

CSE 331

Abstraction

James Wilcox and Kevin Zatloukal



HW7

- **HW1–3: write more **realistic** applications**
 - saw how **debugging** gets harder
- **HW4–6: write code **correctly** the first time**
 - checked correctness without a computer
- **HW7–9: write more **complex** applications**
 - most applications have a core, tricky part
 - use the **correctness toolkit** to get that right
 - can work faster where debugging is easier
 - only way to really know the UI is right is to try it

Procedural Abstraction

- **Hide the details of the function from the caller**
 - caller only needs to read the **specification**
 - (“procedure” means function)
- **Caller promises to pass valid inputs**
 - no promises on invalid inputs
- **Implementer then promises to return correct outputs**
 - does not matter how

Procedural Abstraction Example

- Specification of rev is imperative:

```
// @returns same numbers but in reverse order, i.e.
//   rev(nil) := nil
//   rev(cons(x, L)) := rev(L) ++ [x]
const rev = (L: List): List => {
  return rev_acc(L, nil); // faster way
};
```

- code implements a different function
- need to use reasoning to check that these two match
we proved that $\text{rev_acc}(L, \text{nil}) = \text{rev}(L)$ for all L by structural induction

Other Properties of High-Quality Code

- Professionals are expected to write **high-quality** code
- Correctness is the most important part of quality
 - users **hate** products that do not work properly

- Also includes the following

- easy to change
- easy to understand
- modular

abstraction provides
all three properties

start with rev straight from the spec
later change it to a faster version

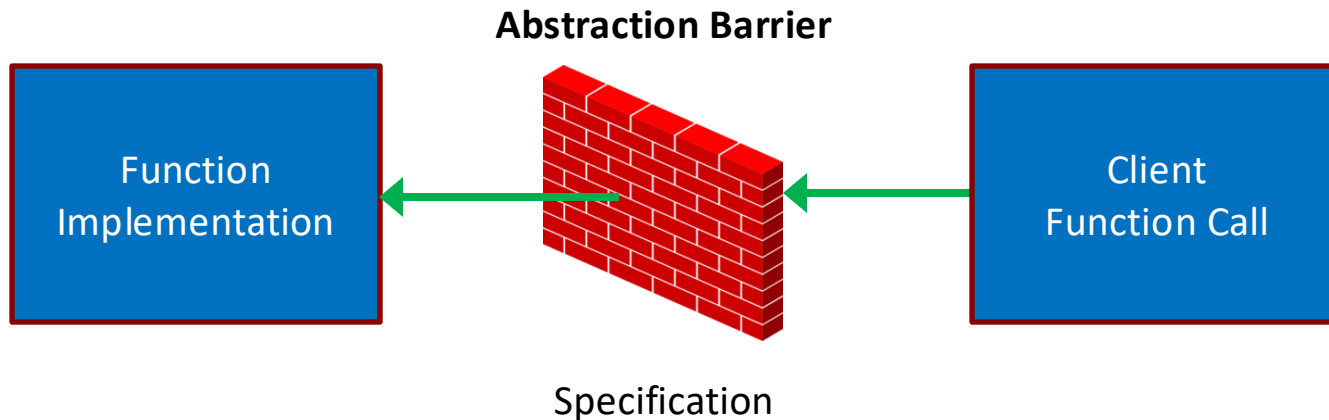
Benefits of Specifications

Clear specifications help with **understandability** and

- **Correctness**
 - reasoning requires clear definition of what the function does
- **Changeability**
 - implementer is free to write any code that meets spec
 - client can pass any inputs that satisfy requirements
- **Modularity**
 - people can work on different parts once specs are agreed

Abstraction Barrier

- Specification is an...



- specification is the “barrier” between the sides
- clients depend only on the spec
- implementer can write any code that satisfies the spec

Performance Improvements

- Before, we saw rev-acc, which is faster than rev
 - faster *algorithm* for reversing a list
 - rare to see this
- Most perf improvements change ***data structures***
 - different kind of abstraction barrier for data
- Let's see an example...

Last Element of a List

`last(nil)` := undefined

`last(x :: nil)` := x

`last(x :: y :: L)` := `last(y :: L)`

- **Runs in $\Theta(n)$ time**

- walks down to the end of the list
- no faster way to do this on a list

- **We could cache the last element**

- new data type just dropped:

analogous idea:
store references to both
“front” and “back” nodes

```
type FastLastList = {list: List, last: bigint | undefined}
```

empty list has undefined last

Fast-Last List

```
type FastLastList = {list: List, last: bigint|undefined}
```

- **How do we switch to this type?**
 - change every `List` into `FastLastList`
- **Will still have functions that operate on List**
 - e.g., `len`, `sum`, `concat`, `rev`
- **Suppose `F` is a `FastLastList`**
 - instead of calling `rev(F)`, we have call `rev(F.list)`
 - cleaner to introduce a helper function

Fast-Last List

```
type FastLastList = {list: List, last: bigint|undefined}

const getLast = (F: FastLastList): bigint|undefined => {
  return F.last;
};

const toList = (F: FastLastList): List<bigint> => {
  return F.list;
};
```

- **How do we switch to this type?**
 - **change every List into FastLastList**
 - **replace F with toList(F) where a List is expected**

Another Fast List

- Suppose we often need the 2nd to last, 3rd to last, ... (back of the list). How can we make it faster?
 - store the list in *reverse* order!

```
type FastBackList = List<bigint>;
```

```
const getLast = (F: FastBackList): bigint|undefined => {  
  return (F.kind === "nil") ? undefined : F.hd;  
};
```

```
const getSecondToLast = (F: FastBackList): bigint|undefined => {  
  return (F.kind === "nil") ? undefined :  
    (F.tl.kind === "nil") ? undefined : F.tl.hd;  
};
```

```
const toList = (F: FastBackList): List<bigint> => {  
  return rev(F);  
};
```

Another Fast List

```
type FastBackList = List<bigint>;

const getLast = (F: FastBackList): bigint|undefined => {
  return (F.kind === "nil") ? undefined : F.hd;
};

const toList = (F: FastBackList): List<bigint> => {
  return rev(F);
};
```

- **Problems with this solution...**

- **no type errors if someone forgets to call toList!**

```
const F: FastBackList = ...;
return concat(F, cons(1, nil)); // bad!
```

Another Fast List — Take Two

```
type FastBackList =  
  {list: List<bigint>, origList: List< bigint >};  
  
const getLast = (F: FastBackList): bigint|undefined => {  
  return (F.list.kind === "nil") ? undefined : F.list.hd;  
};  
  
const toList = (F: FastBackList): List<bigint> => {  
  return F.origList;  
};
```

- **Still some problems...**
 - **no type errors if someone grabs the field directly**

```
const F: FastBackList = ...;  
return concat(F.list, cons(1, nil)); // bad!
```

Another Fast List — Take Three

```
const F: FastBackList = ...;  
return concat(F.list, cons(1, nil)); // bad!
```

- **Only way to completely stop this is to hide `F.list`**
 - do not give them the data, just the functions

```
type FastList = {  
  getLast: () => bigint|undefined,  
  toList: () => List<bigint>  
};
```

- the only way to get the list is to call `F.toList()`
- seems weird... but we can make it look familiar

Another Fast List — Take Three

```
interface FastList {  
    getLast(): bigint | undefined;  
    toList(): List<bigint>;  
}
```

- In TypeScript, “interface” is synonym for “record type”

- You’ve seen this in Java

Java interface is a record where
field values are functions (methods)

```
interface FastList {  
    int getLast() throws EmptyList;  
    List<Integer> toList();  
}
```

- in 331, our interfaces will only include functions (methods)

Data Abstraction

Data Abstraction

- **Give clients only operations, not data**
 - operations are “public”, data is “private”
- **We call this an Abstract Data Type (ADT)**
 - invented by Barbara Liskov in the 1970s
 - fundamental concept in computer science
 - built into Java, JavaScript, etc.
 - data abstraction via procedural abstraction
- **Critical for the properties we want**
 - easier to change data structure
 - easier to understand (hides details)
 - more modular



How to Make a FastList — Attempt One

```
const makeFastList = (list: List<bigint>): FastList => {  
  const last = last(list);  
  return {  
    getLast: () => { return last; },  
    toList: () => { return list; }  
  };  
};
```

- **Values in `getLast` and `toList` fields are functions**
- **There is a cleaner way to do this**
 - will also look more familiar

How to Make a FastList

```
class FastLastList implements FastList {
  last: bigint|undefined; // should be "readonly"
  list: List<bigint>;

  constructor(list: List<bigint>) {
    this.last = last(list);
    this.list = list;
  }

  getLast = () => { return this.last; };
  toList = () => { return this.list; };
}
```

- Can create a new record using **"new"**
 - each record has fields `list`, `last`, `getLast`, `toList`
 - bodies of functions use **"this"** to refer to the record

How to Make a FastList

```
class FastLastList implements FastList {
  last: bigint|undefined; // should be "readonly"
  list: List<bigint>;

  constructor(list: List<bigint>) {
    this.last = last(list);
    this.list = list;
  }

  getLast = () => { return this.last; };
  toList = () => { return this.list; };
}
```

- Can create a new record using **“new”**
 - all four assignments are executed on each call to **“new”**
 - `getLast` **and** `toList` are always the same functions

How to Make a FastList

```
class FastLastList implements FastList {
  last: bigint|undefined; // should be "readonly"
  list: List<bigint>;

  constructor(list: List<bigint>) {
    this.last = last(list);
    this.list = list;
  }

  getLast = () => { return this.last; };
  toList = () => { return this.list; };
}
```

- **Implements the FastList interface**
 - i.e., it has the expected `getLast` and `toList` fields
 - (okay for records to have more fields than required)

Another Way to Make a FastList

```
class FastBackList implements FastList {
  original: List<bigint>;
  reversed: List<bigint>; // in reverse order

  constructor(list: List<bigint>) {
    this.original = list;
    this.reversed = rev(list);
  }

  getLast = () => {
    return (this.reversed.kind === "nil") ?
      undefined : this.reversed.hd;
  };

  toList = () => { return this.original; }
}
```

How Do Clients Get a FastList

```
const makeFastList = (list: List<bigint>): FastList => {  
  return new FastLastList(list);  
};
```

- **Export only FastList and makeFastList**
 - completely hides the data representation from clients
- **This is called a “factory function”**
 - another **design pattern**
 - can change implementations easily in the future
becomes FastBackList with a one-line change
- **Difficult to add to the list with this interface**
 - requires three calls: toList, cons, makeFastList

Another Way To Do It

```
interface FastList {
  cons(x: bigint): FastList;
  getLast(): bigint|undefined;
  toList(): List<bigint>;
};

const makeFastList = (): FastList => {
  return new FastBackList(nil);
};
```

- **New method `cons` returns list with `x` in front**
 - example of a “producer” method (others are “observers”)
produces a new list for you
 - now, we only need to make an empty `FastList`
anything else can be built via `cons`

Another Way To Do It (Even Better)

```
interface FastList {
  cons(x: bigint): FastList;
  getLast(): bigint|undefined;
  toList(): List<bigint>;
};

const nilList: FastList = new FastBackList(nil);

const makeFastList = (): FastList => {
  return nilList;
};
```

- No need to create a new object using “**new**” every time
 - can reuse the same instance
 - only possible since these are immutable!
 - example of the “singleton” **design pattern**

Full ADT Design Pattern for 331

We will use the following **design pattern** for ADTs:

- “**interface**” used for defining ADTs
 - declares the methods available
- “**class**” used for implementing ADTs
 - defines the fields and methods
 - implements the ADT interface above
- **Factory function** used to create instances

Stick to regular functions for rest of the code!

Specifications for ADTs

Specifications for ADTs

- Run into problems when we try to write specs
 - for example, what goes after `@return`?
 - don't want to say returns the `.list` field (or reverse of that)
 - we want to hide those details from clients

```
interface FastList {  
    /**  
     * Returns the last element of the list.  
     * @returns ??  
     */  
    getLast: () => bigint | undefined;  
};
```

- Need some terminology to clear up confusion

ADT Terminology

New terminology for specifying ADTs

Concrete State / Representation

actual fields of the record and the data stored in them

Last example: `{list: List, last: bigint|undefined}`

Abstract State / Representation

how clients should *think* about the object

Last example: `List` (i.e., `nil` or `cons`)

- We've had different abstract and concrete types all along!
 - in our math, `List` is an inductive type (abstract)
 - in our code, `List` is a string or a record (concrete)

List State: Concrete vs Abstract

Inductive types also differ in abstract / concrete states:

Concrete State / Representation

actual fields of the record and the data stored in them

Last example: `{kind:"nil"} | {kind:"cons", hd:bigint, tl:List}`

Abstract State / Representation

how clients should *think* about the object

Last example: List (i.e., nil or cons)

- Inductive types also use a **design pattern** to work in TypeScript
 - details are different than ADTs (e.g., no interfaces)

ADT Terminology

New terminology for specifying ADTs

Concrete State / Representation

actual fields of the record and the data stored in them

Last example: `{kind:"nil"} | {kind:"cons", hd:bigint, tl:List}`

Abstract State / Representation

how clients should *think* about the object

Last example: List (i.e., nil or cons)

- Term “**object**” (or “**obj**”) will refer to abstract state
 - “object” means mathematical object
 - “obj” is the mathematical value that the record represents

Specifying FastList

```
/**
 * A list of integers that can retrieve the last
 * element in O(1) time.
 */
export interface FastList {
  /**
   * Returns the last element of the list (O(1) time).
   * @returns last(obj)
   */
  getLast(): bigint | undefined;
}
```

- “obj” refers to the abstract state (the list, in this case)
 - actual state will be a record with fields `last` and `list`

Specifying FastList

```
/**
 * A list of integers that can retrieve the last
 * element in O(1) time.
 */
export interface FastList {
  ...
  /**
   * Returns a new list with x in front of this list.
   * @returns cons(x, obj)
   */
  cons(x: bigint): FastList;
}
```

- **Producer method: makes a new list for you**
 - “obj” above is a list, so `cons(x, obj)` makes sense in math

Specifying FastList

```
/**
 * A list of integers that can retrieve the last
 * element in O(1) time.
 */
export interface FastList {
  ...
  /**
   * Returns a new list with x in front of this list.
   * @returns cons(x, obj)
   */
  cons(x: bigint): FastList;
}
```

- Specification does not talk about fields, just “obj”
 - fields are *hidden* from clients

Specifying FastList

```
/**
 * A list of integers that can retrieve the last
 * element in O(1) time.
 */
export interface FastList {
  ...
  /**
   * ??
   * @returns ??
   */
  toList(): List<bigint>;
}
```

- How do we specify this?

Specifying FastList

```
/**
 * A list of integers that can retrieve the last
 * element in O(1) time.
 */
export interface FastList {
  ...
  /**
   * Returns the object as a regular list of items.
   * @returns obj
   */
  toList(): List<bigint>;
}
```

- In math, this function does nothing (“@returns obj”)
 - two *different* concrete representations of the same idea
 - details of the representations are *hidden* from clients

Recall: ADTs

- **Abstraction over data**
 - hide the details of the data representation
 - only give users a set of **operations** (the interface)
data abstraction via procedural abstraction
- **Interface can make clever data structures possible**
- **Some commonly used ADTs**
 - **stack**: add & remove from one end
 - **queue**: add to one end, remove from other
 - **set**: add, remove, & check if contained in list
 - **map**: add, remove, & get value for (key, value) pair

Documenting an ADT Implementation

Documenting an ADT Implementation

- Last lecture, we saw how to write an ADT spec
- Key idea is the “**abstract state**”
 - simple definition of the object (easier to think about)
 - clients use that to **reason** about calls to this code
- Write specifications in terms of the abstract state
 - describe the return value in terms of “**obj**”
- We also need to reason about ADT implementation
 - for this, we do want to talk about fields
 - fields are hidden from clients, but visible to implementers

Documenting an ADT Implementation

- We also need to document the ADT implementation
 - for this, we need two new tools

Abstraction Function

defines what abstract state the field values currently represent

- Maps the field values to the object they represent
 - object is math, so this is a *mathematical* function
 - there is no such function in the code — just a tool for reasoning
 - will usually write this as an *equation*
 - obj = ... right-hand side uses the fields

Documenting the FastList ADT

```
class FastLastList implements FastList {  
    // AF: obj = this.list  
    last: bigint | undefined;  
    list: List<bigint>;  
    ...  
}
```

- **Abstraction Function (AF) gives the abstract state**
 - obj = abstract state
 - this = concrete state (record with fields .last and .list)
 - AF relates abstract state to the current concrete state
 - okay that “last” is not involved here
 - specifications only talk about “obj”, not “this”
 - “this” will appear in our reasoning

Documenting an ADT Implementation

- We also need to document the ADT implementation
 - for this, we need two new tools

Abstraction Function

defines what abstract state the field values currently represent
only needs to be defined when RI is true

Representation Invariants (RI)

facts about the field values that should always be true
defines what field values are allowed
AF only needs to apply when RI is true

Documenting the FastList ADT

```
class FastLastList implements FastList {  
    // RI: this.last = last(this.list)  
    // AF: obj = this.list  
    last: bigint | undefined;  
    list: List<bigint>;  
    ...  
}
```

- **Representation Invariant (RI)** holds info about `this.last`
 - fields cannot have *just any* number and list of numbers
 - they must fit together by satisfying RI
 - last must be the last number in the list stored

Correctness of FastList Constructor

```
class FastLastList implements FastList {  
    // RI: this.last = last(this.list)  
    // AF: obj = this.list  
    last: bigint | undefined;  
    list: List<bigint>;  
  
    constructor(L: List<bigint>) {  
        this.list = L;  
        this.last = last(this.list);  
    }  
    ...  
}
```

- **Constructor must ensure that RI holds at end**
 - we can see that it does in this case
 - since we **don't mutate**, they will *always* be true

Correctness of FastList Constructor

```
class FastLastList implements FastList {
  // RI: this.last = last(this.list)
  // AF: obj = this.list
  last: bigint | undefined;
  list: List<bigint>;

  // makes obj = L
  constructor(L: List<bigint>) {
    this.list = L;
    this.last = last(this.list);
  }
}
```

- **Constructor must create the requested abstract state**
 - client wants obj to be the passed in list
 - we can see that $obj = this.list = L$

Correctness of getLast

```
class FastLastList implements FastList {
  // RI: this.last = last(this.list)
  // AF: obj = this.list
  ...
  // @returns last(obj)
  getLast = (): bigint | undefined => {
    return this.last;
  };
}
```

- Use both RI and AF to check correctness

last(obj) =

Correctness of getLast

```
class FastLastList implements FastList {  
  // RI: this.last = last(this.list)  
  // AF: obj = this.list  
  
  ...  
  // @returns last(obj)  
  getLast = (): bigint | undefined => {  
    return this.last;  
  };  
}
```

- Use both RI and AF to check correctness

last(obj)	= last(this.list)	by AF
	= this.last	by RI

Correctness of ADT implementation

- **Check that the constructor...**
 - creates a concrete state satisfying RI
 - creates the abstract state required by the spec
- **Check the correctness of each method...**
 - check value returned is the one stated by the spec
 - may need to use both RI and AF

ADTs: the Good and the Bad

- **Provides data abstraction**
 - can change data structures without breaking clients
- **Comes at a cost**
 - more work to specify and check correctness
- **Not everything needs to be an ADT**
 - don't be like Java and make everything a class
- **Prefer concrete types for most things**
 - concrete types are easier to think about
 - introduce ADTs when the first *change* occurs

Immutable Queues

Immutable Queue

- A queue is a list that can *only* be changed two ways:
 - add elements to the front
 - remove elements from the back

```
// List that only supports adding to the front and  
// removing from the end
```

```
interface NumberQueue {
```

```
    // @returns len(obj)  
    size(): bigint;
```

```
    // @returns [x] ++ obj  
    enqueue(x: bigint): NumberQueue;
```

```
    // @requires len(obj) > 0  
    // @returns (x, Q) with obj = Q ++ [x]  
    dequeue(): [bigint, NumberQueue];
```

```
}
```

observer

producer

producer

Implementing a Queue with a List

```
// Implements a queue with a list.  
class ListQueue implements NumberQueue {  
  
    // AF: obj = this.items  
    items: List<bigint>;  
}
```

- **Easiest implementation is concrete = abstract state**
 - just store the abstract state in a field
- **Still requires extra work to check correctness...**
 - abstraction barrier comes with a cost

Implementing a Queue with a List

```
// Implements a queue with a list.
class ListQueue implements NumberQueue {

    // AF: obj = this.items
    items: List<bigint>;

    // @returns len(obj)
    size = (): bigint => {
        return len(this.items);
    };
}
```

- **Correctness of** `size`:

`len(this.items) = len(obj)`

by AF

nothing is "straight from the spec" anymore

Implementing a Queue with a List

```
// Implements a queue with a list.
class ListQueue implements NumberQueue {

    // AF: obj = this.items
    items: List<bigint>;

    // makes obj = items
    constructor(items: List<bigint>) {
        this.items = items;
    }
}
```

- **Correctness of** `constructor`:

<code>items</code>	<code>= this.items</code>	(from code)
	<code>= obj</code>	AF

Implementing a Queue with a List

```
// Implements a queue with a list.
class ListQueue implements NumberQueue {

  // AF: obj = this.items
  items: List<bigint>;

  // @returns [x] ++ obj
  enqueue = (x: bigint): NumberQueue => {
    return new ListQueue(cons(x, this.items));
  };
}
```

- **Correctness of** enqueue:

return value = $x :: \text{this.items}$
= $x :: \text{obj}$
= $[] \# (x :: \text{obj})$
= $[x] \# \text{obj}$

spec of constructor
AF
def of concat
def of concat

Implementing a Queue with a List

```
// Implements a queue with a list.
class ListQueue implements NumberQueue {

    // AF: obj = this.items
    items: List<bigint>;

    // @requires len(obj) > 0
    // @returns (x, Q) with obj = Q ++ [x]
    dequeue = (): [bigint, NumberQueue] => {
        return [last(this.items),
                prefix(len(this.items) - 1n, this.items)];
    };
};
```

- **Declarative spec, so more reasoning is required!**
 - also, slower than necessary ($\theta(n)$ dequeue)
 - we'll skip correctness here and do something faster in a moment...

Summary of `ListQueue`

- **Simplest possible implementation of ADT**
 - abstract state = concrete state of one field
- **Reasoning about every method is more complex**
 - must apply AF to relate return value to spec's postcondition
code uses fields, but postcondition uses "obj"
 - this is the cost of the abstraction barrier

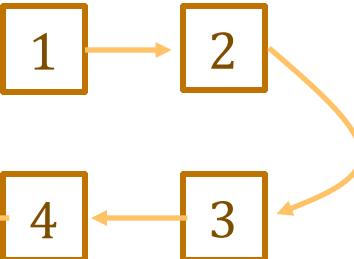
Implementing a Queue with Two Lists

```
// Implements a queue using two lists.  
class ListPairQueue implements NumberQueue {  
    // AF: obj = this.front ++ rev(this.back)  
    front: List<bigint>;  
    back: List<bigint>;    // in reverse order
```

- **Back part stored in reverse order**
 - head of front is the first element
 - head of back is the *last* element

this.front = 

this.back = 

obj = 

Implementing a Queue with Two Lists

```
// Implements a queue using two lists.
class ListPairQueue implements NumberQueue {

    // AF: obj = this.front ++ rev(this.back)
    // RI: if this.back = nil, then this.front = nil
    front: List<bigint>;
    back: List<bigint>;
}
```

- If back is nil, then the queue is *empty*
 - if back = nil, then front = nil (by RI) and thus

obj =

Implementing a Queue with Two Lists

```
// Implements a queue using two lists.
class ListPairQueue implements NumberQueue {

    // AF: obj = this.front ++ rev(this.back)
    // RI: if this.back = nil, then this.front = nil
    front: List<bigint>;
    back: List<bigint>;
}
```

- If back is nil, then the queue is *empty*
 - if back = nil, then front = nil (by RI) and thus

obj = nil # rev(nil)	by AF
= rev(nil)	def of concat
= nil	def of rev

- if the queue is not empty, then back is not nil
(311 alert: this is the contrapositive)

Implementing a Queue with Two Lists

```
// Implements a queue using two lists.
class ListPairQueue implements NumberQueue {

    // AF: obj = this.front ++ rev(this.back)
    // RI: if this.back = nil, then this.front = nil
    front: List<bigint>;
    back: List<bigint>;

    // makes obj = front ++ rev(back)
    constructor(front: List<bigint>, back: List<bigint>) {
        ...
    }
}
```

- Will implement this later...

Implementing a Queue with Two Lists

```
// AF: obj = this.front ++ rev(this.back)
front: List<bigint>;
back: List<bigint>;

// @returns len(obj)
size = (): bigint => {
  return len(this.front) + len(this.back);
};
```

- **Correctness of `size`:**

`len(obj) =`

Implementing a Queue with Two Lists

```
// AF: obj = this.front ++ rev(this.back)
front: List<bigint>;
back: List<bigint>;

// @returns len(obj)
size = (): bigint => {
  return len(this.front) + len(this.back);
};
```

- **Correctness of `size`:**

$$\begin{aligned} \text{len}(\text{obj}) &= \text{len}(\text{this.front} \# \text{rev}(\text{this.back})) \\ &= \text{len}(\text{this.front}) + \text{len}(\text{rev}(\text{this.back})) \\ &= \text{len}(\text{this.front}) + \text{len}(\text{this.back}) \end{aligned}$$

by AF
by Example 3
by another
induction

Implementing a Queue with Two Lists

```
// AF: obj = this.front ++ rev(this.back)
front: List<bigint>;
back: List<bigint>;

// @returns [x] ++ obj
enqueue = (x: bigint): NumberQueue => {
  return new ListPairQueue(cons(x, this.front), this.back)
}
```

- **Correctness of enqueue:**

ret value =

Implementing a Queue with Two Lists

```
// AF: obj = this.front ++ rev(this.back)
front: List<bigint>;
back: List<bigint>;

// @returns [x] ++ obj
enqueue = (x: bigint): NumberQueue => {
  return new ListPairQueue(cons(x, this.front), this.back)
}
```

- **Correctness of enqueue:**

$$\begin{aligned} \text{ret value} &= (x :: \text{this.front}) \# \text{rev}(\text{this.back}) \\ &= x :: (\text{this.front} \# \text{rev}(\text{this.back})) \\ &= x :: \text{obj} \\ &= [] \# (x :: \text{obj}) \\ &= [x] \# \text{obj} \end{aligned}$$

spec of constructor
def of concat
AF
def of concat
def of concat

Implementing a Queue with Two Lists

```
// AF: obj = this.front ++ rev(this.back)
front: List<bigint>;
back: List<bigint>;

// @requires len(obj) > 0
// @returns (x, Q) with obj = Q ++ [x]
dequeue = (): [bigint, NumberQueue] => {
  return [this.back.hd,
    new ListPairQueue(this.front, this.back.tl)];
};
```

- as noted previously, precondition means $\text{this.back} \neq \text{nil}$
- as we know, this means $\text{this.back} = x :: L$
where $x = \text{this.back.hd}$ and some $L = \text{this.back.tl}$

Implementing a Queue with Two Lists

```
// @requires len(obj) > 0
// @returns (x, Q) with obj = Q ++ [x]
dequeue = (): [bigint, NumberQueue] => {
  return [this.back.hd,
          new ListPairQueue(this.front, this.back.tl)];
};
```

– $\text{this.back} = x :: L$, where $x = \text{this.back.hd}$ and $L = \text{this.back.tl}$

obj =

...

...

= $(\text{this.front} \# \text{rev}(\text{this.back.tl})) \# [\text{this.back.hd}]$

Implementing a Queue with Two Lists

```
// @requires len(obj) > 0
// @returns (x, Q) with obj = Q ++ [x]
dequeue = (): [bigint, NumberQueue] => {
  return [this.back.hd,
          new ListPairQueue(this.front, this.back.tl)];
};
```

– $\text{this.back} = x :: L$, where $x = \text{this.back.hd}$ and $L = \text{this.back.tl}$

obj =

...

...

= (this.front # rev(L)) # [this.back.hd]

= (this.front # rev(this.back.tl)) # [this.back.hd] **since** $L = \text{this.back.tl}$

Implementing a Queue with Two Lists

```
// @requires len(obj) > 0
// @returns (x, Q) with obj = Q ++ [x]
dequeue = (): [bigint, NumberQueue] => {
  return [this.back.hd,
    new ListPairQueue(this.front, this.back.tl)];
};
```

– $\text{this.back} = x :: L$, where $x = \text{this.back.hd}$ and $L = \text{this.back.tl}$

obj =

...

...

= (this.front # rev(L)) # [x]

= (this.front # rev(L)) # [this.back.hd] **since** $x = \text{this.back.hd}$

= (this.front # rev(this.back.tl)) # [this.back.hd] **since** $L = \text{this.back.tl}$

Implementing a Queue with Two Lists

```
// @requires len(obj) > 0
// @returns (x, Q) with obj = Q ++ [x]
dequeue = (): [bigint, NumberQueue] => {
  return [this.back.hd,
    new ListPairQueue(this.front, this.back.tl)];
};
```

– $\text{this.back} = x :: L$, where $x = \text{this.back.hd}$ and $L = \text{this.back.tl}$

$\text{obj} = \text{this.front} \# \text{rev}(\text{this.back})$
 $= \text{this.front} \# \text{rev}(x :: L)$
 $= \text{this.front} \# (\text{rev}(L) \# [x])$
 $= (\text{this.front} \# \text{rev}(L)) \# [x]$

by AF
since $\text{back} = x :: L$
def of rev

Implementing a Queue with Two Lists

```
// AF: obj = this.front ++ rev(this.back)
// RI: if this.back = nil, then this.front = nil
front: List<bigint>;
back: List<bigint>;

// makes obj = front ++ rev(back)
constructor(front: List<bigint>, back: List<bigint>) {
  if (back.kind === "nil") {
    this.front = nil;
    this.back = rev(front);           holds since this.front = nil
  } else {
    this.front = front;
    this.back = back;                holds since this.back ≠ nil
  }
}
```

- Need to check that RI holds at end of constructor

Implementing a Queue with Two Lists

```
// AF: obj = this.front ++ rev(this.back)
// RI: if this.back = nil, then this.front = nil
front: List<bigint>;
back: List<bigint>;

// makes obj = front ++ rev(back)
constructor(front: List<bigint>, back: List<bigint>) {
  if (back.kind === "nil") {
    this.front = nil;
    this.back = rev(front);           obj = nil # rev(rev(front)) ??
  } else {
    this.front = front;
    this.back = back;                obj = front # rev(back)
  }
}
```

- Need to check this creates correct abstract state

Implementing a Queue with Two Lists

```
// AF: obj = this.front ++ rev(this.back)
// RI: if this.back = nil, then this.front = nil
front: List<bigint>;
back: List<bigint>;

constructor(front: List<bigint>, back: List<bigint>) {
  if (back.kind === "nil") {
    this.front = nil;
    this.back = rev(front);
  } else {
    ...
  }
}
```



```
obj = nil # rev(rev(front))
    = nil # front
    = front
    = front # nil
    = front # rev(nil)
    = front # rev(back)
```

AF
because I said so
def of concat

def of rev
since back = nil

Enums

Inductive Data Types

- Describe a set by ways of creating its elements

- each is a “constructor”

`type T := A | B | C(x : \mathbb{Z}) | D(x : \mathbb{S}^* , t : T) | E(s : T, t : T)`

- constructors taking arguments of type T are "recursive"

- A, B, C have no recursive arguments

- D has one recursive argument

- E has two recursive arguments

Inductive Data Types

- Describe a set by ways of creating its elements

- each is a “constructor”

`type T := A | B | C(x : \mathbb{Z}) | D(x : \mathbb{S}^* , t : T) | E(s : T, t : T)`

- Categories of inductive data types...

- no constructors with recursive arguments = “generalized enums”
- constructor with **1** recursive arguments = “generalized lists”
- constructor with **2+** recursive arguments = “generalized trees”

- Even **enums** come up all the time...

Example: Auction pages

- Auction site has three different “pages”

Current Auctions

- Oak Cabinet ends in 10 min
- Red Couch ends in 15 min
- Blue Bicycle

New

Oak Cabinet

A beautiful solid oak cabinet. Perfect for any bedroom. Dimensions are 42” x 60”.

Current Bid: \$250

Name

Fred

Bid

251

Submit

New Auction

Name

Bob

Item

Table Lamp

...

App component needs to show one of these components.

Must keep track of which one we are currently showing.

Auction App.tsx

```
type Page = {kind: "list"}
           | {kind: "new"}
           | {kind: "details", name: string};
```

```
type AppState = {page: Page};
```

- **Page is an inductive data type:**

```
type Page := list | new | details(name: S*)
```

- App keeps track of the current page
- note that "details" has an argument (which auction's details)

Auction App.tsx

```
type Page = {kind: "list"}
           | {kind: "new"}
           | {kind: "details", name: string};

type AppState = {page: Page};

class App extends Component<{}, AppState> {
  render = (): JSX.Element => {
    if (this.state.page.kind === "list") {
      return <AuctionList/>;
    } else if (this.state.page.kind === "new") {
      return <NewAuction/>;
    } else {
      return <AuctionDetails
                name={this.state.page.name}/>;
    }
  };
};
```


Trees

Trees

- **Trees are inductive types with a constructor that has 2+ recursive arguments**
- **These come up all the time...**
 - no constructors with recursive arguments = “generalized enums”
 - constructor with 1 recursive arguments = “generalized lists”
 - constructor with 2+ recursive arguments = “generalized trees”
- **Some prominent examples of trees:**
 - HTML: used to describe UI
 - JSON: used to describe just about any data

Structural Induction

```
type T := A
      | B
      | C(x : ℤ)
      | D(x : S*, t : T)
      | E(s : T, t : T)
```

- **To prove $P(t)$ for all $t : T$:**

prove $P(A)$

prove $P(B)$

prove $P(C(x))$

prove $P(D(x, t))$

prove $P(E(s, t))$

– **(this is proof by cases)**

Structural Induction

```
type T := A
      | B
      | C(x : ℤ)
      | D(x : S*, t : T)
      | E(s : T, t : T)
```

- **To prove $P(t)$ for all $t : T$:**

prove $P(A)$

prove $P(B)$

prove $P(C(x))$

prove $P(D(x, t))$ **assuming $P(t)$**

prove $P(E(s, t))$ **assuming $P(s)$ and $P(t)$**

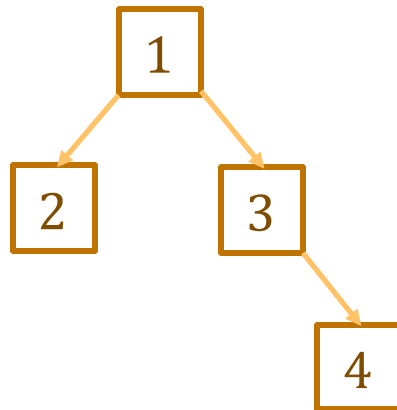
– **this is structural induction!**

Binary Trees

`type Tree := empty | node(x : \mathbb{Z} , L : Tree, R : Tree)`

- **Inductive definition of binary trees of integers**

`node(1, node(2, empty, empty), node(3, empty, node(4, empty, empty)))`



Functions on Trees

`type Tree := empty | node(x: \mathbb{Z} , L: Tree, R: Tree)`

`num-nodes : Tree \rightarrow \mathbb{N}`

`num-nodes(empty) := 0`

`num-nodes(node(x, L, R)) := 1 + num-nodes(L) + num-nodes(R)`

- **How many nodes are in the tree?**

Functions on Trees

`type Tree := empty | node(x: \mathbb{Z} , L: Tree, R: Tree)`

`num-edges : Tree \rightarrow \mathbb{N}`

`num-edges(empty) := -1`

`num-edges(node(x, L, R)) := 2 + num-edges(L) + num-edges(R)`

- **How many edges are in the tree?**
 - "edge" is a move from one node to another

Edges in Tree

$\text{num-edges} : \text{Tree} \rightarrow \mathbb{N}$

$\text{num-edges}(\text{empty}) \quad := -1$

$\text{num-edges}(\text{node}(x, L, R)) \quad := 2 + \text{num-edges}(L) + \text{num-edges}(R)$

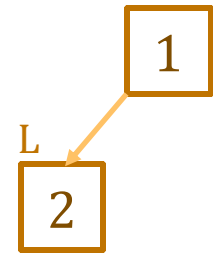
- **Why a "-1" here?**

$\text{num-edges}(\text{node}(x, L, \text{empty}))$

$= 2 + \text{num-edges}(L) + \text{num-edges}(\text{empty})$

$= 2 + \text{num-edges}(L) + -1$

$= 1 + \text{num-edges}(L)$



$\text{num-edges}(\text{node}(x, \text{empty}, \text{empty}))$

$= 2 + \text{num-edges}(\text{empty}) + \text{num-edges}(\text{empty})$

$= 2 + -1 + -1$

$= 0$



Structural Induction

Let $P(T)$ be the claim " $\text{num-nodes}(T) = \text{num-edges}(T) + 1$ "

Prove $P(T)$ holds for any tree T by structural induction

Base Case: prove $P(\text{empty})$

$$\begin{aligned} \text{num-nodes}(\text{empty}) \\ = 0 \end{aligned}$$

def of num-nodes

Structural Induction

Let $P(T)$ be the claim " $\text{num-nodes}(T) = \text{num-edges}(T) + 1$ "

Prove $P(T)$ holds for any tree T by structural induction

Base Case: prove $P(\text{empty})$

$\text{num-nodes}(\text{empty})$

$= 0$

...

$= \text{num-edges}(\text{empty}) + 1$

def of num-nodes

??

Structural Induction

Let $P(T)$ be the claim " $\text{num-nodes}(T) = \text{num-edges}(T) + 1$ "

Prove $P(T)$ holds for any tree T by structural induction

Base Case: prove $P(\text{empty})$

$\text{num-nodes}(\text{empty})$

$= 0$

def of num-nodes

$= -1 + 1$

$= \text{num-edges}(\text{empty}) + 1$

def of num-edges

Structural Induction

Let $P(T)$ be the claim " $\text{num-nodes}(T) = \text{num-edges}(T) + 1$ "

Inductive Hypothesis: assume $P(L)$ and $P(R)$

– assume P for both subtrees

Inductive Step: prove $P(\text{node}(x, L, R))$

– use known facts and definitions and Inductive Hypotheses

Structural Induction

Let $P(T)$ be the claim " $\text{num-nodes}(T) = \text{num-edges}(T) + 1$ "

Inductive Step: prove $P(\text{node}(x, L, R))$

$$\begin{aligned} \text{num-nodes}(\text{node}(x, L, R)) & \\ &= 1 + \text{num-nodes}(L) + \text{num-nodes}(R) && \text{def of num-nodes} \\ &= 1 + \text{num-edges}(L) + 1 + \text{num-nodes}(R) && \text{Ind. Hyp.} \\ &= 1 + \text{num-edges}(L) + 1 + \text{num-edges}(R) + 1 && \text{Ind. Hyp.} \end{aligned}$$

$$\text{num-nodes}(\text{node}(x, L, R)) := 1 + \text{num-nodes}(L) + \text{num-nodes}(R)$$

$$\text{num-edges}(\text{node}(x, L, R)) := 2 + \text{num-edges}(L) + \text{num-edges}(R)$$

Structural Induction

Let $P(T)$ be the claim " $\text{num-nodes}(T) = \text{num-edges}(T) + 1$ "

Inductive Step: prove $P(\text{node}(x, L, R))$

$\text{num-nodes}(\text{node}(x, L, R))$	
$= 1 + \text{num-nodes}(L) + \text{num-nodes}(R)$	def of num-nodes
$= 1 + \text{num-edges}(L) + 1 + \text{num-nodes}(R)$	Ind. Hyp.
$= 1 + \text{num-edges}(L) + 1 + \text{num-edges}(R) + 1$	Ind. Hyp.
$= \dots$	
$= \text{num-edges}(\text{node}(x, L, R)) + 1$??

$$\text{num-nodes}(\text{node}(x, L, R)) := 1 + \text{num-nodes}(L) + \text{num-nodes}(R)$$

$$\text{num-edges}(\text{node}(x, L, R)) := 2 + \text{num-edges}(L) + \text{num-edges}(R)$$

Structural Induction

Let $P(T)$ be the claim " $\text{num-nodes}(T) = \text{num-edges}(T) + 1$ "

Inductive Step: prove $P(\text{node}(x, L, R))$

$$\begin{aligned} \text{num-nodes}(\text{node}(x, L, R)) & \\ &= 1 + \text{num-nodes}(L) + \text{num-nodes}(R) && \text{def of num-nodes} \\ &= 1 + \text{num-edges}(L) + 1 + \text{num-nodes}(R) && \text{Ind. Hyp.} \\ &= 1 + \text{num-edges}(L) + 1 + \text{num-edges}(R) + 1 && \text{Ind. Hyp.} \\ &= 2 + \text{num-edges}(L) + \text{num-edges}(R) + 1 \\ &= \text{num-edges}(\text{node}(x, L, R)) + 1 && \text{def of num-edges} \end{aligned}$$

$$\text{num-nodes}(\text{node}(x, L, R)) := 1 + \text{num-nodes}(L) + \text{num-nodes}(R)$$

$$\text{num-edges}(\text{node}(x, L, R)) := 2 + \text{num-edges}(L) + \text{num-edges}(R)$$

Common ADTs

- **Some commonly used ADTs**
 - **stack**: add & remove from one end
 - **queue**: add to one end, remove from other
 - **set**: add, remove, & check if contained in list
 - **map**: add, remove, & get value for (key, value) pair
- **All of these are specified by lists**
 - maps are "association lists" (lists of pairs)

Association Lists

- **A list of pairs $\text{List}\langle(K,V)\rangle$ is an "association list"**
 - can be used to describe a map from keys to values
 - **set the value associated with a key:**

$\text{set-value} : (K, V, \text{List}\langle(K, V)\rangle) \rightarrow \text{List}\langle(K, V)\rangle$

$\text{set-value}(x, v, L) := (x, v) :: L$

- **first pair with that key has the current value**
- **could choose to remove any later pairs with this key**
 - saves memory and makes debugging harder (hooray!)

Association Lists

- **A list of pairs $\text{List}\langle(K, V)\rangle$ is an "association list"**
 - can be used to describe a map from keys to values
 - retrieve the (first) value associated with a key:

$\text{get-value} : (K, \text{List}\langle(K, V)\rangle) \rightarrow V$

$\text{get-value}(x, \text{nil}) \quad := \text{undefined}$

$\text{get-value}(x, (y, v) :: L) \quad := v \quad \text{if } x = y$

$\text{get-value}(x, (y, v) :: L) \quad := \text{get-value}(x, L) \quad \text{if } x \neq y$

$\text{contains-key} : (K, \text{List}\langle(K, V)\rangle) \rightarrow \mathbb{B}$

$\text{contains-key}(x, \text{nil}) \quad := \text{false}$

$\text{contains-key}(x, (y, v) :: L) \quad := \text{true} \quad \text{if } x = y$

$\text{contains-key}(x, (y, v) :: L) \quad := \text{contains-key}(x, L) \quad \text{if } x \neq y$

Notice anything about these functions?

Association Lists

Two association lists are "the same" if they return the same values for each key

- Can see that get/set work as expected:
 - get the value just set (v):

get-value(x, set-value(x, v, L))
= get-value(x, (x, v) :: L) def of set-value
= v def of get-value

- get the value of a key not just set ($x \neq y$):

get-value(y, set-value(x, v, L))
= get-value(y, (x, v) :: L) def of set-value
= get-value(y, L) def of get-value (since $x \neq y$)

set-value(x, v, L) := (x, v) :: L get-value(x, (y, v) :: L) := v if $x = y$
get-value(x, (y, v) :: L) := get-value(x, L) if $x \neq y$

Immutable Map

- An "association list" also called a "map"

```
// List of (key, value) pairs
interface Map<K, V> {

    // @returns contains-key(x, obj)
containsKey(x: K): boolean;

    // @requires containsKey(x, obj)
// @returns get-value(x, obj)
getValue(x: K): V;

    // @returns set-value(x, v, obj)
setValue(x: K, v: V): Map<K, V>;
}
```

observer

observer

producer

Mutable Map

- An "association list" also called a "map"

```
// List of (key, value) pairs
interface Map<K, V> {

    // @returns contains-key(x, obj)
containsKey(x: K): boolean;

    // @requires containsKey(x, obj)
    // @returns get-value(x, obj)
getValue(x: K): V;

    // @modifies obj
    // @effects obj = set-value(x, v, obj)
setValue(x: K, v: V): void;
}
```

observer

observer

mutator

This version saves some memory and ...
makes debugging harder and...

Introduces possible aliasing bugs!

Common ADTs

- **Some commonly used ADTs**
 - **stack**: add & remove from one end
 - **queue**: add to one end, remove from other
 - **set**: add, remove, & check if contained in list
 - **map**: add, remove, & get value for (key, value) pair
- **All of these are specified by lists**
 - maps are "association lists" (lists of pairs)
- **Set and Map can be implemented with trees**

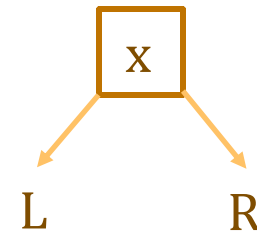
Binary Search Trees (BSTs)

`type BST := empty | node(x : \mathbb{Z} , v : \mathbb{Z} , L : BST, R : BST)`

- stores a value "v" as well as a key "x"
- BSTs add an extra **rep invariant** to every node

`contains-key(y, L) → (y < x)`

`contains-key(z, R) → (x < z)`



Binary Search Trees (BSTs)

`type BST := empty | node(x : \mathbb{Z} , v : \mathbb{Z} , L : BST, R : BST)`

- **Get the value associated with a key in the tree:**

`get-value : (\mathbb{Z} , BST) \rightarrow \mathbb{Z}`

`get-value(x, empty) := undefined`

`get-value(x, node(y, w, L, R)) := w if x = y`

`get-value(x, node(y, w, L, R)) := get-value(x, L) if x < y`

`get-value(x, node(y, w, L, R)) := get-value(x, R) if y < x`

Binary Search Trees (BSTs)

`type BST := empty | node(x : \mathbb{Z} , v : \mathbb{Z} , L : BST, R : BST)`

- **Set a (key, value) in the tree:**

`set-value : (\mathbb{Z} , \mathbb{Z} , BST) \rightarrow BST`

`set-value(x, v, empty) := node(x, v, empty, empty)`

`set-value(x, v, node(y, w, L, R)) := node(x, v, L, R) if $x = y$`

`set-value(x, v, node(y, w, L, R)) := node(y, w, set-value(x, v, L), R) if $x < y$`

`set-value(x, v, node(y, w, L, R)) := node(y, w, L, set-value(x, v, R)) if $y < x$`

- add a new node if the key is not present
- replace the value if the key is present

Binary Search Trees (BSTs)

`type BST := empty | node(x : \mathbb{Z} , v : \mathbb{Z} , L : BST, R : BST)`

- **Set a (key, value) in the tree:**

`set-value : (\mathbb{Z} , \mathbb{Z} , BST) \rightarrow BST`

`set-value(x, v, empty) := node(x, v, empty, empty)`

`set-value(x, v, node(y, w, L, R)) := node(x, v, L, R) if x = y`

`set-value(x, v, node(y, w, L, R)) := node(y, w, set-value(x, v, L), R) if x < y`

`set-value(x, v, node(y, w, L, R)) := node(y, w, L, set-value(x, v, R)) if y < x`

- note that this does **not mutate** the existing tree
- the old tree is still around and unchanged

Binary Search Trees (BSTs)

set-value(5, 7, node(6, a, L₁, R₁))

= node(6, a, set-value(5, 7, node(3, b, L₂, R₂)), R₁)

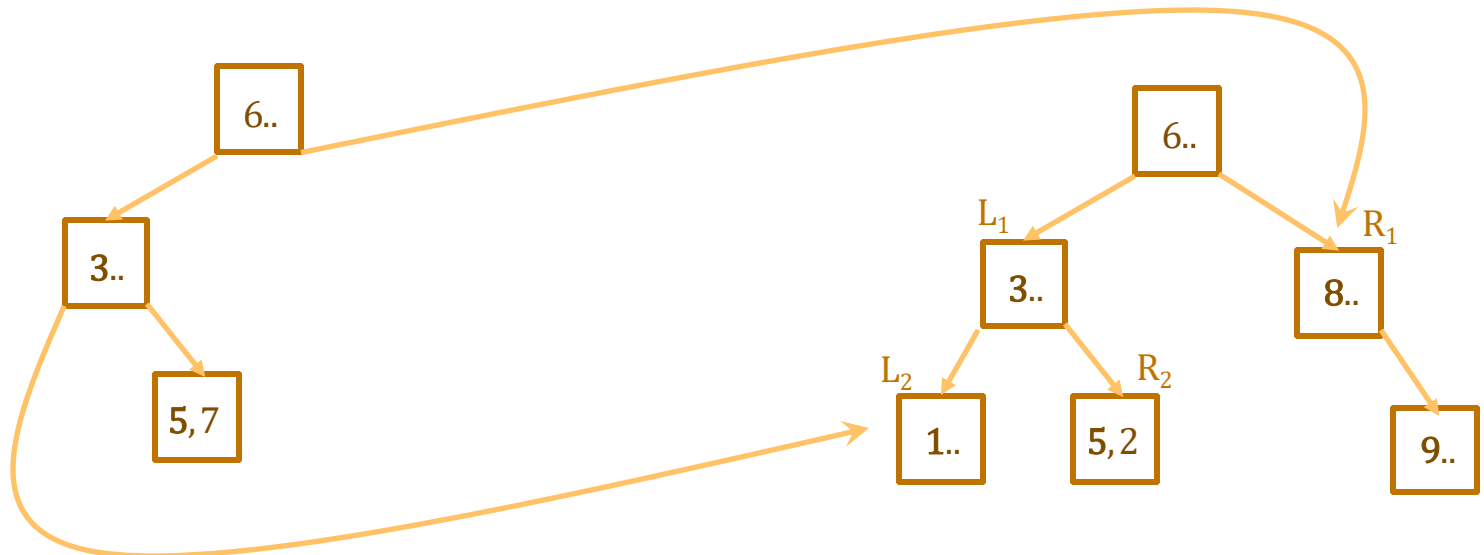
def of set-value (5 < 6)

= node(6, a, node(3, b, L₂, set-value(5, 7, node(5, 2, empty, empty))), R₁) ... (5 > 3)

= node(6, a, node(3, b, L₂, node(5, 7, empty, empty))), R₁) **def of set-value**

- **only copies the path to 5 in the tree**

only O(log n) extra memory for a balanced tree



Binary Search Trees (BSTs)

- Use **reasoning** to make sure this works...
 - easier to reason than to *debug and then reason*
 - get the value just set (v):

$$\text{get-value}(x, \text{set-value}(x, v, T)) = v \text{ ??}$$

- get the value of a key not just set ($x \neq y$):

$$\text{get-value}(y, \text{set-value}(x, v, T)) = \text{get-value}(y, T) \text{ ??}$$

Binary Search Trees (BSTs)

- Use **reasoning** to make sure this works...
 - easier to reason than to *debug and then reason*
 - get the value just set (v):

$$\text{get-value}(x, \text{set-value}(x, v, T)) = v$$

- **how do we prove this for all T : BST?**
last time, it was just a calculation

Structural Induction

Let $P(T)$ be the claim "get-value(x, set-value(x, v, T)) = v"

Prove $P(T)$ holds for any BST T by structural induction

Base Case: prove $P(\text{empty})$

$$\begin{aligned} & \text{get-value}(x, \text{set-value}(x, v, \text{empty})) \\ &= \text{get-value}(x, \text{node}(x, v, \text{empty}, \text{empty})) && \text{def of set-value} \\ &= v && \text{def of get-value} \end{aligned}$$

set-value(x, v, empty)	:= node(x, v, empty, empty)		
set-value(x, v, node(y, w, L, R))	:= node(x, v, L, R)	if x = y	get-value(x, node(y, w, L, R)) := v
set-value(x, v, node(y, w, L, R))	:= node(y, w, set-value(x, v, L), R)	if x < y	get-value(x, node(y, w, L, R)) := get-value(x, L)
set-value(x, v, node(y, w, L, R))	:= node(y, w, L, set-value(x, v, R))	if y < x	get-value(x, node(y, w, L, R)) := get-value(x, R)

Structural Induction

$P(T) := \text{"get-value}(x, \text{set-value}(x, v, T)) = v\text{"}$

Inductive Hypothesis: assume $P(L)$ and $P(R)$

– assume P for both subtrees

Inductive Step: prove $P(\text{node}(y, w, L, R))$

– use known facts and definitions and Inductive Hypotheses

Structural Induction

$P(T) := \text{"get-value}(x, \text{set-value}(x, v, T)) = v\text{"}$

Inductive Step: prove $P(\text{node}(y, w, L, R))$

$\text{get-value}(x, \text{set-value}(x, v, \text{node}(y, w, L, R)))$
 $= ??$

Don't know which rule of definition applies!

Need to continue by cases.

$\text{set-value}(x, v, \text{empty})$	$:= \text{node}(x, v, \text{empty}, \text{empty})$		
$\text{set-value}(x, v, \text{node}(y, w, L, R))$	$:= \text{node}(x, v, L, R)$	if $x = y$	$\text{get-value}(x, \text{node}(y, w, L, R)) := v$
$\text{set-value}(x, v, \text{node}(y, w, L, R))$	$:= \text{node}(y, w, \text{set-value}(x, v, L), R)$	if $x < y$	$\text{get-value}(x, \text{node}(y, w, L, R)) := \text{get-value}(x, L)$
$\text{set-value}(x, v, \text{node}(y, w, L, R))$	$:= \text{node}(y, w, L, \text{set-value}(x, v, R))$	if $y < x$	$\text{get-value}(x, \text{node}(y, w, L, R)) := \text{get-value}(x, R)$

Structural Induction

$P(T) := \text{"get-value}(x, \text{set-value}(x, v, T)) = v\text{"}$

Inductive Step: prove $P(\text{node}(y, w, L, R))$

Suppose that $x = y$.

$\text{get-value}(x, \text{set-value}(x, v, \text{node}(y, w, L, R)))$

$= \text{get-value}(x, \text{node}(x, v, L, R))$

$= v$

def of set-value (since $x=y$)

def of get-value

$\text{set-value}(x, v, \text{empty}) := \text{node}(x, v, \text{empty}, \text{empty})$

$\text{set-value}(x, v, \text{node}(y, w, L, R)) := \text{node}(x, v, L, R)$

$\text{set-value}(x, v, \text{node}(y, w, L, R)) := \text{node}(y, w, \text{set-value}(x, v, L), R)$

$\text{set-value}(x, v, \text{node}(y, w, L, R)) := \text{node}(y, w, L, \text{set-value}(x, v, R))$

if $x = y$

if $x < y$

if $y < x$

$\text{get-value}(x, \text{node}(y, w, L, R)) := v$

$\text{get-value}(x, \text{node}(y, w, L, R)) := \text{get-value}(x, L)$

$\text{get-value}(x, \text{node}(y, w, L, R)) := \text{get-value}(x, R)$

Structural Induction

$P(T) := \text{"get-value}(x, \text{set-value}(x, v, T)) = v\text{"}$

Inductive Step: prove $P(\text{node}(y, w, L, R))$

Suppose that $x < y$.

$\text{get-value}(x, \text{set-value}(x, v, \text{node}(y, w, L, R)))$	
$= \text{get-value}(x, \text{node}(y, w, \text{set-value}(x, v, L), R))$	def of set-value (since $x < y$)
$= \text{get-value}(x, \text{set-value}(x, v, L))$	def of get-value (since $x < y$)
$= v$	Ind. Hyp.

Suppose that $x > y$ (Analogous)

$\text{set-value}(x, v, \text{empty})$	$:= \text{node}(x, v, \text{empty}, \text{empty})$		
$\text{set-value}(x, v, \text{node}(y, w, L, R))$	$:= \text{node}(x, v, L, R)$	if $x = y$	$\text{get-value}(x, \text{node}(y, w, L, R)) := v$
$\text{set-value}(x, v, \text{node}(y, w, L, R))$	$:= \text{node}(y, w, \text{set-value}(x, v, L), R)$	if $x < y$	$\text{get-value}(x, \text{node}(y, w, L, R)) := \text{get-value}(x, L)$
$\text{set-value}(x, v, \text{node}(y, w, L, R))$	$:= \text{node}(y, w, L, \text{set-value}(x, v, R))$	if $y < x$	$\text{get-value}(x, \text{node}(y, w, L, R)) := \text{get-value}(x, R)$