Hashing

Lecture 15

March 13, 2013

Part I

Hash Tables

Dictionary Data Structure

1. $\mathcal{U}$: universe of keys with total order: numbers, strings, etc.
2. Data structure to store a subset $\mathbf{S} \subseteq \mathcal{U}$
3. **Operations:**
    1. **Search/lookup**: given $\mathbf{x} \in \mathcal{U}$ is $\mathbf{x} \in \mathbf{S}$?
    2. **Insert**: given $\mathbf{x} \not\in \mathbf{S}$ add $\mathbf{x}$ to $\mathbf{S}$.
    3. **Delete**: given $\mathbf{x} \in \mathbf{S}$ delete $\mathbf{x}$ from $\mathbf{S}$
4. **Static** structure: $\mathbf{S}$ given in advance or changes very infrequently, main operations are lookups.
5. **Dynamic** structure: $\mathbf{S}$ changes rapidly so inserts and deletes as important as lookups.

Dictionary Data Structures

Common solutions:

1. Static:
   1. Store $\mathbf{S}$ as a *sorted* array
   2. **Lookup**: Binary search in $\mathbf{O(\log |S|)}$ time (comparisons)
2. Dynamic:
   1. Store $\mathbf{S}$ in a *balanced* binary search tree
   2. Lookup, Insert, Delete in $\mathbf{O(\log |S|)}$ time (comparisons)

Dictionary Data Structures

Question: "Should Tables be Sorted?"
(also title of famous paper by Turing award winner Andy Yao)

Hashing is a widely used & powerful technique for dictionaries.

Motivation:

1. Universe $\mathcal{U}$ may not be (naturally) totally ordered.
2. Keys correspond to large objects (images, graphs etc) for which comparisons are very expensive.
3. Want to improve "average" performance of lookups to $O(1)$ even at cost of extra space or errors with small probability: many applications for fast lookups in networking, security, etc.

Dictionary Data Structures

Question: "Should Tables be Sorted?"
(also title of famous paper by Turing award winner Andy Yao)

Hashing is a widely used & powerful technique for dictionaries.

Motivation:

1. Universe $\mathcal{U}$ may not be (naturally) totally ordered.
2. Keys correspond to large objects (images, graphs etc) for which comparisons are very expensive.
3. Want to improve "average" performance of lookups to $\mathbf{O(1)}$ even at cost of extra space or errors with small probability: many applications for fast lookups in networking, security, etc.

Hashing and Hash Tables

Hash Table data structure:

1. A (hash) table/array $\mathbf{T}$ of size $\mathbf{m}$ (the table **size**).
2. A hash function $\mathbf{h} : \mathcal{U} \to \{0, \ldots, \mathbf{m} - 1\}$.
3. Item $\mathbf{x} \in \mathcal{U}$ hashes to slot $\mathbf{h(x)}$ in $\mathbf{T}$.

Given $\mathbf{S} \subseteq \mathcal{U}$. How do we store $\mathbf{S}$ and how do we do lookups?

Ideal situation:

1. Each element $\mathbf{x} \in \mathbf{S}$ hashes to a distinct slot in $\mathbf{T}$. Store $\mathbf{x}$ in slot $\mathbf{h(x)}$
2. **Lookup**: Given $\mathbf{y} \in \mathcal{U}$ check if $\mathbf{T[h(y)] = y}$. $\mathbf{O(1)}$ time!

Collisions unavoidable. Several different techniques to handle them.

Hashing and Hash Tables

Hash Table data structure:

1. A (hash) table/array $\mathbf{T}$ of size $\mathbf{m}$ (the table **size**).
2. A hash function $\mathbf{h} : \mathcal{U} \to \{0, \ldots, \mathbf{m} - 1\}$.
3. Item $\mathbf{x} \in \mathcal{U}$ hashes to slot $\mathbf{h(x)}$ in $\mathbf{T}$.

Given $\mathbf{S} \subseteq \mathcal{U}$. How do we store $\mathbf{S}$ and how do we do lookups?

Ideal situation:

1. Each element $\mathbf{x} \in \mathbf{S}$ hashes to a distinct slot in $\mathbf{T}$. Store $\mathbf{x}$ in slot $\mathbf{h(x)}$
2. **Lookup**: Given $\mathbf{y} \in \mathcal{U}$ check if $\mathbf{T[h(y)] = y}$. $\mathbf{O(1)}$ time!

Collisions unavoidable. Several different techniques to handle them.

Hashing and Hash Tables

Hash Table data structure:

1. A (hash) table/array $\mathbf{T}$ of size $\mathbf{m}$ (the table **size**).
2. A hash function $\mathbf{h} : \mathcal{U} \rightarrow \{0, \ldots, m-1\}$.
3. Item $\mathbf{x} \in \mathcal{U}$ hashes to slot $\mathbf{h(x)}$ in $\mathbf{T}$.

Given $\mathbf{S} \subseteq \mathcal{U}$. How do we store $\mathbf{S}$ and how do we do lookups?

Ideal situation:

1. Each element $\mathbf{x} \in \mathbf{S}$ hashes to a distinct slot in $\mathbf{T}$. Store $\mathbf{x}$ in slot $\mathbf{h(x)}$
2. **Lookup**: Given $\mathbf{y} \in \mathcal{U}$ check if $\mathbf{T[h(y)] = y}$. $\mathbf{O(1)}$ time!

Collisions unavoidable. Several different techniques to handle them.

Hashing and Hash Tables

Hash Table data structure:

1. A (hash) table/array $\mathbf{T}$ of size $\mathbf{m}$ (the table **size**).
2. A hash function $\mathbf{h} : \mathcal{U} \rightarrow \{\mathbf{0}, \ldots, \mathbf{m} - \mathbf{1}\}$.
3. Item $\mathbf{x} \in \mathcal{U}$ hashes to slot $\mathbf{h(x)}$ in $\mathbf{T}$.

Given $\mathbf{S} \subseteq \mathcal{U}$. How do we store $\mathbf{S}$ and how do we do lookups?

Ideal situation:

1. Each element $\mathbf{x} \in \mathbf{S}$ hashes to a distinct slot in $\mathbf{T}$. Store $\mathbf{x}$ in slot $\mathbf{h(x)}$
2. **Lookup**: Given $\mathbf{y} \in \mathcal{U}$ check if $\mathbf{T[h(y)] = y}$. $\mathbf{O(1)}$ time!

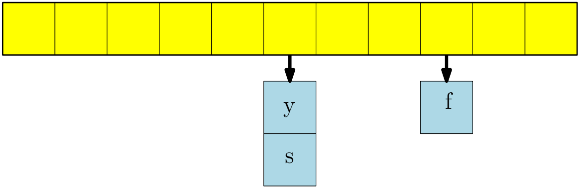
Collisions unavoidable. Several different techniques to handle them.

Handling Collisions: Chaining

Collision: $\mathbf{h(x) = h(y)}$ for some $\mathbf{x \neq y}$.

Chaining to handle collisions:

1. For each slot $\mathbf{i}$ store all items hashed to slot $\mathbf{i}$ in a linked list. $\mathbf{T[i]}$ points to the linked list
2. **Lookup**: to find if $\mathbf{y} \in \mathcal{U}$ is in $\mathbf{T}$, check the linked list at $\mathbf{T[h(y)]}$. Time proportion to size of linked list.



This is also known as **Open hashing**.

Handling Collisions

Several other techniques:

1. Open addressing.
   Every element has a list of places it can be (in certain order). Check in this order.
2. ...
3. Cuckoo hashing.
   Every value has two possible locations. When inserting, insert in one of the locations, otherwise, kick stored value to its other location. Repeat till stable. if no stability then rebuild table.
4. Others.

Understanding Hashing

Does hashing give $\mathbf{O(1)}$ time per operation for dictionaries?

Questions:

1. Complexity of evaluating $\mathbf{h}$ on a given element?
2. Relative sizes of the universe $\mathcal{U}$ and the set to be stored $\mathbf{S}$.
3. Size of table relative to size of $\mathbf{S}$.
4. Worst-case vs average-case vs randomized (expected) time?
5. How do we choose $\mathbf{h}$?

Understanding Hashing

Does hashing give $\mathbf{O(1)}$ time per operation for dictionaries?

Questions:

1. Complexity of evaluating $\mathbf{h}$ on a given element?
2. Relative sizes of the universe $\mathcal{U}$ and the set to be stored $\mathbf{S}$.
3. Size of table relative to size of $\mathbf{S}$.
4. Worst-case vs average-case vs randomized (expected) time?
5. How do we choose $\mathbf{h}$?

Understanding Hashing

1. Complexity of evaluating $\mathbf{h}$ on a given element? Should be small.
2. Relative sizes of the universe $\mathcal{U}$ and the set to be stored $\mathbf{S}$: typically $|\mathcal{U}| \gg |\mathbf{S}|$.
3. Size of table relative to size of $\mathbf{S}$. The **load factor** of $\mathbf{T}$ is the ratio $\mathbf{n/t}$ where $\mathbf{n} = |\mathbf{S}|$ and $\mathbf{m} = |\mathbf{T}|$. Typically $\mathbf{n/t}$ is a small constant smaller than $\mathbf{1}$.
   Also known as the **fill factor**.

Main and interrelated questions:

1. Worst-case vs average-case vs randomized (expected) time?
2. How do we choose $\mathbf{h}$?

Understanding Hashing

1. Complexity of evaluating $\mathbf{h}$ on a given element? Should be small.
2. Relative sizes of the universe $\mathcal{U}$ and the set to be stored $\mathbf{S}$: typically $|\mathcal{U}| \gg |\mathbf{S}|$.
3. Size of table relative to size of $\mathbf{S}$. The **load factor** of $\mathbf{T}$ is the ratio $\mathbf{n}/\mathbf{t}$ where $\mathbf{n} = |\mathbf{S}|$ and $\mathbf{m} = |\mathbf{T}|$. Typically $\mathbf{n}/\mathbf{t}$ is a small constant smaller than $\mathbf{1}$.
   Also known as the **fill factor**.

Main and interrelated questions:

1. Worst-case vs average-case vs randomized (expected) time?
2. How do we choose $\mathbf{h}$?

Single hash function

1. $\mathcal{U}$: universe (very large).
2. Assume $\mathbf{N} = |\mathcal{U}| \gg \mathbf{m}$ where $\mathbf{m}$ is size of table $\mathbf{T}$. In particular assume $\mathbf{N} \geq \mathbf{m}^2$ (very conservative).
3. Fix hash function $\mathbf{h} : \mathcal{U} \to \{0, \ldots, \mathbf{m} - 1\}$.
4. $\mathbf{N}$ items hashed to $\mathbf{m}$ slots. By pigeon hole principle there is some $\mathbf{i} \in \{0, \ldots, \mathbf{m} - 1\}$ such that $\mathbf{N}/\mathbf{m} \geq \mathbf{m}$ elements of $\mathcal{U}$ get hashed to $\mathbf{i}$ (!).
5. Implies that there is a set $\mathbf{S} \subseteq \mathcal{U}$ where $|\mathbf{S}| = \mathbf{m}$ such that all of $\mathbf{S}$ hashes to same slot. Ooops.

Lesson: For every hash function there is a very bad set. Bad set. Bad.

Single hash function

1. $\mathcal{U}$: universe (very large).
2. Assume $\mathbf{N} = |\mathcal{U}| \gg \mathbf{m}$ where $\mathbf{m}$ is size of table $\mathbf{T}$. In particular assume $\mathbf{N} \geq \mathbf{m}^2$ (very conservative).
3. Fix hash function $\mathbf{h} : \mathcal{U} \rightarrow \{\mathbf{0}, \ldots, \mathbf{m} - \mathbf{1}\}$.
4. $\mathbf{N}$ items hashed to $\mathbf{m}$ slots. By pigeon hole principle there is some $\mathbf{i} \in \{\mathbf{0}, \ldots, \mathbf{m} - \mathbf{1}\}$ such that $\mathbf{N}/\mathbf{m} \geq \mathbf{m}$ elements of $\mathcal{U}$ get hashed to $\mathbf{i}$ (!).
5. Implies that there is a set $\mathbf{S} \subseteq \mathcal{U}$ where $|\mathbf{S}| = \mathbf{m}$ such that all of $\mathbf{S}$ hashes to same slot. Ooops.

Lesson: For every hash function there is a very bad set. Bad set. Bad.

Picking a hash function

1. Hash function are often chosen in an ad hoc fashion. Implicit assumption is that input behaves well.
2. Theory and sound practice suggests that a hash function should be chosen properly with guarantees on its behavior.

Parameters: $\mathbf{N} = |\mathcal{U}|$, $\mathbf{m} = |\mathbf{T}|$, $\mathbf{n} = |\mathbf{S}|$

1. $\mathcal{H}$ is a **family** of hash functions: each function $\mathbf{h} \in \mathcal{H}$ should be efficient to evaluate (that is, to compute $\mathbf{h}(\mathbf{x})$).
2. $\mathbf{h}$ is chosen **randomly** from $\mathcal{H}$ (typically uniformly at random). Implicitly assumes that $\mathcal{H}$ allows an efficient sampling.
3. Randomized guarantee: should have the property that for any *fixed* set $\mathbf{S} \subseteq \mathcal{U}$ of size $\mathbf{m}$ the expected number of collisions for a function chosen from $\mathcal{H}$ should be "small". Here the expectation is over the randomness in choice of $\mathbf{h}$.

Picking a hash function

1. Hash function are often chosen in an ad hoc fashion. Implicit assumption is that input behaves well.
2. Theory and sound practice suggests that a hash function should be chosen properly with guarantees on its behavior.

Parameters: $\mathbf{N} = |\mathcal{U}|$, $\mathbf{m} = |\mathbf{T}|$, $\mathbf{n} = |\mathbf{S}|$

1. $\mathcal{H}$ is a **family** of hash functions: each function $\mathbf{h} \in \mathcal{H}$ should be efficient to evaluate (that is, to compute $\mathbf{h(x)}$).
2. $\mathbf{h}$ is chosen **randomly** from $\mathcal{H}$ (typically uniformly at random). Implicitly assumes that $\mathcal{H}$ allows an efficient sampling.
3. Randomized guarantee: should have the property that for any *fixed* set $\mathbf{S} \subseteq \mathcal{U}$ of size $\mathbf{m}$ the expected number of collisions for a function chosen from $\mathcal{H}$ should be "small". Here the expectation is over the randomness in choice of $\mathbf{h}$.

Picking a hash function

Question: Why not let $\mathcal{H}$ be the set of *all* functions from $\mathcal{U}$ to $\{0, 1, \ldots, m-1\}$?

1. Too many functions! A random function has high complexity!
   # of functions: $M = m^{|\mathcal{U}|}$.
   Bits to encode such a function $\approx \log M = |\mathcal{U}| \log m$.

Question: Are there good and compact families $\mathcal{H}$?

1. Yes... But what it means for $\mathcal{H}$ to be good and compact.

Picking a hash function

Question: Why not let $\mathcal{H}$ be the set of *all* functions from $\mathcal{U}$ to $\{0, 1, \ldots, m-1\}$?

1. Too many functions! A random function has high complexity!
   \# of functions: $\mathbf{M} = \mathbf{m}^{|\mathcal{U}|}$.
   Bits to encode such a function $\approx \log \mathbf{M} = |\mathcal{U}| \log \mathbf{m}$.

Question: Are there good and compact families $\mathcal{H}$?

1. Yes... But what it means for $\mathcal{H}$ to be good and compact.

Picking a hash function

Question: Why not let $\mathcal{H}$ be the set of *all* functions from $\mathcal{U}$ to $\{0, 1, \ldots, m-1\}$?

1. Too many functions! A random function has high complexity!
   # of functions: $\mathbf{M} = \mathbf{m}^{|\mathcal{U}|}$.
   Bits to encode such a function $\approx \log \mathbf{M} = |\mathcal{U}| \log \mathbf{m}$.

Question: Are there good and compact families $\mathcal{H}$?

1. Yes... But what it means for $\mathcal{H}$ to be good and compact.

Picking a hash function

Question: Why not let $\mathcal{H}$ be the set of *all* functions from $\mathcal{U}$ to $\{0, 1, \ldots, m-1\}$?

1. Too many functions! A random function has high complexity!
   \# of functions: $\mathbf{M} = \mathbf{m}^{|\mathcal{U}|}$.
   Bits to encode such a function $\approx \log \mathbf{M} = |\mathcal{U}| \log \mathbf{m}$.

Question: Are there good and compact families $\mathcal{H}$?

1. Yes... But what it means for $\mathcal{H}$ to be good and compact.

Uniform hashing

Question: What are good properties of $\mathcal{H}$ in distributing data?

1. Consider any element $x \in \mathcal{U}$. Then if $h \in \mathcal{H}$ is picked randomly then x should go into a random slot in T. In other words $\Pr[h(x) = i] = 1/m$ for every $0 \le i < m$.
2. Consider any two distinct elements $x, y \in \mathcal{U}$. Then if $h \in \mathcal{H}$ is picked randomly then the probability of a collision between x and y should be at most $1/m$. In other words $\Pr[h(x) = h(y)] = 1/m$ (cannot be smaller).
3. Second property is stronger than the first and the crucial issue.

Definition

A family hash function $\mathcal{H}$ is **2-universal** if for all distinct $x, y \in \mathcal{U}$, $\Pr[h(x) = h(y)] = 1/m$ where m is the table size.

Note: The set of all hash functions satisfies stronger properties!

Uniform hashing

Question: What are good properties of $\mathcal{H}$ in distributing data?

1. Consider any element $\mathbf{x} \in \mathcal{U}$. Then if $\mathbf{h} \in \mathcal{H}$ is picked randomly then $\mathbf{x}$ should go into a random slot in $\mathbf{T}$. In other words $\Pr[\mathbf{h}(\mathbf{x}) = \mathbf{i}] = \mathbf{1}/\mathbf{m}$ for every $\mathbf{0} \leq \mathbf{i} < \mathbf{m}$.
2. Consider any two distinct elements $\mathbf{x}, \mathbf{y} \in \mathcal{U}$. Then if $\mathbf{h} \in \mathcal{H}$ is picked randomly then the probability of a collision between $\mathbf{x}$ and $\mathbf{y}$ should be at most $\mathbf{1}/\mathbf{m}$. In other words $\Pr[\mathbf{h}(\mathbf{x}) = \mathbf{h}(\mathbf{y})] = \mathbf{1}/\mathbf{m}$ (cannot be smaller).
3. Second property is stronger than the first and the crucial issue.

Definition

A family hash function $\mathcal{H}$ is **2-universal** if for all distinct $\mathbf{x}, \mathbf{y} \in \mathcal{U}$, $\Pr[\mathbf{h}(\mathbf{x}) = \mathbf{h}(\mathbf{y})] = \mathbf{1}/\mathbf{m}$ where $\mathbf{m}$ is the table size.

Note: The set of all hash functions satisfies stronger properties!

Uniform hashing

Question: What are good properties of $\mathcal{H}$ in distributing data?

1. Consider any element $\mathbf{x} \in \mathcal{U}$. Then if $\mathbf{h} \in \mathcal{H}$ is picked randomly then $\mathbf{x}$ should go into a random slot in $\mathbf{T}$. In other words $\Pr[\mathbf{h}(\mathbf{x}) = \mathbf{i}] = \mathbf{1}/\mathbf{m}$ for every $\mathbf{0} \leq \mathbf{i} < \mathbf{m}$.
2. Consider any two distinct elements $\mathbf{x}, \mathbf{y} \in \mathcal{U}$. Then if $\mathbf{h} \in \mathcal{H}$ is picked randomly then the probability of a collision between $\mathbf{x}$ and $\mathbf{y}$ should be at most $\mathbf{1}/\mathbf{m}$. In other words $\Pr[\mathbf{h}(\mathbf{x}) = \mathbf{h}(\mathbf{y})] = \mathbf{1}/\mathbf{m}$ (cannot be smaller).
3. Second property is stronger than the first and the crucial issue.

Definition

A family hash function $\mathcal{H}$ is **2-universal** if for all distinct $\mathbf{x}, \mathbf{y} \in \mathcal{U}$, $\Pr[\mathbf{h}(\mathbf{x}) = \mathbf{h}(\mathbf{y})] = \mathbf{1}/\mathbf{m}$ where $\mathbf{m}$ is the table size.

Note: The set of all hash functions satisfies stronger properties!

Uniform hashing

Question: What are good properties of $\mathcal{H}$ in distributing data?

1. Consider any element $\mathbf{x} \in \mathcal{U}$. Then if $\mathbf{h} \in \mathcal{H}$ is picked randomly then $\mathbf{x}$ should go into a random slot in $\mathbf{T}$. In other words $\Pr[\mathbf{h}(\mathbf{x}) = \mathbf{i}] = \mathbf{1}/\mathbf{m}$ for every $\mathbf{0} \leq \mathbf{i} < \mathbf{m}$.
2. Consider any two distinct elements $\mathbf{x}, \mathbf{y} \in \mathcal{U}$. Then if $\mathbf{h} \in \mathcal{H}$ is picked randomly then the probability of a collision between $\mathbf{x}$ and $\mathbf{y}$ should be at most $\mathbf{1}/\mathbf{m}$. In other words $\Pr[\mathbf{h}(\mathbf{x}) = \mathbf{h}(\mathbf{y})] = \mathbf{1}/\mathbf{m}$ (cannot be smaller).
3. Second property is stronger than the first and the crucial issue.

Definition

A family hash function $\mathcal{H}$ is **2-universal** if for all distinct $\mathbf{x}, \mathbf{y} \in \mathcal{U}$, $\Pr[\mathbf{h}(\mathbf{x}) = \mathbf{h}(\mathbf{y})] = \mathbf{1}/\mathbf{m}$ where $\mathbf{m}$ is the table size.

Note: The set of all hash functions satisfies stronger properties!

Uniform hashing

Question: What are good properties of $\mathcal{H}$ in distributing data?

1. Consider any element $\mathbf{x} \in \mathcal{U}$. Then if $\mathbf{h} \in \mathcal{H}$ is picked randomly then $\mathbf{x}$ should go into a random slot in $\mathbf{T}$. In other words $\Pr[\mathbf{h}(\mathbf{x}) = \mathbf{i}] = \mathbf{1}/\mathbf{m}$ for every $\mathbf{0} \leq \mathbf{i} < \mathbf{m}$.
2. Consider any two distinct elements $\mathbf{x}, \mathbf{y} \in \mathcal{U}$. Then if $\mathbf{h} \in \mathcal{H}$ is picked randomly then the probability of a collision between $\mathbf{x}$ and $\mathbf{y}$ should be at most $\mathbf{1}/\mathbf{m}$. In other words $\Pr[\mathbf{h}(\mathbf{x}) = \mathbf{h}(\mathbf{y})] = \mathbf{1}/\mathbf{m}$ (cannot be smaller).
3. Second property is stronger than the first and the crucial issue.

Definition

A family hash function $\mathcal{H}$ is **2-universal** if for all distinct $\mathbf{x}, \mathbf{y} \in \mathcal{U}$, $\Pr[\mathbf{h}(\mathbf{x}) = \mathbf{h}(\mathbf{y})] = \mathbf{1}/\mathbf{m}$ where $\mathbf{m}$ is the table size.

Note: The set of all hash functions satisfies stronger properties!

Analyzing Uniform Hashing

1. $\mathbf{T}$ is hash table of size $\mathbf{m}$.
2. $\mathbf{S} \subseteq \mathcal{U}$ is a **fixed** set of size $\leq \mathbf{m}$.
3. $\mathbf{h}$ is chosen randomly from a uniform hash family $\mathcal{H}$.
4. $\mathbf{x}$ is a *fixed* element of $\mathcal{U}$. Assume for simplicity that $\mathbf{x} \notin \mathbf{S}$.

Question: What is the *expected* time to look up $\mathbf{x}$ in $\mathbf{T}$ using $\mathbf{h}$ assuming chaining used to resolve collisions?

Analyzing Uniform Hashing

Question: What is the *expected* time to look up $\mathbf{x}$ in $\mathbf{T}$ using $\mathbf{h}$ assuming chaining used to resolve collisions?

1. The time to look up $\mathbf{x}$ is the size of the list at $\mathbf{T[h(x)]}$: same as the number of elements in $\mathbf{S}$ that collide with $\mathbf{x}$ under $\mathbf{h}$.
2. Let $\ell(\mathbf{x})$ be this number. We want $\mathrm{E}[\ell(\mathbf{x})]$
3. For $\mathbf{y} \in \mathbf{S}$ let $\mathbf{A_y}$ be the even that $\mathbf{x}, \mathbf{y}$ collide and $\mathbf{D_y}$ be the corresponding indicator variable.

Analyzing Uniform Hashing

Continued...

Number of elements colliding with $\mathbf{x}$: $\ell(\mathbf{x}) = \sum_{\mathbf{y} \in \mathbf{S}} \mathbf{D_y}$.

$$
\begin{aligned}
\Rightarrow \mathrm{E}[\ell(\mathbf{x})] &= \sum_{\mathbf{y} \in \mathbf{S}} \mathrm{E}[\mathbf{D_y}] && \text{linearity of expectation} \\
&= \sum_{\mathbf{y} \in \mathbf{S}} \mathbf{Pr}[\mathbf{h}(\mathbf{x}) = \mathbf{h}(\mathbf{y})] \\
&= \sum_{\mathbf{y} \in \mathbf{S}} \frac{\mathbf{1}}{\mathbf{m}} && \text{since } \mathcal{H} \text{ is a uniform hash family} \\
&= |\mathbf{S}|/\mathbf{m} \\
&\leq \mathbf{1} \quad \text{if } |\mathbf{S}| \leq \mathbf{m}
\end{aligned}
$$

Analyzing Uniform Hashing

Question: What is the *expected* time to look up $\mathbf{x}$ in $\mathbf{T}$ using $\mathbf{h}$ assuming chaining used to resolve collisions?

Answer: $\mathbf{O(n/m)}$.

Comments:

1. $\mathbf{O(1)}$ expected time also holds for insertion.
2. Analysis assumes static set $\mathbf{S}$ but holds as long as $\mathbf{S}$ is a set formed with at most $\mathbf{O(m)}$ insertions and deletions.
3. **Worst-case**: look up time can be large! How large? $\mathbf{\Omega(\log n/\log\log n)}$
   [Lower bound holds even under stronger assumptions.]

Analyzing Uniform Hashing

Question: What is the *expected* time to look up $\mathbf{x}$ in $\mathbf{T}$ using $\mathbf{h}$ assuming chaining used to resolve collisions?

Answer: $\mathbf{O(n/m)}$.

Comments:

1. $\mathbf{O(1)}$ expected time also holds for insertion.
2. Analysis assumes static set $\mathbf{S}$ but holds as long as $\mathbf{S}$ is a set formed with at most $\mathbf{O(m)}$ insertions and deletions.
3. **Worst-case**: look up time can be large! How large?
   $\mathbf{\Omega(\log n / \log\log n)}$
   [Lower bound holds even under stronger assumptions.]

Rehashing, amortization and...

... making the hash table dynamic

Previous analysis assumed fixed $\mathbf{S}$ of size $\simeq \mathbf{m}$.

Question: What happens as items are inserted and deleted?

1. If $|\mathbf{S}|$ grows to more than $\mathbf{cm}$ for some constant $\mathbf{c}$ then hash table performance clearly degrades.
2. If $|\mathbf{S}|$ stays around $\simeq \mathbf{m}$ but incurs many insertions and deletions then the initial random hash function is no longer random enough!

Solution: Rebuild hash table periodically!

1. Choose a new table size based on current number of elements in table.
2. Choose a new random hash function and rehash the elements.
3. Discard old table and hash function.

Question: When to rebuild? How expensive?

Rehashing, amortization and...

... making the hash table dynamic

Previous analysis assumed fixed $\mathbf{S}$ of size $\simeq \mathbf{m}$.

Question: What happens as items are inserted and deleted?

1. If $|\mathbf{S}|$ grows to more than $\mathbf{cm}$ for some constant $\mathbf{c}$ then hash table performance clearly degrades.
2. If $|\mathbf{S}|$ stays around $\simeq \mathbf{m}$ but incurs many insertions and deletions then the initial random hash function is no longer random enough!

Solution: Rebuild hash table periodically!

1. Choose a new table size based on current number of elements in table.
2. Choose a new random hash function and rehash the elements.
3. Discard old table and hash function.

Question: When to rebuild? How expensive?

Rebuilding the hash table

1. Start with table size $\mathbf{m}$ where $\mathbf{m}$ is some estimate of $|\mathbf{S}|$ (can be some large constant).
2. If $|\mathbf{S}|$ grows to more than twice current table size, build new hash table (choose a new random hash function) with double the current number of elements. Can also use similar trick if table size falls below quarter the size.
3. If $|\mathbf{S}|$ stays roughly the same but more than $\mathbf{c}|\mathbf{S}|$ operations on table for some chosen constant $\mathbf{c}$ (say $\mathbf{10}$), rebuild.

The **amortize** cost of rebuilding to previously performed operations. Rebuilding ensures $\mathbf{O(1)}$ expected analysis holds even when $\mathbf{S}$ changes. Hence $\mathbf{O(1)}$ expected look up/insert/delete time *dynamic* data dictionary data structure!

Some math required...

Lemma

Let $\mathbf{p}$ *be a prime number,*
$\mathbf{x}$*: an integer number in* $\{1, \ldots, \mathbf{p} - 1\}$.
$\implies$ *There exists a unique* $\mathbf{y}$ *s.t.* $\mathbf{xy} = 1 \mod \mathbf{p}$.

In other words: For every element there is a unique inverse.
$\implies \mathbb{Z}_{\mathbf{p}} = \{0, 1, \ldots, \mathbf{p} - 1\}$ when working module $\mathbf{p}$ is a field.

Proof of lemma

Claim

Let $\mathbf{p}$ *be a prime number. For any* $\alpha, \beta, \mathbf{i} \in \{1, \ldots, \mathbf{p}-1\}$ *s.t.* $\alpha \neq \beta$, *we have that* $\alpha \mathbf{i} \neq \beta \mathbf{i} \mod \mathbf{p}$.

Proof.

Assume for the sake of contradiction $\alpha \mathbf{i} = \beta \mathbf{i} \mod \mathbf{p}$. Then

$$
\begin{aligned}
& \mathbf{i}(\alpha - \beta) = 0 \mod \mathbf{p} \\
\implies \quad & \mathbf{p} \text{ divides } \mathbf{i}(\alpha - \beta) \\
\implies \quad & \mathbf{p} \text{ divides } \alpha - \beta \\
\implies \quad & \alpha - \beta = 0 \\
\implies \quad & \alpha = \beta.
\end{aligned}
$$

And that is a contradiction. □

Proof of lemma...

Uniqueness.

Lemma

Let $\mathbf{p}$ *be a prime number,*
$\mathbf{x}$*: an integer number in* $\{1, \ldots, \mathbf{p} - 1\}$*.*
$\implies$ *There exists a unique* $\mathbf{y}$ *s.t.* $\mathbf{xy} = 1 \mod \mathbf{p}$*.*

Proof.

Assume the lemma is false and there are two distinct numbers $\mathbf{y}, \mathbf{z} \in \{1, \ldots, \mathbf{p} - 1\}$ such that

$$\mathbf{xy} = 1 \mod \mathbf{p} \quad \text{and} \quad \mathbf{xz} = 1 \mod \mathbf{p}.$$

But this contradicts the above claim (set $\mathbf{i} = \mathbf{x}$, $\alpha = \mathbf{y}$ and $\beta = \mathbf{z}$). $\square$

Proof of lemma...

Existence

Proof.

By claim, for any $\alpha \in \{1, \ldots, p-1\}$ we have that $\{\alpha * 1 \mod p, \alpha * 2 \mod p, \ldots, \alpha * (p-1) \mod p\} = \{1, 2, \ldots, p-1\}$.

$\implies$ There exists a number $y \in \{1, \ldots, p-1\}$ such that $\alpha y = 1 \mod p$. $\square$

Constructing Universal Hash Families

Parameters: $\mathbf{N} = |\mathcal{U}|$, $\mathbf{m} = |\mathbf{T}|$, $\mathbf{n} = |\mathbf{S}|$

1. Choose a **prime** number $\mathbf{p} \geq \mathbf{N}$. $\mathbb{Z}_\mathbf{p} = \{0, 1, \ldots, \mathbf{p} - 1\}$ is a field.
2. For $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_\mathbf{p}$, $\mathbf{a} \neq 0$, define the hash function $\mathbf{h}_{\mathbf{a},\mathbf{b}}$ as $\mathbf{h}_{\mathbf{a},\mathbf{b}}(\mathbf{x}) = ((\mathbf{ax} + \mathbf{b}) \mod \mathbf{p}) \mod \mathbf{m}$.
3. Let $\mathcal{H} = \{\mathbf{h}_{\mathbf{a},\mathbf{b}} \mid \mathbf{a}, \mathbf{b} \in \mathbb{Z}_\mathbf{p}, \mathbf{a} \neq 0\}$. Note that $|\mathcal{H}| = \mathbf{p}(\mathbf{p} - 1)$.

Theorem

$\mathcal{H}$ is a 2-universal hash family.

Comments:

1. Hash family is of small size, easy to sample from.
2. Easy to store a hash function ($\mathbf{a}, \mathbf{b}$ have to be stored) and evaluate it.

Constructing Universal Hash Families

Parameters: $\mathbf{N} = |\mathcal{U}|$, $\mathbf{m} = |\mathbf{T}|$, $\mathbf{n} = |\mathbf{S}|$

1. Choose a **prime** number $\mathbf{p} \geq \mathbf{N}$. $\mathbb{Z}_\mathbf{p} = \{0, 1, \ldots, \mathbf{p} - 1\}$ is a field.
2. For $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_\mathbf{p}$, $\mathbf{a} \neq 0$, define the hash function $\mathbf{h}_{\mathbf{a},\mathbf{b}}$ as $\mathbf{h}_{\mathbf{a},\mathbf{b}}(\mathbf{x}) = ((\mathbf{ax} + \mathbf{b}) \mod \mathbf{p}) \mod \mathbf{m}$.
3. Let $\mathcal{H} = \{\mathbf{h}_{\mathbf{a},\mathbf{b}} \mid \mathbf{a}, \mathbf{b} \in \mathbb{Z}_\mathbf{p}, \mathbf{a} \neq 0\}$. Note that $|\mathcal{H}| = \mathbf{p}(\mathbf{p} - 1)$.

Theorem

$\mathcal{H}$ is a 2-universal hash family.

Comments:

1. Hash family is of small size, easy to sample from.
2. Easy to store a hash function ($\mathbf{a}, \mathbf{b}$ have to be stored) and evaluate it.

Constructing Universal Hash Families

Parameters: $\mathbf{N} = |\mathcal{U}|$, $\mathbf{m} = |\mathbf{T}|$, $\mathbf{n} = |\mathbf{S}|$

1. Choose a **prime** number $\mathbf{p} \geq \mathbf{N}$. $\mathbb{Z}_\mathbf{p} = \{0, 1, \ldots, \mathbf{p} - 1\}$ is a field.
2. For $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_\mathbf{p}$, $\mathbf{a} \neq 0$, define the hash function $\mathbf{h}_{\mathbf{a},\mathbf{b}}$ as $\mathbf{h}_{\mathbf{a},\mathbf{b}}(\mathbf{x}) = ((\mathbf{ax} + \mathbf{b}) \mod \mathbf{p}) \mod \mathbf{m}$.
3. Let $\mathcal{H} = \{\mathbf{h}_{\mathbf{a},\mathbf{b}} \mid \mathbf{a}, \mathbf{b} \in \mathbb{Z}_\mathbf{p}, \mathbf{a} \neq 0\}$. Note that $|\mathcal{H}| = \mathbf{p}(\mathbf{p} - 1)$.

Theorem

$\mathcal{H}$ is a $\mathbf{2}$-universal hash family.

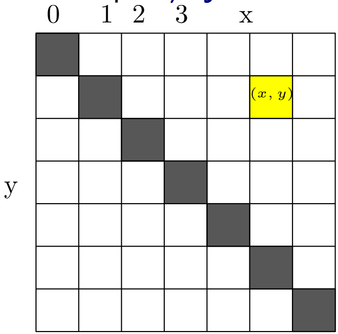
Comments:

1. Hash family is of small size, easy to sample from.
2. Easy to store a hash function ($\mathbf{a}, \mathbf{b}$ have to be stored) and evaluate it.

What the is going on?

$\mathbf{h_{a,b}(x) = ((ax + b) \mod p) \mod m}$

First map $\mathbf{x} \neq \mathbf{y}$ to $\mathbf{r} = \mathbf{h(x)}$ and $\mathbf{s} = \mathbf{h(y)}$.

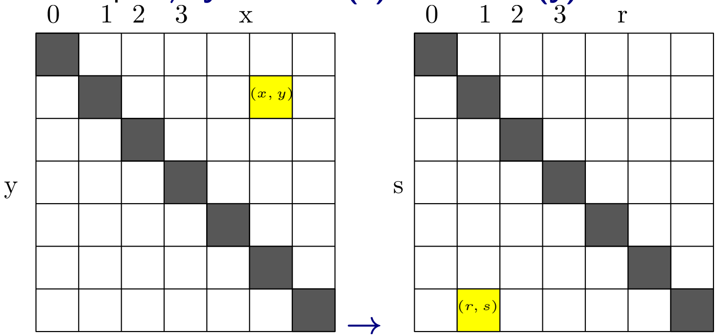


This is a random uniform mapping (choosing **a** and **b**) – every cell has the same probability to be the target, for fixed **x** and **y**.

What the is going on?

$\mathbf{h_{a,b}(x) = ((ax + b) \mod p) \mod m}$

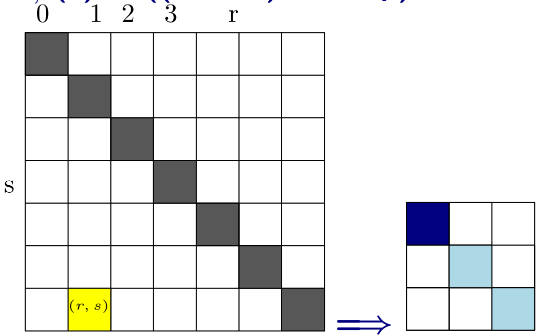
First map $\mathbf{x} \neq \mathbf{y}$ to $\mathbf{r} = \mathbf{h(x)}$ and $\mathbf{s} = \mathbf{h(y)}$.



This is a random uniform mapping (choosing **a** and **b**) – every cell has the same probability to be the target, for fixed **x** and **y**.

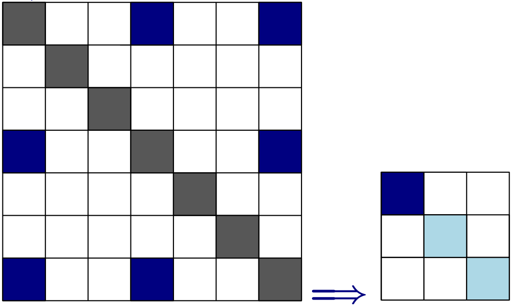
What the is going on?

$$h_{a,b}(x) = ((ax + b) \mod p) \mod m$$



What the is going on?

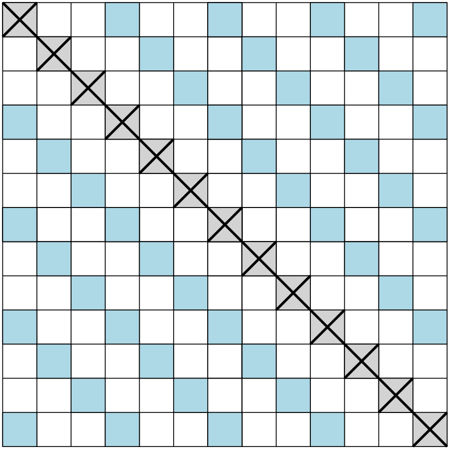
$$h_{a,b}(x) = ((ax + b) \mod p) \mod m$$



What the is going on?

$h_{a,b}(x) = ((ax + b) \mod p) \mod m$

1. First part of mapping maps (x, y) to a random location $(h_{a,b}(x), h_{a,b}(y))$ in the "matrix".
2. $(h_{a,b}(x), h_{a,b}(y))$ is not on main diagonal.
3. All blue locations are "bad" – map by $\mod m$ to a location of collusion.
4. But... at most $1/m$ fraction of allowable locations in the matrix are bad.



Constructing Universal Hash Families

Theorem

$\mathcal{H}$ is a (2)-universal hash family.

Proof.

Fix $\mathbf{x}, \mathbf{y} \in \mathcal{U}$. What is the probability they will collide if $\mathbf{h}$ is picked randomly from $\mathcal{H}$?

1. Let $\mathbf{a}, \mathbf{b}$ be *bad* for $\mathbf{x}, \mathbf{y}$ if $\mathbf{h}_{\mathbf{a},\mathbf{b}}(\mathbf{x}) = \mathbf{h}_{\mathbf{a},\mathbf{b}}(\mathbf{y})$.
2. **Claim:** Number of bad pairs is at most $\mathbf{p}(\mathbf{p}-\mathbf{1})/\mathbf{m}$.
3. Total number of hash functions is $\mathbf{p}(\mathbf{p}-\mathbf{1})$ and hence probability of a collision is $\leq \mathbf{1}/\mathbf{m}$.

□

Constructing Universal Hash Families

Theorem

$\mathcal{H}$ is a (2)-universal hash family.

Proof.

Fix $\mathbf{x}, \mathbf{y} \in \mathcal{U}$. What is the probability they will collide if $\mathbf{h}$ is picked randomly from $\mathcal{H}$?

1. Let $\mathbf{a}, \mathbf{b}$ be *bad* for $\mathbf{x}, \mathbf{y}$ if $\mathbf{h_{a,b}(x) = h_{a,b}(y)}$.
2. **Claim:** Number of bad pairs is at most $\mathbf{p(p-1)/m}$.
3. Total number of hash functions is $\mathbf{p(p-1)}$ and hence probability of a collision is $\leq \mathbf{1/m}$. □

Some Lemmas

Lemma

If $\mathbf{x} \neq \mathbf{y}$ *then for any* $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_\mathbf{p}$ *such that* $\mathbf{a} \neq \mathbf{0}$*, we have*

$$\mathbf{ax} + \mathbf{b} \mod \mathbf{p} \neq \mathbf{ay} + \mathbf{b} \mod \mathbf{p}.$$

Proof.

If $\mathbf{ax} + \mathbf{b} \mod \mathbf{p} = \mathbf{ay} + \mathbf{b} \mod \mathbf{p}$ then $\mathbf{a}(\mathbf{x} - \mathbf{y}) \mod \mathbf{p} = \mathbf{0}$ and $\mathbf{a} \neq \mathbf{0}$ and $(\mathbf{x} - \mathbf{y}) \neq \mathbf{0}$. However, $\mathbf{a}$ and $(\mathbf{x} - \mathbf{y})$ cannot divide $\mathbf{p}$ since $\mathbf{p}$ is prime and $\mathbf{a} < \mathbf{p}$ and $(\mathbf{x} - \mathbf{y}) < \mathbf{p}$. □

Some Lemmas

Lemma

If $x \neq y$ *then for each* (r, s) *such that* $r \neq s$ *and* $0 \leq r, s \leq p - 1$ *there is exactly* **one** a, b *such that*

$$ax + b \mod p = r \text{ and } ay + b \mod p = s.$$

Proof.

Solve the two equations:

$$ax + b = r \mod p \qquad \text{and} \qquad ay + b = s \mod p$$

We get $a = \frac{r-s}{x-y} \mod p$ and $b = r - ax \mod p$. □

Understanding the hashing

Once we fix $\mathbf{a}$ and $\mathbf{b}$, and we are given a value $\mathbf{x}$, we compute the hash value of $\mathbf{x}$ in two stages:

1. **Compute**: $\mathbf{r} \leftarrow (\mathbf{ax} + \mathbf{b}) \mod \mathbf{p}$.
2. **Fold**: $\mathbf{r}' \leftarrow \mathbf{r} \mod \mathbf{m}$

Collision...

Given two values $\mathbf{x}$ and $\mathbf{y}$ they might collide because of either steps.

Lemma

$\#$ not equal pairs of $\mathbb{Z}_\mathbf{p} \times \mathbb{Z}_\mathbf{p}$ that are folded to the same number is $\mathbf{p}(\mathbf{p}-1)/\mathbf{m}$.

Folding numbers

Lemma

 # not equal pairs of $\mathbb{Z}_p \times \mathbb{Z}_p$ that are folded to the same number is $\mathbf{p(p-1)/m}$.

Proof.

Consider a pair $(x, y) \in \{0, 1, \ldots, p-1\}^2$ s.t. $x \neq y$. Fix x:

1. There are $\lceil p/m \rceil$ values of y that fold into x. That is

$$x \mod m = y \mod m.$$

2. One of them is when $x = y$.
3. $\implies$ # of colliding pairs $(\lceil p/m \rceil - 1)p \leq (p-1)p/m$

Proof of Claim

of bad pairs is $\mathbf{p(p-1)/m}$

Proof.

Let $\mathbf{a, b} \in \mathbb{Z}_\mathbf{p}$ such that $\mathbf{a \neq 0}$ and $\mathbf{h_{a,b}(x) = h_{a,b}(y)}$.

1. Let $\mathbf{ax + b \mod p = r}$ and $\mathbf{ay + b \mod = s \mod p}$.
2. Collision if and only if $\mathbf{r = s \mod m}$.
3. (Folding error): Number of pairs $\mathbf{(r, s)}$ such that $\mathbf{r \neq s}$ and $\mathbf{0 \leq r, s \leq p - 1}$ and $\mathbf{r = s \mod m}$ is $\mathbf{p(p-1)/m}$.
4. From previous lemma for each bad pair $\mathbf{(a, b)}$ there is a unique pair $\mathbf{(r, s)}$ such that $\mathbf{r = s \mod m}$. Hence total number of bad pairs is $\mathbf{p(p-1)/m}$.

$\square$

Prob of $\mathbf{x}$ and $\mathbf{y}$ to collide: $\frac{\#\text{ bad pairs}}{\#\text{pairs}} = \frac{\mathbf{p(p-1)/m}}{\mathbf{p(p-1)}} = \frac{\mathbf{1}}{\mathbf{m}}$.

Proof of Claim

of bad pairs is $\mathbf{p(p-1)/m}$

Proof.

Let $\mathbf{a, b} \in \mathbb{Z}_\mathbf{p}$ such that $\mathbf{a} \neq \mathbf{0}$ and $\mathbf{h_{a,b}(x) = h_{a,b}(y)}$.

1. Let $\mathbf{ax + b \mod p = r}$ and $\mathbf{ay + b \mod \ = s \mod p}$.
2. Collision if and only if $\mathbf{r = s \mod m}$.
3. (Folding error): Number of pairs $\mathbf{(r, s)}$ such that $\mathbf{r \neq s}$ and $\mathbf{0 \leq r, s \leq p - 1}$ and $\mathbf{r = s \mod m}$ is $\mathbf{p(p-1)/m}$.
4. From previous lemma for each bad pair $\mathbf{(a, b)}$ there is a unique pair $\mathbf{(r, s)}$ such that $\mathbf{r = s \mod m}$. Hence total number of bad pairs is $\mathbf{p(p-1)/m}$.

□

Prob of $\mathbf{x}$ and $\mathbf{y}$ to collide: $\frac{\#\text{ bad pairs}}{\#\text{pairs}} = \frac{\mathbf{p(p-1)/m}}{\mathbf{p(p-1)}} = \frac{\mathbf{1}}{\mathbf{m}}$.

Perfect Hashing

Question: Can we make look up time $\mathbf{O(1)}$ in worst case?

Yes for static dictionaries but then space usage is $\mathbf{O(m)}$ only in expectation.

Practical Issues

Hashing used typically for integers, vectors, strings etc.

- Universal hashing is defined for integers. To implement for other objects need to map objects in some fashion to integers (via representation)
- Practical methods for various important cases such as vectors, strings are studied extensively. See http://en.wikipedia.org/wiki/Universal_hashing for some pointers.
- Recent important paper briding theory and practice of hashing. "The power of simple tabulation hashing" by Mikkel Thorup and Mihai Patrascu, 2011. See http://en.wikipedia.org/wiki/Tabulation_hashing

Bloom Filters

Hashing:

1. To insert $\mathbf{x}$ in dictionary store $\mathbf{x}$ in table in location $\mathbf{h(x)}$
2. To lookup $\mathbf{y}$ in dictionary check contents of location $\mathbf{h(y)}$

Bloom Filter: tradeoff space for false positives

1. Storing items in dictionary expensive in terms of memory, especially if items are unwieldy objects such a long strings, images, etc with *non-uniform* sizes.
2. To insert $\mathbf{x}$ in dictionary set *bit* to $\mathbf{1}$ in location $\mathbf{h(x)}$ (initially all bits are set to $\mathbf{0}$)
3. To lookup $\mathbf{y}$ if bit in location $\mathbf{h(y)}$ is $\mathbf{1}$ say yes, else no.

Bloom Filters

Hashing:

1. To insert $\mathbf{x}$ in dictionary store $\mathbf{x}$ in table in location $\mathbf{h(x)}$
2. To lookup $\mathbf{y}$ in dictionary check contents of location $\mathbf{h(y)}$

Bloom Filter: tradeoff space for false positives

1. Storing items in dictionary expensive in terms of memory, especially if items are unwieldy objects such a long strings, images, etc with *non-uniform* sizes.
2. To insert $\mathbf{x}$ in dictionary set *bit* to $\mathbf{1}$ in location $\mathbf{h(x)}$ (initially all bits are set to $\mathbf{0}$)
3. To lookup $\mathbf{y}$ if bit in location $\mathbf{h(y)}$ is $\mathbf{1}$ say yes, else no.

Bloom Filters

Bloom Filter: tradeoff space for false positives

1. To insert x in dictionary set *bit* to 1 in location $h(x)$ (initially all bits are set to 0)
2. To lookup y if bit in location $h(y)$ is 1 say yes, else no
3. No false negatives but false positives possible due to collisions

Reducing false positives:

1. Pick k hash functions $h_1, h_2, \ldots, h_k$ *independently*
2. To insert x for $1 \leq i \leq k$ set bit in location $h_i(x)$ in table i to 1
3. To lookup y compute $h_i(y)$ for $1 \leq i \leq k$ and say yes only if each bit in the corresponding location is 1, otherwise say no. If probability of false positive for one hash function is $\alpha < 1$ then with k independent hash function it is α^k.

Bloom Filters

Bloom Filter: tradeoff space for false positives

1. To insert x in dictionary set *bit* to 1 in location $h(x)$ (initially all bits are set to 0)
2. To lookup y if bit in location $h(y)$ is 1 say yes, else no
3. No false negatives but false positives possible due to collisions

Reducing false positives:

1. Pick k hash functions $h_1, h_2, \ldots, h_k$ *independently*
2. To insert x for $1 \leq i \leq k$ set bit in location $h_i(x)$ in table i to 1
3. To lookup y compute $h_i(y)$ for $1 \leq i \leq k$ and say yes only if each bit in the corresponding location is 1, otherwise say no. If probability of false positive for one hash function is $\alpha < 1$ then with k independent hash function it is α^k.

Take away points

1. Hashing is a powerful and important technique for dictionaries. Many practical applications.
2. Randomization fundamental to understanding hashing.
3. Good and efficient hashing possible in theory and practice with proper definitions (universal, perfect, etc).
4. Related ideas of creating a compact fingerprint/sketch for objects is very powerful in theory and practice.
5. Many applications in practice.

Notes

Notes

Notes

Notes