j} a_i(u_i - v_i) \bmod p \quad (2)$$

Hence, there is only one value $0 \leq a_j \leq p - 1$ such that $a_j(v_j - u_j) = C \bmod p$ where C is a fixed number. Suppose there are 2 values a_j and a'_j so that $a_j(v_j - u_j) = a'_j(v_j - u_j)$. However, we know that a_j, a'_j are both less than p . So a_j and a'_j has to be the same, which means the probability that u and v collide is exactly $1/p$. Hence the hash function is universal.