Representing elements in U by elements in A.

every $\vec{a} \in A$ gives a mapping from $A \to [p]$.

$$h_{\vec{a}} : \vec{x} \mapsto (\vec{a}^T \cdot \vec{x}) \bmod p.$$

We need to show:

Pf (Thm) $\forall \vec{x}, \vec{y} \in A, \vec{x} \neq \vec{y}$,

$$Pr_{\vec{a} \sim A} [\vec{a}^T \cdot \vec{x} = \vec{a}^T \vec{y} \bmod p] \leq \frac{1}{p}.$$

$$\| $$

$$Pr_{\vec{a} \sim A} [h_{\vec{a}}(\vec{x}) = h_{\vec{a}}(y)] \leq \frac{1}{p}$$

Pf (Lemma) If $\alpha z = \beta z \bmod p$

$$\alpha z - \beta z = 0 \bmod p$$

$$(\alpha - \beta) \cdot z = 0 \bmod p.$$

$z \neq 0$, p is a prime number.

$$\Rightarrow \alpha - \beta = 0 \bmod p.$$

Remark: When $r = 1$, $x, y \in [p]$, $x \neq y$,

$ax = ay \bmod p \Leftrightarrow a(x-y) = 0 \bmod p$

$\Rightarrow a = 0$. which happens w.p. $\frac{1}{p}$.

When $r > 1$. if $\vec{x}, \vec{y} \in A$ are unequal,
there must exist $i \le r$ s.t. $x_i \neq y_i$.

It suffices to prove

$$a_i x_i + \sum_{j \neq i} a_j x_j = a_i y_i + \sum_{j \neq i} a_j y_j \mod p$$

happens with small prob.

$$a_i (x_i - y_i) = \sum_{j \neq i} a_j (y_j - x_j) \mod p.$$

Let K be $\sum_{j \neq i} a_j (y_j - x_j)$,
we will see that only one value of a_i
makes $a_i (x_i - y_i) = K \mod p$.

Suppose this is not true, then $\exists\, a_i \neq a_i'$ s.t.

$$a_i (x_i - y_i) = a_i' (x_i - y_i) \mod p$$

$\Rightarrow$ ~~a_i~~ $a_i = a_i'$ $\Rightarrow\Leftarrow$.

Hence $\exists!\, a_i$ s.t. $a_i (x_i - y_i) = K \mod p$.

and this happens w.p. $\frac{1}{p}$. ☒