Hashing

Thanks to
Prof. Charles E. Leiserson

Symbol-table problem

Symbol table $T$ holding $n$ records:

Operations on $T$:

- INSERT($T$, $x$)
- DELETE($T$, $x$)
- SEARCH($T$, $k$)

How should the data structure $T$ be organized?

Hash functions

Idea: Use a hash function $h$ to map the universe $U$ of all keys into $\{0, 1, \ldots, m-1\}$:

When a record to be inserted maps to an already occupied slot in $T$, a collision occurs.
Resolving collisions by chaining

• Records in the same slot are linked into a list.

![Diagram](image)

$h(49) = h(86) = h(52) = i$

Analysis of chaining

We make the assumption of simple uniform hashing:

• Each key $k \in K$ of keys is equally likely to be hashed to any slot of table $T$, independent of where other keys are hashed.

Let $n$ be the number of keys in the table, and let $m$ be the number of slots.

Define the load factor of $T$ to be

$$\alpha = \frac{n}{m} = \text{average number of keys per slot}.$$  

Search cost

Expected time to search for a record with a given key $= \Theta(1 + \alpha)$.

- apply hash function and access slot
- search the list

Expected search time $= \Theta(1)$ if $\alpha = O(1)$, or equivalently, if $n = O(m)$. 
Choosing a hash function

The assumption of simple uniform hashing is hard to guarantee, but several common techniques tend to work well in practice as long as their deficiencies can be avoided.

Desirata:
• A good hash function should distribute the keys uniformly into the slots of the table.
• Regularity in the key distribution should not affect this uniformity.
• Hope: if \( k_1 \neq k_2 \) in any bit, then \( h(k_1) \neq h(k_2) \)

Division method

Assume all keys are integers, and define

\[ h(k) = k \mod m. \]

Deficiency: Don’t pick an \( m \) that has a small divisor \( d \). A preponderance of keys that are congruent modulo \( d \) can adversely affect uniformity.

Extreme deficiency: If \( m = 2^r \), then the hash doesn’t even depend on all the bits of \( k \):
• If \( k = 1011000111011010 \) and \( r = 6 \), then \( h(k) = 011010 \).

Division method (continued)

\[ h(k) = k \mod m. \]

Pick \( m \) to be a prime not too close to a power of 2 or 10 and not otherwise used prominently in the computing environment.

Annoyance:
• Sometimes, making the table size a prime is inconvenient.

But, this method is popular, although the next method we’ll see is usually superior.
**Multiplication method**

Assume that all keys are integers, \( m = 2^r \), and our computer has \( w \)-bit words. Define

\[ h(k) = (A \cdot k \mod 2^w) \text{ rsh } (w - r), \]

where \text{ rsh } is the “bit-wise right-shift” operator and \( A \) is an odd integer in the range \( 2^{w-1} < A < 2^w \).

- Don’t pick \( A \) too close to \( 2^w \).
- Multiplication modulo \( 2^w \) is fast.
- The \text{ rsh } operator is fast.

---

**Multiplication method example**

\[ h(k) = (A \cdot k \mod 2^w) \text{ rsh } (w - r) \]

Suppose that \( m = 8 = 2^3 \) and that our computer has \( w = 7 \)-bit words:

\[
\begin{array}{c}
1 & 0 & 1 & 1 & 0 & 0 & 1 \\
\times & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\
\hline
1 & 0 & 0 & 1 & 0 & 0 & 1 & 1
\end{array}
\]

- \( A \)
- \( h(k) \)
- \( 2A \)

**Dot-product method**

**Randomized strategy:**

Let \( m \) be prime. Decompose key \( k \) into \( r + 1 \) digits, each with value in the set \( \{0, 1, \ldots, m-1\} \).

That is, let \( k = (k_0, k_1, \ldots, k_r) \), where \( 0 \leq k_i < m \).

E.g. \( m=256 \) implies breaking into single characters.

Pick \( a = (a_0, a_1, \ldots, a_r) \) where each \( a_i \) is chosen randomly from \( \{0, 1, \ldots, m-1\} \).

Define \( h_a(k) = \sum_{i=0}^{r} (a_i \cdot k_i) \mod m \)

- Excellent in practice, but expensive to compute.
Resolving collisions by open addressing - cont

No storage is used outside of the hash table itself.

• The probe sequence \( h(k,0), h(k,1), \ldots, h(k,m-1) \) should be a permutation of \( \{0, 1, \ldots, m-1\} \).

• The table may fill up, and deletion is difficult (but not impossible).

Resolving collisions by open addressing

No storage is used outside of the hash table itself.

• The hash function depends on both the key and probe number:
  \[ h : U \times \{0, 1, \ldots, m-1\} \to \{0, 1, \ldots, m-1\}, \]
  E.g. \( h(k,i) = (k+i) \mod m \)

Inserting a key \( k \):
we check \( T[h(k,0)] \). If empty we insert \( k \) there. Otherwise, we check \( T[h(k,1)] \). If empty we insert \( k \) there. Otherwise,… otherwise etc for \( h(k,2), h(k,3), \ldots, h(k,m-1) \).

Finding a key \( k \):
we check if \( T[h(k,0)] = k \). If not, if empty, stop. otherwise we check if \( T[h(k,1)] = k \). If not, if empty, stop. otherwise etc for \( h(k,2), h(k,3), \ldots, h(k,m-1) \).

Deletion is interesting (wait for it)

Example of open addressing

Insert key \( k = 496 \):

0. Probe \( h(496,0) \)

\[ T \]

\[ \begin{array}{cccc}
0 & 131 & 304 & 481 \\
586 & collision & & \\
\end{array} \]

\( m-1 \)
Example of open addressing

Insert key $k = 496$:

0. Probe $h(496,0)$
1. Probe $h(496,1)$

Search for key $k = 496$:

0. Probe $h(496,0)$
1. Probe $h(496,1)$
2. Probe $h(496,2)$

Search uses the same probe sequence, terminating successfully if it finds the key and unsuccessfully if it encounters an empty slot.
Deletion

To delete(k), find it and replace it with a dummy (also refer to as 'NULL' or a 'gravestone')

During search(k), a cell containing a dummy is not considered empty. But
During insert (k), a cell containing a dummy is considered empty. But

Deletion and Maintenance

Scan the table from time to time, and get rid of all of all dummies.
If the load factor is too high, allocate a larger array, pick a new hash function and copy non-dummies into the new array)

Probing strategies

Linear probing:  
Given an ordinary hash function h'(k), linear probing uses the hash function

\[ h(k,i) = (h'(k) + i) \mod m. \]

This method, though simple, suffers from primary clustering, where long runs of occupied slots build up, increasing the average search time. Moreover, the long runs of occupied slots tend to get longer.
**Probing strategies**

**Double hashing**

Given two ordinary hash functions $h_1(k)$ and $h_2(k)$, double hashing uses the hash function

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

This method generally produces excellent results, but $h_2(k)$ must be relatively prime to $m$. One way is to make $m$ a power of 2 and design $h_2(k)$ to produce only odd numbers.

**Analysis of open addressing**

We make the assumption of *uniform hashing*:

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

**Theorem.** Given an open-addressed hash table with load factor $\alpha = n/m < 1$, the expected number of probes in an unsuccessful search is at most $1/(1-\alpha)$.

**Proof of the theorem**

*Proof.*

• At least one probe is always necessary.
• With probability $n/m$, the first probe hits an occupied slot, and a second probe is necessary.
• With probability $(n-1)/(m-1)$, the second probe hits an occupied slot, and a third probe is necessary.
• With probability $(n-2)/(m-2)$, the third probe hits an occupied slot, etc.

Observe that $\frac{n-i}{m-i} < \frac{n}{m} = \alpha$ for $i = 1, 2, \ldots, n$. 

Proof (continued)

Therefore, the expected number of probes is

\[
1 + \frac{n}{m} \left( 1 + \frac{n-1}{m-1} \left( 1 + \frac{n-2}{m-2} \left( \cdots \left( 1 + \frac{1}{m-n+1} \right) \cdots \right) \right) \right)
\]

\[
\leq 1 + \alpha \left( 1 + \alpha \left( 1 + \alpha \left( \cdots \left( 1 + \alpha \right) \cdots \right) \right) \right)
\]

\[
\leq 1 + \alpha + \alpha^2 + \alpha^3 + \cdots
\]

\[
= \sum_{i=0}^{\infty} \alpha^i = \frac{1}{1-\alpha} \quad \text{The textbook has a more rigorous proof.}
\]

Implications of the theorem

• If \( \alpha \) is constant, then accessing an open-addressed hash table takes constant time.
• If the table is half full, then the expected number of probes is \( 1/(1-0.5) = 2 \).
• If the table is 90% full, then the expected number of probes is \( 1/(1-0.9) = 10 \).

Fact from number theory

\textbf{Theorem.} Let \( m \) be prime, and let \( A, z \) be integers \( 0 < A < m \).

Then in the sequence \( iA \pmod{m} \) each number appears exactly once \( (i=1, 2, \ldots, m-1) \).

In other words, for every \( z \), there is exactly one \( 0 \leq i < m \) such that \( iA \equiv z \pmod{m} \).

\textbf{Example:} \( m = 7, \ A = 3 \)

\[
\begin{array}{c|ccccccc}
    i & 1 & 2 & 3 & 4 & 5 & 6 \\
    \hline
    iA & 3 & 6 & 2 & 5 & 1 & 4 \\
\end{array}
\]
A weakness of hashing

**Problem:** For any hash function $h$, a set of keys exists that can cause the average access time of a hash table to skyrocket.

- An adversary can pick all keys from $\{k \in U : h(k) = i\}$ for some slot $i$.

**IDEA:** Choose the hash function at random, independently of the keys.

- Even if an adversary can see your code, he or she cannot find a bad set of keys, since he or she does not know exactly which hash function will be chosen.

---

Universal hashing

**Definition.** Let $U$ be a universe of keys, and let $H = \{h_1, \ldots, h_B\}$ be a finite collection of $|H|$ hash functions. Each $h_i$ is a function mapping $U$ to $\{0, 1, \ldots, m-1\}$.

We say $H$ is **universal** if for all $x, y \in U$, where $x \neq y$, we have $|\{h \in H : h(x) = h(y)\}| \leq |H| / m$.

That is, the chance of a collision between $x$ and $y$ is $\leq 1/m$ if we choose $h$ randomly from $H$.

Yet another way to visualize it: We say that $h$ is a bad member of $H$ (bad for $x$ and $y$) if $h(x) = h(y)$.

$H$ is universal if of the percentage of bad members $\leq 1/m$.

---

Why Universality is Good

- Assume $h \in H$ is a hash function, Let $K$ be a set of $n$ pairwise-different keys, and $x, y$ are two different keys of $K$.
- Assume $n = n/m < 0.5$. Pick at random $h \in H$. Let $x \in K$.
- **Theorem:** The expected number of keys in $K$ that collide with $x$ is $\leq 0.5$.
- **Proof:** Let us define a "flag" $\mathcal{F}(x, y)$ which is 1 if $h(x) = h(y)$, and 0 otherwise.

The number of keys in $K$ that $h$ maps to the same slot it maps $x$ to is $\sum_{y \in K} \mathcal{F}(x, y)$. This is the number of collisions that $x$ "suffers."

- Let $\mu = |K|$. The average number of collisions that $x$ suffers, when $h \in H$ is picked randomly is

$$\mathbb{E}[\sum_{y \in K} \mathcal{F}(x, y)] = \frac{\mu}{m} \mu (\frac{1}{m}) = \frac{\mu^2}{m} = \frac{n}{m} \cdot \frac{1}{2} = \frac{n}{2m}$$

$\Box$
Constructing Universal Families

Let \( m \) be prime. Decompose key \( k \) into \( r + 1 \) digits, each with value in the set \( \{0, 1, \ldots, m-1\} \). That is, let \( k = \langle k_0, k_1, \ldots, k_r \rangle \), where \( 0 \leq k_i < m \).

**Randomized strategy:**

Pick \( a = \langle a_0, a_1, \ldots, a_r \rangle \) where each \( a_i \) is chosen randomly from \( \{0, 1, \ldots, m-1\} \).

Define \( h_a(k) = \sum_{i=0}^{r} a_i k_i \mod m \).

**Dot product, modulo \( m \)**

How big is \( H = \{ h_a \} \)? \( |H| = m^{r+1} \). ← REMEMBER THIS!

---

**Congruence**

A definition that actually saves lots of ink

we write

\[ a \equiv b \mod n \]

and read this as “\( a \) is congruent to \( b \) modulo \( n \)” if \( a \mod n = b \mod n \)

So \( 11 \equiv 1 \mod 10 \)

\( 1 \equiv 11 \mod 10 \)
\( 21 \equiv 1 \mod 10 \)
\( 27 \equiv 17 \mod 10 \)

etc
**Universality of dot-product hash functions**

**Theorem.** The set $H = \{h_a\}$ is universal.

**Proof.** Suppose that $x = (x_0, x_1, \ldots, x_r)$ and $y = (y_0, y_1, \ldots, y_r)$ be distinct keys. Thus, they differ in at least one digit position, wlog $x_0 \neq y_0$.

For how many $h_a \in H$ do $x$ and $y$ collide?

We must have $h_a(x) = h_a(y)$, which implies that

$$\sum_{i=0}^r a_i x_i \equiv \sum_{i=0}^r a_i y_i \pmod{m}.$$

**Proof (continued)**

Equivalently, we have

$$\sum_{i=0}^r a_i (x_i - y_i) \equiv 0 \pmod{m}$$

or

$$a_0 (x_0 - y_0) + \sum_{i=1}^r a_i (x_i - y_i) \equiv 0 \pmod{m},$$

which implies that

$$a_0 (x_0 - y_0) \equiv -\sum_{i=1}^r a_i (x_i - y_i) \pmod{m}.$$

**Fact from number theory**

**Theorem.** Let $m$ be prime, and let $A, \nu$ be integers $0 < A < m$, $0 \leq \nu < m$.

Then in the sequence $i A \pmod{m}$ each number appears exactly once ($i = 1, 2, \ldots, m-1$).

In other words, for every $z$, there is exactly one $0 \leq i < m$ such that

$$i A \equiv z \pmod{m}.$$  

**Example:** $m = 7$, $A = 3$

<table>
<thead>
<tr>
<th>$i$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i A$</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>
Back to the proof

We have

\[ a_0(x_0 - y_0) \equiv -\sum_{i=1}^{r} a_i(x_i - y_i) \mod m \]

We already decided about the values of all \( a_i \) excluding \( a_0 \).

Thus, for any choices of \( a_1, a_2, \ldots, a_r \), **exactly one** choice of \( a_0 \) causes \( x \) and \( y \) to collide.

Proof (completed)

**Q.** How many \( h_a \)'s cause \( x \) and \( y \) to collide?

**A.** There are \( m \) choices for each of \( a_1, a_2, \ldots, a_r \), but once these are chosen, exactly one choice for \( a_0 \) causes \( x \) and \( y \) to collide, namely

\[ a_0(x_0 - y_0) \equiv -\sum_{i=1}^{r} a_i(x_i - y_i) \mod m \]

Thus, the number of \( h_a \)'s that cause \( x \) and \( y \) to collide is \( m^r \cdot 1 = m^r = |H|/m \). □

Proof (completed)

**Q.** How many \( h_a \)'s cause \( x \) and \( y \) to collide?

**A.** There are \( m \) choices for each of \( a_1, a_2, \ldots, a_r \), but once these are chosen, exactly one choice for \( a_0 \) causes \( x \) and \( y \) to collide, namely

\[ a_0(x_0 - y_0) \equiv -\sum_{i=1}^{r} a_i(x_i - y_i) \mod m \]

Thus, the number of \( h_a \)'s that cause \( x \) and \( y \) to collide is \( m^r \cdot 1 = m^r = |H|/m \). □