Синтез тестов с гарантированной полнотой для входо-выходных полуавтоматов

И.Б. Бурдонов, Н.В. Евтушенко, А.С. Косачев

Институт системного программирования им. В.П. Иванникова *Российской академии наук*

Аннотация. В статье исследуется проблема построения конечных тестов с гарантированной полнотой для входо-выходных полуавтоматов на основе модели «черного ящика», когда известна только верхняя оценка на число состояний тестируемого полуавтомата, но неизвестна его структура. В данной работе мы предлагаем способ построения конечного автомата, соответствующего полуавтомату-спецификации, и показываем, что конечные тесты, построенные по такому автомату без явного перечисления полуавтоматов-реализаций, являются полными относительно различных моделей неисправности.

Ключевые слова: входо-выходной полуавтомат, конечный автомат, модель неисправности, полный тест

Deriving Tests with Guaranteed Fault Coverage for Input / Output Automata

I.B. Burdonov, N.V. Yevtushenko, A.S. Kossachev

Institute for System Programming of the Russian Academy of Sciences

Abstract. The paper is devoted to deriving finite test suites with guaranteed fault coverage for Input / Output automata using the ‘black-box’ model when only the upper bound on the number of states of an implementation automaton under test is known but there is no knowledge about its structure. We propose a methods for deriving a finite State Machine (FSM) for a given automaton and show that finite tests derived by the known FSM based test suites without explicit enumeration of implementation automata are complete with respect a number of fault models.

Key words: Input / Output automaton, Finite State Machine (FSM), fault model, complete test suite

1. Введение

Проблема построения проверяющих тестов с гарантированной полнотой на основе автоматных моделей имеет большую историю [1-4]. Наиболее полные результаты получены для модели конечного автомата, в которой после каждого входного воздействия ожидается выходной сигнал [5], что позволяет избежать состязаний между входными и выходными действиями и наличия тупиковых ситуаций. Для такой модели предложены методы синтеза полных конечных тестов, т.е. тестов, обнаруживающих каждую реализацию, неконформную спецификации из заданного конечного класса реализаций, без явного перечисления возможных реализаций. Такие методы разработаны для полностью определенных и частичных автоматов, детерминированных и недетерминированных автоматов [1-4, 6-9]. Однако возможности модели конечного автомата являются ограниченными, и достаточно часто в качестве спецификации дискретных систем рассматривается модель входо-выходного полуавтомата, в которой следующий входной сигнал может быть подан до получения выходного сигнала на предыдущее входное воздействие, что приводит к состязаниям между входными и выходными символами, входной сигнал может быть подан после получения нескольких выходных сигналов, а также возможно наличие ненаблюдаемого действия, что ведет к возникновению тупиковых ситуаций. Несмотря на достаточно большое количество публикаций по синтезу проверяющих тестов на основе такой модели [10, 11], конечные тесты с гарантированной полнотой строятся по модели неисправности, в которой все полуавтоматы-реализации явно перечислены или общая длина теста становится бесконечной, и соответственно, при ограниченном времени тестирования полнота тестирования остается неизвестной. В работе [12] нами предложены правила для подачи входных последовательностей на входо-выходной полуавтомат, которые позволяют избежать состязаний между входными и выходными воздействиями и тупиковых ситуаций. В этом случае по входо-выходному полуавтомату можно построить подходящий конечный автомат, и соответственно синтезировать тесты с гарантированной полнотой известными конечно автоматными методами. В настоящей работе мы рассматриваем несколько моделей неисправности, для которых возможен синтез конечных полных проверяющих тестов конечно автоматными методами.

Структура статьи следующая. Второй раздел содержит необходимые определения и обозначения. В третьем разделе вводятся понятия модели неисправности, в то время как четвертый раздел посвящен методам синтеза полных проверяющих тестов относительно введенной модели неисправности. В заключении подводятся итоги работы, и обсуждаются перспективы дальнейших научных исследований.

2. Определения и обозначения

Конечный входо-выходной *полуавтомат* (англояз. I/O-*automaton*) [10-12] или далее просто полуавтомат есть пятерка $\mathsf{S} = (S, s_0, I, O, h_S)$, где S – конечное непустое множество состояний с выделенным начальным состоянием s_0, I и O – конечные непересекающиеся входной и выходной алфавиты, причем их объединение не является пустым, и $h_S \subseteq S \times (I \cup O) \times S$ – отношение поведения или отношение переходов.

В полуавтомате есть переход из состояния s в состояние s' под действием a, если $(s, a, s') \in h_S$. Полуавтомат является *наблюдаемым*, если в каждом состоянии для каждого действия определено не более одного перехода [12]; в противном случае входо-выходной полуавтомат *ненаблюдаемый*. Полуавтомат является *недетерминированным*, если в некотором состоянии определены несколько выходных действий [12]; в противном случае входо-выходной полуавтомат *детерминированный*. Полуавтомат является трассовой моделью и описывает поведение моделируемой системы на последовательностях действий из алфавита $I \cup O$. Входной символ из I *определен* в состоянии s, если в этом состоянии есть переход под действием этого входного символа. Полуавтомат называется полностью определенным (по входным символам), если в каждом состоянии определен переход по любому входному действию; иначе, полуавтомат называется *частично определенным*. В состоянии s последовательность из $I \cup O$ является *допустимой*, если ее можно получить посредством последовательных переходов из этого состояния. Пусть S_{st} есть множество состояний, в которых нет переходов, помеченных выходными действиями; такие состояния часто называют *устойчивыми,* поскольку полуавтомат может оставаться в таком состоянии, пока не будет подан входной символ. Если в состоянии определены входные и выходные действия, то такое состояние будем называть *смешанным* состоянием. Множество тупиковых состояний, т.е. состояний, в которых не определено ни одного перехода, будем обозначать S_{und}, которые, по определению, также являются устойчивыми. Трасса в состоянии s называется *полной*, если финальное состояние является устойчивым. Для наблюдения перехода полуавтомата в устойчивое состояние, вводится специальный «молчащий» выходной символ $\delta \notin I \cup O$ (англ. quiescence) [10]. Таким образом, можно полагать, что в каждом устойчивом состоянии полуавтомата есть петля, помеченная символом δ, который рассматривается как выходной символ, и расширенный полуавтомат с выходным алфавитом $O \cup \{\delta\}$ обозначается S^{δ}. Соответственно, трасса σ полуавтомата S в состоянии s является полной, если и только если в полуавтомате S^{δ} в состоянии s есть трасса σδ, так называемая δ-трасса. Фактически, мы этим подчеркиваем, что ни один выходной символ из O не может появиться после трассы σ. По определению, из трассы полуавтомата S^{δ} можно получить трассу S после удаления δ, и обратно, после добавления

любого количества символов δ после любого полного префикса σ получается трасса полуавтомата S^{δ}.

3. Тестирование на основе входо-выходных полуавтоматов

Процесс тестирования интерактивных систем на основе формальных моделей (англ. Model Based Testing, MBT) обычно содержит три этапа. 1) На тестируемую реализацию подается тестовая (-ые) последовательность (-ти); 2) наблюдается выданная выходная последовательность; и 3) принимается решение о соответствии тестируемой реализации заданной спецификации. Процесс тестирования называется *безусловным*, если множество входных последовательностей задано заранее и не меняется в процессе тестирования. Тестирование называется *адаптивным*, если следующий входной символ в тестовой последовательности зависит от реакции тестируемой реализации на предыдущие входные воздействия. Вводится модель неисправности, которая при функциональном тестировании обычно является тройкой FM = <S, ≅, Ω>, где S – формальная (автоматная) спецификация системы, ≈ отношение конформности между спецификацией и тестируемой реализацией, Ω - множество реализаций, поведение которых описано той же (автоматной) моделью, что и спецификация. *Тестом* называется множество (адаптивных) входных последовательностей, и общая длина тестовых последовательностей называется *длиной* теста. Тест называется *исчерпывающим* относительно модели неисправности FM, если любая реализация, не конформная спецификации, обнаруживается тестом. Тест называется *значимым* (англ. *sound*), если любая реализация, конформная спецификации, не обнаруживается тестом. Тест, который является исчерпывающим и значимым называется *полным*. Для конечных автоматов, в которых за каждым входным символом следует выходной символ, существуют методы построения полных тестов относительно различных моделей неисправности, в которых спецификация системы может быть полностью определенным или частичным автоматом, детерминированным или недетерминированным автоматом, наблюдаемым или ненаблюдаемым автоматом. Более того, множество реализаций может быть задано явным перечислением (модель «белого ящика»), в виде мутационного автомата или функции неисправности (модель «серого ящика»), когда частично известна структура тестируемой реализации, и когда известно только ограничение на число состояний тестируемой реализации (модель «черного ящика»).

Для входо-выходных полуавтоматов методы синтеза полных тестов разработаны для различных отношений конформности [11], но построенный полный тест является конечным только для случая, когда множество тестируемых реализаций задано явным перечислением (модель «белого ящика») или при возможности наблюдения состояний тестируемой системы, т.е. для очень узкого класса моделей неисправности при использовании модели «серого ящика».

В данной работе мы вводим специальные гипотезы о подаче тестовых последовательностей на систему, поведение которой описано входо-выходным полуавтоматом, чтобы избежать состязаний между входными и выходными действиями, и тупиковых ситуаций. При выполнении этих гипотез по модели неисправности для входо-выходных полуавтоматов строится модель неисправности для классических автоматов. Если существует соответствующий метод построения полного теста для классического автомата, то этот тест можно преобразовать в алгоритм синтеза полного теста для входо-выходного полуавтомата.

Правила подачи входных последовательностей на входо-выходной полуавтомат

Для того, чтобы предотвратить состязания между входными и выходными символами в смешанных состояниях и тупиковые ситуации из-за отсутствия выходного символа, при тестировании систем, поведение которых описано входо-выходным полуавтоматом, обычно используются следующие правила при подаче входных последовательностей.

П1. После подачи входного символа в течение времени $T_{вых}$ ожидается выходной сигнал. Если такой сигнал появляется, то таймер «сбрасывается» до подачи следующего входного символа. Если выходной символ не появляется в течение $T_{вых}$, то полагается, что полуавтомат выдает «молчащий» символ δ, и таймер «сбрасывается» до подачи следующего входного символа.

П2. Чтобы избежать состязаний между входными и выходными символами в состоянии s, используется специальный входной «ждущий» символ ω и копия s' состояния s; в состояние s' копируются переходы из состояния s под действием выходных символов и добавляется переход из s в состояние s' под действием символа ω. В результате получается полуавтомат $\mathsf{S}^{\delta\omega}$ [12]. При попадании полуавтомата в состояние, в котором определены входные символы, входной символ, отличный от ω, должен быть подан достаточно «быстро» в пределах таймаута $T_{вх}$; если входной символ в течение этого времен не подается, то предполагается, что был подан входной символ ω, и в течение $T_{вых}$ ожидается выходной символ.

Если из трассы полуавтомата $\mathsf{S}^{\delta\omega}$ удалить символы δ и ω, то получится трасса полуавтомата S, и обратно, если σ есть трасса полуавтомата S, то после добавления в любого числа δ после любого полного префикса σ и символа ω перед каждым выходным символом, включая δ, то получится трасса полуавтомата $\mathsf{S}^{\delta\omega}$.

4. Построение полных проверяющих тестов для входо-выходных полуавтоматов

Полуавтомат $\mathsf{S}^{\delta\omega}$ «очень похож» на классический конечный автомат, поскольку в каждом состоянии определены только входные или только выходные символы, и после каждого входного символа присутствует выходной

символ. Соответственно, по такому полуавтомату можно построить конечный автомат с тем же множеством трасс [12], по которому и строить полные тесты относительно различных моделей неисправности известными конечно автоматными методами.

Входной и выходной алфавиты и множество состояний конечного автомата $M^{\delta\omega}{}_S$ совпадает с таковыми для полуавтомата S, и $M^{\delta\omega}{}_S$ строится по следующим правилам:

- существует переход из состояния s в состояние q с выходным символом δ под действием входного символа $i \in I$, если и только если в полуавтомате $\boldsymbol{S}$ существует переход из s в q под действием i;

- существует переход из состояния s в состояние q с выходным символом o под действием входного символа $\omega \notin I$, если и только если в полуавтомате $\boldsymbol{S}$ существует переход из s в q с выходным символом o;

- в состоянии s есть петля, помеченная парой ω/δ, если и только $s \in S_{st}$.

В качестве примера рассмотрим полуавтомат S на рис. 1 и соответствующий ему автомат $M^{\delta\omega}{}_S$.

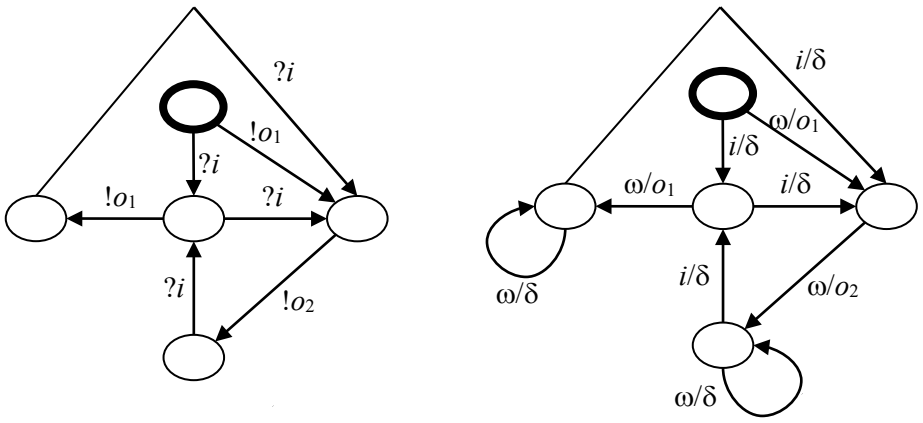

Рис. 1. Полуавтомат S и соответствующий ему конечный автомат $M^{\delta\omega}{}_S$.

По построению автомата $M^{\delta\omega}{}_S$, можно показать, что для преобразования трассы σ полуавтомата S в трассу автомата $M^{\delta\omega}{}_S$ необходимо добавить между любыми двумя входными символами трассы символ δ, а между любыми двумя выходными символами трассы символ ω.

Пусть FM = <S, ≈, Ω>, есть модель неисправности, в которой S – входо-выходной полуавтомат, ≈ - трассовое отношение конформности на множестве полуавтоматв с одинаковыми входным и выходным алфавитами, и Ω есть множество входо-выходных полуавтоматов, число состояний каждого из которых не превышает заранее заданного числа m, и поведение любой тестируемой реализации описывается некоторым полуавтоматом из множества Ω. Для построения полного проверяющего теста относительно такой модели

неисправности (при сохранении правил П1 и П2 подачи входной последовательности) можно использовать следующие шаги.

1) Преобразуем полуавтомат-спецификацию в конечный автомат и соответствующим образом преобразуем модель неисправности.
2) Если известны методы построения полного проверяющего теста для конечно автоматной модели неисправности, то строим такой полный тест.

Ниже мы рассматриваем модели неисправности на основе входо-выходных полуавтоматов, для которых можно построить полный проверяющий тест на основе выше описанных шагов.

4. Построение полного проверяющего теста для входо-выходных полуавтоматов с использованием конечно автоматной модели

Пусть FM = <S, ≈, Ω(m)>, есть модель неисправности, в которой S – входо-выходной полуавтомат, ≈ - трассовое отношение конформности на множестве полуавтоматов с одинаковыми входным и выходным алфавитами, и Ω(m) есть множество входо-выходных полуавтоматов, число состояний каждого из которых не превышает заранее заданного числа m, и поведение любой тестируемой реализации описывается некоторым полуавтоматом из множества Ω(m).

1) Пусть в модели FM = <S, ≈, Ω(m)> полуавтомат-спецификация является детерминированным, в каждом состоянии поведение полуавтомата определено для любой входной последовательности, включая входной символ ω, Ω(m) есть множество полностью определенных детерминированных полуавтоматов с числом состояний не более m; отношение конформности ≈ есть трассовая эквивалентность ≅. В этом случае полный проверяющий тест относительно FM = <S, ≅, Ω(m)> можно построить по конечно автоматной модели < $M^{\delta\omega}{}_S$, ≅, $\Omega^{\delta\omega}(m)$>, в которой $\Omega^{\delta\omega}(m)$ содержит соответствующий конечный автомат $M^{\delta\omega}{}_P$ для каждого автомата-реализации P ∈ Ω(m), одним из известных методов, W-методом или его различными модификациями [4], построив приведенную форму автомата $M^{\delta\omega}{}_S$, в которой любые два состояния отличаются по реакции на некоторую входную последовательность. Если m совпадает с числом состояний приведенной формы автомата-спецификации $M^{\delta\omega}{}_S$, то сложность построения и общая длина полного проверяющего теста являются полиномиальными относительно m. Если m больше числа n состояний приведенной формы автомата $M^{\delta\omega}{}_S$, то общая длина полного проверяющего теста пропорциональна $(|I|+1)^{m-n}$, где I – входной алфавит спецификации.

2) Полуавтомат-спецификация является детерминированным, однако поведение полуавтомата не обязательно определено для любой входной последовательности, включая входной символ ω. Поведение любой реализации описано детерминированным полностью полуавтоматом не более, чем с m состояниями; отношение конформности есть трассовая квази эквивалентность. Иными словами, поведение полуавтомата-реализации должно совпадать с

поведением полуавтомата-спецификации на каждой входной последовательности, определенной в начальном состоянии.

Полный проверяющий тест можно также построить относительно конечно автоматной модели неисправности FM = < $M^{\delta\omega}_S$, ≅, $\Omega^{\delta\omega}(m)$ > одним из известных методов; однако W-метод или некоторые его модификации в этом случае не работают; одним из методов, позволяющих построить тест по частичному детерминированному автомату спецификации является HSI- метод [4].

Рассмотрим полуавтомат S на рисунке 1 и соответствующий ему конечный автомат $M^{\delta\omega}_S$. Построим полный проверяющий тест относительно модели FM = <S, ≈, Ω(5)> HSI-методом. Построенный тест содержит 5 последовательностей общей длиной 25, и обнаруживает любой полуавтомат-реализацию не более, чем с 5 состояниями, поведение которого отличается от полуавтомата-спецификации хотя бы на одной определенной входной последовательности.

Следует отметить, что, если соответствующий частичный автомат не является приведенным, то тесты получаются более длинными, чем для полностью определенного полуавтомата-спецификации, однако теоретические оценки сложности построения и общей длины полного проверяющего теста совпадают с таковыми для полностью определенных полуавтоматов.

3) Полуавтомат-спецификация является полностью определенным и наблюдаемым, но может быть недетерминированным. Если все полуавтоматы множества Ω полностью определенные и наблюдаемые с числом состояний не больше *m*, то полный проверяющий тест можно построить методом, предложенным в [9]. Однако в этом случае действует предположение о «всех погодных условиях», т.е. предполагается, что каждая тестовая последовательность подается на тестируемую реализацию достаточное количество раз, чтобы была возможность пронаблюдать все возможные выходные последовательности реализации. При наличии предположения о «всех погодных условиях» теоретические оценки сложности построения и общей длины полного проверяющего теста совпадают с таковыми для детерминированных полуавтоматов.

4) Полуавтомат-спецификация является наблюдаемым, но может быть недетерминированным и частично определенным. В этом случае, отмечается, что полный проверяющий тест должен быть адаптивным, и в работе [9] приводится алгоритм построения такого теста относительно квази эквивалентности.

5) Полуавтомат-спецификация является полностью определенным и наблюдаемым, но может быть недетерминированным, все полуавтоматы множества Ω детерминированные с числом состояний не больше *m*, и отношение конформности является отношением редукции. Полный проверяющий тест можно построить методом, предложенным в [9]. В этом случае теоретические оценки длины тестовых последовательностей будут выше, чем для отношения эквивалентности, однако каждую тестовую

последовательность достаточно подать на полуавтомат-реализацию только один раз.

6) Полуавтомат-спецификация является наблюдаемым, но может быть недетерминированным и частично определенным. В этом случае, отмечается, что полный проверяющий тест должен быть адаптивным, и в работе [9] приводится алгоритм построения такого теста для конечно автоматной модели относительно квази эквивалентности.

7) Отношение конформности есть отношение неразделимости, т.е. для любой входной последовательности и любого полуавтомата-реализации [12] множества выходных реакций на эту последовательность пересекаются. Конечный полный проверяющий тест можно построить по конечно автоматной модели, и в этом случае нет необходимости в предположении о «всех погодных условиях» [12]. Тем не менее, длина теста становится экспоненциальной относительно числа состояний полуавтомата-спецификации.

Если полуавтомат-спецификация является ненаблюдаемым, то для использования конечно автоматных моделей неисправности в предыдущих случаях необходимо построить его наблюдаемую форму, число состояний в которой, а, следовательно, и длина проверяющего теста, могут быть экспоненциальными относительно числа состояний исходного ненаблюдаемого полуавтомата.

Тесты, построенные конечно автоматными методами, активно используется при тестировании телекоммуникационных протоколов, а также программного обеспечения для микропроцессоров. В частности, в [13 - 15] приведены примеры протоколов, в реализациях которых были найдены несоответствия спецификациям. В работе [16] рассмотрено использование полуавтоматной модели для проверки наличия состязаний в композиции SDN контроллера и переключателя.

Заключение

В настоящей работе проблема построения конечных тестов с гарантированной полнотой на основе входо-выходного полуавтомата для модели «черного ящика» сводится к построению такого теста для конечно автоматной модели. Соответственно, оценки сложности для таких тестов для подходящей модели неисправности совпадают с оценками сложности для подходящих классических конечных автоматов. Поскольку для конечных автоматов адаптивность в некоторых случаях позволяет снизить сложность построения и длину проверяющего теста [5], в дальнейшем авторы предполагают рассмотреть адаптивные тестовые последовательности для полуавтоматов, а также выделить классы с «хорошими» оценками сложности для таких экспериментов.

Работа выполнена при поддержке Российского научного фонда, проект № 22-29-01189.

Литература

1. Hennie, F. C. Fault-Detecting Experiments for Sequential Circuits // Proc. Fifth Ann. Symp. Switching Circuit Theory and Logical Design, 1964. — P. 95-110
2. Василевский, М. П. О распознавании неисправности автоматов // Кибернетика, 1973 (4). — С. 98-108.
3. Bochmann, G., Petrenko A. Protocol testing: review of methods and relevance for software testing // Proc. of International Symposium on Software Testing and Analysis. 1994. — P. 109–123.
4. Dorofeeva, R., El-Fakih, K., Cavalli, A., Maag, S., Yevtushenko, N. FSM-based conformance testing methods: A survey annotated with experimental evaluation // Information & Software Technology, 2010, 52 (12). — P. 1286-1297.
5. Гилл, А. Введение в теорию конечных автоматов // М.: Наука, 1966. — 272 с.
6. Lee, D, Yannakakis, M. Principles and methods of testing finite-state machines - a survey // Proceedings of the IEEE, 1996, 84 (8). — P. 1089-1123.
7. Petrenko, A., Yevtushenko, N. Testing from Partial Deterministic FSM Specifications // IEEE Trans. Computers. — 2005, 54(9). — P. 1154-1165.
8. Hierons, R. M. Adaptive Testing of a Deterministic Implementation Against a Nondeterministic Finite State Machine // The Computer Journal, 1998, 41(5). — P. 349-355.
9. Petrenko, A., Yevtushenko, N. Conformance Tests as Checking Experiments for Partial Nondeterministic FSM // Lecture Notes in Computer Science, 2005, 3997. — P. 118–133.
10. Tretmans, J. A formal approach to conformance testing // Proc. of the Intern. Workshop on Protocol Test Systems, 1993, — P. 257 – 276.
11. Бурдонов, И.Б., Косачев, А.С., Кулямин, В.В. Теория соответствия для систем с блокировками и разрушениями // М.: ФИЗМАТЛИТ. 2008. — 412 с.
12. Yevtushenko, N., Burdonov, I., Kossachev, A. Deriving Distinguishing Sequences for Input/Output Automata // Proc. of the IEEE East-West Design & Test Symposium, 2020, — P. 1-5.
13. N. Kushik, M. Forostyanova, S. Prokopenko, N. Yevtushenko. Studying the optimal height of the EFSM equivalent for testing telecommunication protocols // Proc. of the International Conference on Advances in Computing, Communication and Information Technology, 2014, — P. 159-163.
14. Жигулин М.В., А.В. Коломеец, Н.Г. Кушик, А.В. Шабалдин. Тестирование программной реализации протокола IRC на основе модели расширенного автомата // Известия Томского политехнического университета. — 2011. — Т. 318, № 5. — С. 81-84.
15. Жигулин М.В. Методы синтеза проверяющих тестов с гарантированной полнотой для контроля дискретных управляющих систем на основе временных автоматов. дис. ... канд. тех. наук — Томск, 2012. — 109 С.
16. Vinarskii, E., Lopez, J., Kushik, N., Yevtushenko, N., Zeghlache, D.: A model checking based approach for detecting sdn races. In Proc. of the 31st IFIP WG 6.1 Intern. Conf, on Testing Software and Systems, ICTSS, 2019, P. 194–211.