TESTING BY DUALIZATION

Yishuai Li

A DISSERTATION

in

Computer and Information Science

Presented to the Faculties of the University of Pennsylvania

in

Partial Fulfillment of the Requirements for the

Degree of Doctor of Philosophy

2022

Supervisor of Dissertation

Benjamin C. Pierce
Professor of Computer and Information Science

Graduate Group Chairperson

Mayur Naik, Professor of Computer and Information Science

Dissertation Commitee

Steve Zdancewic, Professor of Computer and Information Science, Chair
Mayur Naik, Professor of Computer and Information Science
Boon Thau Loo, Professor of Computer and Information Science
John Hughes, Professor of Computing Science, Chalmers University of Technology

Acknowledgments

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

ABSTRACT

TESTING BY DUALIZATION

Yishuai Li
Benjamin C. Pierce

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Contents

List of Figures

CHAPTER 1

Introduction

Software engineering requires rigorous testing of rapidly evolving programs, which costs manpower comparable to developing the product itself. To guarantee programs' compliance with the specification, we need testers that can tell compliant implementations from violating ones.

This thesis studies the testing of interactive systems' semantics: The system under test (SUT) interacts with the tester by sending and receiving messages, and the tester determines whether the messages sent by the SUT are valid or not with respect to the protocol specification.

This chapter provides a brief view of interactive testing (Section 1.1), explains why nondeterminism makes this problem difficult (Sections 1.2–1.3), and discusses how language designs address the challenges caused by nondeterminism (Section 1.4).

1.1. Interactive Testing

Suppose we want to test a web server that supports GET and PUT methods:

```
CoFixpoint server (data: key → value) :=
  request ← recv;;
  match request with
  | GET k   ⇒ send (data k);; server  data
  | PUT k v ⇒ send  Done   ;; server (data [k ↦ v])
  end.
```

We can write a tester client that interacts with the server and determines whether it behaves correctly:

```
CoFixpoint tester (data: key → value) :=
  request ← random;;
  send request;;
  response ← recv;;
  match request with
  | GET k   ⇒ if response =? data k
              then tester data
              else reject
  | PUT k v ⇒ if response =? Done
              then tester (data [k ↦ v])
              else reject
  end.
```

This tester implements a reference server internally that computes the expected behavior. The behavior is then compared against that produced by the SUT. The tester rejects the SUT upon any difference from the computed expectation.

The above tester can be viewed as two modules: (i) a *test harness* that interacts with the server and produces transactions of sends and receives, and (ii) a *validator* that determines whether the transactions are valid or not:

```
(* Compute the expected response and next state of the server. *)
Definition serverSpec request data :=
  match request with
  | GET k   ⇒ (data k, data)
  | PUT k v ⇒ (Done   , data [k ↦ v])
  end.
(* Validate the transaction against the stateful specification. *)
Definition validate spec request response data :=
  let (expect, next) := spec request data in
  if response =? expect then Success next else Failure.
(* Produce transactions for the validator. *)
CoFixpoint harness validator state :=
  request ← random;;
  send request;;
  response ← recv;;
  if validator request response state is Success next
  then harness validator next
  else reject.
Definition tester := harness (validate serverSpec).
```

Such testing method works for deterministic systems, whose behavior can be precisely computed from its input. Whereas, many systems are allowed to behave nondeterministically. How to test systems that involve randomness? How to validate servers' behavior against concurrent clients? The following sections discuss nondeterminism by partitioning it in two ways, and explains how they pose challenges to the validator and the test harness.

1.2. Internal and external nondeterminism

When people talk to each other, voice is transmitted over substances. When testers interact with the SUT, messages are transmitted via the runtime environment. The specification might allow SUTs to behave differently from each other, just like people speaking in different accents, we call it *internal nondeterminism*. The runtime environment might affect the transmission of messages, just like solids transmit voice faster than liquids and gases, we call it *external nondeterminism*.

1.2.1. Internal nondeterminism. Within the SUT, correct behavior may be underspecified. For example, HTTP [5] allows requests to be conditional: If the client has a local copy of some resource and the copy on the server has not changed, then the server needn't resend the resource. To achieve this, an HTTP server may generate a short string, called an “entity tag” (ETag), identifying the content of some resource, and send it to the client:

```
/* Client: */                   /* Server: */
GET /target HTTP/1.1            HTTP/1.1 200 OK
                                ETag: "tag-foo"
                                ... content of /target ...
```

The next time the client requests the same resource, it can include the ETag in the GET request, informing the server not to send the content if its ETag still matches:

```
/* Client: */                   /* Server: */
GET /target HTTP/1.1            HTTP/1.1 304 Not Modified
If-None-Match: "tag-foo"
```

If the ETag does not match, the server responds with code 200 and the updated content as usual.

Similarly, if a client wants to modify the server's resource atomically by compare-and-swap, it can include the ETag in the PUT request as `If-Match` precondition, which instructs the server to only update the content if its current ETag matches:

```
/* Client: */                   /* Server: */
PUT /target HTTP/1.1            HTTP/1.1 204 No Content
If-Match: "tag-foo"
... content (A) ...
```

```
/* Client: */                   /* Server: */
GET /target HTTP/1.1            HTTP/1.1 200 OK
                                ETag: "tag-bar"
                                ... content (A) ...
```

If the ETag does not match, then the server should not perform the requested operation, and should reject with code 412:

```
/* Client: */                   /* Server: */
PUT /target HTTP/1.1            HTTP/1.1 412 Precondition Failed
If-Match: "tag-baz"
... content (B) ...
```

```
/* Client: */                    /* Server: */
GET /target HTTP/1.1             HTTP/1.1 200 ok
                                 ETag: "tag-bar"
                                 ... content (A) ...
```

Whether a server's response should be judged *valid* or not depends on the ETag it generated when creating the resource. If the tester doesn't know the server's internal state (*e.g.*, before receiving any 200 response that includes an ETag), and cannot enumerate all of them (as ETags can be arbitrary strings), then it needs to maintain a space of all possible values, and narrow the space upon further interactions with the server. For example, "If the server has revealed some resource's ETag as `"tag-foo"`, then it must not reject requests targetting this resource conditioned over `If-Match: "tag-foo"`, until the resource has been modified"; and "Had the server previously rejected an `If-Match` request, it must reject the same request until its target has been modified."

This idea of remembering matched and mismatched ETags is implemented in Figure 1.1. For each key, the validator maintains three internal states: (i) The value stored in `data`, (ii) the corresponding resource's ETag, if known by the tester, stored in `tag_is`, and (iii) ETags that should not match with the resource's, stored in `tag_is_not`. Each pair of request and response contributes to the validator's knowledge of the target resource. The tester rejects the SUT if the observed behavior does not match its knowledge gained in previous interactions.

Even a simple nondeterminism like ETags requires such careful design of the validator, based on thorough comprehension of the specification. For more complex protocols, we hope to construct the validator in a reasonable way.

1.2.2. External nondeterminism. To discuss the nondeterminism caused by the environment, we need to define the environment concept in testing scenario.

DEFINITION 1.1 (Environment, input, output, and observations). *Environment* is the substance that the tester and the SUT interact with. *Input* is the subset of the environment that the tester can manipulate. *Output* is the subset of the environment that the SUT can alter. *Observation* is the tester's view of the environment.

When testing servers, the environment is the network stack between the client and the server. The input is the request sent by the client, and the output is the response sent by the server. The response is transmitted via the network, until reaching the client side as observations.

The tester shown in Section 1.1 runs one client at a time. It waits for the response before sending the next request, as shown in Figure 1.2. Such tester's observation is guaranteed identical to the SUT's output, so it only needs to scan the requests and responses with one stateful validator.

To reveal the server's behavior upon concurrent requests, the tester needs to simulate multiple clients, sending new requests before receiving previous responses. The network delay might cause the server to receive requests in a different order from

```
Definition validate request response
           (data      : key → value)
           (tag_is    : key → Maybe etag)
           (tag_is_not: key → list etag) :=
  match request, response with
  | PUT k t v, NoContent ⇒
    if t ∈ tag_is_not k then Failure
    else if (tag_is k =? Unknown) || strong_match (tag_is k) t
    then (* Now the tester knows that the data in [k]
          * is updated to [v], but its new ETag is unknown. *)
      Success (data       [k ↦ v],
               tag_is     [k ↦ Unknown],
               tag_is_not [k ↦ [] ])
    else Failure
  | PUT k t v, PreconditionFailed ⇒
    if strong_match (tag_is k) t then Failure
    else (* Now the tester knows that the ETag of [k]
          * is other than [t]. *)
      Success (data, tag_is, tag_is_not [k ↦ t::(tag_is_not k)])
  | GET k t, NotModified ⇒
    if t ∈ tag_is_not then Failure
    else if (tag_is k =? Unknown) || weak_match (tag_is k) t
    then (* Now the tester knows that the ETag of [k]
          * is equal to [t]. *)
      Success (data, tag_is [k ↦ Known t], tag_is_not)
    else Failure
  | GET k t0, OK t v ⇒
    if weak_match (tag_is k) t0 then Failure
    else if data k =? v
    then (* Now the tester knows the ETag of [k]. *)
      Success (data, tag_is [k ↦ Known t], tag_is_not)
    else Failure
  | _, _ ⇒ Failure
  end.
```

FIGURE 1.1. Ad hoc tester for HTTP/1.1 conditional requests. `PUT k t v` represents a PUT request that changes `k`'s value into `v` only if its ETag matches `t`; `GET k t` is a GET request for `k`'s value only if its ETag does not match `t`; `OK t v` indicates that the request target's value is `v` and its ETag is `t`.

that on the tester side. Vice versa, responses sent by the server might be reordered before arriving at the tester, as shown in Figure 1.3. Such tester's observation can be explained by various outputs on the SUT side. The validator needs to consider all possible outputs that can explain such observation, and see if anyone of them complies

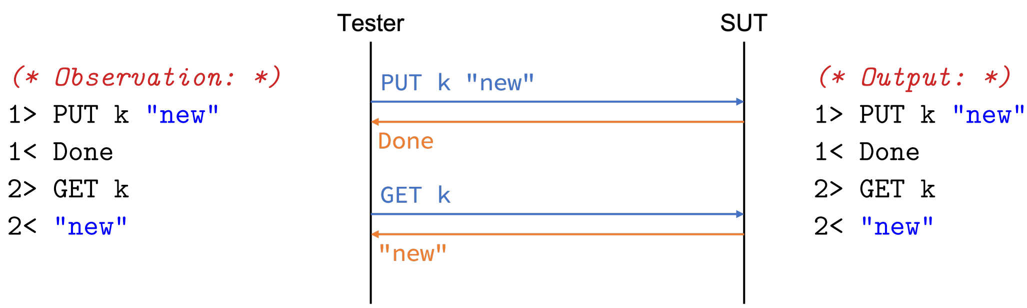


FIGURE 1.2. Upon no concurrency, the observation is identical to the output.

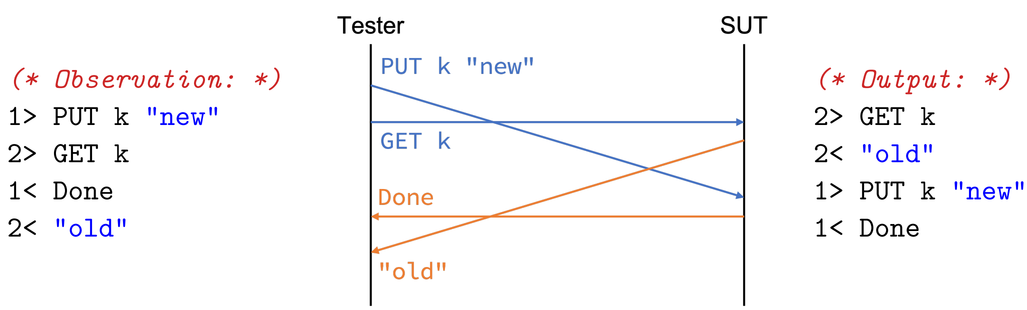


FIGURE 1.3. Acceptable: The observation can be explained by a valid output reordered by the network environment.

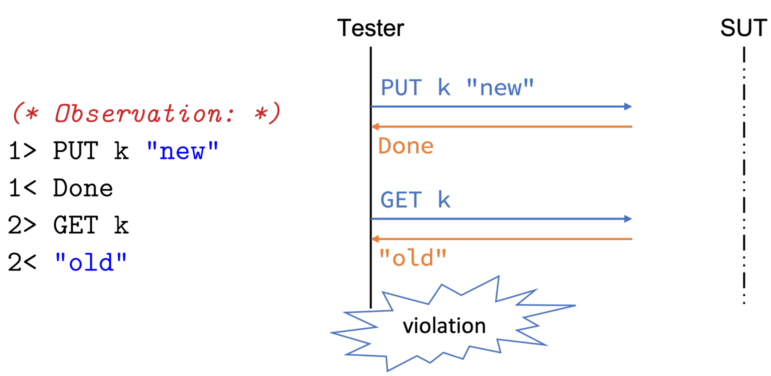


FIGURE 1.4. Unacceptable: The tester received the `Done` response before sending the `GET` request, thus the SUT must have processed the `PUT` request before the `GET` request. Therefore, the `"old"` response must be invalid.

with the specification. If no valid output can explain the observation, then the tester should reject the SUT, as shown in Figure 1.4.

We hope to construct a tester that can handle external nondeterminism systematically, and provide a generic way for reasoning on the environment.

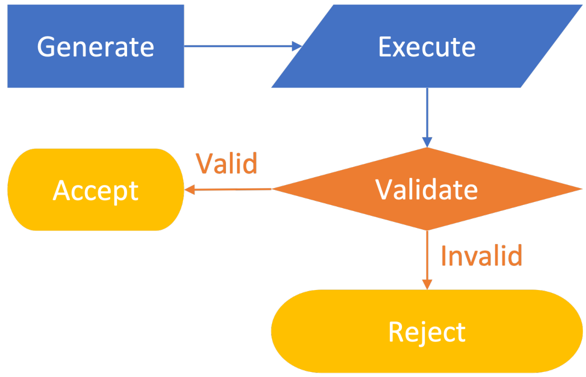


FIGURE 1.5. Simple tester architecture without shrinking.

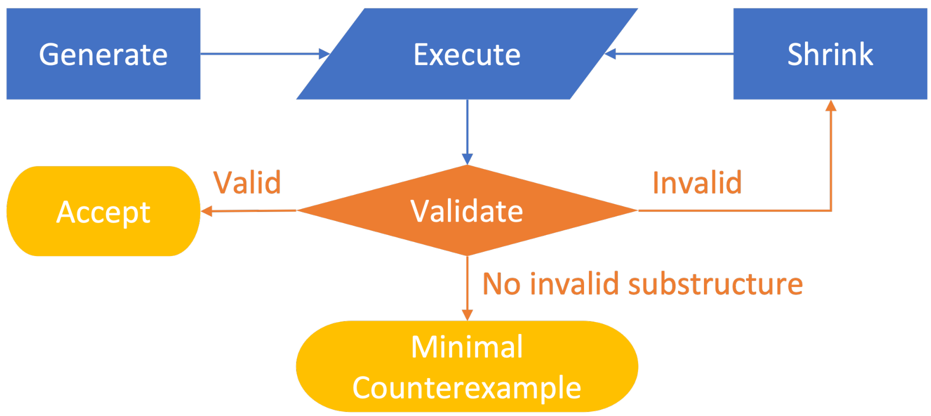


FIGURE 1.6. Tester architecture with shrinking mechanism.

1.3. Test harness and inter-execution nondeterminism

A good tester consists of (i) a validator that accurately determines whether its observations are valid or not, and (ii) a test harness that can reveal invalid observations effectively. Section 1.2 has explained the challenges in the validator. Here we discuss the test harness.

1.3.1. Test harness. Intuitively, a tester generates test input and executes the test. It then validates the observation and accepts/rejects the SUT, as shown in Figure 1.5.

However, to achieve better coverage, a randomized generator might produce huge test input. Suppose the tester has revealed invalid observation after thousands of interactions, such report provides limited intuition of where the bug was introduced. To help developers locate the bug more effectively, the tester should present a *minimal counterexample* that can reproduce the violation. This is done by *shrinking* the failing input and rerunning the test with the input's substructures. As shown in Figure 1.6, if a test input has no substructure that can cause any failure, then we report it as the minimal counterexample.

The test harness consists of generator, shrinker, and executor. This thesis studies the generator and the shrinker that produce the test input. The executor that produces observations based on the input is discussed in the related works chapter.

Interesting test inputs are those that are more likely to reveal invalid observations. Such subset is usually sparse and cannot be enumerated within reasonable budget *e.g.* in Subsection 1.2.1, request ETags that match the target resources'. The tester needs to manipulate the inputs' distribution, by implementing heuristics that emphasize certain input patterns. Such heuristics is challenged by another form of nondeterminism discussed as follows.

1.3.2. Inter-execution nondeterminism. Consider HTTP/1.1, where requests may be conditioned over timestamps. If a client has cached a version with a certain timestamp, then it can send the timestamp as `If-Modified-Since` precondition. The server should not transmit the request target's content if its `Last-Modified` timestamp is not newer than the precondition's:

```
/* Client: */
GET /index.html HTTP/1.1
If-Modified-Since: Mon, 7 Mar 2022 07:41:07 GMT
                           /* Server: */
                           HTTP/1.1 200 OK
                           Last-Modified: Tue, 8 Mar 2022 07:41:07 GMT
                           ... content of target ...
/* Client: */
GET /index.html HTTP/1.1
If-Modified-Since: Tue, 8 Mar 2022 07:41:07 GMT
                           /* Server: */
                           HTTP/1.1 304 Not Modified
```

In this scenario, an interesting candidate for the `If-Modified-Since` precondition is the `Last-Modified` timestamp of a previous response. To emphasize this request pattern, the tester needs to implement heuristics that generates test inputs based on previous observations.

In case the tester has revealed invalid observations from the server, it needs to rerun the test with shrunk input. The timestamps on the server might be different from the previous execution, so an interesting timestamp in a previous run might become trivial in this run.

Such inter-execution nondeterminism poses challenges to the input minimization process: To preserve the input pattern, the shrunk HTTP/1.1 request should use the timestamps from the new execution. We hope to implement a generic shrinking mechanism that can reproduce the heuristics in the test generator's design.

1.4. Contribution

This thesis addresses the challenges in testing caused by various forms of nondeterminism. I introduce symbolic languages for specifying the protocol and representing test input, and *dualize* the specification into the tester's (1) validator, (2) generator, and (3) shrinker:

(1) The specification is written as a reference implementation—a nondeterministic program that exhibits all possible behavior allowed by the protocol. Internal and external nondeterminism are represented by symbolic variables, and the space of nondeterministic behavior is defined by all possible assignments of the variables.

    For internal nondeterminism, the validator computes the symbolic representation of the SUT's output. The symbolic output expectation is then *unified* against the tester's observations, reducing the protocol compliance problem into constraint solving.

    For external nondeterminism, I introduce a model that specifies the environment. The environment model describes the relation between the SUT's output and the tester's observations. By composing the environment model with the reference implementation, we get a tester-side specification that defines the space of valid observations.

(2) Test generation heuristics are defined as computations from observations to the next input. To specify such heuristics in a generic way, I introduce intermediate representations for observations and test inputs, which are protocol-independent.

    Heuristics in this framework produces symbolic test inputs that are parameterized over observations. During execution, the test harness computes the concrete input by *instantiating* the symbolic input's arguments with runtime observations.

(3) The language for test inputs is designed with inter-execution nondeterminism in mind. By instantiating the inputs' symbolic intermediate representation with different observations, the test harness gets different test inputs but preserves the pattern.

    To minimize counterexamples, the test harness only needs to shrink the inputs' symbolic representation. When rerunning the test, the shrunk input is reinstantiated with the new observations, thus reproduces the heuristics by the test generator.

Thesis claim. Symbolic abstract representation can address challenges in testing interactive systems with uncertain behavior. Specifying protocols with symbolic reference implementation enables validating observations of systems with internal and external nondeterminism. Representing test input and observations symbolically allows generating and shrinking interesting test cases despite inter-execution nondeterminism. Combining these methods result in a rigorous tester that can capture protocol violations effectively.

This claim is supported by the following publications:

(1) *From C to Interaction Trees: Specifying, Verifying, and Testing a Networked Server* [10], with Nicolas Koh, Yao Li, Li-yao Xia, Lennart Beringer, Wolf Honoré, and William Mansky, where I developed a tester program based on a swap server's specification written as ITrees [16], and evaluated the tester's effectiveness by mutation testing.

(2) *Verifying an HTTP Key-Value Server with Interaction Trees and VST* [17], with Hengchu Zhang, Wolf Honoré, Nicolas Koh, Yao Li, Li-yao Xia, Lennart Beringer, and William Mansky, where I developed the top-level specification for HTTP/1.1, and derived a tester client that revealed liveness and interrupt-handling bugs in our HTTP server, despite it was formally verified.
(3) *Model-Based Testing of Networked Applications* [11], which describes my technique of specifying HTTP/1.1 with symbolic reference implementations, and from the specification, automatically deriving a tester program that can find bugs in Apache and Nginx.
(4) *Testing by Dualization* (to be submitted to OOPSLA), a theory for interactive testing, explaining how to specify protocols using abstract model implementations, and how to guarantee the soundness and completeness of validators derived from the abstract model.

Outline. This thesis is structured as follows:

CHAPTER 2

Dualization Theory

This chapter provides a theoretic view for validators, and shows how to address internal nondeterminism by dualizing symbolic specifications.

Section 2.1 defines the concepts in testing. Section 2.2 introduces a simple language that exhibits internal nondeterminism. From specifications written in this language, Section 2.3 derives validators by dualization. The derived validators are proven correct in Section 2.4.

2.1. Concepts

Testers are programs that determine whether implementations are compliant or not, based on its observations. This section defines the basic concepts and notations in interactive testing.

DEFINITION 2.1 (Implementations and Traces). *Implementations* are programs that can interact with their environment. *Traces* are the outputs and inputs during execution.[1] "Implementation i can *produce* trace t" is written as "$i \xrightarrow{t}$".

DEFINITION 2.2 (Specification, Validity, and Compliance). A *specification* is a description of valid traces. "Trace t is *valid* per specification s" is written as "$\mathsf{valid}_s\ t$".

An implementation i *complies* with a specification s (written "$\mathsf{comply}_s\ i$") if it only produces traces that are valid per the specification:

$$\mathsf{comply}_s\ i \quad \triangleq \quad \forall t, (i \xrightarrow{t}) \implies \mathsf{valid}_s\ t$$

DEFINITION 2.3 (Tester components and correctness). A tester consists of (i) a *validator* that accepts or rejects traces, and (ii) a *test harness* that triggers different traces with various input.

A tester is *correct* if its acceptances and rejections are sound and complete. A tester is *rejection-sound* if it only rejects incompliant implementations; it is *rejection-complete* if it can reject all incompliant implementations, provided sufficient time of execution.[2]

The tester's correctness is based on its components' properties: A rejection-sound tester requires its validator to be *rejection-sound*; A rejection-complete tester consists of (i) a *rejection-complete* validator and (ii) an *exhaustive* test harness that can eventually trigger invalid traces.

[1] This chapter focuses on internal nondeterminism, and assumes no external nondeterminism. The tester's observation is considered identical to the SUT's output.

[2] The semantics of "soundness" and "completeness" vary among contexts. This thesis inherits terminologies from existing literature [14], but explicitly use "rejection-" prefix for clarity. "Rejection soundness" is equivalent to "acceptance completeness", and vice versa.

Definition 2.4 (Correctness of validators). A validator v is *rejection-sound* with respect to specification s (written as "$v\ \mathsf{sound}^{\mathfrak{Rej}}_s$") if it only rejects traces that are invalid per s:

$$v\ \mathsf{sound}^{\mathfrak{Rej}}_s \quad \triangleq \quad \forall t, \neg(\mathsf{accept}_v\ t) \implies \neg(\mathsf{valid}_s\ t)$$

A validator v is *rejection-complete* with respect to specification s (written as "$v\ \mathsf{complete}^{\mathfrak{Rej}}_s$") if it rejects all behaviors that are invalid per s:

$$v\ \mathsf{complete}^{\mathfrak{Rej}}_s \quad \triangleq \quad \forall t, \neg(\mathsf{valid}_s\ t) \implies \neg(\mathsf{accept}_v\ t)$$

The rest of this chapter shows how to build validators that can be proven sound and complete.

2.2. QAC language family

To illustrate how to write specifications for testing purposes, this section introduces the "query-answer-choice" (QAC) language family for specifying network protocols that involve internal nondeterminism.

2.2.1. Specifying protocols with server models. Network protocols can be specified with "reference implementations" *i.e.* model programs that exhibit the space of valid behavior. Networked servers can be modelled as infinite stateful programs that compute the answer for each query.

Definition 2.5 (Deterministic server model). Let Q be the query type, A be the response type, and S be some server state type. Then a deterministic server is an infinite loop, defined by a loop body and an initial state. The loop body is a state monad that takes a query, produces the response based on its current state, and computes the next server state:

$$\begin{aligned}
&\mathsf{DeterministicServer} \triangleq \{\exists S, (Q \times S \to A \times S) \times S\} \\
&\mathsf{stepDeterministicServer} : Q \times \mathsf{DeterministicServer} \to A \times \mathsf{DeterministicServer} \\
&\mathsf{stepDeterministicServer}(q, \mathsf{pack}\ S = \sigma\ \mathsf{with}\ (\mathsf{sstep}, \mathit{state})) \triangleq \\
&\qquad \mathsf{let}\ (a, \mathit{state}') = \mathsf{sstep}(q, \mathit{state})\ \mathsf{in} \\
&\qquad (a, \mathsf{pack}\ S = \sigma\ \mathsf{with}\ (\mathsf{sstep}, \mathit{state}'))
\end{aligned}$$

Here $\mathsf{pack}\ S = \sigma\ \mathsf{with}\ (\mathsf{sstep}, \mathit{state})$ is an instance of the $\mathsf{DeterministicServer}$ existential type [12], where sstep is of type $Q \times \sigma \to A \times \sigma$, and state has type σ.

For example, consider an CMP-SET protocol: The server stores a number `S`. If the client sends a request that is smaller than `S`, then the server responds with `0`. Otherwise, the server sets `S` to the request, and responds with `1`:

```
int S = 0;
while (true) {
  int request = recv();
  if (request <= S) send(0);
  else { S = request; send(1); }
}
```

Such server can be modelled as:

$$\mathsf{pack}\ S = \mathbb{Z}\ \mathsf{with}\ (\lambda(q,s) \Rightarrow \begin{cases}(0,s) & q \leq s\\ (1,q) & \text{otherwise}\end{cases},\\ 0)$$

In general, servers' responses and transitions might depend on choices that are invisible to the testers. These choices include inter-implementation nondetermism like algorithm design, and inter-execution nondeterminism like random numbers and timestamps.

Definition 2.6 (Nondeterministic server model). Let C be the space of invisible choices, then a nondeterministic server is specified as:

$$\begin{aligned}
&\mathsf{Server} \triangleq \{\exists S, (Q \times C \times S \to A \times S) \times S\}\\
&\mathsf{stepServer} : Q \times C \times \mathsf{Server} \to A \times \mathsf{Server}\\
&\mathsf{stepServer}(q, c, \mathsf{pack}\ S = \sigma\ \mathsf{with}\ (\mathsf{sstep}, \mathit{state})) \triangleq\\
&\qquad \mathsf{let}\ (a, \mathit{state}') = \mathsf{sstep}(q, c, \mathit{state})\ \mathsf{in}\\
&\qquad (a, \mathsf{pack}\ S = \sigma\ \mathsf{with}\ (\mathsf{sstep}, \mathit{state}'))
\end{aligned}$$

Consider changing the aforementioned CMP-SET into CMP-RST: When the request is greater than `S`, the server resets `S` to a random number:

```c
int S = 0;
while (true) {
  int request = recv();
  if (request <= S) send(0);
  else { S = rand(); send(1); }
}
```

Its corresponding server model can be written as

$$\mathsf{pack}\ S = \mathbb{Z}\ \mathsf{with}\ (\lambda(q,c,s) \Rightarrow \begin{cases}(0,s) & q \leq s\\ (1,c) & \text{otherwise}\end{cases},\\ 0)$$

2.2.2. Validating traces. In the QAC language family, a trace is a list of $Q \times A$ pairs. The validator takes a trace and determines whether it is valid per the protocol specification.

Definition 2.7 (Trace validity). Trace t is valid per protocol specification s (written as "$\mathsf{valid}_s\ t$") if and only if it can be *produced* by the specification *i.e.* server model:

$$\mathsf{valid}_s\ t \quad \triangleq \quad \exists s', s \xrightarrow{t} s'$$

Here the producibility relation in Section 2.1 is expanded with an argument s' representing the post-transition state, pronounced "specification s can produce trace t and step to specification s' ":

(1) A server model can produce an empty trace and step to itself:

$$s \xrightarrow{\varepsilon} s$$

(2) A server model can produce a non-empty trace if it can produce the head of the trace, and step to some server model that produces the tail of the trace:

$$s \xrightarrow{t+(q,a)} s_2 \quad \triangleq \quad \exists s_1, s \xrightarrow{t} s_1 \wedge \exists c, \mathsf{stepServer}(q, c, s_1) = (a, s_2)$$

The validator is encoded as an infinite loop, where the loop body is a state monad that determines whether each $Q \times A$ pair is valid.

Definition 2.8 (Validator). Let V be some validator state type, then a validator starts from an initial state, takes a query and its corresponding response, determines whether the interaction are valid, and computes the next validator state upon valid:

$$\mathsf{Validator} \triangleq \{\exists V, (Q \times A \times V \to \mathsf{option}\ V) \times V\}$$

$$\mathsf{stepValidator} : Q \times A \times \mathsf{Validator} \to \mathsf{option\ Validator}$$

$$\mathsf{stepValidator}(q, a, \mathsf{pack}\ V = \beta\ \mathsf{with}\ (\mathsf{vstep}, \mathit{state}))$$

$$\triangleq \begin{cases} \mathsf{Some}\ (\mathsf{pack}\ V = \beta\ \mathsf{with}\ (\mathsf{vstep}, \mathit{state}')) & \mathsf{vstep}(q, a, \mathit{state}) = \mathsf{Some}\ \mathit{state}' \\ \mathsf{None} & \mathsf{vstep}(q, a, \mathit{state}) = \mathsf{None} \end{cases}$$

For example, a validator for the CMP-SET protocol is written as:

$$\mathsf{pack}\ V = \mathbb{Z}\ \mathsf{with}\ (\lambda(q, a, v) \Rightarrow \begin{cases} \mathsf{if}\ a\ \mathsf{is}\ 0\ \mathsf{then\ Some}\ v\ \mathsf{else\ None} & q \leq v \\ \mathsf{if}\ a\ \mathsf{is}\ 1\ \mathsf{then\ Some}\ q\ \mathsf{else\ None} & \text{otherwise} \end{cases},$$
$$0)$$

Definition 2.9 (Trace acceptance). A validator accepts a trace if its step function *consumes* the entire trace:

$$\mathsf{accept}_v\ t \quad \triangleq \quad \exists v', v \xrightarrow{t} v'$$

Here the cossumability relation "$v \xrightarrow{t} v'$ " is pronounced "validator v can consume trace t and step into validator v' ":

(1) A validator can consume an empty trace and step to itself:

$$v \xrightarrow{\varepsilon} v$$

(2) A validator consumes a non-empty trace if it can consume the head of the trace, and step to some validator that can consume the tail of the trace:

$$v \xrightarrow{t+(q,a)} v_2 \quad \triangleq \quad \exists v_1, v \xrightarrow{t} v_1 \wedge \mathsf{stepValidator}(q, a, v_1) = \mathsf{Some}\ v_2$$

2.2.3. Soundness and completeness of validators. We can now phrase the correctness properties in Section 2.1 in terms of the QAC language family:

(1) A rejection-sound (*i.e.* acceptance-complete) validator consumes all traces that are producible by the protocol specification:

$$\begin{aligned} v\ \mathsf{sound}_s^{\mathfrak{Rej}} &\triangleq \forall t, \neg(\mathsf{accept}_v\ t) \implies \neg(\mathsf{valid}_s\ t) \\ &\triangleq \forall t, (\exists s', s \xrightarrow{t} s') \implies \exists v', v \xrightarrow{t} v' \end{aligned}$$

(2) A rejection-complete (*i.e.* acceptance-sound) validator only consumes traces that are producible by the protocol specification:

$$\begin{aligned} v\ \mathsf{complete}_s^{\mathfrak{Rej}} &\triangleq \forall t, \neg(\mathsf{valid}_s\ t) \implies \neg(\mathsf{accept}_v\ t) \\ &\triangleq \forall t, (\exists v', v \xrightarrow{t} v') \implies \exists s', s \xrightarrow{t} s' \end{aligned}$$

2.3. Dualizing specifications into validators

So far we have defined the QAC language family, where specifications and validators are represented as state monads. This section will show how to derive validators from the specification.

2.3.1. Encoding specifications and validators. To write an algorithm from the specification to the validator, we need to analyze the computations defined by the specification's model program. The QAC language family only provides a state monad interface, which is not destructable by itself. We need to introduce a programming language to represent the specification, and derive validators by interpreting programs written in that language.

Definition 2.10 (Server and validator of a program). A program $p \in \mathsf{Prog}$ is a representation of computation that can be "instantiated" into a server model:

$$\mathsf{serverOf} : \mathsf{Prog} \to \mathsf{Server}$$

A program can also be "interpreted" into other computations, including validators:

$$\mathsf{validatorOf} : \mathsf{Prog} \to \mathsf{Validator}$$

To encode specifications for protocols like CMP-RST, we introduce a simple Prog language, which supports arithmetic operations and memory access:

$$\begin{array}{lcll} \mathsf{Prog} & \triangleq & \mathsf{return} & \text{end computation and send response} \\ & | & !dst \coloneqq \mathsf{SExp}; \mathsf{Prog} & \text{write to address } dst \in \mathbb{N} \\ & | & \mathsf{if}\ \mathsf{SExp} \le \mathsf{SExp}\ \mathsf{then}\ \mathsf{Prog}\ \mathsf{else}\ \mathsf{Prog} & \text{conditional branch} \\ \mathsf{SExp} & \triangleq & \mathbb{Z} & \text{constant integer} \\ & | & !src & \text{read from address } src \in \mathbb{N} \\ & | & \mathsf{SExp}\ op\ \mathsf{SExp} & op \in \{+, -, \times, \div\} \end{array}$$

Servers specified in this Prog language are defined as follows:

(1) The server state is a key-value mapping, where the keys are natural numbers, and the values are integers.
(2) The initial server state maps all keys to zero:

$$\mathsf{serverOf}(p) \triangleq \mathsf{pack}\ S = \mathbb{N} \to \mathbb{Z}\ \mathsf{with}\ (\mathsf{sstep}_p, (\_ \mapsto 0))$$

(3) The server's query, response, and choices (Q, A, C) are all natural numbers.
(4) At the beginning of each server loop, the query is written to address !0, and the internal choice is written to address !1.
(5) After writing the query and response, the server executes the Prog model, which manipulates the key-value store.
(6) When the Prog model returns, the server sends back the value stored in address !0 as the response.

Let $p \in \mathsf{Prog}$ be the model program, then the server's loop body sstep_p is defined as:

$$\begin{array}{lll}
\mathsf{sstep}_p(q, c, s_0) & \triangleq & \mathsf{let}\ s_1 = s_0[1 \mapsto c]\ \mathsf{in} \\
& & \mathsf{let}\ s_2 = s_1[0 \mapsto q]\ \mathsf{in} \\
& & \mathsf{let}\ s_3 = \mathsf{exec}(p, s_2)\ \mathsf{in} \\
& & (s_3!0, s_3) \\
\mathsf{exec}(p, s) & \triangleq & \begin{cases} s & p\ \mathsf{is\ return} \\ \mathsf{exec}(p', s[dst \mapsto e^s]) & p\ \mathsf{is}\ !dst := e; p' \\ \mathsf{exec}(\mathsf{if}\ {e_1}^s \le {e_2}^s\ \mathsf{then}\ p_1\ \mathsf{else}\ p_2, s) & p\ \mathsf{is\ if}\ e_1 \le e_2\ \mathsf{then}\ p_1\ \mathsf{else}\ p_2 \end{cases} \\
e^s & \triangleq & \begin{cases} z & e\ \mathsf{is}\ z : \mathbb{Z} \\ s!src & e\ \mathsf{is}\ !src \\ {e_1}^s\ op\ {e_2}^s & e\ \mathsf{is}\ e_1\ op\ e_2 \end{cases}
\end{array}$$

Here "e^s" is pronounced "evaluating server expression ($e : \mathsf{SExp}$) with state ($s : \mathbb{N} \to \mathbb{Z}$)". It substitutes all occurences of "$!src$" with the value stored at address src of mapping s, written as "$s!src$". "$s[k \mapsto v]$" is pronounced "updating mapping s at address k to value v". It produces a new state where k is mapped to v, while other addresses remain unchanged from s:

$$s[k \mapsto v]!k' \triangleq \begin{cases} v & k' = k \\ s!k' & k' \neq k \end{cases}$$

To specify protocols with this Prog language, the model program should read the query from address !0, and parameterize the space of nondeterministic behavior over the internal choice in address !1. When the model program returns, it should have stored the computed response in address !0. Addresses greater than !1 are only writable by the specification, and can be used for storing the server state.

For example, the CMP-RST specification in Section 2.2 can be written in Prog as:

$$\begin{array}{ll} \mathsf{if}\ !0 \le !2\ \mathsf{then}\ !0 := 0; \mathsf{return} & (1) \\ \mathsf{else}\ !0 := 1; !2 := !1; \mathsf{return} & (2) \end{array}$$

When the query is less than or equal to the value stored in !2 (case 1), the server writes response 0 to address !0, and leave address !2 untouched. For queries greater than the value in !2 (case 2), the server writes 1 as response, and updates address !2 with the internal choice stored in !1.

This Prog language features arithmetic operations, conditional branches, memory access, and internal nondeterminism. It also exhibits a tree structure that allows inductive reasoning. The rest of this section derives validators from Prog models, and prove the correctness of such derived validators.

2.3.2. Dualize model program into validator. The validator of a model $p \in \mathsf{Prog}$ needs to determine whether the trace is producible by p. More specifically, whether the responses in the trace can be *explained* by p's return value stored at address !0.

The idea is similar to `tester` in Section 1.1, which `validate`s the trace by executing the `serverSpec`, and comparing the expected response against the tester's observation.

However, when the specification is nondeterministic, the expectation of response A is parameterized over the internal choice C. Therefore, the validator should determine whether there exists such C that led the specification to produce the observed A.

This reduces the trace validation problem to constraint solving. Upon observing a response, the validator adds a constraint that the observation can be explained by running the specification with certain value of choices.

More specifically, the validator executes the Prog model and represents internal choices with *symbolic variables*. These variables are carried along the program execution, so the expected responses are computed as *symbolic expressions* that might depend on those variables. The validator then constraints that the symbolic response is equal to the concrete observation.

To achieve this goal, the validator needs to store the symbolic expression for each address of the server model. It also needs to remember all the constraints added upon observation. We store these information as "validation states":

$$(\mathbb{N} \to \mathsf{VExp}) \times \mathsf{set\ constraint}$$

Here the $\mathsf{constraint}$s are relations between validator expressions (VExps) that may depend on symbolic variables:

$$\begin{array}{lcll} \mathsf{constraint} & \triangleq & \mathsf{VExp}\ \mathit{cmp}\ \mathsf{VExp} & \mathit{cmp} \in \{<, \leq, \equiv\} \\ \mathsf{VExp} & \triangleq & \mathbb{Z} & \text{constant integer} \\ & | & \#x & \text{variable } x \in \mathsf{var} \\ & | & \mathsf{VExp}\ \mathit{op}\ \mathsf{VExp} & \mathit{op} \in \{+, -, \times, \div\} \end{array}$$

In practice, we use an equivalent definition for the validator state:

$$(\mathbb{N} \to \mathsf{var}) \times \mathsf{set\ constraint}$$

The key-expression mapping $(k \mapsto e)$ above can be simulated with the key-variable $(k \mapsto x)$ mapping here, by adding $(\#x \equiv e)$ to the set of constraints. We alter the type interface for convenience of developing the validator, which will be later explained in more details.

Notice that the internal choices might affect branch conditions, so the validator doesn't know which branch in the specification was taken. Therefore, it should maintain multiple validation states, one for each possible execution path of the specification:

$$\mathsf{set}\ ((\mathbb{N} \to \mathsf{var}) \times \mathsf{set\ constraint})$$

The initial state of the validator is a single validation state that corresponds to the specification's initial state:

$$\{(\_ \mapsto \#0, \{\#0 \equiv 0\})\}$$

Here the initial validation state says "all addresses are mapped to variable #0, and the value of variable #0 is constrained to be zero". This reflects the initial server state that maps all addresses to zero value.

The validator's loop body is derived by dualzing the server model:

(1) When the server performs a write operation $!\mathit{dst} := \mathit{exp}$, the validator creates a fresh variable x to represent the new value stored in address $!\mathit{dst}$, and adds a constraint that says x's value is equal to that of exp.

(2) When the server makes a nondeterministic branch $\mathsf{if}\ e_1 \le e_2\ \mathsf{then}\ p_1\ \mathsf{else}\ p_2$, consider both cases: (a) If p_1 was taken, then the validator should add a constraint $e_1 \le e_2$; or (b) If p_2 was taken, then the validator should add constraint $e_2 < e_1$.
(3) Before executing the program, the server writes the internal choice c to address !1. Accordingly, the validator creates a fresh variable to represent the new value stored in address !1, without adding any constraint.
(4) After executing the program, the server sends back the value stored in !0 as response. Accordingly, the validator adds a constraint that says the variable representing address !0 is equal to the observed response.
(5) When the constraints of a validation state becomes unsatisfiable, it indicates that the server model cannot explain the observation. This is because either (i) the observation is invalid *i.e.* not producible by the server model, or (ii) the observation is valid, but was produced by a different execution path of the server model.
(6) The validator accepts the trace if it can be produced by any execution path of the server model. Since each execution path corresponds to a validation state, the validator only needs to remove the unsatisfiable state from the set of states. If the set of validation states becomes empty, it indicates that the observation cannot be explained by any execution path of the specification, so the validator should reject the trace.

This mechanism is formalized in Figure 2.1. Here notation "$x \leftarrow v; f(x)$" is a monadic bind for sets: Let f map each element (vs, cs) in v to a set of validation states $(f(vs, cs) : \mathsf{set}\ ((\mathbb{N} \to \mathbb{N}) \times \mathsf{set\ constraint}))$. The return value of vstep'_p is the union of all result sets.

The validator assumes a constraint solver that can determine whether a set of constraints is satisfiable, *i.e.* whether there exists an *assignment* of variables $(\mathsf{var} \to \mathbb{Z})$ that satisfy all the constraints:

$$\forall cs, \mathsf{solvable}\ cs \iff \exists (asgn : \mathsf{var} \to \mathbb{Z}), asgn\ \mathsf{satisfy}\ cs$$

$$asgn\ \mathsf{satisfy}\ cs \triangleq \forall (e_1\ cmp\ e_2) \in cs, {e_1}^{asgn}\ cmp\ {e_2}^{asgn}$$

$$e^{asgn} \triangleq \begin{cases} z & e\ \mathsf{is}\ z : \mathbb{Z} \\ asgn!x & e\ \mathsf{is}\ \#x \\ {e_1}^{asgn}\ op\ {e_2}^{asgn} & e\ \mathsf{is}\ e_1\ op\ e_2 \end{cases}$$

Here "e^{asgn}" is pronounced "evaluating validator expression $(e : \mathsf{VExp})$ with assignment $(asgn : \mathsf{var} \to \mathbb{Z})$". It substitutes all occurences of "$\#x$" with their assigned value $(asgn!x)$.

When the Prog model writes to memories or makes conditional branches, the operands are represented as specification expressions (SExp) that refer to server addresses. To construct the constraints over symbolic variables, the validator translates the expressions $(e : \mathsf{SExp})$ into validator expressions $(e^{vs} : \mathsf{VExp})$ by *symbolizing* it with the validation state $(vs : \mathbb{N} \to \mathsf{var})$, which substitutes all addresses $(!src)$ with their corresponding variable $\#(vs!src)$.

$$
\begin{array}{lll}
\mathsf{validatorOf}(p) & \triangleq & \mathsf{pack}\ V = \mathsf{set}\ ((\mathbb{N} \to \mathsf{var}) \times \mathsf{set\ constraint})\ \mathsf{with} \\
& & (\mathsf{vstep}_p, \{(\_ \mapsto \#0, \{\#0 \equiv 0\})\}) \\
\mathsf{vstep}_p(q, a, v) & \triangleq & \mathsf{let}\ v' = \mathsf{vstep}'_p(q, a, v)\ \mathsf{in} \\
& & \mathsf{if}\ v'\ \mathsf{is}\ \varnothing\ \mathsf{then\ None\ else\ Some}\ v' \qquad (6) \\
\mathsf{vstep}'_p(q, a, v) & \triangleq & v_0 \leftarrow v; \\
& & \mathsf{let}\ v_1 = \mathsf{havoc}(1, v_0)\ \mathsf{in} \\
& & \mathsf{let}\ v_2 = \mathsf{write}(0, q, v_1)\ \mathsf{in} \\
& & (vs_3, cs_3) \leftarrow \mathsf{exec}(p, v_2); \\
& & \mathsf{let}\ cs_4 = cs_3 \cup \{\#(vs_3!0) \equiv a\}\ \mathsf{in} \qquad (4) \\
& & \mathsf{if\ solvable}\ cs_4\ \mathsf{then}\ \{(vs_3, cs_4)\}\ \mathsf{else}\ \varnothing \qquad (5) \\
\mathsf{exec}(p, (vs, cs)) & \triangleq & \begin{cases} \{(vs, cs)\} & p\ \mathsf{is\ return} \\ \mathsf{exec}(p', \mathsf{write}(d, e, (vs, cs))) & p\ \mathsf{is}\ !d \coloneqq e; p' \\ \begin{pmatrix} \mathsf{let}\ v_1 = (vs, cs \cup \{{e_1}^{vs} \le {e_2}^{vs}\})\ \mathsf{in} \\ \mathsf{let}\ v_2 = (vs, cs \cup \{{e_2}^{vs} < {e_1}^{vs}\})\ \mathsf{in} \\ \mathsf{exec}(p_1, v_1) \cup \mathsf{exec}(p_2, v_2) \qquad (2) \end{pmatrix} & \begin{array}{l} p\ \mathsf{is} \\ \mathsf{if}\ e_1 \le e_2 \\ \mathsf{then}\ p_1\ \mathsf{else}\ p_2 \end{array} \end{cases} \\
\mathsf{write}(d, e, (vs, cs)) & \triangleq & \mathsf{let}\ x_e = \mathsf{fresh}\ (vs, cs)\ \mathsf{in} \qquad (1) \\
& & (vs[d \mapsto x_e], cs \cup \{\#x_e \equiv e^{vs}\}) \\
\mathsf{havoc}(d, (vs, cs)) & \triangleq & \mathsf{let}\ x_c = \mathsf{fresh}\ (vs, cs)\ \mathsf{in}\ (vs[d \mapsto x_c], cs) \qquad (3) \\
e^{vs} & \triangleq & \begin{cases} n & e\ \mathsf{is}\ n : \mathbb{N} \\ \#(vs!src) & e\ \mathsf{is}\ !src \\ {e_1}^{vs}\ op\ {e_2}^{vs} & e\ \mathsf{is}\ e_1\ op\ e_2 \end{cases}
\end{array}
$$

FIGURE 2.1. Dualizing server model into validator, with derivation rules annotated.

For example, by dualizing the Prog model for CMP-RST in Subsection 2.3.1, we get a validator as shown in Figure 2.2. Such derived validators are proven sound and complete in the following section.

2.4. Soundness and completeness of derived validators

So far we have introduced the QAC language family for representing servers and validators, and demonstrated the derivation mechanism with a Prog language. Next I'll show how to prove that QAC validators are sound and complete:

$$
\begin{array}{l}
\forall p : \mathsf{Prog},\ \mathsf{let}\ s = \mathsf{serverOf}(p)\ \mathsf{in} \\
\qquad \mathsf{let}\ v = \mathsf{validatorOf}(p)\ \mathsf{in} \\
\qquad v\ \mathsf{sound}_s^{\mathfrak{Rej}} \land v\ \mathsf{complete}_s^{\mathfrak{Rej}} \\
\qquad i.e.\ \forall t : \mathsf{list}\ (Q \times A), \\
\qquad\qquad \mathsf{valid}_s\ t \iff \mathsf{accept}_v\ t \\
\qquad\qquad i.e.\ \exists s', s \xrightarrow{t} s' \iff \exists v', v \xrightarrow{t} v'
\end{array}
$$

This section first presents a generic framework for proving validators' correctness properties, and then demonstrates its usage by applying it to Prog-based validators.

$$
\begin{array}{lll}
\multicolumn{3}{l}{\mathsf{validatorOf}(\texttt{CMP-RST}) \triangleq \mathsf{pack}\ V = \mathsf{set}\ ((\mathbb{N} \to \mathsf{var}) \times \mathsf{set\ constraint})\ \mathsf{with}} \\
(\quad \lambda(q,a,v) \Rightarrow & \mathsf{let}\ v' = (vs_0, cs_0) \leftarrow v; & \\
& \quad \mathsf{let}\ vs_1 \ = vs_0[1 \mapsto \mathsf{fresh}\ vs_0] \quad \mathsf{in} & (1) \\
& \quad \mathsf{let}\ x_q \ = \mathsf{fresh}\ (vs_1, cs_0) \quad \mathsf{in} & \\
& \quad \mathsf{let}\ vs_2 \ = vs_1[0 \mapsto x_q] \quad \mathsf{in} & \\
& \quad \mathsf{let}\ cs_2 \ = cs_0 \cup \{\#x_q \equiv q\} \quad \mathsf{in} & \\
& \quad \mathsf{let}\ cs_{3a0} = cs_2 \cup \{\#(vs_2!0) \leq \#(vs_2!2))\} \quad \mathsf{in} & (2a) \\
& \quad \mathsf{let}\ x_{3a1} \ = \mathsf{fresh}\ (vs_2, cs_{3a0}) \quad \mathsf{in} & \\
& \quad \mathsf{let}\ vs_{3a1} = vs_2[0 \mapsto x_{3a1}] \quad \mathsf{in} & \\
& \quad \mathsf{let}\ cs_{3a1} = cs_{3a0} \cup \{\#x_{3a1} \equiv 0\} \quad \mathsf{in} & \\
& \quad \mathsf{let}\ cs_{3b0} = cs_2 \cup \{\#(vs_2!2) < \#(vs_2!0)\} \quad \mathsf{in} & (2b) \\
& \quad \mathsf{let}\ x_{3b1} \ = \mathsf{fresh}\ (vs_2, cs_{3b0}) \quad \mathsf{in} & \\
& \quad \mathsf{let}\ vs_{3b1} = vs_2[0 \mapsto x_{3b1}] \quad \mathsf{in} & \\
& \quad \mathsf{let}\ cs_{3b1} = cs_{3b0} \cup \{\#x_{3b1} \equiv 1\} \quad \mathsf{in} & \\
& \quad \mathsf{let}\ x_{3b2} \ = \mathsf{fresh}\ (vs_{3b1}, cs_{3b1}) \quad \mathsf{in} & \\
& \quad \mathsf{let}\ vs_{3b2} = vs_{3b1}[2 \mapsto x_{3b2}] \quad \mathsf{in} & \\
& \quad \mathsf{let}\ cs_{3b2} = cs_{3b1} \cup \{\#x_{3b2} \equiv \#(vs_{3b2}!1)\} \quad \mathsf{in} & \\
& \quad ((vs_4, cs_4) \leftarrow \{(vs_{3a1}, cs_{3a1}), (vs_{3b2}, cs_{3b2})\}; & (3) \\
& \quad \mathsf{let}\ cs_5 \ = cs_4 \cup \{\#(vs_4!0) \equiv a\} \quad \mathsf{in} & \\
& \quad \mathsf{if\ solvable}\ cs_5\ \mathsf{then}\ \{(vs_4, cs_5)\}\ \mathsf{else}\ \varnothing & \\
& \mathsf{in} & \\
& \mathsf{if}\ v'\ \mathsf{is}\ \varnothing\ \mathsf{then\ None\ else\ Some}\ v' & \\
, \quad \{(\_ \mapsto \#0, \{\#0 \equiv 0\})\} & &)
\end{array}
$$

FIGURE 2.2. Validator for CMP-RST, derived from Prog model. This program consists of three parts: (1) symbolizing the query and internal choice before executing the model, (2) considering both branches in the model program, propagating a validation state for each branch, (3) filtering the validation states by constraint satisfiability, removing invalid states.

2.4.1. Proof strategy. Both the specification and the validator are infinite loops, and the correctness property is defined as equivalence between production and consumption of traces. Therefore, we can prove this bisimulation relation by introducing some loop invariant, and show that it is preserved in each step between the specification and the validator.

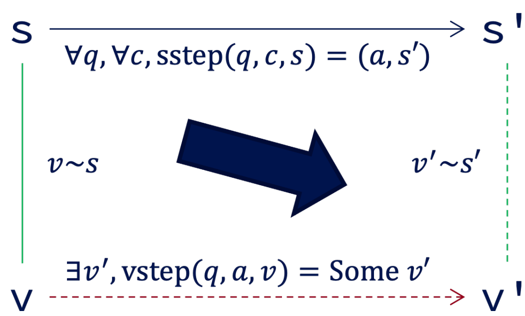
Rejection soundness (acceptance completeness). To prove that any trace producible by server $\mathsf{pack}\ S = \sigma\ \mathsf{with}\ (\mathsf{sstep}, s_0)$ is consumable by validator $\mathsf{pack}\ V = \beta\ \mathsf{with}\ (\mathsf{vstep}, v_0)$, we need forward induction on the server's execution path, and show that every step has a corresponding validator step:

- The initial server state s_0 reflects the initial validator state v_0:

$$(v_0 : \beta) \sim (s_0 : \sigma) \qquad \text{(RejSound-Init)}$$

- Any server step $\mathsf{sstep}(q, c, s) = (a, s')$ whose pre-execution state s reflects some pre-validation state v can be consumed by the validator into a post-validation state v' that reflects the post-execution state s':

$$\begin{aligned}&\forall (q : Q)(c : C)(a : A)(s, s' : \sigma)(v : \beta), \\ &\mathsf{sstep}(q, c, s) = (a, s') \wedge v \sim s \\ &\quad \Longrightarrow \exists v' : \beta, \mathsf{vstep}(q, a, v) = \mathsf{Some}\ v' \wedge v' \sim s'\end{aligned} \tag{RejSound-Step}$$



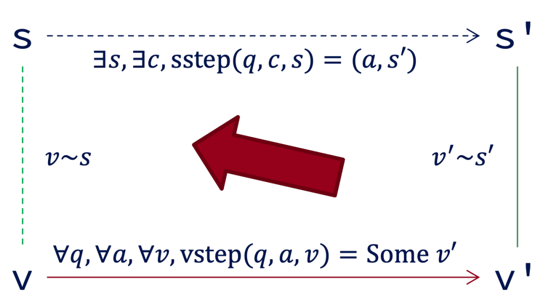
Rejection completeness (acceptance soundness). To prove that any trace consumable by validator $\mathsf{pack}\ V = \beta\ \mathsf{with}\ (\mathsf{vstep}, v_0)$ is producible by server $\mathsf{pack}\ S = \sigma\ \mathsf{with}\ (\mathsf{sstep}, s_0)$, we need backward induction on the validator's execution path, and show that every step has a corresponding server step:

- Any accepting validator step $\mathsf{vstep}(q, a, v) = \mathsf{Some}\ v'$ has some server state s' that reflects the post-validation state v':

$$\begin{aligned}&\forall (q : Q)(a : A)(v, v' : \beta), \mathsf{vstep}(q, a, v) = \mathsf{Some}\ v' \\ &\qquad\qquad \Longrightarrow \exists s' : \sigma, v' \sim s'\end{aligned} \tag{RejComplete-End}$$

- Any accepting validator step $\mathsf{vstep}(q, a, v) = \mathsf{Some}\ v'$ whose post-validation state v' reflects some post-execution server state s' has a corresponding server step from a pre-execution state s that reflects the pre-validation state v:

$$\begin{aligned}&\forall (q : Q)(a : A)(v, v' : \beta)(s' : \sigma), \\ &\mathsf{vstep}(q, a, v) = \mathsf{Some}\ v' \wedge v' \sim s' \\ &\quad \Longrightarrow \exists (s : \sigma)(c : C), \mathsf{sstep}(q, c, s) = (a, s') \wedge v \sim s\end{aligned} \tag{RejComplete-Step}$$



- The initial validator state v_0 only reflects the initial server state s_0:

$$\{s \mid v_0 \sim s\} = \{s_0\} \qquad \text{(RejComplete-Init)}$$

Rejection soundness is proven by forward induction, while rejection completeness is proven by backward induction. This is because the choice C is known from the server step, but unknown from the validator step: Given a validator step, we cannot predict "what choices the server will make in the future", but can analyze "what choices the server might have made in the past". This proof strategy is further explained with the Prog example.

2.4.2. Case study: Proving Prog-based validators' correctness. For specifications written in the Prog language, the validator is derived by dualizing the server model. It maintains a set of validation states, each state corresponds to a possible execution path of the model program.

A validation state is accepting if its constraints are satisfiable, *i.e.* there exists an assignment of the symbolic variables that can unify the trace with the server model.

The validator accepts the trace if any of its validation states is accepting, which indicates that some execution path of the server model can produce the trace.

Given an accepting validation state, we can construct the server steps that produce the trace, using the assignment ($\mathsf{var} \to \mathbb{Z}$) that satisfies the constraints. This assignment evaluates internal choices' symbolic variables into concrete values, and evaluates the validator's key-variable mapping ($\mathbb{N} \to \mathsf{var}$) to the server's key-value mapping ($\mathbb{N} \to \mathbb{Z}$).

Therefore, we only need to show that each server and validator step preserves the existence of such assignment that relates their states.

For the rest of this section, $\beta = \mathsf{set}\ ((\mathbb{N} \to \mathsf{var}) \times \mathsf{set\ constraint})$ represents the validator state type, and $\sigma = \mathbb{N} \to \mathbb{Z}$ represents the server state type.

Definition 2.11 (Invariant between Prog-based specification and validator). Validator state v *simulates* server state s if it contains a validation state (vs, cs) that *reflects* the server state, *i.e.* (1) There exists an assignment $asgn$ that can satisfy the constraints cs; and (2) The key-variable mapping vs can be evaluated with $asgn$ (written as vs^{asgn}) into a key-value mapping that is equivalent with s:

$$\begin{array}{lcl} (v : \beta) \sim (s : \sigma) & \triangleq & \exists ((vs, cs) \in v)(asgn : \mathsf{var} \to \mathbb{Z}), asgn\ \mathsf{satisfy}\ cs \wedge vs^{asgn} \equiv s \\ vs^{asgn} & \triangleq & addr \mapsto asgn!(vs!addr) \end{array}$$

Lemma 2.1 (RejSound-Init).

$$\begin{array}{ll} \text{If:} & vs = (\_ \mapsto \#0) \qquad cs = \{\#0 \equiv 0\} \qquad s = (\_ \mapsto 0) \\ \text{Then:} & \{(vs, cs)\} \sim s \end{array}$$

Proof. Since (vs, cs) is the only element in the validator state, we only need to show that:

$$\exists (asgn : \mathsf{var} \to \mathbb{Z}), asgn\ \mathsf{satisfy}\ cs \wedge vs^{asgn} \equiv s$$

By constructing the assignment as:

$$asgn = (\_ \mapsto 0)$$

We have:

$$\#0^{asgn} = 0$$

Thus:

$$asgn \ \mathsf{satisfy} \ cs$$

We also know that:

$$\forall k, asgn!(vs!k) = 0 = (s!k)$$

Thus:

$$vs^{asgn} \equiv s$$

$\square$

LEMMA 2.2 (RejSound-Step).

$$\begin{aligned}
&\forall (p : \mathsf{Prog})(q, c, a : \mathbb{Z})(s, s' : \sigma)(v : \beta),\\
&\mathsf{sstep}_p(q, c, s) = (a, s') \land v \sim s\\
&\implies \exists v' : \beta, \mathsf{vstep}_p(q, a, v) = \mathsf{Some}\ v' \land v' \sim s'
\end{aligned}$$

PROOF. The invariant $v \sim s$ tells us that v contains a validation state that reflects the server state s_0:

$$\exists((vs, cs) \in v)(asgn : \mathsf{var} \to \mathbb{Z}), asgn \ \mathsf{satisfy} \ cs \land vs^{asgn} \equiv s$$

Since the server's internal choice was provided, we can compute the server's actual execution path. For each small step of the server's execution, we can construct its corresponding validator small step, based on the derivation rules in Section 2.3. By making the same internal choice and branch decisions as the server did, we can construct the assignment that unifies the validator with the server. The proof details are shown in Section A.1. $\square$

LEMMA 2.3 (RejComplete-End).

$$\begin{aligned}
&\forall (p : \mathsf{Prog})(q, a : \mathbb{Z})(v, v' : \beta), \mathsf{vstep}_p(q, a, v) = \mathsf{Some}\ v'\\
&\qquad\qquad\qquad\qquad \implies \exists s' : \sigma, v' \sim s'
\end{aligned}$$

PROOF. Since vstep_p checks the nonemptiness of the result, we know that v' must be nonempty. Consider validation state $(vs', cs') \in v'$. Since vstep'_p checks that $(\mathsf{solvable}\ cs')$, we know that:

$$\exists asgn, \quad asgn \ \mathsf{satisfy} \ cs'$$

Let:

$$s' = vs'^{\,asgn}$$

Then we have:

$$\begin{aligned}
&(vs', cs') \in v' \land asgn \ \mathsf{satisfy} \ cs' \land vs'^{\,asgn} \equiv s'\\
&i.e.\ v' \sim s'
\end{aligned}$$

$\square$

Lemma 2.4 (RejComplete-Step).

$$\begin{aligned}&\forall (p : \mathsf{Prog})(q, a : \mathbb{Z})(v, v' : \beta)(s' : \sigma),\\ &\mathsf{vstep}_p(q, a, v) = \mathsf{Some}\ v' \land v' \sim s'\\ &\quad \implies \exists (s : \sigma)(c : \mathbb{Z}), \mathsf{sstep}_p(q, c, s) = (a, s') \land v \sim s\end{aligned}$$

This bisimulation definition satisfies the hypotheses for proving soundness and completeness:

Hypotheses RejSound-Init and RejComplete-Init are immediate from the initial states' definition: The initial server state is all-zero map. The initial validator state is a singleton that maps all addresses to a variable that is constrained to have value zero.

Hypothesis RejComplete-End is based on the fact that vstep_p checks the nonemptiness of the result:

$$\forall q\ a\ v\ v', \mathsf{vstep}_p(q, a, v) = \mathsf{Some}\ v' \implies (\mathsf{vstep}'_p(q, a, v) = v' \land \exists (vs, cs) \in v')$$

and that vstep'_p guards the satisfiability of all constraints in its result:

$$\forall q\ a\ vs\ cs, (vs, cs) \in \mathsf{vstep}'_p(q, a, v) \implies \exists asgn, asgn\ \mathsf{satisfy}\ cs$$

Therefore, any element in the resulting validator state can construct a simulating server state:

$$\forall asgn\ cs\ vs\ v, (asgn\ \mathsf{satisfy}\ cs \land (vs, cs) \in v) \implies v \sim vs^{asgn}$$

Hypothesis RejComplete-Init observes that validator design increases the constraints monotonically. Therefore, "assignments that can satisfy the post-validation constraints" is a subset of "assignments that can satisfy the pre-validation constraints":

$$\forall q\, a\, vs\, cs\, vs'\, cs'\, asgn, ((vs', cs') \in \mathsf{vstep}'_p(q, a, (vs, cs)) \land asgn\ \mathsf{satisfy}\ cs') \implies asgn\ \mathsf{satisfy}\ cs$$

As a result, the corresponding pre-step server state and the internal choice can be constructed, and proven to perform the server-side step:

$$\begin{aligned}&\forall q\ a\ vs\ cs\ vs'\ cs'\ asgn,\ (vs', cs') \in \mathsf{vstep}'_p(q, a, (vs, cs))\\ &\qquad\qquad \implies \mathsf{sstep}_p(q, asgn!(\mathsf{fresh}\ vs), vs^{asgn}) = vs'^{\ asgn}\end{aligned}$$

The intuition here is that the assignment includes "all choices made by the server, past and future", which is narrowed upon more and more observations. Therefore, the assignment can instantiate all previous validator states into corresponding servers, and reconstruct the server's execution path by inferring its internal choices.

CHAPTER 3

Testing in Practice

3.1. ITree Specification Language

To write specifications for protocols' rich semantics, I employed "interaction tree" (ITree), a generic data structure for representing interactive programs, introduced by Xia et al. [16]. ITree enables specifying protocols as monadic programs that model valid implementations' possible behavior. The model program can be interpreted into a tester program, to be discussed in Section 3.3.

3.1.1. Language definition. Figure 3.1 defines the type `itree E R`. The definition is *coinductive*, so that it can represent potentially infinite sequences of interactions, as well as divergent behaviors. The parameter `E` is a type of *external interactions*—it defines the interface by which a computation interacts with its environment. `R` is the *result* of the computation: if the computation halts, it returns a value of type `R`.

There are three ways to construct an ITree. The `Ret r` constructor corresponds to the trivial computation that halts and yields the value `r`. The `Tau t` constructor corresponds to a silent step of computation, which does something internal that does not produce any visible effect and then continues as `t`. Representing silent steps explicitly with `Tau` allows us, for example, to represent diverging computation without violating Coq's guardedness condition [3]:

```
CoFixpoint spin {E R} : itree E R := Tau spin.
```

```
CoInductive itree (E : Type → Type) (R : Type) :=
| Ret (r : R)
| Vis {X : Type} (e : E X) (k : X → itree E R)
| Tau (t : itree E R).

Inductive event (E : Type → Type) : Type :=
| Event : forall X, E X → X → event E.

Definition trace E := list (event E)

Inductive is_trace E R
  : itree E R → trace E → Prop := ...
  (* straightforward definition omitted *)
```

FIGURE 3.1. Interaction trees and their traces of events.

[LYS: Todo: translate to Coq]

```
let acc(sum) =
  x := recv(); send(x+sum); acc(x+sum) in
let tee(m) =
  match m with
  | x := recv(); m'(x) ⇒
    a := recv(); print("IN" ++ a); tee(m'(a))
  | send(a); m' ⇒
    print("OUT" ++ a); send(a); tee(m')
  end in
tee(acc(0))
(* ... is equivalent to ... *)
let tee_acc(sum) =
  a := recv(); print("IN" ++ a);
  print("OUT" ++ (a+sum)); send(a+sum);
  tee_acc(a+sum) in
tee_acc(0)
```

FIGURE 3.2. Interpretation example. `acc` receives a number and returns the sum of numbers received so far. `tee` prints all the numbers sent and received. Interpreting `acc` with interpretor `tee` results in a program that's equivalent to `tee_acc`.

The final, and most interesting, way to build an ITree is with the `Vis X e k` constructor. Here, `e : E X` is a "visible" external effect (including any outputs provided by the computation to its environment) and `X` is the type of data that the environment provides in response to the event. The constructor also specifies a continuation, `k`, which produces the rest of the computation given the response from the environment. `Vis` creates branches in the interaction tree because `k` can behave differently for distinct values of type `X`.

ITree programs can be written in monadic style, where "`x ← u;; k(x)`" substitutes all occurences of "`Ret r`" in `u` with "`k(r)`". Events in an ITree might be sending and receiving messages, or other primitives actions like making internal choices. For example, a QAC server can be defined as:

```
Definition trigger {E R} (e: E R) : itree E R := Vis _ e Ret.
Variant qacE : Type → Type :=  (* event type *)
  Recv   : qacE Q              (* receive a query *)
| Send   : A → qacE unit       (* send a response *)
| Choice : qacE C.             (* make a choice   *)
CoInductive server (sstep: Q → C → S → A * S) (s: S) : itree qacE void :=
  q ← trigger Recv;; c ← trigger Choice;;
  let (a, s') := sstep q c s in trigger (Send a);; server sstep s'.
```

3.1.2. Interpreting interaction trees. Interaction tree programs can be destructed into an interaction event followed by another interaction tree program. Such structure allows us to *interpret* one program into another. Figure 3.2 shows an example of interpretation: The original `acc` program sends and receives messages, and the `tee` interpretor transforms the `acc` into another program that also prints the messages sent and received.

Such interpretation is done by pattern matching on the program's structure in Line 4. Based on what the original program wants to do next, the interpretor defines what the result program should do in Line 6 and Line 8. These programs defined in accordance to events are called *handlers*. By writing different handlers for the events, interpretors can construct new programs in various ways, as shown in following subsections. Further details about interpreting interaction trees are explained by Xia et al. [16].

3.2. Handling External Nondeterminism

3.2.1. Modelling the network. The space of network reorderings can be modelled by a *network model*, which is a conceptual program for the "network wire". The wire can be viewed as a buffer, which can absorb packets and later emit them. For example, the network model for concurrent TCP connections is defined as:

```
Variant netE : Type → Type := (* network event type *)
  Send : packet → netE unit   (* emit   a packet to   endpoint *)
| Recv : netE packet          (* absorb a packet from endpoint *)
| Or   : netE bool.           (* nondeterministic choice       *)
Definition or (x y: itree netE void) : itree netE void :=
  b ← trigger Or;; if b then x else y.            (* nondeterminstic branch *)
Fixpoint pick_one (l: list packet) : itree netE (option packet) :=
  if l is p::l' then or (Ret (Some p)) (pick_one l')
  else Ret None.
Definition oldest_in_each_conn : list packet → list packet := ...
CoFixpoint tcp (buffer: list packet) : itree netE void :=  (* TCP network model *)
  let absorb := pkt ← trigger Recv;; tcp (buffer ++ [pkt]) in
  let emit p := trigger (Send p);; tcp (remove pkt buffer)  in
  let pkts := oldest_in_each_conn buffer in
  opkt ← pick_one pkts;;     (* oldest packet in any connection may be emitted *)
  if opkt is Some pkt then emit pkt else absorb.
```

The network model introduces an `Or` event to describe different paths the system might take. `(or x y)` represents a system that is allowed to behave as either `x` or `y`.

Notice the `pick_one` function: Given an empty list, it must return `None`, which indicates the network must absorb some packet before emitting anything. Given a non-empty list, it might return some element in the list, which means the network might emit that packet; or it can return `None`, meaning the network can still absorb packets before emitting any. This constructs a network model that reflects TCP, where messages are never lost but might be indefinitely delayed.

3.2.2. Network composition. The network model is *composed* with the server model, yielding a model that exhibits the "server delayed by the network" behavior. The composition is to attach the server model as one end on the network model: Assume two message buffers between the server and the network, `bi` stores the packets emitted by the network but not yet consumed by the server, while `bo` stores the packets produced by the server but not yet absorbed by the network. The network absorbs packets in two ways, either from the servers outgoing buffer `bo` or from the clients; Conversely, when the network emits a packet, it either goes to the client or is appended to the server's incoming buffer `bi`: [3]

```
Definition toServer: packet → bool := ... (* check the packet's destination *)
CoFixpoint compose (srv net: itree netE void) (bi bo: list packet) : itree netE void :=
  match srv, net with
  | Vis vs ks, Vis vn kn ⇒
    let step_net := (* take a step in the network model *)
      match vn with
      | Recv ⇒     (* absorb from server whenever possible   *)
        if bo is pkt::bo' then compose srv (kn pkt) bi bo'
                   (* absorb from client if server is silent *)
        else pkt ← trigger Recv;; compose srv (kn pkt) bi bo
      | Send pkt ⇒ (* emit packet to its destination *)
        if toServer pkt then       compose srv (kn tt) (bi++[pkt]) bo)
        else  trigger (Send pkt);; compose srv (kn tt)  bi bo
      | Or ⇒ b ← trigger Or;; compose srv (kn b) bi bo
      end in
    match vs with
    | Recv ⇒       (* consume packet from incoming buffer *)
      if bi is pkt::bi' then compose (ks pkt) net bi' bo
      else step_net (* server is starving *)
    | Send pkt ⇒   (* produce packet to   outgoing buffer *)
      compose (ks tt) net bi (bo++[pkt])
    | Or ⇒ b ← trigger Or;; compose (ks b) net bi bo
    end
  | Ret vd, _ | _, Ret vd ⇒ match vd in void with end
  end.
```

Notice that the composed model schedules the server at a higher priority than the network model. Such design is to avoid divergence of the derived tester program, which was explained in more detail by Li, Pierce, and Zdancewic [11].

[3]Here for simplicity, the server model uses the same `netE` as the network model. In practice, the server can be specified with a more flexible type interface like `qacE` in **??**, provided its events are pairable with the network model's `Send` and `Recv`.

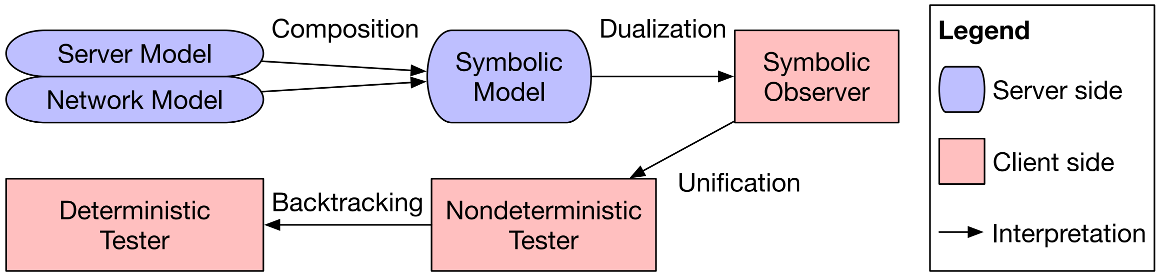


FIGURE 3.3. Deriving tester program from specification

3.3. From Specification to Tester

From the server and network models, I derived a tester client that interacts with servers over the network, and validates the observations against the protocol specification, as shown in Figure 3.3.

3.3.1. Dualizing ITree model. To *observe* the server's behavior, we have to interpret the specified server-side events into tester-side events: When the server should send a certain message, the tester expects to receive the specified message, and rejects the server upon receiving an unexpected message; when the server should receive some message, the tester generates a message and sends it to the server, as shown in Figure 3.4.

Besides sending and receiving messages, the model also has `IF` branches conditioned over symbolic expressions, like that shown in **??**. Upon nondeterministic branching, the tester needs to determine which branch was actually taken, by constructing observers for both branches. Each branch represents a possible explanation of the server's behavior. Upon further interacting with the server, some branches might fail because its conjecture cannot explain what it has observed. The tester rejects the server if all branches have failed, indicating that the server corresponds to no possible case in the model.

Dualizing the server-side model produces an observer model that performs interactions to reveal the server's behavior and check its validity. This model includes all possible observations from a valid server, and needs to `determine` which branch in the server model matches the observed behavior. The model validates its observations with unification events `unify` and `guard`. These primitive events are handled by later interpretations: The `unify` and `guard` events in each branch are instantiated into symbolic evaluation logic that decides whether this branch should fail or not; The `determine` events are instantiated into backtracking searches to find if all branches have failed, which rejects the server.

3.3.2. Symbolic Evaluation. In this interpretation phase, we handle nondeterminism at data level by handling `fresh` events in the server model, as well as `unify` and `guard` events introduced by dualization. The interpretor instantiates these events into symbolic evaluation algorithms.

As shown in Figure 3.5 (skip Line 18–28 for now—we'll explain that part later), the tester checks whether the observed/conjectured value matches the specification, by

```
let observe (server) =
  match server with
  | pkt := recv(); s'(pkt) ⇒
    p := gen_pkt(); send(p); observe (s'(p))
  | send(pkt); s' ⇒
    p := recv(); guard(pkt, p); observe (s')
  | IF (x, s1, s2) ⇒
    (* Allow validating observation with [s1],
     * provided [x] is unifiable with [true];
     * Or, unify [x] with [false],
     * and validate observation with [s2]. *)
    determine(unify(x, true ); observe (s1),
              unify(x, false); observe (s2))
  | r  := _(); s'(r) ⇒
    r1 := _(); observe (s'(r1))
  end
```

FIGURE 3.4. Dualizing server model into observer model. Upon `recv` events, the observer generates a packet and sends it to the server. For `send` events, the observer receives a packet `p1`, and fails if it does not match the specified `pkt`. When the server makes nondeterminstic `IF` branches, the observer `determines` between the branches by `unifying` the branch condition with its conjectured value, and then observing the corresponding branch.

maintaining the constraints on the symbolic variables. These constraints are initially empty when the variables are generated by `fresh` events. As the test runs into `unify` and `guard` events, it adds constraints `assert`ing that the observed value matches the specification, and checks whether the constraints are still compatible. Incompatibility among constraints indicates that the server has exhibited behavior that cannot be explained by the model, implying violation against the current branch of specification.

3.3.3. Handling Incoming Connections. In addition to generating data internally, the server might exhibit another kind of nondeterminism related to the outgoing connections it creates. For example, when a client uses an HTTP server as proxy, requesting resources from another server, the proxy server should create a new connection to the target server. However, as shown in **??**, when the tester receives a request from an accepted connection, it does not know which client's request the proxy was forwarding, due to network delays.

Outgoing connections created by the server model are identified by "model connection identifiers" (`mcid`), and the tester accepts incoming connections identified by "physical connection identifiers" (`pcid`). As shown in Line 18–28 of Figure 3.5, to determine which `mcid` in the specification does a runtime `pcid` corresponds to, the tester maintains a `mapping` between the connection identifiers. Such mapping ensures

```
(* unifyS = list variable * list constraint    *)
(* new_var : unifyS → variable * unifyS        *)
(* assert : exp T * T * unifyS → option unifyS *)
let unifier (observer, map : mcid → pcid,
         vars : unifyS) =
  match observer with
  | x := fresh(); o'(x) ⇒
    let (x1, vars') = new_var(vars) in
    unifier (o'(x1), vars', map)
  | unify(x, v); o' ⇒
    match assert(x, v, vars) with
    | Some vars' ⇒ unifier (o', vars', map)
    | None ⇒ failwith "Unexpected payload"
    end
  | guard(p0, p1); o' ⇒
    match assert(p0, p1, vars) with
    | Some vars' ⇒
      let mc = p0.source in
      let pc = p1.source in
      if mc.is_created_by_server
      then match map[mc] with
           | pc ⇒ unifier (o', vars', map)
           | unknown ⇒
             let map' = update(map, mc, pc) in
             unifier (o', vars', map')
           | others ⇒
             failwith "Unexpected connection"
           end
      else unifier (o', vars', map)
    | None ⇒ failwith "Unexpected payload"
    end
  | r  := _(); o'(r) ⇒
    r1 := _(); unifier (o'(r1), vars, map)
  end
```

FIGURE 3.5. Instantiating symbolic events. The tester maintains a `unifyState` which stores the constraints on symbolic variables. When the specification creates a `fresh` symbol, the tester creates an entry for the symbol with no initial constraints. Upon `unify` and `guard` events, the tester checks whether the `assert`ion is compatible with the current constraints. If yes, it updates the constraints and move on; otherwise, it raises an error on the current branch.

the tester to check interactions on an accepted connection against the right connection specified by the server model.

3.3.4. Backtracking. Symbolic evaluation determines whether the observations matches the tester's conjectures on each branch. So far, the derived tester is a nondeterministic program that rejects the server if and only if all possible branches have raised some error. To simulate this tester on a deterministic machine, we execute one branch until it fails. Upon failure in the current branch, the simulator switches to another possible branch, until it exhausts all possibilities and rejects the server, as shown in Line 9–13 of Figure 3.6.

When switching from one branch to another, the tester cannot revert its previous interactions with the server. Therefore, it must match the server model against all interactions it has performed, and filter out the mismatching branches, as shown in Line 15 and Line 21 of Figure 3.6.

We've now derived a tester from the server model. The specified server runs forever, and so does the tester (upon no violations observed). We accept the server if the tester hasn't rejected it after some large, pre-determined number of steps of execution.

```
(* filter : event T * T * list M → list M *)
(* [filter(e, r, l)] returns a subset in [l],
 * where the model programs' next event is [e]
 * that returns [r]. *)
let backtrack (current, others) =
  match current with
  | determine(t1, t2) ⇒
    backtrack (t1, t2::others)
  | failwith error ⇒ (* current branch failed *)
    match others with
    | [] ⇒ failwith error
    | another::ot' ⇒ backtrack (another, ot')
    end
  | send(pkt); t' ⇒
    let ot' = filter(SEND, pkt, others) in
    send(pkt); backtrack (t', ot')
  | pkt := recv(); t'(pkt) ⇒
    opkt := maybe_recv();
    match opkt with
    | Some p1 ⇒
      let ot' = filter(RECV, pkt, others) in
      backtrack (t'(p1), ot')
    | None ⇒              (* no packet arrived *)
      match others with
      | [] ⇒ backtrack (current, []) (* retry *)
      | another::ot' ⇒              (* postpone *)
        backtrack (another, ot'++[current])
      end
    end
  end in
backtrack (tester_nondet, [])
```

FIGURE 3.6. From nondeterministic model to deterministic tester program. If the model makes nondeterministic branches, the tester picks a branch to start with, and puts the other branch into a set of other possibilities. If the current branch has failed, the tester looks for other possible branches to continue checking. When the current branch sends a packet, the tester filters the set of other possibilities, and only keeps the branches that match the current send event. If the model wants to receive a packet, the tester handles both cases whether some packet has arrived or not.

CHAPTER 4

Test Harness Design

4.1. Overview

As shown in Figure 4.1, the test framework consists of a *validator* that determines whether the SUT's behavior satisfies the specification, and a *test harness* that provides test inputs for the validator.

A *validator* is a client-side model program that observes messages sent and received and decides whether these interactions are conformant to the specification. For example, a simple validator for echo server is written as:

```
let validateEcho =
  request := sendRequest();
  response := recvResponse();
  if response ≠ request
  then reject
```

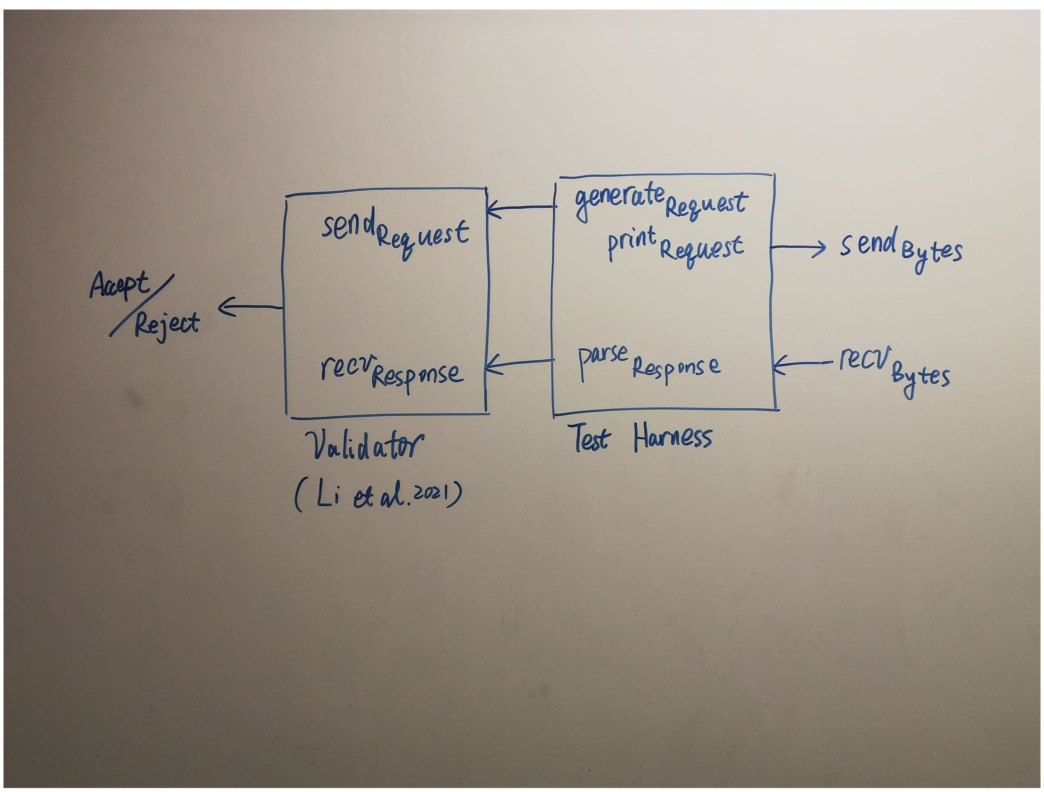


FIGURE 4.1. Test framework overview

```
    else validate
```

Notice that the `sendRequest` event does not take the request to be sent as argument, but in stead returns the request actually sent. The validator only describes the logic that checks messages sent and received, while the test harness computes what requests to send.

The *test harness* takes a validator and turns it into an executable program that performs network interactions. It handles the validator's send and receive events, and generates the requests to be sent. A simple test harness for the validator above is written as:

```
let execute(v) =
  match v with
  | x := sendRequest(); v'(x) ⇒
    request := arbitraryRequest();
    sendBytes(print(request));
    execute(v'(request))
  | x := recvRequest(); v'(x) ⇒
    responseBytes := recvBytes();
    execute(v'(parse(responseBytes)))
  | reject ⇒ reject
  end in
execute(validateEcho)
(* ... is equivalent to ... *)
let executeValidateEcho =
  request := arbitraryRequest();
  sendBytes(print(request));
  responseBytes := recvBytes();
  if parse(responseBytes) ≠ request
  then reject
  else executeValidateEcho
```

The `arbitraryRequest` generator here produces requests randomly. To generate requests that depend on previously observed messages, my framework will extend the test harness in Figure 4.1 that records a trace of messages.

4.2. Architecture

Figure 4.2 shows the test harness architecture for networked servers. This framework involves four languages: (1) An *application representation* (AR) which provides flexible abstraction for encoding the validation logic per protocol under test; (2) *Bytes* that the tester interacts with the SUT over network; between them, (3) The *intermediate representation* (IR) for encoding the trace in an application-independent way; and (4) The *symbolic representation* called "J-expressions" (Jexp) which encodes the input generated and shrunk by the test harness.

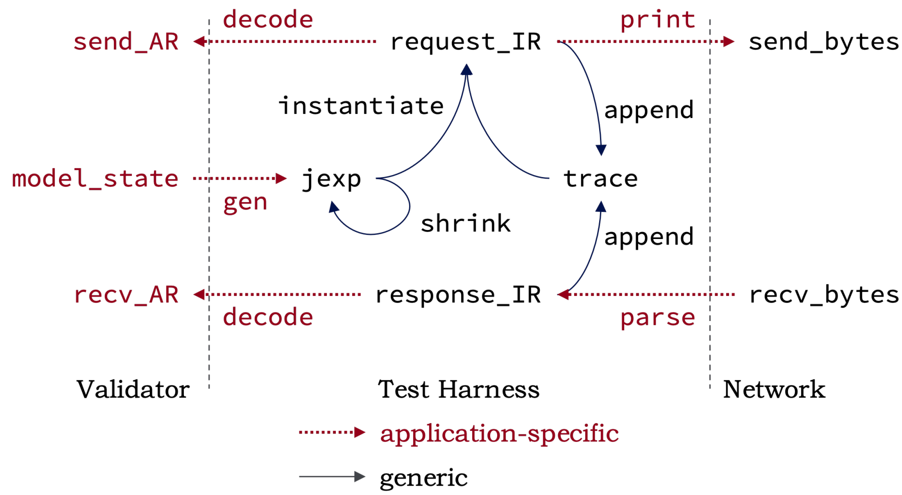


FIGURE 4.2. Test harness architecture. The test harness first generates J-expressions based on the model state provided by the validator. The J-expression is a symbolic expressions that are instantiated by the trace into requests' IR. When a violation is detected, the failing Jexp is shrunk into sub-expressions, and instantiated by the trace in new runs. The dotted arrows are application-specific algorithms, while the solid arrows are generic over all protocols.

4.3. Intermediate representation language

The purpose of introducing an IR in this framework is to enable a generic method for generating requests that refer to specific fields in the trace. For example, when testing conditional HTTP requests, the generator wants to include "a precondition that uses the ETag field of a previous response"; when testing an online store, the generator wants to provide "an order ID that the server has mentioned before".

The IR in this framework is JSON, which allows syntax trees to be arbitrarily wide and deep, and provides sufficient flexibility for network protocols in general. The J-expression is an extension of JSON that can refer to specific fields in the trace:

$$\begin{aligned}
\mathsf{JSON}^{\mathsf{T}} &\triangleq \mathsf{T} \mid \{\mathsf{object}^{\mathsf{T}}\} \mid [\mathsf{array}^{\mathsf{T}}] \mid \mathsf{string} \mid \mathbb{N} \mid \mathbb{B} \mid \mathsf{null} \\
\mathsf{object}^{\mathsf{T}} &\triangleq \varepsilon \mid \text{"}\mathsf{string}\text{"} : \mathsf{JSON}^{\mathsf{T}}, \mathsf{object}^{\mathsf{T}} \\
\mathsf{array}^{\mathsf{T}} &\triangleq \varepsilon \mid \mathsf{JSON}^{\mathsf{T}}, \mathsf{array}^{\mathsf{T}} \\
\mathsf{IR} &\triangleq \mathsf{JSON}^{\mathsf{IR}} \\
\mathsf{Jexp} &\triangleq \mathsf{JSON}^{\mathit{label}.\mathsf{Jpath}.\mathit{function}} \\
&\quad \text{where } \mathit{label} \in \mathbb{N}, \mathit{function} \in \mathsf{IR} \to \mathsf{IR} \\
\mathsf{Jpath} &\triangleq \mathsf{this} \mid \mathsf{Jpath}\#\mathit{index} \mid \mathsf{Jpath}@\mathit{field} \\
&\quad \text{where } \mathit{index} \in \mathbb{N}, \mathit{field} \in \mathsf{string}
\end{aligned}$$

The extended syntax "*label*.Jpath.*function*" is a symbolic expression that, given a runtime trace, can compute an IR of the request. For example, J-expression "3.this@"`orders`"#2.`id`" can be pronounced: "Look at the message labelled 3 in the trace, its 'order' field should be an array. Find the 2nd element in that array, and

```
Example response1 : http_response :=
  Response (Status (Version 1 1) 200 (Some "OK"))
           [Field "ETag" "tag-foo";
            Field "Content-Length" "11"]
           (Some "content-bar").

Example response2 : store_response :=
  Response__ListOrders [(233, (12, 100, 34, 500));
                        (996, (56, 400, 78, 20))].
```

```
{
  "version": {
    "major": 1,
    "minor": 1
  },
  "code": 200,
  "reason": "OK",
  "fields": {
    "ETag": "tag-foo",
    "Content-Length": "11"
  },
  "body": "content-bar"
}
```

```
{
  "code": 200,
  "orders": [
    {
      "ID": 233,
      "BuyerID": 12,
      "BuyAmount": 100,
      "SellerID": 34,
      "SellAmount": 500
    },
    {
      "ID": 996,
      "BuyerID": 56,
      "BuyAmount": 400,
      "SellerID": 78,
      "SellAmount": 20
    }
  ]
}
```

FIGURE 4.3. Application message example for HTTP and online store protocols, and their corresponding intermediate representation

use it `identically` (as-is)." Such representation enables the test harness to shrink counterexamples (encoded in Jexp) in a protocol-independent way.

To represent the correspondence between requests and responses, the trace labels each message, and the request-response pair have the same label. Figure 4.4 shows a trace of messages sent and received by the tester client.

4.4. Instantiating requests during runtime

To instantiate a Jexp into request IR, the test harness substitutes all occurences of "*label*.Jpath.*function*" with its corresponding IR computed from the trace. However,

```json
[
  {
    "label": 10,
    "message": {
      "method": "GET",
      "path": "index.html"
    }
  },
  {
    "label": 20,
    "message": {
      "method": "DELETE",
      "path": "index.html"
    }
  },
  {
    "label": 20,
    "message": {
      "code": 204,
      "reason": "No Content",
    }
  },
  {
    "label": 10,
    "message": {
      "code": 410,
      "reason": "Gone"
    }
  }
]
```

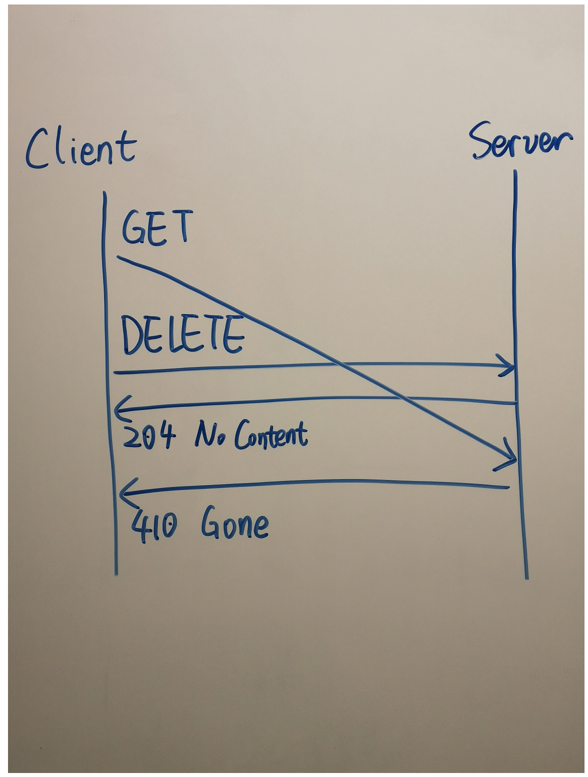


FIGURE 4.4. Example client-side trace and its corresponding IR

due to external nondeterminism, the expected message label might be delayed and not available in the trace. Also, considering inter-execution nondeterminism, arrays in observed messages might not have enough elements as expected in the Jexp. In these cases, the test harness searches for other labels in the trace and other elements in the arrays as a fallback fulfillment to construct the request.

[LYS: Todo: add instantiation algorithm.]

This idea of shrinking symbolic representations can be applied to scenarios beyond networked servers. For example, the HTTP testing experiment in **??** has also used this technique to locate the bug pattern.

CHAPTER 5

Evaluation

To evaluate whether our derived tester is effective at finding bugs, we ran the tester against mainstream HTTP servers, as well as server implementations with bugs inserted by us.

5.1. Experiment Setup

5.1.1. Systems Under Test (SUTs). We ran the tests against Apache HTTP Server [4], which is among the most popular servers on the World Wide Web. We used the latest release 2.4.46, and edited the configuration file to enable WebDAV and proxy modules. Our tester found a violation against RFC 7232 in the Apache server, so we modified its source code before creating mutants.

We've also tried testing Nginx and found another violation against RFC 7232. However, the module structure of Nginx made it difficult to fix the bug instantly. (The issue was first reported 8 years ago and still not fixed!) Therefore, no mutation testing was performed on Nginx.

5.1.2. Infrastructure. The tests were performed on a laptop computer (with Intel Core i7 CPU at 3.1 GHz, 16GB LPDDR3 memory at 2133MHz, and macOS 10.15.7). The SUT was deployed as a Docker instance, using the same host machine as the tester runs on. They communicate with POSIX system calls, in the same way as over Internet except using address `localhost`. The round-trip time (RTT) of local loopback is 0.08 ± 0.04 microsecond (at 90% confidence).

5.2. Results

5.2.1. Finding Bugs in Real-World Servers and Mutants. Our tester rejected the unmodified Apache HTTP Server, which uses strong comparison for PUT requests conditioned over `If-None-Match`, while RFC 7232 specified that `If-None-Match` preconditions must be evaluated with weak comparison[BCP: What are strong and weak comparison? [LYS: ETag jargons.]]. We reported this bug to the developers, and figured out that Apache was conforming with an obsoleted HTTP/1.1 standard [7]. The latest standard has changed the semantics of `If-None-Match` preconditions, but Apache didn't update the logic correspondingly.

We created 20 mutants by manually modifying the Apache source code. The tester rejected all the 20 mutants, located in various modules of the Apache server: `core`, `http`, `dav`, and `proxy`. They appear both in control flow (*e.g.*, early return, skipped condition) and in data values (*e.g.*, wrong arguments, flip bit, buffer off by one byte).

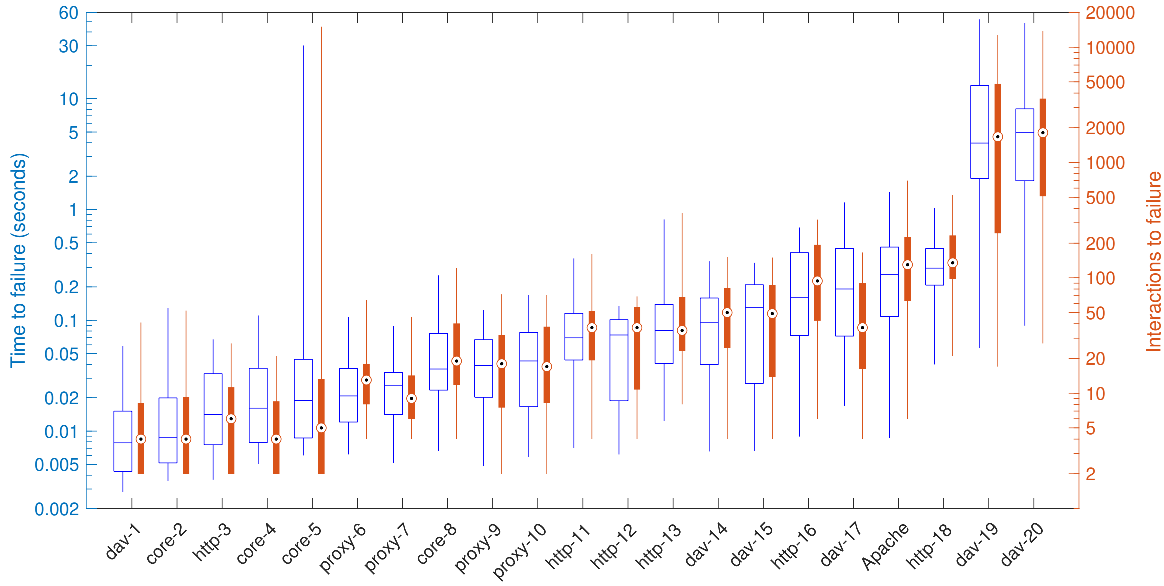


FIGURE 5.1. Cost of detecting bug in each server/mutant. The left box with median line is the tester's execution time before rejecting the server, which includes interacting with the server and checking its responses. The right bar with median circle is the number of HTTP/1.1 messages sent and received by the tester before finding the bug. Results beyond 25%–75% are covered by whiskers.

We didn't use automatic mutant generators because (i) Existing tools could not mutate all modules we're interested in; and (ii) The automatically generated mutants could not cause semantic violations against our protocol specification.

When testing Nginx, we found that the server did not check the preconditions of PUT requests. We then browsed the Nginx bug tracker and found a similar ticket opened by Haverbeke [8]. These results show that our tester is capable of finding bugs in server implementations, including those we're unaware of.

5.2.2. Performance. As shown in Figure 5.1, the tester rejected all buggy implementations within 1 minute. In most cases, the tester could find the bug within 1 second.

Some bugs took longer time to find, and they usually required more interactions to reveal. This may be caused by (1) The counter-example has a certain pattern that our generator didn't optimize for, or (2) The tester did produce a counter-example, but failed to reject the wrong behavior. We determine the real cause by analysing the bugs and their counterexamples:

- Mutants 19 and 20 are related to the WebDAV module, which handles PUT requests that modify the target's contents. The buggy servers wrote to a different target from that requested, but responds a successful status to the client. The tester cannot tell that the server is faulty until it queries the target's latest contents and observes an unexpected value. To reject the server

[LYS: Duplicates with Figure 1.3 and Figure 1.4.]

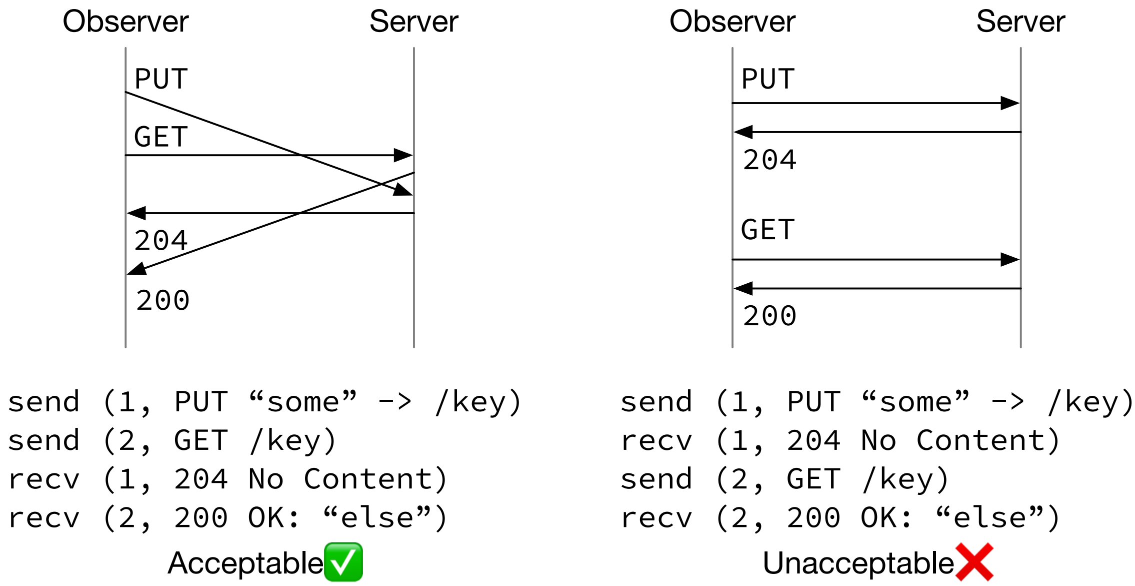


FIGURE 5.2. The trace on the left does not convince the tester that the server is buggy, because there exists a certain network delay that explains why the PUT request was not reflected in the 200 response. When the trace is ordered as shown on the right, the tester cannot imagine any network reordering that causes such observation, thus must reject the server.

with full confidence, these observations must be made in a certain order, as shown in Figure 5.2.

- Mutant 18 is similar to the bug in vanilla Apache: the server should have responded with 304 Not Modified, but sent back 200 OK instead. To reveal such violation, a minimal counterexample consists of 4 messages: (1) GET request, (2) 200 OK response with some ETag `x`, (3) GET request conditioned over `If-None-Match: x`, and (4) 200 OK response, indicating that the ETag `x` did not match itself. Notice that (2) must be observed before (3), otherwise the tester will not reject the server, with a similar reason as Figure 5.2.
- Mutant 5 causes the server to skip some code in the core module, and send nonscence messages when it should respond with 404 Not Found. The counterexample can be as small as one GET request on a non-existential target, followed by a non-404, non-200 response. However, our tester generates request targets within a small range, so the requests' targets are likely to be created by the tester's previous PUT requests. Narrowing the range of test case generation might improve the performance in aforementioned Mutants 18–20, but Mutant 5 shows that it could also degrade the performance of finding some bugs.
- The mutants in proxy module caused the server to forward wrong requests or responses. When the origin server part of the tester accepts a connection

from the proxy, it does not know for which client the proxy is forwarding requests. Therefore, the tester needs to check the requests sent by all clients, and make sure none of them matches the incoming proxy request, before rejecting the proxy.

These examples show that the time-consuming issue of some mutants are likely caused by limitations in the test case generators. Cases like Mutant 5 can be optimized by tuning the request generator based on the tester model's runtime state, but for Mutants 18–20, the requests should be sent at specific time periods so that the resulting trace is unacceptable per specification. How to produce a specific order of messages is to be explored in future work.

CHAPTER 6

Related Work

6.1. Specifying and Testing Protocols

Modelling languages for specifying protocols can be partitioned into three styles, according to Anand et al. [1]: (1) *Process-oriented* notations that describe the SUT's behavior in a procedural style, using various domain-specific languages like our interaction trees; (2) *State-oriented* notations that specify what behavior the SUT should exhibit in a given state, which includes variants of labelled transition systems (LTS); and (3) *Scenario-oriented* notations that describe the expected behavior from an outside observer's point of view (*i.e.,* "god's-eye view").

The area of model-based testing is well-studied, diverse, and difficult to navigate [1]. Here we focus on techniques that have been practiced in testing real-world programs, which includes notations (1) and (2). Notation (3) is infeasible for protocols with nontrivial nondeterminism, because the specification needs to define observer-side knowledge of the SUT's all possible internal states, making it complex to implement and hard to reason about, as shown in Figure 1.1.

Language of Temporal Ordering Specification (LOTOS) [**Bolognesi1987**] is the ISO standard for specifying OSI protocols. It defines distributed concurrent systems as *processes* that interact via *channels*, and represents internal nondeterminism as choices among processes.

Using a formal language strongly insired by LOTOS, Tretmans and Laar [15] implemented a test generation tool for symbolic transition systems called TorXakis, which has been used for testing Dropbox [15].

TorXakis provides limited support for internal nondeterminism. Unlike our testing framework that incorporates symbolic evalutation, TorXakis enumerates all possible values of internally generated data, until finding a corresponding case that matches the tester's observation. This requires the server model to generate data within a reasonably small range, and thus cannot handle generic choices like HTTP entity tags, which can be arbitrary strings.

Bishop et al. [2] have developed rigorous specifications for transport-layer protocols TCP, UDP, and the Sockets API, and validated the specifications against mainstream implementations in FreeBSD, Linux, and WinXP. Their specification represents internal nondeterminism as symbolic states of the model, which is then evaluated using a special-purpose symbolic model checker. They focused on developing a post-hoc specification that matches existing systems, and wrote a separate tool for generating test cases.

6.2. Reasoning about Network Delays

For property-based testing against distributed applications like Dropbox, Hughes et al. [9] have introduced “conjectured events” to represent uploading and downloading events that nodes may perform at any time invisibly.

Sun, Xu, and Elbaum [13] symbolised the time elapsed to transmit packets from one end to another, and developed a symbolic-execution-based tester that found transmission-related bugs in Linux TFTP upon certain network delays. Their tester used a fixed trace of packets to interact with the server, and the generated test cases were the packets’ delay time.

CHAPTER 7

Discussions

CHAPTER 8

Conclusion

Bibliography

[1] Saswat Anand et al. "An orchestrated survey of methodologies for automated software test case generation". In: *Journal of Systems and Software* 86.8 (2013), pp. 1978–2001. ISSN: 0164-1212. DOI: https://doi.org/10.1016/j.jss.2013.02.061. URL: http://www.sciencedirect.com/science/article/pii/S0164121213000563.

[2] Steve Bishop et al. "Engineering with Logic: Rigorous Test-Oracle Specification and Validation for TCP/IP and the Sockets API". In: *J. ACM* 66.1 (Dec. 2018). ISSN: 0004-5411. DOI: 10.1145/3243650. URL: https://doi.org/10.1145/3243650.

[3] Adam Chlipala. "Infinite Data and Proofs". In: *Certified Programming with Dependent Types*. MIT Press, 2017. URL: http://adam.chlipala.net/cpdt/html/Cpdt.Coinductive.html.

[4] Roy T. Fielding and Gail Kaiser. "The Apache HTTP Server Project". In: *IEEE Internet Computing* 1.4 (July 1997), pp. 88–90. ISSN: 1941-0131. DOI: 10.1109/4236.612229.

[5] Roy T. Fielding and Julian Reschke. *Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests*. RFC 7232. June 2014. DOI: 10.17487/RFC7232. URL: https://rfc-editor.org/rfc/rfc7232.txt.

[6] Roy T. Fielding and Julian Reschke. *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*. RFC 7231. June 2014. DOI: 10.17487/RFC7231. URL: https://rfc-editor.org/rfc/rfc7231.txt.

[7] Roy T. Fielding et al. *Hypertext Transfer Protocol – HTTP/1.1*. RFC 2616. June 1999. DOI: 10.17487/RFC2616. URL: https://rfc-editor.org/rfc/rfc2616.txt.

[8] Marijn Haverbeke. *DAV module does not respect if-unmodified-since*. Nov. 2012. URL: https://trac.nginx.org/nginx/ticket/242.

[9] John Hughes et al. "Mysteries of DropBox: Property-Based Testing of a Distributed Synchronization Service". In: *2016 IEEE International Conference on Software Testing, Verification and Validation, ICST 2016, Chicago, IL, USA, April 11-15, 2016*. 2016, pp. 135–145. DOI: 10.1109/ICST.2016.37. URL: https://doi.org/10.1109/ICST.2016.37.

[10] Nicolas Koh et al. "From C to Interaction Trees: Specifying, Verifying, and Testing a Networked Server". In: *Proceedings of the 8th ACM SIGPLAN International Conference on Certified Programs and Proofs*. CPP 2019. Cascais, Portugal: ACM, 2019, pp. 234–248. ISBN: 978-1-4503-6222-1. DOI: 10.1145/3293880.3294106. URL: http://doi.acm.org/10.1145/3293880.3294106.

[11] Yishuai Li, Benjamin C. Pierce, and Steve Zdancewic. "Model-Based Testing of Networked Applications". In: *ACM SIGSOFT International Symposium on Software Testing and Analysis*. 2021.

[12] Benjamin C. Pierce. *Types and Programming Languages*. MIT Press, 2002.

[13] Wei Sun, Lisong Xu, and Sebastian Elbaum. "Improving the Cost-Effectiveness of Symbolic Testing Techniques for Transport Protocol Implementations under Packet Dynamics". In: *Proceedings of the 26th ACM SIGSOFT International Symposium on Software Testing and Analysis*. ISSTA 2017. Santa Barbara, CA, USA: Association for Computing Machinery, 2017, pp. 79–89. ISBN: 9781450350761. DOI: `10.1145/3092703.3092706`. URL: `https://doi.org/10.1145/3092703.3092706`.

[14] Jan Tretmans. "Conformance testing with labelled transition systems: Implementation relations and test generation". In: *Computer Networks and ISDN Systems* 29.1 (1996). Protocol Testing, pp. 49–79. ISSN: 0169-7552. DOI: `https://doi.org/10.1016/S0169-7552(96)00017-7`. URL: `http://www.sciencedirect.com/science/article/pii/S0169755296000177`.

[15] Jan Tretmans and Piërre van de Laar. "Model-Based Testing with TorXakis: The Mysteries of Dropbox Revisited". In: *Strahonja, V.(ed.), CECIIS: 30th Central European Conference on Information and Intelligent Systems, October 2-4, 2019, Varazdin, Croatia. Proceedings*. Zagreb: Faculty of Organization and Informatics, University of Zagreb. 2019, pp. 247–258.

[16] Li-yao Xia et al. "Interaction Trees: Representing Recursive and Impure Programs in Coq". In: *Proc. ACM Program. Lang.* 4.POPL (Dec. 2019), 51:1–51:32. ISSN: 2475-1421. DOI: `10.1145/3371119`. URL: `http://doi.acm.org/10.1145/3371119`.

[17] Hengchu Zhang et al. "Verifying an HTTP Key-Value Server with Interaction Trees and VST". In: *12th International Conference on Interactive Theorem Proving (ITP 2021)*. Ed. by Liron Cohen and Cezary Kaliszyk. Vol. 193. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021, 32:1–32:19. ISBN: 978-3-95977-188-7. DOI: `10.4230/LIPIcs.ITP.2021.32`. URL: `https://drops.dagstuhl.de/opus/volltexte/2021/13927`.

APPENDIX A

Mathematical Proof of Derived Validators' Correctness

A.1. Forward preservation lemma for rejection soundness

Hypothesis RejSound-Step

$$\begin{aligned}
&\forall (p : \mathsf{Prog})(q, c, a : \mathbb{Z})(s_0, s' : \sigma)(v : \beta),\\
&\mathsf{sstep}_p(q, c, s_0) = (a, s') \wedge v \sim s_0\\
&\ \implies \exists v' : \beta, \mathsf{vstep}_p(q, a, v) = \mathsf{Some}\ v' \wedge v' \sim s'
\end{aligned}$$

The invariant $v \sim s_0$ tells us that v contains a validation state that reflects the server state s_0:

$$\exists ((vs_0, cs_0) \in v)(asgn_0 : \mathsf{var} \to \mathbb{Z}), asgn_0\ \mathsf{satisfy}\ cs_0 \wedge {vs_0}^{asgn_0} \equiv s_0$$

The corresponding validator step is constructed by analyzing the server step, and proving small-step bisimulation for each derivation rule in Section 2.3.

Write. The server writes some expression $(e : \mathsf{SExp})$ to an address $!dst$. According to Rule 1, the validator creates a fresh variable x_e for address $!dst$, and constraints that $(\#x_e \equiv e^{vs})$.[4]

We need to show that:

$$\begin{aligned}
&\forall vs, cs, s, asgn,\\
&asgn\ \mathsf{satisfy}\ cs \wedge vs^{asgn} \equiv s\\
&\ \implies \forall d, e,\ \begin{array}{lll} \mathsf{let}\ s' & = s[d \mapsto e^s] & \mathsf{in}\\ \mathsf{let}\ (vs', cs') & = \mathsf{write}(d, e, (vs, cs)) & \mathsf{in}\\ \exists asgn', & asgn'\ \mathsf{satisfy}\ cs' \wedge vs'^{\ asgn'} \equiv s' & \end{array}
\end{aligned}$$

Proof. Based on the definition of write, we need to show that:

$$\begin{aligned}
&\mathsf{let}\ x_e = \mathsf{fresh}\ (vs, cs)\ \mathsf{in}\\
&\mathsf{let}\ vs' = vs[d \mapsto x_e]\ \mathsf{in}\\
&\mathsf{let}\ cs' = cs \cup \{x_e \equiv e^{vs}\}\ \mathsf{in}\\
&\exists asgn', \quad asgn'\ \mathsf{satisfy}\ cs' \wedge vs'^{\ asgn'} \equiv s'
\end{aligned}$$

Let:

$$asgn' = asgn[x_e \mapsto e^s]$$

In order to prove $(asgn'\ \mathsf{satisfy}\ cs')$, we introduce some generic lemmas to show that $(asgn'\ \mathsf{satisfy}\ cs)$ and $({x_e}^{asgn'} \equiv (e^{vs})^{asgn'})$:

[4] If unspecified, (vs, cs) represents the pre-small-step validator state, and s represents the pre-small-step server state.

Lemma A.1 (Fresh variable preserves satisfaction).

$$\begin{array}{l}\forall(cs : \textsf{set constraint})(asgn : \textsf{var} \to \mathbb{Z}),\\ asgn\ \textsf{satisfy}\ cs\\ \quad\Longrightarrow\ \begin{array}{lll}\multicolumn{3}{l}{\forall(z:\mathbb{Z}), vs,}\\ \textsf{let}\ x & = \textsf{fresh}\ (vs, cs) & \textsf{in}\\ \textsf{let}\ asgn' & = asgn[x \mapsto z] & \textsf{in}\\ \multicolumn{3}{l}{asgn'\ \textsf{satisfy}\ cs}\end{array}\end{array}$$

Proof. Since x is fresh in cs, we have:

$$\forall(e_1\ cmp\ e_2) \in cs, \quad {e_1}^{asgn'} = {e_1}^{asgn} \wedge {e_2}^{asgn'} = {e_2}^{asgn}$$

Thus:

$$\begin{array}{l}\forall(e_1\ cmp\ e_2) \in cs, \quad {e_1}^{asgn'}\ cmp\ {e_2}^{asgn'}\\ i.e.\ asgn'\ \textsf{satisfy}\ cs\end{array}$$

□

Lemma A.2 (Fresh variable preserves evaluation).

$$\begin{array}{lll}\multicolumn{3}{l}{\forall(vs : \mathbb{N} \to \textsf{var})(asgn : \textsf{var} \to \mathbb{Z})(z : \mathbb{Z}), cs,}\\ \textsf{let}\ x & = \textsf{fresh}\ (vs, cs) & \textsf{in}\\ \textsf{let}\ asgn' & = asgn[x \mapsto z] & \textsf{in}\\ \multicolumn{3}{l}{\forall(e : \textsf{SExp}), (e^{vs})^{asgn'} = (e^{vs})^{asgn}}\end{array}$$

Proof. Assume to the contrary that:

$$(e^{vs})^{asgn'} \neq (e^{vs})^{asgn}$$

Since $asgn'$ is the same as $asgn$ except for variable $\#x$, we know that $(e^{vs} : \textsf{VExp})$ must involve $\#x$. Therefore, e must involve some address $!k$ such that $(vs!k = x)$. This contradicts the fact that x is fresh in vs. □

Lemma A.3 (Symbolization preserves evaluation).

$$\begin{array}{l}\forall(vs : \mathbb{N} \to \textsf{var})(asgn : \textsf{var} \to \mathbb{Z})(s : \mathbb{N} \to \mathbb{Z}),\\ vs^{asgn} \equiv s \implies \forall(e : \textsf{SExp}), \quad (e^{vs})^{asgn} \equiv e^{s}\end{array}$$

Proof. Based on the definition of symbolization and evaluation:

- e^{vs} substitutes all occurences of $!k$ in e with $\#(vs!k)$;
- $(e^{vs})^{asgn}$ substitutes all occurences of $\#(vs!k)$ to $asgn!(vs!k)$;
- e^{s} substitutes all occurences of $!k$ in e with $(s!k)$.

From the hypothesis that $(vs^{asgn} \equiv s)$, we have:

$$\forall(k : \mathbb{N}), \quad asgn!(vs!k) \equiv (s!k)$$

Therefore, we know that all occurences of $!k$ were mapped to the same value between the two evaluation paths. □

Based on Lemma A.2, we have:

$$(e^{vs})^{asgn'} = (e^{vs})^{asgn}$$

Also, since x_e is free in vs, and $asgn'$ is the same as $asgn$ except for x_e, we have:

$$\forall k, asgn'!(vs'!k) = \begin{cases} asgn'!x_e = e^s = (s'!k) & k \text{ is } d \\ asgn!(vs!k) = (s!k) = (s'!k) & \text{otherwise} \end{cases}$$

Therefore:

$$vs'^{\ asgn'} \equiv s'$$

□

Havoc. When the server writes some internal choice c to address d, according to Rule 3, the validator creates a fresh variable for address $!d$.

We need to show that:

$$\begin{aligned}
&\forall vs, cs, s, asgn, \\
&asgn \text{ satisfy } cs \land vs^{asgn'} \equiv s \\
&\implies \forall d, c, \ \ \text{let } s' \ = s[d \mapsto c] \quad \text{in} \\
&\qquad\qquad\qquad \text{let } x_c \ = \text{fresh } (vs, cs) \quad \text{in} \\
&\qquad\qquad\qquad \exists asgn', \quad asgn' \text{ satisfy } cs \land vs^{asgn'} \equiv s'
\end{aligned}$$

PROOF. Let:

$$asgn' = asgn[x_c \mapsto c]$$

Since x_c is free in cs, we have □

APPENDIX B

Unstructured contents

B.1. Challenges: Testing Internal and Network Nondeterminism

To illustrate the challenges in testing networked applications, we discuss two features of HTTP/1.1—conditional requests [5] and message forwarding [6]—showcasing internal nondeterminism and network nondeterminism, respectively.

Internal Nondeterminsm. HTTP/1.1 requests can be conditional: if the client has a local copy of some resource and the copy on the server has not changed, then the server needn't resend the resource. To achieve this, an HTTP/1.1 server may generate a short string, called an "entity tag" (ETag), identifying the content of some resource, and send it to the client:

```
/* Client: */
GET /target HTTP/1.1

/* Server: */
HTTP/1.1 200 OK
ETag: "tag-foo"
... content of /target ...
```

The next time the client requests the same resource, it can include the ETag in the GET request, informing the server not to send the content if its ETag still matches:

```
/* Client: */
GET /target HTTP/1.1
If-None-Match: "tag-foo"

/* Server: */
HTTP/1.1 304 Not Modified
```

If the tag does not match, the server responds with code 200 and the updated content as usual. Similarly, if a client wants to modify the server's resource atomically by compare-and-swap, it can include the ETag in the PUT request as `If-Match` precondition, which instructs the server to only update the content if its current ETag matches.

[LY: This is a good example, but how general is the problem, since one might question the popularity of ETags? On the other hand, if your testing framework targets application layer protocols rather than just HTTP, maybe there are more similar examples? For example, file/mail servers or databases might also require some synchronization mechanisms similar to compare-and-swap? And there might be other examples that's not compare-and-swap?][BCP: Agree that this is important to discuss.] [LYS: Mentioned at the end of this section.]

Thus, whether a server's response should be judged *valid* or not depends on the ETag it generated when creating the resource. If the tester doesn't know the server's internal state (*e.g.*, before receiving any 200 response including the ETag), and cannot enumerate all of them (as ETags can be arbitrary strings), then it needs to maintain a space of all possible values, narrowing the space upon further interactions with the server.

It is possible, but tricky, to write an ad hoc tester for HTTP/1.1 by manually "dualizing" the behaviors described by the informal specification documents (RFCs). The protocol document describes *how* a valid server should handle requests, while the tester needs to determine *what* responses received from the server are valid. For example, "If the server has revealed some resource's ETag as `"foo"`, then it must not reject requests targetting this resource conditioned over `If-Match: "foo"`, until the resource has been modified"; and "Had the server previously rejected an `If-Match` request, it must reject the same request until its target has been modified." Figure 1.1 shows a hand-written tester for checking this bit of ETag functionality; we hope the reader will agree that this testing logic is not straightforward to derive from the informal "server's eye" specifications.

Network Nondeterminism. When testing an HTTP/1.1 server over the network, although TCP preserves message ordering within each connection, it does not guarantee any order between different connections. Consider a proxy model in **??**: it specifies how a server should forward messages. [BCP: I don't understand why we are talking about proxies here: a simple "server + several clients" situation is enough to create network nondeterminism. (I would expect that proxying might create *additional* possibilities for nondeterminism, of course.) [LYS: We need to talk about proxy somewhere, and I didn't find a good place elsewhere.]] [BCP: Moreover, the more I look at figures 2–5 the more confusing I find them. Only figure 5 mentions connections, but — for example, in figure 3, if we assume just a single connection between the observer and the proxy and a single connection from the proxy back to the observer, then the reordering shown in the figure is NOT valid. [LYS: Updated figure. No proxy uses the same connection for multiple requests. The proxy never knows if there's a next request that can use the same connection.]] When the forwarded messages are scrambled as in **??**, the tester should be *loose* enough to accept the server, because a valid server may exhibit such reordering due to network delays. The tester should also be *strict* enough to reject a server that behaves as **??**, because no network delay can let the proxy forward a message before the observer sends it.

The kinds of nondeterminism exemplified here can be found in many other scenarios: (i) Servers may use some (unknown) algorithm to generate internal state for nonces, sequence numbers, caching metadata, *etc*, featuring internal nondeterminism. (ii) When the server runs multiple threads concurrently (*e.g.* to serve multiple clients), the operating system might schedule these threads nondeterministically. When testing the server over the network, such "nondeterminism outside the code of the server program but still within the machine on which the server is executing" is indistinguishable from nondeterminism caused by network delays, and thus can be covered by the concept "network nondeterminism."

B.2. Specification Language

A specification in our framework consists of two parts: a server model specifying server-side behavior,[BCP: there was a discussion of this somewhere else: isn't our "application model" here just specifying HTTP and WebDAV? And so isn't it also generic? [LYS: Not generic over all L7 protocols.]] and a network model describing network delays. By composing these two models, we get a tester-side specification of valid observations over the network.

Formally, our specifications are written as *interaction trees*, a generic data structure for representing interactive programs in Coq. This language allows us to write rigorous mathematical specifications, and transform the specification into tester conveniently. In this paper, we present models as pseudocode for readability. Technical details about interaction trees can be found in [16].

Subsection B.2.1 shows how to handle network nondeterminism. Subsection B.2.2 then expands the model to address internal nondeterminism.

B.2.1. Server and Network Models. The *server model* specifies how the server code interacts with the network interface. For example, an extremely simplistic model of an HTTP proxy[BCP: again, it feels like proxies are coming out of nowhere [LYS: I'll try to make proxy more like a part of HTTP than an extension.]] (shown in **??**) is written as:

```
let proxy() =
    msg := recv();
    send(msg);
    proxy()
```

An implementation is said to be *valid* if it is indistinguishable from the model when viewed from across the network. Consider the following proxy implementation that reorders messages: [BCP: Why are we suddenly switching to C syntax?? [LYS: To distinguish implementation from specification.]]

```
void proxy_implementation() {
  while (true) {
    recv(&msg1); recv(&msg2);
    send(msg2);  send(msg1);
  }
}
```

This reordered implementation is valid, because the model itself may exhibit the same behavior when observed over the network, as shown in **??**. This "implementation's behavior is explainable by the model, considering network delays" relation is called *network refinement* by Koh et al. [10].

To specify network refinement in a testable way, we introduce the *network model*, a conceptual implementation of the transport-layer environment between the server and the tester. It models the network as a nondeterministic machine that absorbs packets and, after some time, emits them again. **??** shows the network model for concurrent TCP connections: The network either receives a packet from some node, or sends the first packet en route of some connection. This model preserves the message order within each connection, but it exhibits all possible reorderings among different connections.

The network model does not distinguish between server and tester. When one end `send`s some message, the network `recv`s the message and `send`s it after some cycles of delay; it is then observed by the other end via some `recv` call.

In Subsection B.3.3, we compose the server and network models to yield an observer-side specification for testing purposes.

B.2.2. Symbolic Representation of Nondeterministic Data. To incorporate symbolic evaluation in our testing framework, our specification needs to represent internally generated data as symbols. Consider HTTP PUT requests with `If-Match` preconditions: Upon success, the server generates a new ETag for the updated content, and the tester does not know the ETag's value immediately. Our symbolic model in **??** represents the server's generated ETags as fresh variables. The server's future behavior might depend on whether a request's ETag matches the generated (symbolic) ETag. Such matching produces a symbolic boolean expression, which cannot be evaluated into a boolean value without enough constraints on its variables. Our model introduces `IF` operator to condition branches over a symbolic boolean expression. Which branch the server actually took is decided by the derived tester in **??**.

In Subsection B.3.2, we implement the symbolic evaluation process that checks servers' observable behavior against this symbolic model.

B.3. Derivation: from Server Specification to Testing Program

From the specified the application and network models, our framework automatically derives a tester program that interacts with the server and determines its validity. The derivation framework is shown in outline in Figure 3.3. Each box is an interaction tree program, and the arrows are "interpretors" that transform one interaction tree into another. Subsection B.3.1 explains the concept of interpretation, and the rest of this section describes how to interpret the specification into a tester program.

B.3.1. Interpreting Interaction Trees.

B.3.2. From Server Specification to Tester Program. For simplicity, we first explain how to handle servers' internal nondeterminism with symbolic evaluation. This subsection covers a subgraph of Figure 3.3, starting with dualizing the symbolic model. Here we use the server model itself as the symbolic model, assuming no reorderings by network delays. We will compose the server model with the network model in Subsection B.3.3, addressing network nondeterminism.

Test Case Generation. Counterexamples are sparsely distributed, especially when the bugs are related to server's internally generated data like ETags, which can hardly be matched by a random test case generator. After observing the `ETag` field of some response, the generator can send more requests with the same ETag value, rather than choosing an unknown value arbitrarily.

As shown in Figure B.1, our derivation framework allows passing the programs' internal state as the events' parameters, so the test case generator can utilize the

```
let http_server (http_st) =
  request := recv_HTTP(http_st);
  (response, st') := process(request, http_st);
  http_server (st')
...
let observer (server) =
  match server with
  | req := recv_HTTP(http_st); s'(req) ⇒
    r1  := gen_Observer(http_st);
    send(r1); observe (s'(r1))
...
let unifier (observer, vars, conn) =
  match observer with
  | req := gen_Observer(http_st); o'(req) ⇒
    r1  := gen_Unifier(http_st, vars, conn);
    unifier (o'(r1), vars, conn)
...
```

FIGURE B.1. Embedding programs' internal state into the events. By expanding the events' parameters, we enrich the test case generator's knowledge along the interpretations.

states in all intermediate interpretation phases, and apply heuristics to emphasise certain bug patterns.

Notice that the state-passing strategy only allows tuning *what* messages to send. To reveal bugs more efficiently in an interactive scenario, we need to tune *when* the interactions are made, which is further discussed in Section 5.2. Generating test cases in certain orders is to be explored in future work.

```
1  let compose (net, bi, bo, srv) =
2    let step_net =
3      match net with
4      | send(pkt); n' ⇒
5        if pkt.to_server
6        then compose (n', bi++[pkt], bo, srv)
7        else send(pkt);    (* to client *)
8             compose (n', bi, bo, srv)
9        end
10     | pkt := recv(); n'(pkt) ⇒
11       match bo with
12       | p0::b' ⇒ compose (n'(p0), bi, b', srv)
13       | []     ⇒ p1 := recv();
14                  compose (n'(p1), bi, bo, srv)
15       end
16     | r  := _(); n'(r) ⇒
17       r1 := _(); compose (n'(r1), bi, bo, srv)
18     end in
19   match srv with
20   | send(pkt); s' ⇒
21     compose (net, bi, bo++[pkt], s')
22   | pkt := recv(); s'(pkt) ⇒
23     match bi with
24     | p0::b' ⇒ compose (net, b', bo, s'(p0))
25     | []     ⇒ step_net
26     end
27   | r  := _(); s'(r) ⇒
28     r1 := _(); compose (net, bi, bo, s'(r1))
29   end in
30 compose (tcp, [], [], http)
31
```

FIGURE B.2. Composing `http` server model with `tcp` network model by interpreting their events and passing messages from one model to another. The composing function takes four parameters: server and network models as `srv` and `net`, and the message buffers between them. When `srv` wants to `send` a packet in Line 21, the packet is appended to the outgoing buffer `bo` until absorbed by `net` in Line 12, and eventually emitted to the client in Line 7. Conversely, packets sent by clients are absorbed by `net` in Line 13, emitted to the application's incoming buffer `bi` in Line 6, until `srv` consumes it in Line 24.

B.3.3. Network Composition. We have shown how to derive a tester from the server model itself. The server model describes how a reference server processes messages. For protocols like HTTP/1.1 where servers are expected to handle one request at a time, a reasonable server model should be "linear" that serves one client after another. As a result, the derived tester only simulates a single client, and does not attempt to observe the server's behavior via multiple simultaneous connections.

The network model describes how messages sent by one end of the network are eventually received by the other end. When interacting with multiple clients, a valid server's observable behavior should be explainable by "server delayed by the network", as discussed in Subsection B.2.1. To model this set of observations, we compose the server and network models by attaching the server model as one end on the network model.

As shown in Figure B.2, we `compose` the events of server and network models. Messages sent by the server are received by the network and sent to clients after some delay, and vice versa. Such composition produces a model that branches nondeterministically, and includes all possible interactions of a valid HTTP server that appear on the client side.

The composed model does not introduce new events that were not included in the server model: The network model in **??** does perform nondeterministc `or` branches, but `or(x,y)` is a syntactic sugar for `b := fresh(); IF(b,x,y)`. Therefore, using the same derivation algorithm from the server model to single-connection tester program, we can derive the composed server+network model into a multi-connection tester.

Notice that the server and network events are scheduled at different priorities: The composition algorithm steps into the network model lazily, not until the server is blocked in Line 25. When the network wants to `recv` some packet in Line 10, it prioritizes packets sent by the server, and only receives from the clients if the server's outgoing buffer has been exhausted. Such design is to enforce the tester to terminate upon observing invalid behavior: When the server's behavior violates the model, the tester should check all possible branches and determine that none of them can lead to such behavior. If the model steps further into the network, it would include infinitely many `absorb` branches in **??**, so the derived tester will never exhaust "all" branches and reject the server. Scheduling network events only when the server model is blocked produces sufficient nondeterminism to accept valid servers.