Anagramma

Mostrare che la funzione di hash $h(k) = k \bmod m$, quando $m = 2^p - 1$ e le chiavi k consistono di w parole di p bit è invariante rispetto a permutazioni delle parole costituenti la chiave.

Soluzione. L'osservazione fondamentale è che possiamo vedere la chiave come un numero in base 2^p, con le parole che la costituiscono (che variano nel range $0 \ldots 2^p - 1$ che rappresentano le sue cifre.

Si conclude dunque osservando che dato un numero n espresso in base b e dette $a_k, \ldots, a_1, a_0$ le sue cifre, ovvero

$$n = a_k \ldots a_1 a_0$$

allora

$$n \bmod (b-1) = \Sigma_{j=0}^{k} a_j \bmod (b-1) \tag{1}$$

Da questo deriva immediatamente che se due numeri n_1 e n_2 si ottengono l'uno dall'altro permutando le cifre, dunque hanno cifre identiche, varrà $n_1 \bmod (b-1) = n_2 \bmod (b-1)$.

La proprietà (1) può essere dimostrata per induzione su k.

- $(k = 0)$ Banale.
- $(k \to k+1)$ Sia $n = a_{k+1} a_k \ldots a_1 a_0$. Detto $n' = a_k \ldots a_1 a_0$, per ipotesi induttiva, vale $n' \bmod (b-1) = \Sigma_{j=0}^{k} a_j \bmod (b-1)$. Poiché $n = a_{k+1} b^{k+1} + n'$, utilizzando le semplici proprietà del resto ovvero

  $$(x + y) \bmod b = (x \bmod b + y \bmod b) \bmod b$$
  $$(x \cdot y) \bmod b = (x \bmod b \cdot y \bmod b) \bmod b$$

  abbiamo che

  $$\begin{aligned}
  & n \bmod (b-1) \\
  & = (a_{k+1} b^{k+1} + n') \bmod (b-1) \\
  & = (a_{k+1} b^{k+1} \bmod (b-1) + n' \bmod (b-1)) \bmod (b-1) \\
  & = ((a_{k+1} \bmod (b-1))(b \bmod (b-1))^{k+1}) \bmod (b-1) + n' \bmod (b-1)) \bmod (b-1) \\
  & = ((a_{k+1} \bmod (b-1))1^{k+1}) \bmod (b-1) + n' \bmod (b-1)) \bmod (b-1) \\
  & = (a_{k+1} \bmod (b-1)) + n' \bmod (b-1)) \bmod (b-1) \\
  & = (a_{k+1} \bmod (b-1)) + \Sigma_{j=0}^{k} a_j \bmod (b-1)) \bmod (b-1) \\
  & = \Sigma_{j=0}^{k+1} a_j \bmod (b-1)
  \end{aligned}$$

  e questo conclude la prova.