УДК 629.78.018

Б.Б. МИХНИЧ, В.Г. СИМОН

Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Украина

ФОРМАЛЬНАЯ ВЕРИФИКАЦИЯ ДИНАМИЧЕСКИ МОДИФИЦИРУЕМЫХ МОДЕЛЕЙ РАБОЧИХ ПОТОКОВ WINDOWS WORKFLOW FOUNDATION

Рассматривается механизм верификации рабочих потоков приложений, построенных по спецификации Windows Workflow Foundation и способных изменять бизнес-логику на этапе выполнения. Предложен механизм преобразования рабочих потоков в нотации сетей Петри и приведён пример такого преобразования. Для верификации предлагается использовать математический аппарат сетей Петри, анализируя свойства бездефектности замкнутой эквивалентной сети Петри. Дано определение требований, характеризующих бездефектную сеть Петри.

Ключевые слова: *сети Петри, Windows Workflow Foundation, рабочие потоки, бездефектность, формальная верификация.*

Введение

Создание гарантоспособных систем невозможно без применения методов формальной верификации программного обеспечения, под которой будем понимать формальное доказательство на абстрактной математической модели корректности алгоритмов управления, при этом предполагается, что соответствие между математической моделью и структурой системы считается изначально заданным.

В современной программной инженерии появляются новые подходы к разработке программных продуктов, которые активно используются разработчиками программного обеспечения. Один из таких подходов основан на технологии Windows Workflow Foundation (WWF), которая ориентирована на визуальное проектирование и использует декларативную модель программирования. Для такого подхода становится необходимым и возможным верификация каркасной логики разрабатываемого приложения.

В данной статье предлагается применение четкого математического аппарата для верификации разрабатываемых процессов WWF, который позволяет качественно оценить рассматриваемый алгоритм и вовремя выявить ошибки.

1. Цель исследований

Примерами математических объектов, часто используемых для моделирования систем, являются: конечный автомат; помеченная модель состояний и переходов; сеть Петри; временной автомат; гибридный автомат; алгебра процессов; формальная семантика языков программирования, например операционная семантика, денотационная семантика, аксиоматическая семантика и логика Хоара. WWF – одна из фундаментальных технологий компании Microsoft, входит в состав .NET Framework 3.0 [1], который изначально установлен в Windows Vista и может быть установлен в Windows 2003 Server и Windows XP SP2.

Данная технология позволяет определять, запускать на выполнение и управлять рабочими процессами. WWF предоставляет объектную модель и средства разработки приложений, основанных на принципах рабочих потоков, и может использоваться в самом широком спектре сценариев – от взаимодействия с пользователем до управления распределенными бизнес-процессами. При разработке приложений с использованием технологии WWF профессиональным программистом в среде .Net имеются встроенные средства верификации рабочих потоков. Процессы Workflow можно определить двумя способами: императивно, т.е. на любом из .NET-языков, например, C# или VB.NET; декларативно на XAML (eXtensible Application Markup Language) – язык интерфейсов. В WWF при помощи XAML можно определять последовательности выполняемых действий (workflows) редактирование которых возможно как в графическом, так и в текстовом виде.

WWF предоставляет возможность модификации рабочих потоков конечным пользователем в виде дополнительного инструментария настройки бизнес логики приложения. Инструментарий конечного пользователя является дополнительным средством адаптирования приложения и обычно не содержит развитых встроенных средств контроля рабочих потоков, поэтому предлагается организовать анализ корректности описанных рабочих потоков.

Поскольку в WWF процессы описываются в виде графических схем, возможен их перевод в нотацию сетей Петри и последующий качественный анализ с применением математического аппарата.

Язык сетей Петри обладает формальной семантикой, наглядным графическим представлением,

выразительностью. Его развитый математический аппарат позволяет проверять множество свойств моделируемых рабочих потоков и вырабатывать разнообразные методы для их анализа.

Целью исследований является обоснование возможности применения сетей Петри для верификации моделей WWF.

2. Метод верификации моделей WWF на основе сетей Петри

2.1. Введение в теорию сетей Петри

Сеть Петри представляет собой ориентированный двудольный граф с двумя типами вершин, которые называются позициями и переходами. Вершины соединены направленными дугами. Вершины одного и того же типа не могут быть соединены дугой. Графически позиции изображаются кругами, а переходы – прямоугольниками.

Сеть Петри определяется как тройка (P,T,F), где P – конечное множесво позиций; T – конечное множество переходов ($P \cap T = \varnothing$); $F \subseteq (P \times T) \cup (T \times P)$ – множество дуг (определяющих направление потока в сети). В каждый момент времени позиция содержит нуль или более фишек, изображаемых точками. В процессе исполнения сети число фишек может меняться. Переходы являются активными компонентами сети Петри. Они меняют состояние сети в соответствии со следующими правилами срабатывания:

1) переход t называется активным, если каждая входная позиция для t позиция p содержит по крайней мере одну фишку;

2) активный переход может сработать. Если переход t срабатывает, то t забирает по одной фишке из каждой входной для t позиции и помещает по одной фишке в каждую выходную для t позицию.

Введём следующие условные обозначения: **p** – входная позиция перехода t, если в сети имеется дуга, направленная от p к t; **•t** – множество входных позиций перехода t; **t•** – обозначается множество выходных позиций; **•p** – множество переходов, для которых p является входной позицией; **p•** – множество переходов, для которых p является выходной позицией; **M** – состояние сети, называемое разметкой, определяется, как распределение фишек по позициям; $M_1 \xrightarrow{t} M_2$ – переход t является активным в состоянии M_1 и срабатывание t переводит состояние M_1 в состояние M_1; (PN, M) – сеть Петри PN с начальным состоянием M;

2.2. Преобразование WWF в нотацию сетей Петри

В среде разработки WWF построение Workflow модели осуществляется путём моделирования последовательной, условной, параллельной и итеративной маршрутизации, используя базовый набор активностей, состоящий из 28 компонент, которые можно представить в виде элементарных функциональных блоков И-разветвление, И-слияние, ИЛИ-разветвление и ИЛИ-слияние.

Если для представления и анализа рабочих потоков, построенных по спецификации WWF использовать сети Петри то задачи следует моделировать переходами, а причинные зависимости позициями и дугами. Позиция соответствует условию, которое может использоваться в качестве пред- и/или постусловия для задач. И-разветвлению соответствует переход с двумя и более выходными позициями, а И-слиянию – переход с двумя или более выходными позициями. ИЛИ-разветвлению и ИЛИ-слиянию соответствуют позиции с несколькими выходными /входными дугами. В следующем подразделе будут показаны способы преобразования базовых активностей WWF к нотации сетей Петри.

Введём определение **WF-сети** [2]: Сеть Петри PN=(P,T,N) называется WF- сетью (сетью потоков работ), тогда и только тогда, когда выполняются следующие три условия: 1) имеется одна позиция-источник $i \in P$, такая что $\bullet i = \varnothing$; 2) имеется одна позиция-сток $o \in P$, такая что $o \bullet = \varnothing$; 3) каждая вершина $x \in P \cup T$ находится на некотором пути от позиции i к позиции o (добавлено для исключения “висячих” задач).

Сеть потоков работ имеет одну входную позицию (**i**) и одну выходную позицию (**o**) , так как каждый экземпляр WF-сети создаётся в момент появления в системе управления потоками работ и удаляется после полной обработки. Таким образом, WF-сеть описывает жизненный цикл экземпляра. Проведём обзор типовых паттернов рабочих потоков и способы их преобразование к сетям Петри.

Существует 20 паттернов [3], при помощи которых можно смоделировать любой рабочий поток, разбитых на 6 групп:

1) базовые паттерны (присутствуют в большинстве языков потоков работ для моделирования последовательной, параллельной и условной маршрутизации);

2) расширенные переходы и синхронизации (расширяют базовые до более сложных случаев разветвления и объединения, примером может служить синхронизирующее соединение, который действует либо как XOR-слияние, либо как AND-слияние, в зависимости от контекста);

3) структурные паттерны (произвольные циклы, неявное завершение);

4) множественные экземпляры (применяются для выполнения некоторой части процесса несколько раз);

5) паттерны состояний (отложенный выбор, параллельная маршрутизация с чередованием, контрольные точки);

6) паттерны отмены (позволяют организовать отмену от одного действия до всего экземпляра).

Для классификации 28 активностей, которые предоставляет WWF, отметим, что они разделены на

2 основные группы: простые и составные активности. К простым активностям относят те, которые состоят из одной позиции, например – вызов внешнего метода, активность встроенного кода, таймер задержки, активность прерывания. К составным активностям относят сложные структуры, такие как активности ветвления (*while*, *ifelse*), активности распараллеливания и синхронизации рабочих потоков и прочие.

Все эти активности реализуются с помощью вышеперечисленных шаблонов, которые однозначно переводятся в нотацию сетей Петри. Приведём пример преобразования ListenActivity (активность прослушивания) WWF к нотации сетей Петри.

Активность прослушивания – это некий аналог активностей IfElse и Parallel и применяется для работы с событиями. Она может содержать два или более контейнеров-последовательностей (EventDriven), каждый из которых содержит произвольный набор вложенных активностей.

Все EventDriven ветви в Listen ожидают прихода сообщения для события, на которое они подписаны. Как только приходит сообщение, соответствующее какой-то из ветвей, начинает выполняться соответствующая EventDriven последовательность.

Данную активность можно промоделировать при помощи паттерна "*множественный выбор*", который представлен на рис. 1.

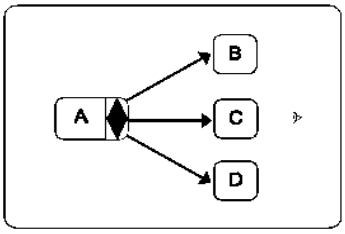

Рис. 1. Реализация паттерна множественный выбор в нотации YAWL

После выполнения активности A будет выбрана либо активность C, либо активность B либо и та, и другая, порождая при этом параллельные потоки. Это решение будет принято в зависимости от условий, которые сосредоточены в этих активностях.

Если условие не срабатывает, тогда необходимо избавиться от меток. На рис. 2 показан механизм избавления от меток при моделировании сетями Петри. Для избавления от ненужных меток можно на каждое условие добавить параллельную пустую ветвь, ведущую в конечную позицию сети. То есть, метка будет продвигаться до тех пор, пока не встретиться конструкция синхронизации.

2.3. Свойства WWF, подлежащие верификации

Опишем структурные свойства сети Петри, анализируя которые, можно проводить формальную верификацию соответствующей данной сети Петри модель WWF.

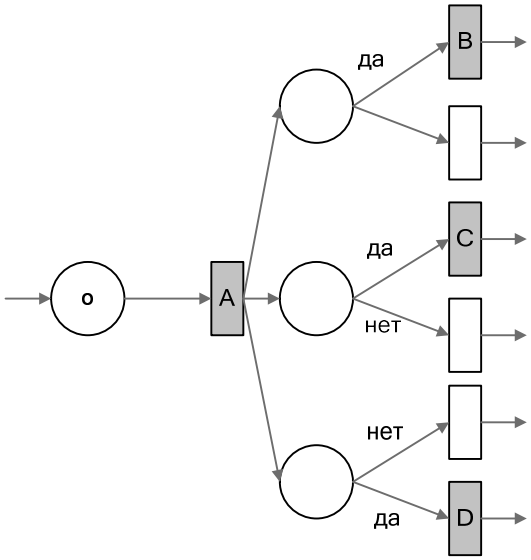

Рис. 2. Реализация паттерна "множественный выбор" и ListenActivity в нотации сетей Петри

Живость. Сеть Петри (PN, M) называется *живой*, если для любого достижимого состояния **M'** и любого перехода **t** существует достижимое из **M'** состояние **M''**, в котором **t** является активным.

Безопасная (Ограниченная) сеть – сеть Петри (PN, M), у которой для любой позиции существует натуральное число **n**, такое, что в любом достижимом состоянии число фишек в позиции **p** не превышает **n**. Сеть называется безопасной, если максимальное число фишек в любой позиции этой сети не превышает 1.

Бездефектность.

При верификации **WF-сети** условия, перечисленные в определении WF-сети, представленном в пункте 2.2 можно проверить статически, т.е. анализируя структуру сети Петри. Но есть и ещё одно условие, которое должно быть выполнено: процедура обработки любого экземпляра, в конце концов, завершается, и в момент завершения позиция **o** содержит одну фишку, а все остальные позиции являются пустыми.

Также не должно быть "мёртвых" задач, т.е. необходимо, чтобы каждую задачу можно было выполнить, следуя подходящему маршруту в WF-сети.

Два этих требования и составляют *свойство бездефектности,* которое помимо всего прочего характеризует динамику сети.

Моделируемая WF-сетью PN=(P,T.F) процедура называется бездефектной, если:

1) для любого состояния **M**, достижимого из состояния **i**, существует последовательность срабатываний, переводящая состояние **M** в состояние **o**:

$$\forall_M (i \xrightarrow{*} M) \Rightarrow (M \xrightarrow{*} o) \qquad (1)$$

2) состояние o является единственным состоянием, которое достижимо из состояния i и содержит хотя бы одну фишку в позиции o:

$$\forall_M (i \xrightarrow{*} M \ \wedge M \geq o) \Rightarrow (M = o) \qquad (2)$$

3) в сети (PN, i) нет мёртвых переходов:

$$\forall_{t \in T} \exists_{M,M'} i \xrightarrow{*} M \xrightarrow{t} M' \qquad (3)$$

Для определения бездефектности WF-сети PN=(P,T,N) необходимо связать живость и ограниченность. Для этого определим расширенную сеть $\underline{PN}=(\underline{P},\underline{T},\underline{N})$, которая получается добавлением нового перехода t*, соединяющего позиции **o** и **i**.

Расширенная сеть Петри $\underline{PN}=(\underline{P},\underline{T},\underline{N})$ определяется следующим образом:

$$\underline{P}=P,\ \underline{T}=T\cup\{t^*\} \text{ и } \underline{F} = F\cup\{\langle o,t^*\rangle, \langle t^*,t\rangle\} \qquad (4)$$

Такую расширенную сеть ещё называют замыканием сети PN, для которой справедлива следующая *теорема*: WF-сеть является бездефектной в том и только в том случае, когда сеть ($\underline{PN}$, i) – живая и ограниченная. Доказательство теоремы приведено в источниках [2, 4]. Следствием из теоремы является то, что для проверки бездефектности можно использовать стандартные методы анализа сетей Петри.

Заключение

Результаты исследования доказывают возможность формальной верификации процессов workflow на основе математического аппарата сетей Петри. Основным свойством WF-сети Петри для верификации рабочих потоков является составное свойство – бездефектность.

Показано, что преобразование моделей рабочих потоков в нотации сетей Петри является однозначным и непротиворечивым.

Представленные модели и методы в дальнейшем планируется использовать как основу инструментальных средств для анализа рабочих потоков и повышения качества программного обеспечения гарантоспособных систем.

Литература

1. C# 2005 и платформа .NET 3.0 для профессионалов / К. Нейгел, Б. Ивьен. – М.: Диалектика. - 2008 – 1376 С.

2. Wil van der Aalst Workflow Management: Models, Methods and Systems / Wil van der Aalst, Kees van Hee. – Cambridge MIT Press, MA, USA. – 2002.

3. Yet Another Workflow Language [Электронный ресурс]. – Режим доступа: http://www.yawl-system.com.

4. Wil van der Aalast. Verification of Workflows nets. / Wil van der Aalast. - Application and Theory of Petri Nets. - Berlin Springer-Verlag. – 1997. - P. 407-426.

Поступила в редакцию 19.01.2009

Рецензент: д-р техн. наук, проф., зав. кафедрой В.М. Вартанян, Национальный аэрокосмический университет им.Н.Е. Жуковского «ХАИ», Харьков, Украина.

ФОРМАЛЬНА ВЕРИФІКАЦІЯ ДИНАМІЧНО МОДИФІКОВАНИХ МОДЕЛЕЙ РОБОЧИХ ПОТОКІВ WINDOWS WORKFLOW FOUNDATION

Б.Б. Міхнич, В.Г. Симон

Розглядається механізм верифікації робочих потоків програм, побудованих за специфікацією Windows Workflow Foundation і здатних змінювати бізнес-логіку під час виконання. Запропоновано механізм перетворення робочих потоків у нотацію мереж Петрі і наведений приклад такого перетворення. Для верифікації запропоновано використовувати математичний апарат мереж Петрі, шляхом аналізу властивостей бездефектної замкнутої еквівалентної мережі Петрі. Дано визначення вимог, що характеризують бездефектну мережу Петрі.

Ключові слова: сіть Петрі, Windows Workflow Foundation, робочі потоки, бездефектність, верифікація.

FORMAL VERIFICATION OF DYNAMICALLY MODIFIED WINDOWS WORKFLOW FOUNDATION WORKFLOW MODELS

B.B. Mikhnich, V.G. Symon

The mechanism of verification of working streams of the applications constructed under specification Windows Workflow Foundation and capable to change business logic at a performance stage is considered. The mechanism of transformation of working streams in the notation of Petri nets offered and the example of such transformation is resulted. For verification it is offered to use a mathematical apparatus of Petri nets, analyzing properties soundness closed equivalent Petri net. Definition of the requirements characterising soundness Petri net is made.

Key words: Windows Workflow Foundation, workflow, soundness, test bench automatization, spacecraft.

Михнич Борис Борисович – аспирант каф. 603 Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: boris.mikhnich@rambler.ru.

Симон Виталий Григорьевич – магистрант каф. 603 Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина.