KODKOD by example

code checking, data repair, debugging and synthesis in 20 minutes

emina torlak

Dagstuhl · April 11, 2012
about kodkod

Kodkod is an efficient SAT-based constraint solver for first order logic with relations, transitive closure, bit-vector arithmetic, and partial models. It provides analyses for both satisfiable and unsatisfiable problems: a finite model finder for the former and a minimal unsatisfiable core extractor for the latter. Kodkod is used in a wide range of applications, including code checking, test-case generation, declarative execution, declarative configuration, and lightweight analysis of Alloy, UML, and Isabelle/HOL.

Designed as a plugin component that can be easily incorporated into other tools, Kodkod provides a clean Java interface for constructing, manipulating, and solving constraints. The implementation is open-source and available for download under the MIT license. The source code is extensively documented and the distribution includes many examples demonstrating the use of the Kodkod API.

contact

Emina Torlak (emina at alum.mit.edu)
some applications of kodkod

checking theorems & designs
› Alloy4 (Alloy), Nitpick (Isabelle/HOL), ProB (B, Event-B, Z and TLA⁺), ExUML (UML)

checking code & memory models
› Forge, Karun, Miniatur, TACO, MemSAT

declarative programming, fault recovery & data structure repair
› Squander, PBnJ, Tarmeem, Cobbler

declarative configuration
› ConfigAssure (networks), Margrave (policies)

test-case generation
› Kesit, Whispec
example: reversing a linked list

class List {
    Node head;

    void reverse() {
        Node near = head;
        Node mid = near.next;
        Node far = mid.next;
        near.next = far;
        while (far != null) {
            mid.next = near;
            near = mid;
            mid = far;
            far = far.next;
        }
        mid.next = near;
        head = mid;
    }
}

class Node {
    Node next;
    String data;
}
example: reversing a linked list

class List {
    Node head;

    void reverse() {
        Node near = head;
        Node mid = near.next;
        Node far = mid.next;

        near.next = far;
        while (far != null) {
            mid.next = near;
            near = mid;
            mid = far;
            far = far.next;
        }

        mid.next = near;
        head = mid;
    }
}

class Node {
    Node next;
    String data; }

invariants, pre and post conditions

class List {
    Node head;

    void reverse() {
        Node near = head;
        Node mid = near.next;
        Node far = mid.next;

        near.next = far;
        while (far != null) {
            mid.next = near;
            near = mid;
            mid = far;
            far = far.next;
        }

        mid.next = near;
        head = mid;
    }
}

class Node {
    Node next;
    String data;
}
invariants, pre and post conditions

class List {
    Node head;

    void reverse() {
        Node near = head;
        Node mid = near.next;
        Node far = mid.next;

        near.next = far;
        while (far != null) {
            mid.next = near;
            near = mid;
            mid = far;
            far = far.next;
        }

        mid.next = near;
        head = mid;
    }
}

class Node {
    Node next;
    String data;
}
invariants, pre and post conditions

class List {
    Node head;
    
    void reverse() {
        Node near = head;
        Node mid = near.next;
        Node far = mid.next;
        
        near.next = far;
        while (far != null) {
            mid.next = near;
            near = mid;
            mid = far;
            far = far.next;
        }
        mid.next = near;
        head = mid;
    }
}

class Node {
    Node next;
    String data;
}
class List {
    Node head;

    void reverse() {
        Node near = head;
        Node mid = near.next;
        Node far = mid.next;

        near.next = far;
        while (far != null) {
            mid.next = near;
            near = mid;
            mid = far;
            far = far.next;
        }

        mid.next = near;
        head = mid;
    }
}

class Node {
    Node next;
    String data;
}
invariants, pre and post conditions

```java
class List {
    Node head;

    void reverse() {
        Node near = head;
        Node mid = near.next;
        Node far = mid.next;

        near.next = far;
        while (far != null) {
            mid.next = near;
            near = mid;
            mid = far;
            far = far.next;
        }

        mid.next = near;
        head = mid;
    }
}

class Node {
    Node next;
    String data;
}
```

@requires Pre(this, head, next)

@ensures Post(this, old(head), head, old(next), next)

@invariant Inv(next)
a relational view of the heap

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

```java
void reverse() {
    Node near = head;
    Node mid = near.next;
    Node far = mid.next;

    near.next = far;
    while (far != null) {
        mid.next = near;
        near = mid;
        mid = far;
        far = far.next;
    }

    mid.next = near;
    head = mid;
}
```

A relational view of the heap

```java
@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near = head;
    Node mid = near.next;
    Node far = mid.next;
    
    near.next = far;
    while (far != null) {
        mid.next = near;
        near = mid;
        mid = far;
        far = far.next;
    }
    mid.next = near;
    head = mid;
}
```

Fields as binary relations
- head ≡ { <this, n2> }, next ≡ { <n2, n1>, ... }
a relational view of the heap

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near = head;
    Node mid = near.next;
    Node far = mid.next;

    near.next = far;
    while (far != null) {
        mid.next = near;
        near = mid;
        mid = far;
        far = far.next;
    }

    mid.next = near;
    head = mid;
}
a relational view of the heap

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near = head;
    Node mid = near.next;
    Node far = mid.next;

    near.next = far;
    while (far != null) {
        mid.next = near;
        near = mid;
        mid = far;
        far = far.next;
    }

    mid.next = near;
    head = mid;
}

fields as binary relations
- head ≡ { <this, n2> }, next ≡ { <n2, n1>, ... }

types as sets (unary relations)
- List ≡ { <this> }, Node ≡ { <n0>, <n1>, <n2> }

objects as scalars (singleton unary relations)
- this ≡ { <this> }, null ≡ { <null> }

![Diagram of a linked list with nodes and pointers](image-url)
a relational view of the heap

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

```java
void reverse() {
    Node near = head;
    Node mid = near.next;
    Node far = mid.next;

    near.next = far;
    while (far != null) {
        mid.next = near;
        near = mid;
        mid = far;
        far = far.next;
    }

    mid.next = near;
    head = mid;
}
```

fields as binary relations
○ head ≡ { <this, n2> }, next ≡ { <n2, n1>, ... }

types as sets (unary relations)
○ List ≡ { <this> }, Node ≡ { <n0>, <n1>, <n2> }

objects as scalars (singleton unary relations)
○ this ≡ { <this> }, null ≡ { <null> }

field access as relational join (.)
○ this.head ≡ { <this> } . { <this, n2> } = { <n2> }

![Diagram of linked list with nodes and pointers]
a relational view of the heap

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

```java
void reverse() {
    Node near = head;
    Node mid = near.next;
    Node far = mid.next;

    near.next = far;
    while (far != null) {
        mid.next = near;
        near = mid;
        mid = far;
        far = far.next;
    }

    mid.next = near;
    head = mid;
}
```

fields as binary relations
- \(\text{head} \equiv \{ <\text{this, n2}> \} \), \(\text{next} \equiv \{ <\text{n2, n1}>, \ldots \} \)

types as sets (unary relations)
- \(\text{List} \equiv \{ <\text{this}> \} \), \(\text{Node} \equiv \{ <\text{n0}, <\text{n1}, <\text{n2}> \} \)

objects as scalars (singleton unary relations)
- \(\text{this} \equiv \{ <\text{this}> \} \), \(\text{null} \equiv \{ <\text{null}> \} \)

field access as relational join (.)
- \(\text{this}.\text{head} \equiv \{ <\text{this}> \}.\{ <\text{this, n2}> \} = \{ <\text{n2}> \} \)

field update as relational override (++)
- \(\text{this}.\text{head} = \text{null} \equiv \text{head} ++ (\text{this} \times \text{null}) = \{ <\text{this, n2}> \} ++ \{ <\text{this, null}> \} = \{ <\text{this, null}> \} \)
code checking with kodkod

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

```java
void reverse() {
    Node near = head;
    Node mid = near.next;
    Node far = mid.next;

    near.next = far;
    while (far != null) {
        mid.next = near;
        near = mid;
        mid = far;
        far = far.next;
    }

    mid.next = near;
    head = mid;
}
```
code checking with kodkod

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

```java
void reverse() {
    Node near = head;
    Node mid = near.next;
    Node far = mid.next;

    near.next = far;
    if (far != null) {
        mid.next = near;
        near = mid;
        mid = far;
        far = far.next;
    }
    assume far == null;
    mid.next = near;
    head = mid;
}
```

finitize loops

- e.g., unwind once
code checking with kodkod

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near₀ = this.head;
    Node mid₀ = near₀.next;
    Node far₀ = mid₀.next;
    near₀.next = far₀;
    if (far₀ != null) {
        mid₀.next = near₀;
        near₀ = mid₀;
        mid₀ = far₀;
        far₀ = far₀.next;
    }
    assume far₀ == null;
    near₂ = phi(guard, near₁, near₀);
    mid₂ = phi(guard, mid₁, mid₀);
    far₂ = phi(guard, far₁, far₀);
    next₂ = phi(guard, next₁, next₀);
    assume far₂ == null;
    next₃ = update(next₂, mid₂, near₂);
    head₀ = update(head, this, mid₀);
}

finitize loops
  › e.g., unwind once

convert to SSA
  › SSA for both locals and fields
code checking with kodkod

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near = this.head;
    Node mid = near.next;
    Node far = mid.next;
    near.next = far;
    while (far != null) {
        mid.next = near;
        near = mid;
        mid = far;
        far = far.next;
    }
    mid.next = near;
    head = mid;
}

finitize loops
› e.g., unwind once

convert to SSA
› SSA for both locals and fields

encode program semantics in relational logic
void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, far0);
    boolean guard = (far0 != null);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}
code checking with kodkod

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near = this.head;
    Node mid = near.next;
    Node far = mid.next;
    near.next = far;
    while (far != null) {
        mid.next = near;
        near = mid;
        mid = far;
        far = far.next;
    }
    mid.next = near;
    head = mid;
}

finitize loops
  › e.g., unwind once

convert to SSA
  › SSA for both locals and fields

encode program semantics in relational logic

specify analysis bounds

for details see
  › Forge [Dennis, 2006, 2008]
  › Miniatur [Dolby et al., 2007]
  › MemSAT [Torlak et al., 2010]
translating code to relational logic

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near₀ = this.head;
    Node mid₀ = near₀.next;
    Node far₀ = mid₀.next;

    next₀ = update(next, near₀, far₀);
    boolean guard = (far₀ != null);
    next₁ = update(next₀, mid₀, near₀);
    near₁ = mid₀;
    mid₁ = far₀;
    far₁ = far₀.next₁;

    near₂ = phi(guard, near₁, near₀);
    mid₂ = phi(guard, mid₁, mid₀);
    far₂ = phi(guard, far₁, far₀);
    next₂ = phi(guard, next₁, next₀);

    assume far₂ == null;

    next₃ = update(next₂, mid₂, near₂);
    head₀ = update(head, this, mid₂);
}
translating code to relational logic

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, far0);
    boolean guard = (far0 != null);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}

this ⊆ List ∧ one this ∧
head ⊆ List → (Node ∪ null) ∧
next ⊆ Node → (Node ∪ null) ∧
data ⊆ Node → (String ∪ null) ∧

encode the post-state relations in terms of the pre-state, using relational joins and overrides

use the pre- and post-state relations to encode invariants, preconditions, and negated postconditions
translating code to relational logic

```
@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, far0);
    boolean guard = (far0 != null);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}
```

encode the post-state relations in terms of the pre-state, using relational joins and overrides

use the pre- and post-state relations to encode invariants, preconditions, and negated postconditions
translating code to relational logic

```java
@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;
    next0 = update(next, near0, far0);
    boolean guard = (far0 != null);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;
    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);
    assume far2 == null;
    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}
```

```plaintext
this ⊆ List ∧ one this ∧
head ⊆ List → (Node ∪ null) ∧
next ⊆ Node → (Node ∪ null) ∧
data ⊆ Node → (String ∪ null) ∧

let near0 = this.head,
    mid0 = near0.next,
    far0 = mid0.next,
    next0 = next ++ (near0 × far0),
    guard = (far0 != null),
    next1 = next0 ++ (mid0 × near0),
    near1 = mid0,
    mid1 = far0,
    far1 = far0.next1,
    near2 = if guard then near1 else near0,
    mid2 = if guard then mid1 else mid0,
    far2 = if guard then far1 else far0,
    next2 = if guard then next1 else next0,
    next3 = next2 ++ (mid2 × near2)
head0 = head ++ (this × mid2) |

far2 = null ∧ Inv(next) ∧ Pre(this, head, next) ∧
¬ (Inv(next3) ∧ Post(this, head, head0, next, next3))
```
specifying analysis bounds

\[
\begin{align*}
\text{this} & \subseteq \text{List} \land \text{one this} \\
\text{head} & \subseteq \text{List} \rightarrow (\text{Node} \cup \text{null}) \\
\text{next} & \subseteq \text{Node} \rightarrow (\text{Node} \cup \text{null}) \\
\text{data} & \subseteq \text{Node} \rightarrow (\text{String} \cup \text{null})
\end{align*}
\]

let \( \text{near}_0 = \text{this}.\text{head} \),
\( \text{mid}_0 = \text{near}_0.\text{next} \),
\( \text{far}_0 = \text{mid}_0.\text{next} \),
\( \text{next}_0 = \text{next} ++ (\text{near}_0 \times \text{far}_0) \),
\( \text{guard} = (\text{far}_0 \neq \text{null}) \),
\( \text{next}_1 = \text{next}_0 ++ (\text{mid}_0 \times \text{near}_0) \),
\( \text{near}_1 = \text{mid}_0 \),
\( \text{mid}_1 = \text{far}_0 \),
\( \text{far}_1 = \text{far}_0.\text{next}_1 \),
\( \text{near}_2 = \text{if guard then near}_1 \text{ else near}_0 \),
\( \text{mid}_2 = \text{if guard then mid}_1 \text{ else mid}_0 \),
\( \text{far}_2 = \text{if guard then far}_1 \text{ else far}_0 \),
\( \text{next}_2 = \text{if guard then next}_1 \text{ else next}_0 \),
\( \text{next}_3 = \text{next}_2 ++ (\text{mid}_2 \times \text{near}_2) \),
\( \text{head}_0 = \text{head} ++ (\text{this} \times \text{mid}_2) \ |
\]

\( \text{far}_2 = \text{null} \land \text{Inv(next)} \land \text{Pre(this, head, next)} \land \\
\text{¬ (Inv(next}_3 \land \text{Post(this, head, head}_0, \text{next}, \text{next}_3))} \)

finite universe of uninterpreted elements

\( \triangleright \text{e.g., 1 List object, 3 of everything else} \)

upper bound on each relation

\( \triangleright \text{set of tuples, drawn from the universe,} \\
\text{that the relation may contain} \)

lower bound on each relation

\( \triangleright \text{set of tuples, drawn from the universe,} \\
\text{that the relation must contain} \)

lower bounds collectively form a partial model
specifying analysis bounds

\[
\begin{align*}
\text{this} & \subseteq \text{List} \land \text{one this} \\
\text{head} & \subseteq \text{List} \to (\text{Node} \cup \text{null}) \\
\text{next} & \subseteq \text{Node} \to (\text{Node} \cup \text{null}) \\
\text{data} & \subseteq \text{Node} \to (\text{String} \cup \text{null})
\end{align*}
\]

\[
\begin{align*}
\text{let } & \text{near}_0 = \text{this}.\text{head}, \\
& \quad \text{mid}_0 = \text{near}_0.\text{next}, \\
& \quad \text{far}_0 = \text{mid}_0.\text{next}, \\
& \quad \text{next}_0 = \text{next} + \left(\text{near}_0 \times \text{far}_0\right), \\
& \quad \text{guard} = (\text{far}_0 \neq \text{null}), \\
& \quad \text{next}_1 = \text{next}_0 + \left(\text{mid}_0 \times \text{near}_0\right), \\
& \quad \text{near}_1 = \text{mid}_0, \\
& \quad \text{mid}_1 = \text{far}_0, \\
& \quad \text{far}_1 = \text{far}_0.\text{next}_1,
\end{align*}
\]

\[
\begin{align*}
\text{near}_2 & = \begin{cases} \text{guard} & \text{then} \text{near}_1 \text{ else } \text{near}_0, \\ \text{mid}_2 & = \begin{cases} \text{guard} & \text{then} \text{mid}_1 \text{ else } \text{mid}_0, \\ \text{far}_2 & = \begin{cases} \text{guard} & \text{then} \text{far}_1 \text{ else } \text{far}_0, \\ \text{next}_2 & = \begin{cases} \text{guard} & \text{then} \text{next}_1 \text{ else } \text{next}_0, \\ \text{next}_3 & = \text{next}_2 + \left(\text{mid}_2 \times \text{near}_2\right), \\
\text{head}_0 & = \text{head} + \left(\text{this} \times \text{mid}_2\right) \mid \\
\text{far}_2 & = \text{null} \land \text{Inv(next)} \land \text{Pre(this, head, next)} \land \\
& \neg (\text{Inv(next}_3) \land \text{Post(this, head, head}_0, \text{next, next}_3))
\end{cases}
\end{cases}
\end{cases}
\end{align*}
\]
specifying analysis bounds

\[
\begin{align*}
\text{this} & \subseteq \text{List} \land \text{one this} \\
\text{head} & \subseteq \text{List} \rightarrow (\text{Node} \cup \text{null}) \\
\text{next} & \subseteq \text{Node} \rightarrow (\text{Node} \cup \text{null}) \\
\text{data} & \subseteq \text{Node} \rightarrow (\text{String} \cup \text{null}) \\
\end{align*}
\]

\[
\begin{align*}
\text{let} \ n_0 &= \text{this.head}, \\
& \quad \ n_1 = \text{near}_0.\text{next}, \\
& \quad \ n_2 = \text{mid}_0.\text{next}, \\
\text{next}_0 &= \text{next} ++ (\text{near}_0 \times \text{far}_0), \\
\text{guard} &= (\text{far}_0 \neq \text{null}), \\
\text{next}_1 &= \text{next}_0 ++ (\text{mid}_0 \times \text{near}_0), \\
\text{near}_1 &= \text{mid}_0, \\
\text{mid}_1 &= \text{far}_0, \\
\text{far}_1 &= \text{far}_0.\text{next}, \\
\text{near}_2 &= \text{if} \ \text{guard} \ \text{then} \ \text{near}_1 \ \text{else} \ \text{near}_0, \\
\text{mid}_2 &= \text{if} \ \text{guard} \ \text{then} \ \text{mid}_1 \ \text{else} \ \text{mid}_0, \\
\text{far}_2 &= \text{if} \ \text{guard} \ \text{then} \ \text{far}_1 \ \text{else} \ \text{far}_0, \\
\text{next}_2 &= \text{if} \ \text{guard} \ \text{then} \ \text{next}_1 \ \text{else} \ \text{next}_0, \\
\text{next}_3 &= \text{next}_2 ++ (\text{mid}_2 \times \text{near}_2) \\
\end{align*}
\]

\[
\begin{align*}
\text{head}_0 &= \text{head} ++ (\text{this} \times \text{mid}_2) \\
\text{far}_2 &= \text{null} \land \text{Inv(}\text{next}\text{)} \land \text{Pre(}\text{this, head, next}\text{)} \land \\
& \quad \lnot (\text{Inv(}\text{next}_3\text{)} \land \text{Post(}\text{this, head, head}_0, \text{next, next}_3)) \\
\end{align*}
\]
specifying analysis bounds

\[
\begin{align*}
\text{this} &\subseteq \text{List} \land \text{one} \text{ this} \\
\text{head} &\subseteq \text{List} \rightarrow (\text{Node} \cup \text{null}) \\
\text{next} &\subseteq \text{Node} \rightarrow (\text{Node} \cup \text{null}) \\
\text{data} &\subseteq \text{Node} \rightarrow (\text{String} \cup \text{null})
\end{align*}
\]

let \( \text{near}_0 = \text{this}.\text{head} \),
\[
\begin{align*}
\text{mid}_0 &= \text{near}_0.\text{next}, \\
\text{far}_0 &= \text{mid}_0.\text{next}, \\
\text{next}_0 &= \text{next} + (\text{near}_0 \times \text{far}_0), \\
\text{guard} &= (\text{far}_0 \neq \text{null}), \\
\text{next}_1 &= \text{next}_0 + (\text{mid}_0 \times \text{near}_0), \\
\text{near}_1 &= \text{mid}_0, \\
\text{mid}_1 &= \text{far}_0, \\
\text{far}_1 &= \text{far}_0.\text{next}_1,
\end{align*}
\]

let \( \text{near}_2 = \text{if} \ \text{guard} \ \text{then} \ \text{near}_1 \ \text{else} \ \text{near}_0, \)
\[
\begin{align*}
\text{mid}_2 &= \text{if} \ \text{guard} \ \text{then} \ \text{mid}_1 \ \text{else} \ \text{mid}_0, \\
\text{far}_2 &= \text{if} \ \text{guard} \ \text{then} \ \text{far}_1 \ \text{else} \ \text{far}_0, \\
\text{next}_2 &= \text{if} \ \text{guard} \ \text{then} \ \text{next}_1 \ \text{else} \ \text{next}_0, \\
\text{next}_3 &= \text{next}_2 + (\text{mid}_2 \times \text{near}_2) \\
\text{head}_0 &= \text{head} + (\text{this} \times \text{mid}_2) \\
\text{far}_2 &= \text{null} \land \text{Inv(\text{next})} \land \text{Pre(\text{this, head, next})} \land \\
&\quad \neg (\text{Inv(\text{next}_3)} \land \text{Post(\text{this, head, head}_0, \text{next}, \text{next}_3)})
\end{align*}
\]

\[
\begin{align*}
\{ \text{this, n0, n1, n2, s0, s1, s2, null} \} \\
\{ \langle \text{null} \rangle \} \subseteq \text{null} \subseteq \{ \langle \text{null} \rangle \} \\
\{ \} \subseteq \text{this} \subseteq \{ \langle \text{this} \rangle \} \\
\{ \} \subseteq \text{List} \subseteq \{ \langle \text{this} \rangle \} \\
\{ \} \subseteq \text{Node} \subseteq \{ \langle \text{n0} \rangle, \langle \text{n1} \rangle, \langle \text{n2} \rangle \} \\
\{ \} \subseteq \text{String} \subseteq \{ \langle \text{s0} \rangle, \langle \text{s1} \rangle, \langle \text{s2} \rangle \}
\end{align*}
\]
specifying analysis bounds

this ⊆ List ∧ one this
head ⊆ List → (Node ∪ null)
next ⊆ Node → (Node ∪ null)
data ⊆ Node → (String ∪ null)

let near0 = this.head,
     mid0 = near0.next,
     far0 = mid0.next,

next0 = next ++ (near0 × far0),
guard = (far0 != null),
next1 = next0 ++ (mid0 × near0),
near1 = mid0,
     mid1 = far0,
     far1 = far0.next1,

near2 = if guard then near1 else near0,
     mid2 = if guard then mid1 else mid0,
     far2 = if guard then far1 else far0,
next2 = if guard then next1 else next0,
next3 = next2 ++ (mid2 × near2)

head0 = head ++ (this × mid2) |

far2 = null ∧ Inv(next) ∧ Pre(this, head, next) ∧
     ¬ (Inv(next3) ∧ Post(this, head, head0, next, next3))
code checking demo
a bug! what to do about it?
data repair: fallback to the specification

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

```java
void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, far0);
    boolean guard = (far0 != null);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}
```
data repair: fallback to the specification

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near₀ = this.head;
    Node mid₀ = near₀.next;
    Node far₀ = mid₀.next;

    next₀ = update(next, near₀, far₀);
    boolean guard = (far₀ != null);
    next₁ = update(next₀, mid₀, near₀);
    near₁ = mid₀;
    mid₁ = far₀;
    far₁ = far₀.next₁;

    near₂ = phi(guard, near₁, near₀);
    mid₂ = phi(guard, mid₁, mid₀);
    far₂ = phi(guard, far₁, far₀);
    next₂ = phi(guard, next₁, next₀);

    assume far₂ == null;

    next₃ = update(next₂, mid₂, near₂);
    head₀ = update(head, this, mid₂);
}
**data repair: fallback to the specification**

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

```java
void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, far0);
    boolean guard = (far0 != null);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}
```

given a (valid) pre-state and a bad post-state at runtime, solve for a post-state that satisfies the specification and continue executing
don’t solve for the pre-state; express it as a partial model
data repair: fallback to the specification

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, far0);
    boolean guard = (far0 != null);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}
data repair using partial models

this ⊆ List ∧ one this ∧
head ⊆ List → (Node ∪ null) ∧
next ⊆ Node → (Node ∪ null) ∧
data ⊆ Node → (String ∪ null) ∧

head₀ ⊆ List → (Node ∪ null) ∧
next₃ ⊆ Node → (Node ∪ null) ∧

Inv(next) ∧ Pre(this, head, next) ∧
Inv(next₃) ∧ Post(this, head, head₀, next, next₃)

{ this, n₀, n₁, n₂, s₀, s₁, s₂, null }
null = { <null> }
this = { <this> }
List = { <this> }
Node = { <n₀>, <n₁>, <n₂> }
String = { <s₁>, <s₂> }
head = { <this, n₂> }
next = { <n₂, n₁>, <n₁, n₀>, <n₀, null> }
data = { <n₂, s₁>, <n₁, s₂>, <n₀, null> }

{} ⊆ head₀ ⊆ { this } × { n₀, n₁, n₂, null }
{} ⊆ next₃ ⊆ { n₀, n₁, n₂ } × { n₀, n₁, n₂, null }

pre-state
data repair using partial models

this ⊆ List ∧ one this ∧
head ⊆ List → (Node ∪ null) ∧
next ⊆ Node → (Node ∪ null) ∧
data ⊆ Node → (String ∪ null) ∧

head₀ ⊆ List → (Node ∪ null) ∧
next₃ ⊆ Node → (Node ∪ null) ∧

Inv(next) ∧ Pre(this, head, next) ∧
Inv(next₃) ∧ Post(this, head, head₀, next, next₃)

encoding of the repair

pre-state

{ this, n₀, n₁, n₂, s₀, s₁, s₂, null }
null = { <null> }
this = { <this> }
List = { <this> }
Node = { <n₀>, <n₁>, <n₂> }
String = { <s₁>, <s₂> }

head = { <this, n₂> }
next = { <n₂, n₁>, <n₁, n₀>, <n₀, null> }
data = { <n₂, s₁>, <n₁, s₂>, <n₀, null> }

{} ⊆ head₀ ⊆ { this } × { n₀, n₁, n₂, null }
{} ⊆ next₃ ⊆ { n₀, n₁, n₂ } × { n₀, n₁, n₂, null }


data repair using partial models

\[
\begin{align*}
\text{this} & \subseteq \text{List} \land \text{one this} \land \\
\text{head} & \subseteq \text{List} \rightarrow (\text{Node} \cup \text{null}) \land \\
\text{next} & \subseteq \text{Node} \rightarrow (\text{Node} \cup \text{null}) \land \\
\text{data} & \subseteq \text{Node} \rightarrow (\text{String} \cup \text{null}) \land \\
\text{head}_0 & \subseteq \text{List} \rightarrow (\text{Node} \cup \text{null}) \land \\
\text{next}_3 & \subseteq \text{Node} \rightarrow (\text{Node} \cup \text{null}) \land \\
\text{Inv}(\text{next}) & \land \text{Pre}(\text{this, head, next}) \land \\
\text{Inv}(\text{next}_3) & \land \text{Post}(\text{this, head, head}_0, \text{next, next}_3)
\end{align*}
\]

\[
\begin{align*}
\{ \text{this, n0, n1, n2, s0, s1, s2, null } \\
\text{null} & = \{ <\text{null}> \} \\
\text{this} & = \{ <\text{this}> \} \\
\text{List} & = \{ <\text{this}> \} \\
\text{Node} & = \{ <\text{n0}, <\text{n1}, <\text{n2}> \} \\
\text{String} & = \{ <\text{s1}, <\text{s2}> \} \\
\text{head} & = \{ <\text{this, n2}> \} \\
\text{next} & = \{ <\text{n2, n1}, <\text{n1, n0}, <\text{n0, null}> \} \\
\text{data} & = \{ <\text{n2, s1}, <\text{n1, s2}, <\text{n0, null}> \} \\
\{ } & \subseteq \text{head}_0 \subseteq \{ \text{this} \} \times \{ \text{n0, n1, n2, null } \} \\
\{ } & \subseteq \text{next}_3 \subseteq \{ \text{n0, n1, n2 } \} \times \{ \text{n0, n1, n2, null } \}
\end{align*}
\]
data repair using partial models

\[
\begin{align*}
\text{this} \subseteq \text{List} & \land \text{one this} \land \\
\text{head} \subseteq \text{List} & \rightarrow (\text{Node} \cup \text{null}) \land \\
\text{next} \subseteq \text{Node} & \rightarrow (\text{Node} \cup \text{null}) \land \\
\text{data} \subseteq \text{Node} & \rightarrow (\text{String} \cup \text{null}) \land
\end{align*}
\]

\[
\begin{align*}
\text{head}_0 \subseteq \text{List} & \rightarrow (\text{Node} \cup \text{null}) \land \\
\text{next}_3 \subseteq \text{Node} & \rightarrow (\text{Node} \cup \text{null}) \land \\
\text{Inv}(\text{next}) & \land \text{Pre}((\text{this}, \text{head}, \text{next}) \land \\
\text{Inv}(\text{next}_3) & \land \text{Post}((\text{this}, \text{head}, \text{head}_0, \text{next}, \text{next}_3)
\end{align*}
\]

\[
\{ \text{this, n0, n1, n2, s0, s1, s2, null} \}
\]

\[
\text{null} = \{ \langle \text{null} \rangle \}
\]

\[
\begin{align*}
\text{this} & = \{ \langle \text{this} \rangle \} \\
\text{List} & = \{ \langle \text{this} \rangle \} \\
\text{Node} & = \{ \langle \text{n0}, \text{n1}, \text{n2} \rangle \} \\
\text{String} & = \{ \langle \text{s1}, \text{s2} \rangle \}
\end{align*}
\]

\[
\begin{align*}
\text{head} & = \{ \langle \text{this, n2} \rangle \} \\
\text{next} & = \{ \langle \text{n2, n1} \rangle, \langle \text{n1, n0} \rangle, \langle \text{n0, null} \rangle \} \\
\text{data} & = \{ \langle \text{n2, s1} \rangle, \langle \text{n1, s2} \rangle, \langle \text{n0, null} \rangle \}
\end{align*}
\]

\[
\begin{align*}
\{ \} & \subseteq \text{head}_0 \subseteq \{ \text{this} \} \times \{ \text{n0, n1, n2, null} \} \\
\{ \} & \subseteq \text{next}_3 \subseteq \{ \text{n0, n1, n2} \} \times \{ \text{n0, n1, n2, null} \}
\end{align*}
\]
data repair demo
but the bug is still lurking in the code ...
fault localization with minimal unsat cores

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, far0);
    boolean guard = (far0 != null);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}
fault localization with minimal unsat cores

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near₀ = this.head;
    Node mid₀ = near₀.next;
    Node far₀ = mid₀.next;

    next₀ = update(next, near₀, far₀);
    boolean guard = (far₀ != null);
    next₁ = update(next₀, mid₀, near₀);
    near₁ = mid₀;
    mid₁ = far₀;
    far₁ = far₀.next₁;

    near₂ = phi(guard, near₁, near₀);
    mid₂ = phi(guard, mid₁, mid₀);
    far₂ = phi(guard, far₁, far₀);
    next₂ = phi(guard, next₁, next₀);

    assume far₂ == null;

    next₃ = update(next₂, mid₂, near₂);
    head₀ = update(head, this, mid₂);
}
fault localization with minimal unsat cores

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

```java
void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, far0);
    boolean guard = (far0 != null);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}
```

given a buggy program, a valid input and the expected output, find a minimal subset of program statements that prevents the execution on the given input from reaching the desired output state

introduce additional “indicator” relations into the encoding
fault localization with minimal unsat cores

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near₀ = this.head;
    Node mid₀ = near₀.next;
    Node far₀ = mid₀.next;

    next₀ = update(next, near₀, far₀);
    boolean guard = (far₀ != null);
    next₁ = update(next₀, mid₀, near₀);
    near₁ = mid₀;
    mid₁ = far₀;
    far₁ = far₀.next₁;

    near₂ = phi(guard, near₁, near₀);
    mid₂ = phi(guard, mid₁, mid₀);
    far₂ = phi(guard, far₁, far₀);
    next₂ = phi(guard, next₁, next₀);

    assume far₂ == null;

    next₃ = update(next₂, mid₂, near₂);
    head₀ = update(head, this, mid₂);
}
fault localization with minimal unsat cores

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, far0);
    boolean guard = (far0 != null);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}
fault localization encoding

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, far0);
    boolean guard = (far0 != null);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}

start with the encoding for validation

let near0 = this.head, mid0 = near0.next, far0 = mid0.next,
next0 = next ++ (near0 × far0), guard = (far0 != null),
next1 = next0 ++ (mid0 × near0), near1 = mid0, mid1 = far0,
far1 = far0.next1,
near2 = if guard then near1 else near0, mid2 = if guard then mid1 else mid0,
far2 = if guard then far1 else far0,
next2 = if guard then next1 else next0, next3 = next2 ++ (mid2 × near2)
head0 = head ++ (this × mid2) |
far2 = null ∧ Inv(next) ∧ Pre(this, head, next) ∧
¬ (Inv(next3) ∧ Post(this, head, head0, next, next3))
fault localization encoding

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

```java
void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, far0);
    boolean guard = (far0 != null);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}
```

let near0 = this.head,
    mid0 = near0.next,
    far0 = mid0.next,

    next0 = next ++ (near0 × far0),
    guard = (far0 != null),
    next1 = next0 ++ (mid0 × near0),
    near1 = mid0,
    mid1 = far0,
    far1 = far0.next1,

    near2 = if guard then near1 else near0,
    mid2 = if guard then mid1 else mid0,
    far2 = if guard then far1 else far0,
    next2 = if guard then next1 else next0,
    next3 = next2 ++ (mid2 × near2)

    head0 = head ++ (this × mid2) |

    far2 = null ∧ Inv(next) ∧ Pre(this, head, next) ∧
    Inv(next3) ∧ Post(this, head, head0, next, next3)
void reverse() {
    Node near₀ = this.head;
    Node mid₀ = near₀.next;
    Node far₀ = mid₀.next;

    next₀ = update(next, near₀, far₀);
    boolean guard = (far₀ != null);
    next₁ = update(next₀, mid₀, near₀);
    near₁ = mid₀;
    mid₁ = far₀;
    far₁ = far₀.next₁;

    near₂ = phi(guard, near₁, near₀);
    mid₂ = phi(guard, mid₁, mid₀);
    far₂ = phi(guard, far₁, far₀);
    next₂ = phi(guard, next₁, next₀);

    assume far₂ == null;

    next₃ = update(next₂, mid₂, near₂);
    head₀ = update(head, this, mid₂);
}

this ⊆ List ∧ one this ∧
head ⊆ List → (Node ∪ null) ∧
next ⊆ Node → (Node ∪ null) ∧
data ⊆ Node → (String ∪ null) ∧

let near₀ = this.head,
    mid₀ = near₀.next,
    far₀ = mid₀.next,

    next₀ = next ++ (near₀ × far₀),
    guard = (far₀ != null),
    next₁ = next₀ ++ (mid₀ × near₀),
    near₁ = mid₀,
    mid₁ = far₀,
    far₁ = far₀.next₁,

    near₂ = if guard then near₁ else near₀,
    mid₂ = if guard then mid₁ else mid₀,
    far₂ = if guard then far₁ else far₀,
    next₂ = if guard then next₁ else next₀,
    next₃ = next₂ ++ (mid₂ × near₂)
head₀ = head ++ (this × mid₂) |

far₂ = null ∧ Inv(next) ∧ Pre(this, head, next) ∧
Inv(next₃) ∧ Post(this, head, head₀, next, next₃)
void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, far0);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    boolean guard = (far0 != null);
    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);

    this ⊆ List ∧ one this ∧
    head ⊆ List → (Node ∪ null) ∧
    next ⊆ Node → (Node ∪ null) ∧
    data ⊆ Node → (String ∪ null) ∧

    near0 = this.head ∧
    mid0 = near0.next ∧
    far0 = mid0.next ∧
    next0 = next ++ (near0 × far0) ∧
    next1 = next0 ++ (mid0 × near0) ∧
    near1 = mid0 ∧
    mid1 = far0 ∧
    far1 = far0.next1 ∧

    let guard = (far0 != null),
    near2 = if guard then near1 else near0,
    mid2 = if guard then mid1 else mid0,
    far2 = if guard then far1 else far0,
    next2 = if guard then next1 else next0 |

    next3 = next2 ++ (mid2 × near2) ∧
    head0 = head ++ (this × mid2) ∧
    far2 = null ∧ Inv(next) ∧ Pre(this, head, next) ∧
    Inv(next3) ∧ Post(this, head, head0, next, next3)
fault localization encoding: partial model

\[ \text{this} \subseteq \text{List} \land \text{one this} \land \]
\[ \text{head} \subseteq \text{List} \to (\text{Node} \cup \text{null}) \land \]
\[ \text{next} \subseteq \text{Node} \to (\text{Node} \cup \text{null}) \land \]
\[ \text{data} \subseteq \text{Node} \to (\text{String} \cup \text{null}) \land \]

\[ \text{near}_0 = \text{this.head} \land \]
\[ \text{mid}_0 = \text{near}_0.\text{next} \land \]
\[ \text{far}_0 = \text{mid}_0.\text{next} \land \]
\[ \text{next}_0 = \text{next} \; \text{++} \; (\text{near}_0 \times \text{far}_0) \land \]
\[ \text{next}_1 = \text{next}_0 \; \text{++} \; (\text{mid}_0 \times \text{near}_0) \land \]
\[ \text{near}_1 = \text{mid}_0 \land \]
\[ \text{mid}_1 = \text{far}_0 \land \]
\[ \text{far}_1 = \text{far}_0.\text{next}_1 \land \]

\[ \text{let guard} = (\text{far}_0 \neq \text{null}), \]
\[ \quad \text{near}_2 = \text{if} \; \text{guard} \; \text{then} \; \text{near}_1 \; \text{else} \; \text{near}_0, \]
\[ \quad \text{mid}_2 = \text{if} \; \text{guard} \; \text{then} \; \text{mid}_1 \; \text{else} \; \text{mid}_0, \]
\[ \quad \text{far}_2 = \text{if} \; \text{guard} \; \text{then} \; \text{far}_1 \; \text{else} \; \text{far}_0, \]
\[ \quad \text{next}_2 = \text{if} \; \text{guard} \; \text{then} \; \text{next}_1 \; \text{else} \; \text{next}_0 | \]
\[ \text{next}_3 = \text{next}_2 \; \text{++} \; (\text{mid}_2 \times \text{near}_2) \land \]
\[ \text{head}_0 = \text{head} \; \text{++} \; (\text{this} \times \text{mid}_2) \land \]
\[ \text{far}_2 = \text{null} \land \text{Inv(} \text{next} \text{)} \land \text{Pre(} \text{this, head, next}) \land \]
\[ \text{Inv(} \text{next}_3 \text{)} \land \text{Post(} \text{this, head, head}_0, \text{next, next}_3 \)
fault localization encoding: partial model

\[
\begin{align*}
\text{this} & \subseteq \text{List} \land \text{one this} \land \\
\text{head} & \subseteq \text{List} \to (\text{Node} \cup \text{null}) \land \\
\text{next} & \subseteq \text{Node} \to (\text{Node} \cup \text{null}) \land \\
\text{data} & \subseteq \text{Node} \to (\text{String} \cup \text{null}) \land \\
\text{near}_0 & = \text{this.head} \land \\
\text{mid}_0 & = \text{near}_0.\text{next} \land \\
\text{far}_0 & = \text{mid}_0.\text{next} \land \\
\text{next}_0 & = \text{next} + (\text{near}_0 \times \text{far}_0) \land \\
\text{next}_1 & = \text{next}_0 + (\text{mid}_0 \times \text{near}_0) \land \\
\text{near}_1 & = \text{mid}_0 \land \\
\text{mid}_1 & = \text{far}_0 \land \\
\text{far}_1 & = \text{far}_0.\text{next}_1 \land \\
\text{let guard} & = (\text{far}_0 \neq \text{null}), \\
& \quad \text{near}_2 = \text{if guard then near}_1 \text{ else near}_0, \\
& \quad \text{mid}_2 = \text{if guard then mid}_1 \text{ else mid}_0, \\
& \quad \text{far}_2 = \text{if guard then far}_1 \text{ else far}_0, \\
& \quad \text{next}_2 = \text{if guard then next}_1 \text{ else next}_0 | \\
& \quad \text{next}_3 = \text{next}_2 + (\text{mid}_2 \times \text{near}_2) \land \\
& \quad \text{head}_0 = \text{head} + (\text{this} \times \text{mid}_2) \land \\
& \quad \text{far}_2 = \text{null} \land \text{Inv(next)} \land \text{Pre(this, head, next)} \land \\
& \quad \text{Inv(next)} \land \text{Post(this, head, head}_0, \text{next, next}_3)
\end{align*}
\]
fault localization encoding: partial model

\[
\text{this} \subseteq \text{List} \land \text{one this} \land \\
\text{head} \subseteq \text{List} \rightarrow (\text{Node} \cup \text{null}) \land \\
\text{next} \subseteq \text{Node} \rightarrow (\text{Node} \cup \text{null}) \land \\
\text{data} \subseteq \text{Node} \rightarrow (\text{String} \cup \text{null}) \land \\
\text{near}_0 = \text{this.head} \land \\
\text{mid}_0 = \text{near}_0.\text{next} \land \\
\text{far}_0 = \text{mid}_0.\text{next} \land \\
\text{next}_0 = \text{next} \text{++} (\text{near}_0 \times \text{far}_0) \land \\
\text{next}_1 = \text{next}_0 \text{++} (\text{mid}_0 \times \text{near}_0) \land \\
\text{near}_1 = \text{mid}_0 \land \\
\text{mid}_1 = \text{far}_0 \land \\
\text{far}_1 = \text{far}_0.\text{next}_1 \land \\
\text{let guard} = (\text{far}_0 \neq \text{null}), \\
\text{near}_2 = \text{if guard then near}_1 \text{ else near}_0, \\
\text{mid}_2 = \text{if guard then mid}_1 \text{ else mid}_0, \\
\text{far}_2 = \text{if guard then far}_1 \text{ else far}_0, \\
\text{next}_2 = \text{if guard then next}_1 \text{ else next}_0 | \\
\text{next}_3 = \text{next}_2 \text{++} (\text{mid}_2 \times \text{near}_2) \land \\
\text{head}_0 = \text{head} \text{++} (\text{this} \times \text{mid}_2) \land \\
\text{far}_2 = \text{null} \land \text{Inv(}\text{next}) \land \text{Pre(}\text{this, head, next}) \land \\
\text{Inv(}\text{next}_3) \land \text{Post(}\text{this, head, head}_0, \text{next, next}_3)
\]

\[
\{ \text{this, n0, n1, n2, s0, s1, s2, null} \}
\]
fault localization encoding: partial model

this ⊆ List ∧ one this ∧
head ⊆ List → (Node ∪ null) ∧
next ⊆ Node → (Node ∪ null) ∧
data ⊆ Node → (String ∪ null) ∧

near₀ = this.head ∧
mid₀ = near₀.next ∧
far₀ = mid₀.next ∧

next₀ = next ++ (near₀ × far₀) ∧
next₁ = next₀ ++ (mid₀ × near₀) ∧
near₁ = mid₀ ∧
mid₁ = far₀ ∧
far₁ = far₀.next₁ ∧

let guard = (far₀ != null),
        near₂ = if guard then near₁ else near₀,
        mid₂ = if guard then mid₁ else mid₀,
        far₂ = if guard then far₁ else far₀,
        next₂ = if guard then next₁ else next₀ |

next₃ = next₂ ++ (mid₂ × near₂) ∧
head₀ = head ++ (this × mid₂) ∧
far₂ = null ∧ Inv(next) ∧ Pre(this, head, next) ∧
Inv(next) ∧ Post(this, head, head₀, next, next₃)

{ this, n₀, n₁, n₂, s₀, s₁, s₂, null }

null = { <null> }
this = { <this> }
List = { <this> }
Node = { <n₀>, <n₁>, <n₂> }
String = { <s₁>, <s₂> }

head = { <this, n₂> }
next = { <n₂, n₁>, <n₁, n₀>, <n₀, null> }
data = { <n₂, s₁>, <n₁, s₂>, <n₀, null> }

let guard = (far₀ != null),
        near₂ = if guard then near₁ else near₀,
        mid₂ = if guard then mid₁ else mid₀,
        far₂ = if guard then far₁ else far₀,
        next₂ = if guard then next₁ else next₀ |

next₃ = next₂ ++ (mid₂ × near₂) ∧
head₀ = head ++ (this × mid₂) ∧
far₂ = null ∧ Inv(next) ∧ Pre(this, head, next) ∧
Inv(next) ∧ Post(this, head, head₀, next, next₃)

{} ⊆ next₀ ⊆ { n₀, n₁, n₂ } × { n₀, n₁, n₂, null }
{} ⊆ next₁ ⊆ { n₀, n₁, n₂ } × { n₀, n₁, n₂, null }
{} ⊆ near₀ ⊆ { n₀, n₁, n₂, null }
{} ⊆ near₁ ⊆ { n₀, n₁, n₂, null }
{} ⊆ mid₀ ⊆ { n₀, n₁, n₂, null }
{} ⊆ mid₁ ⊆ { n₀, n₁, n₂, null }
{} ⊆ far₀ ⊆ { n₀, n₁, n₂, null }
{} ⊆ far₁ ⊆ { n₀, n₁, n₂, null }
fault localization encoding: partial model

\[ \text{this} \subseteq \text{List} \land \text{one this} \land \]

\[ \text{head} \subseteq \text{List} \rightarrow (\text{Node} \cup \text{null}) \land \]

\[ \text{next} \subseteq \text{Node} \rightarrow (\text{Node} \cup \text{null}) \land \]

\[ \text{data} \subseteq \text{Node} \rightarrow (\text{String} \cup \text{null}) \land \]

\[ \text{near}_0 = \text{this.head} \land \]

\[ \text{mid}_0 = \text{near}_0.\text{next} \land \]

\[ \text{far}_0 = \text{mid}_0.\text{next} \land \]

\[ \text{next}_0 = \text{next} ++ (\text{near}_0 \times \text{far}_0) \land \]

\[ \text{next}_1 = \text{next}_0 ++ (\text{mid}_0 \times \text{near}_0) \land \]

\[ \text{near}_1 = \text{mid}_0 \land \]

\[ \text{mid}_1 = \text{far}_0 \land \]

\[ \text{far}_1 = \text{far}_0.\text{next}_1 \land \]

\[
\text{let guard} = (\text{far}_0 != \text{null}),
\]

\[ \text{near}_2 = \text{if guard then near}_1 \text{ else near}_0, \]

\[ \text{mid}_2 = \text{if guard then mid}_1 \text{ else mid}_0, \]

\[ \text{far}_2 = \text{if guard then far}_1 \text{ else far}_0, \]

\[ \text{next}_2 = \text{if guard then next}_1 \text{ else next}_0 | \]

\[ \text{next}_3 = \text{next}_2 ++ (\text{mid}_2 \times \text{near}_2) \land \]

\[ \text{head}_0 = \text{head} ++ (\text{this} \times \text{mid}_2) \land \]

\[ \text{far}_2 = \text{null} \land \text{Inv(next)} \land \text{Pre(this, head, next)} \land \]

\[ \text{Inv(next)} \land \text{Post(this, head, head}_0, \text{next, next}_3) \]

\[ \{ \text{this, n0, n1, n2, s0, s1, s2, null } \}

\[ \text{null} \subseteq \{ <\text{null}> \} \]

\[ \text{this} = \{ <\text{this}> \} \]

\[ \text{List} = \{ <\text{this}> \} \]

\[ \text{Node} = \{ <\text{n0}, <\text{n1}, <\text{n2}> \} \]

\[ \text{String} = \{ <\text{s1}, <\text{s2}> \} \]

\[ \text{head} = \{ <\text{this, n2}> \} \]

\[ \text{next} = \{ <\text{n2, n1}>, <\text{n1, n0}, <\text{n0, null}> \} \]

\[ \text{data} = \{ <\text{n2, s1}, <\text{n1, s2}, <\text{n0, null}> \} \]

\[ \text{head}_0 = \{ <\text{this, n0}> \} \]

\[ \text{next}_3 = \{ <\text{n0, n1}, <\text{n1, n2}, <\text{n2, null} \}

\[ \{ \text{null} \subseteq \text{near}_0 \subseteq \{ \text{n0, n1, n2} \} \times \{ \text{n0, n1, n2} \} \}

\[ \{ \text{null} \subseteq \text{near}_1 \subseteq \{ \text{n0, n1, n2} \} \times \{ \text{n0, n1, n2} \} \}

\[ \{ \text{null} \subseteq \text{near}_0 \subseteq \{ \text{n0, n1, n2} \} \}

\[ \{ \text{null} \subseteq \text{near}_1 \subseteq \{ \text{n0, n1, n2} \} \}

\[ \{ \text{null} \subseteq \text{mid}_0 \subseteq \{ \text{n0, n1, n2} \} \}

\[ \{ \text{null} \subseteq \text{mid}_1 \subseteq \{ \text{n0, n1, n2} \} \}

\[ \{ \text{null} \subseteq \text{far}_0 \subseteq \{ \text{n0, n1, n2} \} \}

\[ \{ \text{null} \subseteq \text{far}_1 \subseteq \{ \text{n0, n1, n2} \} \]
fault localization demo
minimal unsatisfiable core

this ⊆ List ∧ one this ∧
head ⊆ List → (Node ∪ null) ∧
next ⊆ Node → (Node ∪ null) ∧
data ⊆ Node → (String ∪ null) ∧
near₀ = this.head ∧
mid₀ = near₀.next ∧
far₀ = mid₀.next ∧

next₀ = next ++ (near₀ × far₀) ∧
next₁ = next₀ ++ (mid₀ × near₀) ∧
near₁ = mid₀ ∧
mid₁ = far₀ ∧
far₁ = far₀.next₁ ∧

let guard = (far₀ !≠ null),
   near₂ = if guard then near₁ else near₀,
   mid₂ = if guard then mid₁ else mid₀,
   far₂ = if guard then far₁ else far₀,
next₂ = if guard then next₁ else next₀ |

next₃ = next₂ ++ (mid₂ × near₂) ∧
head₀ = head ++ (this × mid₂) ∧
far₂ = null ∧ Inv(next) ∧ Pre(this, head, next) ∧
Inv(next₃) ∧ Post(this, head, head₀, next, next₃)

constraints that are UNSAT (with respect to bounds) but become SAT if any member is removed

{ this, n₀, n₁, n₂, s₀, s₁, s₂, null }
null = { <null> }
this = { <this> }
List = { <this> }
Node = { <n₀>, <n₁>, <n₂> }
String = { <s₁>, <s₂> }

head = { <this, n₂> }
next = { <n₂, n₁>, <n₁, n₀>, <n₀, null> }
data = { <n₂, s₁>, <n₁, s₂>, <n₀, null> }

head₀ = { <this, n₀> }
next₃ = { <n₀, n₁>, <n₁, n₂>, <n₂, null> }

{ } ⊆ next₀ ⊆ { n₀, n₁, n₂ } × { n₀, n₁, n₂, null }
{ } ⊆ next₁ ⊆ { n₀, n₁, n₂ } × { n₀, n₁, n₂, null }
{ } ⊆ near₀ ⊆ { n₀, n₁, n₂, null }
{ } ⊆ near₁ ⊆ { n₀, n₁, n₂, null }
{ } ⊆ mid₀ ⊆ { n₀, n₁, n₂, null }
{ } ⊆ mid₁ ⊆ { n₀, n₁, n₂, null }
{ } ⊆ far₀ ⊆ { n₀, n₁, n₂, null }
{ } ⊆ far₁ ⊆ { n₀, n₁, n₂, null }
minimal unsatisfiable core

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near₀ = this.head;
    Node mid₀ = near₀.next;
    Node far₀ = mid₀.next;

    next₀ = update(next, near₀, far₀);
    next₁ = update(next₀, mid₀, near₀);
    near₁ = mid₀;
    mid₁ = far₀;
    far₁ = far₀.next₁;

    boolean guard = (far₀ != null);
    near₂ = phi(guard, near₁, near₀);
    mid₂ = phi(guard, mid₁, mid₀);
    far₂ = phi(guard, far₁, far₀);
    next₂ = phi(guard, next₁, next₀);

    assume far₂ == null;

    next₃ = update(next₂, mid₂, near₂);
    head₀ = update(head, this, mid₂);
}
synthesizing a sketch-like fix

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, far0);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    boolean guard = (far0 != null);
    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}
synthesizing a sketch-like fix

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

```java
void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, ??);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    boolean guard = (far0 != null);
    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}
```

drill a hole in one of the localized statements
  e.g., at the earliest opportunity for a fix
synthesizing a sketch-like fix

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near₀ = this.head;
    Node mid₀ = near₀.next;
    Node far₀ = mid₀.next;

    next₀ = update(next, near₀, ??);
    next₁ = update(next₀, mid₀, near₀);
    near₁ = mid₀;
    mid₁ = far₀;
    far₁ = far₀.next₁;

    boolean guard = (far₀ != null);
    near₂ = phi(guard, near₁, near₀);
    mid₂ = phi(guard, mid₁, mid₀);
    far₂ = phi(guard, far₁, far₀);
    next₂ = phi(guard, next₁, next₀);

    assume far₂ == null;

    next₃ = update(next₂, mid₂, near₂);
    head₀ = update(head, this, mid₂);
}
synthesizing a sketch-like fix

void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, ??);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    boolean guard = (far0 != null);
    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

drill a hole in one of the localized statements

› e.g., at the earliest opportunity for a fix

we want to replace the hole with an expression from a (small) grammar so that
the program satisfies its spec on all inputs

› e.g., [ variable | null ]

encode the synthesis problem (for one input) using relations that represent syntax,
together with a “meaning” expression connecting syntax to semantics
synthesizing a sketch-like fix

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

```java
void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, ??);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    boolean guard = (far0 != null);
    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}
```

drill a hole in one of the localized statements
  e.g., at the earliest opportunity for a fix
  we want to replace the hole with an expression from a (small) grammar so that
  the program satisfies its spec on all inputs
  e.g., [ variable | null ]

encode the synthesis problem (for one input) using relations that represent syntax, together with a “meaning” expression connecting syntax to semantics

wrap into a CEGIS loop (not done here)
**synthesis encoding**

```java
@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, ??);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    boolean guard = (far0 != null);
    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}
```

This is the first step of the repair encoding:
synthesis encoding

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

void reverse() {
    Node near0 = this.head;
    Node mid0 = near0.next;
    Node far0 = mid0.next;

    next0 = update(next, near0, ??);
    next1 = update(next0, mid0, near0);
    near1 = mid0;
    mid1 = far0;
    far1 = far0.next1;

    boolean guard = (far0 != null);
    near2 = phi(guard, near1, near0);
    mid2 = phi(guard, mid1, mid0);
    far2 = phi(guard, far1, far0);
    next2 = phi(guard, next1, next0);

    assume far2 == null;

    next3 = update(next2, mid2, near2);
    head0 = update(head, this, mid2);
}

this ⊆ List ∧ one this ∧ one hole ∧
head ⊆ List → (Node ∪ null) ∧
next ⊆ Node → (Node ∪ null) ∧
data ⊆ Node → (String ∪ null) ∧

let near0 = this.head,
    mid0 = near0.next,
    far0 = mid0.next,

    meaning = (null × null) ∪ (“head” × this.head) ∪
    (“near0” × near0) ∪ (“mid0” × mid0) ∪ (“far0” × far0)

    next0 = next ++ (near0 × hole.meaning),
    guard = (far0 != null),
    next1 = next0 ++ (mid0 × near0),
    near1 = mid0,
    mid1 = far0,
    far1 = far0.next1,

    near2 = if guard then near1 else near0,
    mid2 = if guard then mid1 else mid0,
    far2 = if guard then far1 else far0,
    next2 = if guard then next1 else next0,
    next3 = next2 ++ (mid2 × near2)
    head0 = head ++ (this × mid2) ∥

    far2 = null ∧ Inv(next) ∧ Pre(this, head, next) ∧
    Inv(next3) ∧ Post(this, head, head0, next, next3)
synthesis encoding: partial model

this ⊆ List ∧ one this ∧ one hole ∧
head ⊆ List → (Node ∪ null) ∧
next ⊆ Node → (Node ∪ null) ∧
data ⊆ Node → (String ∪ null) ∧

let near₀ = this.head,
       mid₀ = near₀.next,
       far₀ = mid₀.next,

meaning = (null × null) ∪ (“head” × this.head) ∪
          (”near₀” × near₀) ∪ (“mid₀” × mid₀) ∪ (“far₀” × far₀)

next₀ = next ++ (near₀ × hole.meaning),
guard = (far₀ != null),
next₁ = next₀ ++ (mid₀ × near₀),
near₁ = mid₀,
mid₁ = far₀,
far₁ = far₀.next₁,

near₂ = if guard then near₁ else near₀,
mid₂ = if guard then mid₁ else mid₀,
far₂ = if guard then far₁ else far₀,
next₂ = if guard then next₁ else next₀,
next₃ = next₂ ++ (mid₂ × near₂)
head₀ = head ++ (this × mid₂) |

far₂ = null ∧ Inv(next) ∧ Pre(this, head, next) ∧
      Inv(next₃) ∧ Post(this, head, head₀, next, next₃)

{ this, n₀, n₁, n₂, s₀, s₁, s₂, null,
  “head”, “near₀”, “mid₀”, “far₀” }

null = { <null> }
this = { <this> }
List = { <this> }
Node = { <n₀>, <n₁>, <n₂> }
String = { <s₁>, <s₂> }

head = { <this, n₂> }
next = { <n₂, n₁>, <n₁, n₀>, <n₀, null> }
data = { <n₂, s₁>, <n₁, s₂>, <n₀, null> }

“head” = { “<head>” }
“near₀” = { “<near₀>” }
“mid₀” = { “<mid₀>” }
“far₀” = { “<far₀>” }

{} ⊆ hole ⊆ { <null>, <“head”>, <“near₀”>,
             <“mid₀”>, <“far₀”> }

![Diagram](image-url)
synthesis demo
patched list reversal

@invariant Inv(next)
@requires Pre(this, head, next)
@ensures Post(this, old(head), head, old(next), next)

```java
void reverse() {
   Node near = head;
   Node mid = near.next;
   Node far = mid.next;

   near.next = null;
   while (far != null) {
      mid.next = near;
      near = mid;
      mid = far;
      far = far.next;
   }

   mid.next = near;
   head = mid;
}
```
alloy.mit.edu/kodkod

questions?