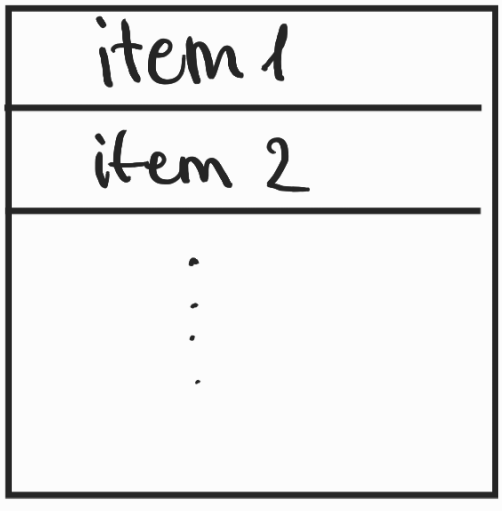
OPEN ADDRESSING, CRYPTOGRAPHIC HASHING

Hashing III

Open addressing
Uniform hashing analysis
Cryptographic hashing

OPEN ADDRESSING -> dealing with collisions

no chaining



one item per slot

$m \geq n$

#slots

#elements

Probing

Hash function specifies order of slots to probe for a key (for insert/search/delete)

$h : U \times \{0, 1, \ldots, m-1\} \to \{0, 1, \ldots, m-1\}$

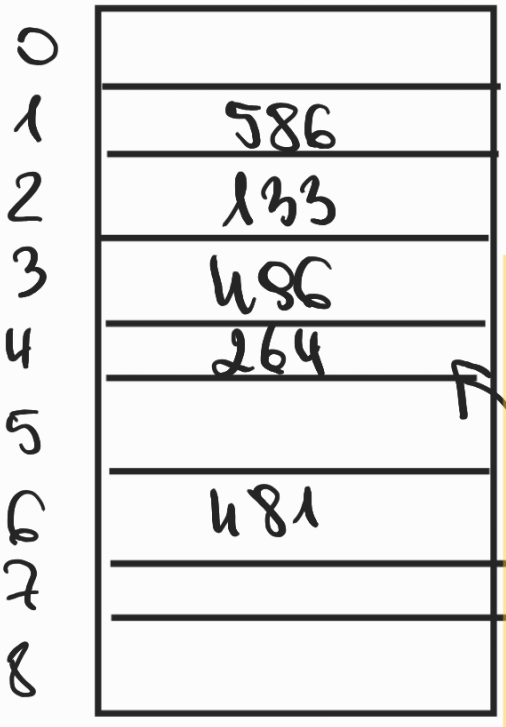
U: universe of keys

trial count

$h(k,1), h(k,2), \ldots h(k,m-1)$

arbitrary key k

to be a permutation of $0, 1, \ldots m-1$



insert 586

$h(586,1) = 1$

$h(481,1) = 6$

insert (496)

$h(496,1) = 4$

UPS, FAIL!

$h(496,2) = 1$

UPS, ALSO FAIL!

$h(496,3) = 3$

None: empty slot

$O(\log)$

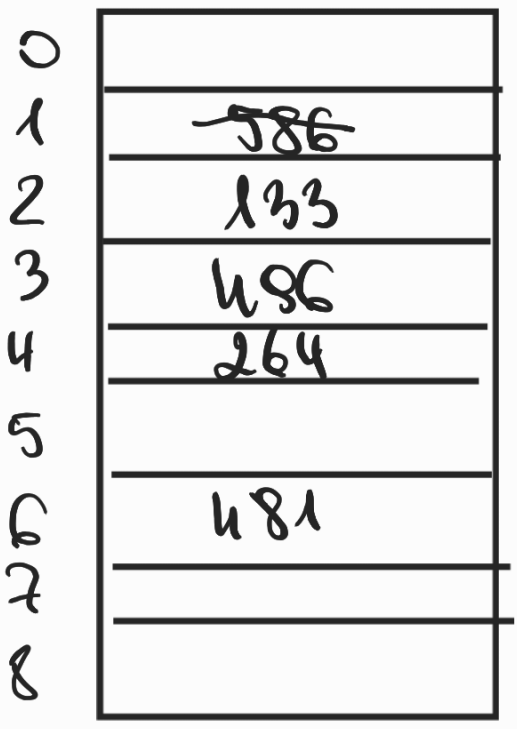
Insert(k, v)

keep probing until an empty slot is found.

Insert item when found

Search(k): as long as the slots encountered are occupied by keys $\neq k$. Keep probing until you either encounter or find an empty slot.

Delete(586)



Search(496)

UPS!

trating me None!

HOW TO FIX IT?

Replace deleted item with DeleteMe flag (different than None)

Insert treats DeleteNe the same as None, but Search keeps going (treats diff from None)

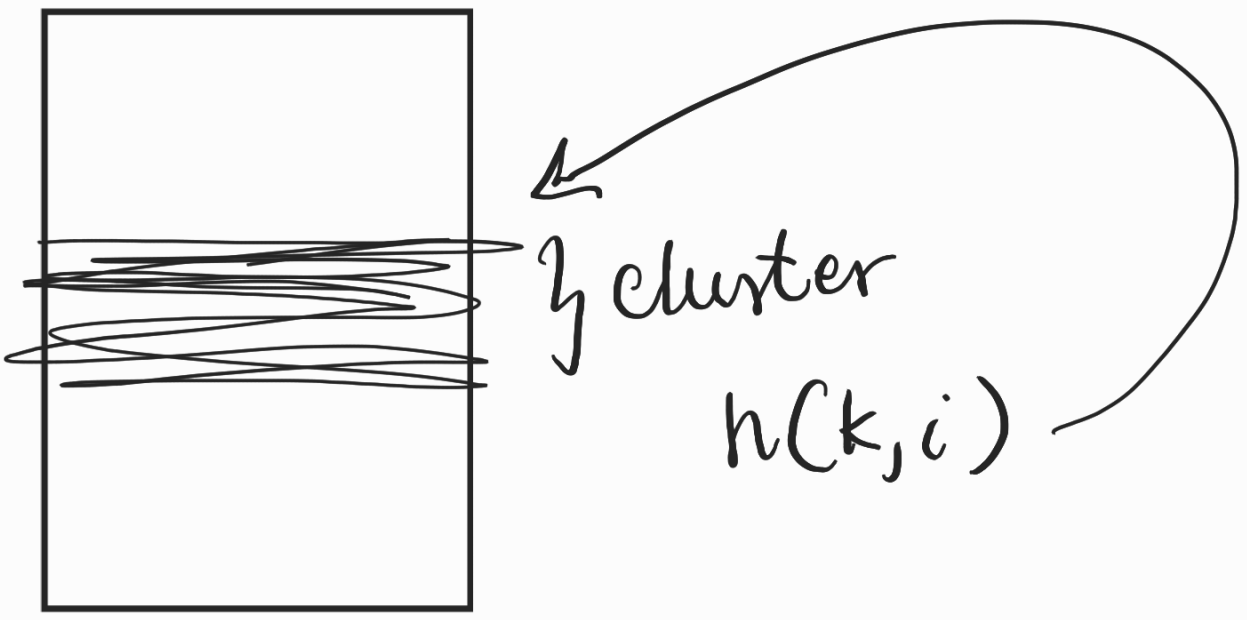
PROBING STRATEGIES

linear probing ← ordinary hash function

$$h(k,i) = (h'(k)+i) \bmod m$$

permutations ✓

cluster:
consecutive groups of occupied slots which keep longer.



$$\alpha = \frac{n}{m} < 0.99$$

$0.01 < \alpha = \frac{n}{m} < 0.99$

$\Theta(\lg n)$ size

DOUBLE HASHING

$$h(k,i) = (h_1(k) + i \cdot h_2(k)) \bmod m$$

if $h_2(k)$ is relatively prime to m => permutation

$m = 2^r$, $h_2(k)$ for all k is odd

Uniform hashing Assumption
≠
Simple Uniform Hashing

Each key is equally likely to have any one of the $m!$ permutations on its probe sequence.

$\alpha = \frac{n}{m}$ Cost of operation insert $\leq \frac{1}{1-\alpha}$

PASSWORD STORAGE

one-way

given $h(x) = Q$ is very hard to find x st $h(x) = Q$