Lemma:
If \( H \) is universal, then for any \( x \in M \) and \( S \subseteq M \), for a random \( h \in H \), \( E[\delta(x, S, h)] \) is \( \leq \frac{|S|}{n} \).

Proof:
\[
E[\delta(x, S, h)] = \frac{1}{|H|} \sum_{h \in H} \delta(x, S, h) \\
= \frac{1}{|H|} \sum_{h \in H} \sum_{y \in S} \delta(x, y, h) \\
= \frac{1}{|H|} \sum_{y \in S} \sum_{h \in H} \delta(x, y, h) \\
\leq \frac{1}{|H|} \sum_{y \in S} \frac{|H|}{n} = \sum_{y \in S} \left( \frac{1}{n} \right) = \frac{|S|}{n}
\]

Theorem:
If a dictionary is implemented using a 2-universal class of hash functions, then the expected time needed to perform \( r \) arbitrary operations is \( \Theta\left(H \frac{s}{n}\right) \) where \( s \) is the total number of inserts.

Construction of a two universal class:
Let \( p \) be a prime number greater than \( m \). Let \( g(x) = x \mod n \) for any \( x \in M \). Let \( F_{a,b}(x) = (ax+b) \mod p \) where \( a \neq 0 \), \( a, b \in \mathbb{Z}_p \). Let \( h_{a,b}(x) = g(F_{a,b}(x)) = ((ax+b) \mod p) \mod n \). Then \( H = \{ h_{a,b}: a \neq 0, a, b \in \mathbb{Z}_p \} \).

Lemma:
For any \( x, y \in M \), \( \delta(Z_p, Z_p, g), (x \neq y) \)

Proof:
This lemma says that \( \delta(x, y, H) \) is equal to the number of pairs \( (r, s) \in Z_p \times Z_p \) (with \( r \neq s \)) s.t. \( r \equiv s \mod n \).
For a given a, b: \( ax \mod p \neq ay \mod p \). Consider \( r, s \in \mathbb{Z}_p \)
if \( ax \equiv r \pmod{p} \) and \( ay \equiv s \pmod{p} \), then we can solve these to get a, b.

**Lemma:**
\( H \) is 2-universal

**Proof:**
For any \( Z \in \mathbb{N} \) let \( A_z = \{ x \in \mathbb{Z}_p : g(x) = Z \} \)
Note that \( |A_z| \leq \left\lfloor \frac{p}{n} \right\rfloor \)
\( \delta(x, y, H) = \delta(Z_p, Z_p, g) \)
\[= p \left( \left\lfloor \frac{p}{n} \right\rfloor - 1 \right) \approx \frac{p(p-1)}{n} \]
Since \( |H| = p(p-1) \), \( \delta(x, y, H) \leq \left\lfloor \frac{|H|}{n} \right\rfloor \)
Note: any \( h \in H \) can be described with \( O(\log m) \) bits.

**Fact:**
For any integer \( m \), there exists a prime number in the range \([m, 2m]\)
Note: we can also design k-universal class of hash functions in a similar way.

**Searching in O(1) time:**
Input: \( k_1, k_2, \ldots, k_n \in M = \{0, 1, 2, \ldots, m-1\} \)
Goal: develop a static data structure where a search takes \( O(1) \) time in the worst case.

Idea: use two levels of hashing
Let \( p=(m+1) \) be a prime without loss of generality.
Let \( N = \{0, 1, 2, \ldots, n-1\} \).
Let \( S \subseteq M \) be any input set with \( |S|=s \)
For any \( 1 \leq k \leq (p-1) \) let \( h_k(x) = (kx \mod p) \mod n \)

Let \( B_i(k,n,s) \) be the set of elements of \( S \) that have a hash value \( i \) under \( h_k \)
\( B_i(k,n,s) = \{ x \in S : h_k(x) = i \} \), \( i = \{0, 1, 2, \ldots, n-1\} \)
Lemma:
\[
\sum_{k=1}^{p-1} \sum_{i=0}^{n-1} \binom{Bi(k,n,s)}{2} \leq \frac{ms^2}{n}
\]

The number of \( \binom{Bi(k,n,s)}{2} \) is nothing but pairs \{x,y\} from S s.t. they collide under \( h_k \) and \( h_k(x) = i \)
\[
\sum_{i=0}^{n-1} \binom{Bi(k,n,s)}{2}
\]
is nothing but the number of pairs \{x,y\} from S that collide under \( h_k \)
\[
\sum_{k=1}^{p-1} \sum_{i=0}^{n-1} \binom{Bi(k,n,s)}{2}
\]
is nothing but the number of tuples \( (k,\{x,y\}) \) s.t. \( x \) and \( y \) collide under \( h_k \).

\( x \) and \( y \) collide under \( h_k \) if:
\[
K(x-y) \mod p \equiv 0 \mod n
\]

\( K(x-y) \mod p \in \{0, \pm n, \pm 2n, \ldots, \pm \left\lfloor \frac{p-1}{n} \right\rfloor n \} \)

Consider the equation \( k(x-y) \mod p = jn \) for a given \( j \), the above equation can be solved to get a unique value for \( k \).

For a given \( x \) and \( y \) there are \( \frac{2(p-1)}{n} \) values for \( k \) s.t. \( x \) and \( y \) collide under \( h_k \)

There are \( \binom{s}{2} \) values for the pair \( (x,y) \)
\[
\sum_{k=1}^{p-1} \sum_{i=0}^{n-1} \binom{Bi(k,n,s)}{2} \leq \frac{2(p-1)}{n} \cdot \frac{s^2}{2} \approx \frac{ms^2}{n}
\]

Corollary:
For any \( S \subseteq M \), \( \exists k \), s.t. \( \sum_{i=0}^{n-1} \binom{Bi(k,n,s)}{2} \leq \frac{s^2}{n} \).