Карпов Юрий Глебович

ТЕМПОРАЛЬНЫЕ ЛОГИКИ ДЛЯ СПЕЦИФИКАЦИИ СВОЙСТВ ПРОГРАММНЫХ И АППАРАТНЫХ СИСТЕМ

Аннотация

В статье вводится темпоральная логика линейного времени (LTL), ее формулы объясняются на многочисленных примерах. Объясняется, как свойства поведения дискретных динамических систем, в частности, реагирующих систем (reactive systems) могут быть заданы в этой логике. Статья является изложением одной из глав книги автора «*Model checking. Верификация параллельных и распределенных программных систем*», которая выходит в издательстве БХВ Петербург.

Ключевые слова: Линейная темпоральная логика, LTL, реагирующие системы (reactive systems), спецификация поведения.

Для верификации автоматизированных систем свойства их поведения должны быть выражены формально логическими утверждениями, которые обеспечат простую, лаконичную и недвусмысленную их запись. Оказывается, что обычная логика высказываний является неадекватной для формулировки подобных утверждений о поведении дискретных систем, то есть об изменении во времени их состояний. Для спецификации таких свойств необходимы логические утверждения, истинность которых зависит от времени. Соответствующие логики называются темпоральными. Достаточно мощные, выразительные и в то же время простые темпоральные логики были построены как простые расширения обычной логики высказываний.

В этой статье мы рассмотрим одно из расширений обычной логики высказываний, так называемые *темпоральные логики*, которые оказались очень продуктивными при формулировке утверждений о поведении дискретных систем, развивающихся во времени.

1. УТВЕРЖДЕНИЯ, ИСТИННОСТЬ КОТОРЫХ ЗАВИСИТ ОТ ВРЕМЕНИ

При всей широте использования классической логики в науке, технике и в обычной жизни очевидны ее ограничения. Классическая логика основывается на самой примитивной модели истины, она не позволяет выразить степень уверенности/неуверенности в истинности высказывания. Формулы логики могут принимать значения только “*да*” и “*нет*” на подходящей интерпретации, но не могут определить интервал возможных значений в некоторой области. Формулы обычной логики истинны или ложны независимо от времени, в статическом мире. Вследствие этого, аппарат классической логики оказался недостаточно выразительным во многих областях применения. Поэтому неудивительно, что

предпринимались многочисленные попытки расширений классической логики в самых различных направлениях, и некоторые из этих попыток оказались весьма успешными.

Если утверждения естественного языка явно или неявно включают зависимость высказываний от времени или от порядка событий во времени, то формализация их в классической логике высказываний обычно неадекватна. Например, коммутативность операции конъюнкции (перестановочность ее аргументов $A \wedge B \equiv B \wedge A$) не выполняется для следующих предложений:

"*Джон умер, и его похоронили*"

не эквивалентно предложению

"*Джона похоронили, и он умер*";

"*Джейн вышла замуж и родила ребенка*"

не эквивалентно предложению

"*Джейн родила ребенка и вышла замуж*";

"*Сообщение послано в канал, и на него пришло подтверждение"*

не эквивалентно предложению

"На сообщение пришло подтверждение, и оно послано в канал".

Анализ этих утверждений в рамках обычной логики высказываний невозможен. Для адекватного формального выражения подобных утверждений нужна логика, позволяющая отразить соотношения моментов времени наступления событий, в естественном языке определяемые такими словами, как "*случилось после*", "*случается иногда*", "*случается всегда*". Это требует формализации высказываний, истинность которых меняется во времени.

Необходимость оперировать высказываниями, истинность которых меняется со временем, возникает часто. Например, высказывание: "*Путин – президент России"* истинно только в определенный период времени. Высказывание "*Светит солнце"*, ложное сегодня, может стать истинным завтра. Утверждение "*Я голоден*" станет ложным после того, как я поем. Многие утверждения, в которых вводятся причинно-следственные отношения, также связаны со временем:

"*Если я видел ее раньше, то я узнаю ее при встрече"*;

"*Раз Персил – всегда Персил";*

"*Мы не друзья, пока ты не извинишься"*.

Утверждение естественного языка:

"*Вчера он сказал, что придет завтра, значит, он сказал, что придет сегодня",*

несомненно, истинно. Но в обычной логике высказываний формальное доказательство истинности этого утверждения невозможно.

Большую долю утверждений, нуждающихся в формализации логической теорией с учетом времени и проверке их, составляют свойства технических систем, обладающих динамикой, то есть поведением во времени, изменяющим некоторые параметры систем. Например:

С1: Посланный запрос когда-нибудь в будущем будет обработан;

С2: Лифт никогда не пройдет мимо этажа, вызов от которого поступил, но еще не обслужен.

Элементарные (атомарные) утверждения в этих высказываниях могут быть истинны в один момент времени и ложны в другой. Мы не можем адекватно представить утверждение С1 с помощью такой формулы логики высказываний:

$Послан_R \Rightarrow Обработан_R$ (то есть *если запрос R послан, то он обработан*).

Действительно, в классической логике утверждения обычно понимаются как истинные либо ложные независимо от времени, а утверждение C1 явно различает разные моменты времени. Оно утверждает, что если *в некоторый момент времени* t запрос R послан, то в *какой-то будущий момент времени* $t' \geq t$ он будет обработан.

Попытаемся выразить эти свойства с помощью логики предикатов первого порядка, вводя в употребление такие выражения, как "*событие p наступило в момент t*". Утверждение C1 при этом будет выглядеть так:

$(\forall t \geq 0)\ [Послан_R(t) \Rightarrow (\exists t' > t)\ Обработан_R(t')]$.

Утверждение C2 в логике предикатов выглядит так (здесь $Лифт_n(t)$ – утверждение: *Лифт в момент t находится на этаже n*):

$(\forall t \geq 0)(\forall t' > t)[Вызов_n(t) \wedge \neg Лифт_n(t) \wedge (\exists t1 : t' \geq t1 \geq t) H_n(t1) \Rightarrow$

$(\exists t2 : t' \geq t2 \geq t)\ Обслуживается_n(t2)]$.

Такая формализация трудно читается, и, как известно, доказательства в логике предикатов проводить довольно сложно. Этот путь формализации зависимых от времени утверждений пока не дал существенных результатов для практики верификации технических систем.

Попытка построения формальной модели, неявно учитывающей время в высказываниях, была предпринята философом и логиком Гансом Райхенбахом [1] для изучения глагольных времен английского языка. В теории Райхенбаха время глагола в предложении характеризуется соотношением моментов наступления событий, о которых говорится и которые подразумеваются в предложении. Используя соотношения во времени двух моментов: момента S, в который сделано высказывание (*Speech time*), и момента E наступления события, о котором говорится в высказывании (*Event time*), можно образовать только три простых времени глагола – настоящее, прошедшее и будущее с соотношениями соответственно E=S, E<S и S<E. Для того чтобы покрыть бульшее число различных глагольных времен, Райхенбах ввел третий момент – момент R точки референции (*Reference time*), то есть момента, на который *ссылается* высказывание. В Future Perfect, когда мы говорим, например, "*I shall have seen John*" (буквально "*Я буду иметь Джона увиденным*"), это высказывание отсылает нас не к тому моменту, когда я увидел Джона, но к моменту, по отношению к которому (*with reference to*) мое видение Джона уже произошло, то есть соотношение между этими моментами времени есть S<E<R.

Формальная модель Райхенбаха позволяет прояснить различия многих времен глаголов английского языка. Например, в предложении "*I saw John*" соотношение между этими моментами R=E<S; а в предложении "*I have seen John*" это соотношение E<R=S (рис. 1).

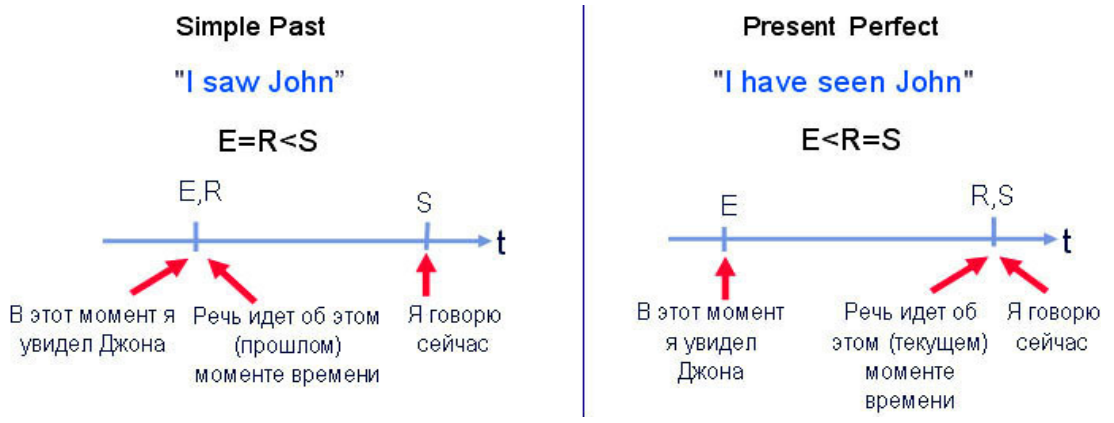

Рис. 1. Различия в формах глаголов Past Indefinite и Present Perfect обусловлено соотношениями моментов наступления событий

Однако возможность использования этого формализма для верификации дискретных систем сомнительна. Прогресс в области верификации был достигнут на пути введения специальных модальностей в обычную логику высказываний.

2. МОДАЛЬНЫЕ И ВРЕМЕННЫЕ ЛОГИКИ: TENSE LOGIC

В приведенных выше примерах высказываний время не присутствует явно. И нам действительно часто неважно, при каких конкретных значениях времени наступали те или иные события, важно только выразить порядок событий, отношения между моментами времени, в которых эти события наступали (вспомним знаменитый тезис Л. Лэмпорта: *Время есть способ упорядочения событий*). Характеристики временных свойств систем используют категории вида "*никогда не будет верно, что ...*", или "*в будущем обязательно случится, что ...*" и тому подобные, характеризующие истинность суждения с учетом отношений между моментами наступления различных событий во времени. Можно расширить классическую логику, разрешив использовать такие категории перед утверждениями логики, например, выражение **F***Получено*(m) можно понимать так: *Когда-нибудь в будущем сообщение m обязательно будет получено*. Такие категории называются ***модальностями***, их можно поместить перед высказываниями, чтобы они как-то характеризовали содержание этих высказываний.

Модальность в логике (от латинского *modus – способ, наклонение*) вводится дополнительным оператором, предваряющим высказывание. Модальный оператор характеризует высказывание, являющееся его операндом. В общем случае модальный оператор не обязательно связан со временем. Например, пусть q – некоторое высказывание. Можно выразить неполную уверенность в истинности утверждения q, сказав: "*Возможно, что q наступит*". Для формализации этого введем модальный оператор **M**. Тогда **M**q имеет смысл "*возможно, что q наступит*", или "*может быть, наступит q*".

Формальные теории устанавливают соотношения между формулами. Например, введем модальный оператор **L**, имеющий смысл "*необходимо, что ...*". Тогда можно следующим образом определить отношение между модальностями **M** и **L**: **L**q ≡¬**M**¬q, что согласуется с интуитивно истинным утверждением:

"*q обязательно наступит, это то же самое, что неверно, что q, возможно, не наступит вовсе*".

Классическая логика, расширенная какими-нибудь операторами модальности, называется модальной логикой. Такое расширение можно определить по-разному, вводя разного типа модальности и даже разную их семантику (формальное определение смысла модальностей). Возможность использования различной семантики проистекает из того, что в естественном языке в разных его применениях трактовки одних и тех же модальных слов часто различны, и даже в одной области применения они обычно смутны, расплывчаты, неоднозначны. Поэтому существует большое число различных модальных логик, каждая из которых удобна в конкретной области применения.

Модальности, которыми можно расширить классическую логику, могут быть связаны и с характеристикой момента времени, в котором утверждается истинность высказывания, зависящего от времени. Логики, расширенные такими модальностями, называются темпоральными, или временными логиками. Мы будем использовать термин *темпоральные логики*.

Определение 1 (темпоральные логики). ***Темпоральные логики*** *– это логики, в которых истинностное значение логических формул зависит от момента времени, в котором вычисляются значения этих формул.*

Темпоральные логики издавна использовались в философии для изучения таких схем рассуждений, которые включали ссылки на время. Основная идея темпоральной логики состоит в том, чтобы фиксировать только *относительный порядок событий* – фактически, текущее, будущее и прошедшее время. Конечно, в некоторых приложениях, например в области верификации систем *реального времени,* явные значения времени и численные ограничения на время должны учитываться, и там следует вводить более сложные формализмы.

В одной из предшественниц современных темпоральных логик – Tense Logic, разработанной английским логиком Артуром Прайором в середине прошлого века [2], были впервые введены две модальности: **F** (от Future): "*когда-нибудь в будущем будет истинно ...*" и **P** (от Past): "*когда-то в прошлом было истинно ...*".

На рис. 2 показано, при каких значениях времени истинны утверждения **F**q и **P**q, если заданы отрезки времени, в которых истинно утверждение q. Обозначим t|=Ф утверждение: "*В момент времени t истинно утверждение Ф*". Тогда (см. рис. 2):

– утверждение q истинно в момент времени t (t |=q), если утверждение q истинно в момент t (что является тождественной истиной, тавтологией);

– утверждение **F**q истинно в момент времени t (t|=**F**q), если для какого-то момента времени t′ в будущем (при некотором t′ ≥ t) q станет истинным (заметьте, что будущее здесь включает настоящее);

– утверждение **P**q истинно в момент времени t (t|=**P**q), если для какого-то момента времени t′ в прошлом (при некотором t′ < t) утверждение q было истинным.

В Tense Logic введены и два дуальных темпоральных оператора: **G** (от слова Globally) и **H** (от слова History) с очевидными соотношениями: **G**q≡¬**F**¬q, **H**q≡¬P¬q. Справедливость этих соотношений очевидна. Например, первого: "*Утверждать, что в будущем утверждение q будет всегда истинно, это то же самое, что утверждать, что неверно, что когда-нибудь в будущем утверждение q станет ложным*". Эти операторы можно определить и независимо от **F** и **P** (см. рис. 2):

– утверждение **G**q истинно в момент времени t (t|=**G**q), если для любого момента времени t′ в будущем (при всех t′≥ t) утверждение q истинно (заметьте, что будущее здесь также включает настоящее);

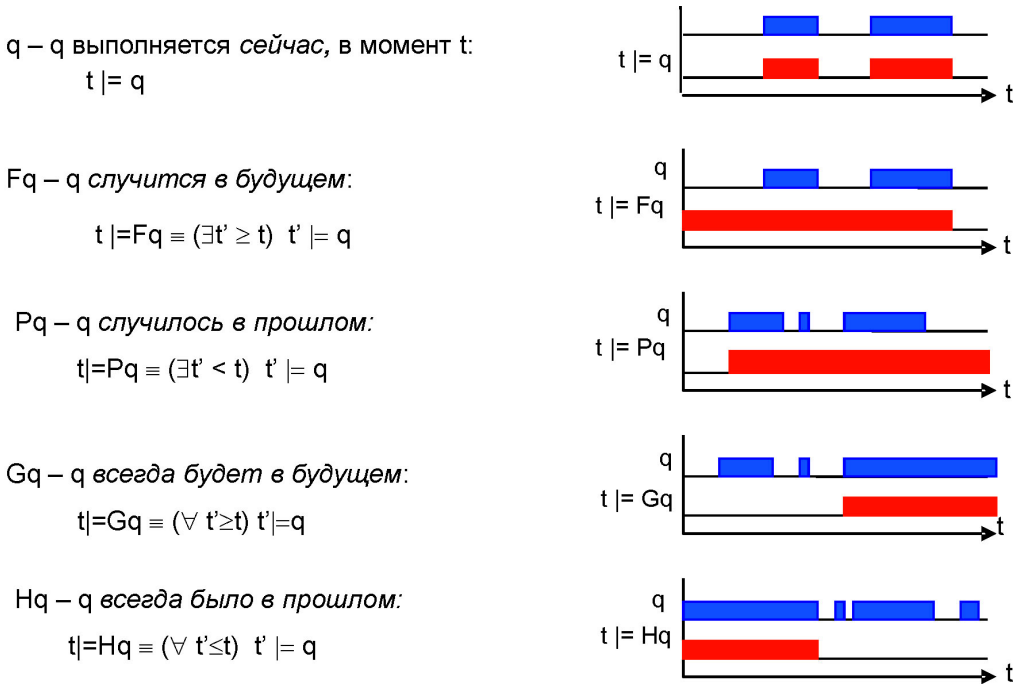

Рис. 2. Темпоральные операторы Tense Logic

– утверждение **H**q истинно в момент времени t (t|=**H**q), если для любого момента времени t′ в прошлом утверждение q истинно.

Уже с помощью двух темпоральных операторов **F** и **G** можно выразить сложные свойства, зависящие от времени. Например:

Утверждение q будет истинным:

всегда в будущем:	**G**q
хотя бы раз в будущем:	**F**q
никогда в будущем:	¬**F**q
бесконечно много раз в будущем:	**GF**q
с какого-то момента постоянно:	**FG**q.

Рассмотрим, как с помощью этих операторов формально записать некоторые утверждения.

События e1 и e2 никогда не произойдут одновременно (взаимное исключение):

G[¬(*e1* ∧ *e2*)]

Посланное сообщение m когда-нибудь в будущем будет получено:

G[$Послано_m$ ⇒ **F** $Получено_m$]

Джейн вышла замуж и родила ребенка:

P(*Джейн_выходит_замуж* ∧ **F***Джейн_рожает_ребенка*)

Джейн родила ребенка и вышла замуж:

P(*Джейн_рожает_ребенка* ∧ **F***Джейн_выходит_замуж*)

Пока ключ зажигания не вставлен, машина не поедет:

G(¬**P***Зажигание* ⇒¬*Старт*).

В темпоральную логику можно ввести еще два оператора: NextTime (**X**) и Until (**U**).

Оператор **Next time**: утверждение **X**q истинно в момент времени t, если q истинно в следующий момент t + 1:

Джон убил, и ему стало страшно:

P(*Джон_убивает* ∧ **XG** *Джону_страшно)*

Если я видел ее раньше, я ее узнаю при встрече:

P*Увидел* ⇒ **G**(*Встретил* ⇒ **X***Узнал*)

Джон умер и его похоронили:

P(*Джон_умирает* ∧ **XF***Джона_хоронят*)

Оператор **Until** (*до тех пор, пока не наступит нечто*) требует двух аргументов – утверждений. Формально он записывается довольно сложно:

t |= p**U**q ≡ (∃t′ ≥ t): (t′|= q ∧ (∀t″: t≤t″< t′): t″|=p).

Утверждение p**U**q истинно в момент времени t, если q истинно в некоторый будущий момент времени t′ ≥ t, а во всем промежутке [t, t′) от момента t до t′ истинно p. Пример развертки во времени, показывающей, когда будет истинно утверждение p**U**q при различных истинностных значениях p и q, показан на рис. 3.

С оператором Until многие сложные утверждения легко представимы в формальной записи, например:

Мы не друзья, пока ты не извинишься:

(¬*Мы_друзья*) **U** *Ты_извиняешься*

pUq – q *случится в будущем, а до него непрерывно будет выполняться* p

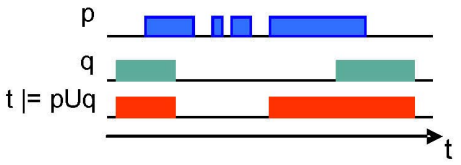

Рис. 3. Темпоральный оператор Until

Лифт никогда не пройдет мимо этажа, вызов от которого поступил, но еще не обслужен:

$$\mathbf{G}\ [\ \textit{Вызов}(n) \Rightarrow (\neg \textit{Лифт}(n)\ )\mathbf{U}\ \textit{Обслуживается}(n)\ ].$$

Через оператор **U** легко выражается оператор **F**:

$$\mathbf{F}q = \textit{true}\ \mathbf{U}\ q,$$

а следовательно, и оператор **G**:

$$\mathbf{G}{=}\neg\mathbf{F}\neg q{=}\neg(\ \textit{true}\ \mathbf{U}\ \neg q\ ).$$

В этой логике для операторов **X** и **U** существуют их аналоги в прошлом: $\mathbf{X}^{-1}$ (*в предыдущий момент времени*, '*вчера*') и **S** (since, '*с тех пор, как*').

Tense Logic позволяет формализовать философские мысли о времени. Например, обозначим атомарное утверждение "*нечто есть*" символом q. Тогда следующее глубокомысленное абсолютно истинное заключение (тавтологию):

"*Будет, что нечто было, если и только если оно или есть сейчас, или будет, или уже было*" можно формализовать так:

$$\mathbf{FP}q \equiv q \vee \mathbf{F}q \vee \mathbf{P}q.$$

Философскую мысль о времени:

"*Любое 'вчера' было когда-то 'завтра', любое 'завтра' когда-нибудь станет 'вчера'*" формально можно записать так:

$$(\mathbf{PX}^{-1}q \Rightarrow \mathbf{PX}q) \wedge (\mathbf{FX}q \Rightarrow \mathbf{FX}^{-1}q).$$

Временная логика помогает точно и однозначно выразить временные соотношения между событиями, о которых повествуют (часто неоднозначные) фразы естественного языка. Обозначим:

Д(x): *x – мой друг*, П(x): *x – президент*.

Используя эти обозначения, можно формально записать несколько совершенно различных интерпретаций предложения "*Мой друг NN будет президентом*":

1. Д(NN) & **FX**П(NN):
   сейчас NN – мой друг, а в будущем он станет президентом;
2. **FX**(Д(NN) & П(NN)):
   в будущем NN станет моим другом, и в это время он уже будет президентом;
3. **F**(Д(NN) & **FX**П(NN))
   в будущем NN станет моим другом, а затем он станет президентом.

3. ТЕМПОРАЛЬНАЯ ЛОГИКА ЛИНЕЙНОГО ВРЕМЕНИ (LTL)

Современная темпоральная логика линейного времени (LTL, Linear Time Logic) является наследницей временной логики Tense Logic Артура Прайора. LTL разработана израильским ученым Амиром Пнуэли [3] для спецификации свойств параллельных технических систем. За разработку этой логики и выделение специального класса программ, реа-

гирующих на внешние события (reactive systems) в 1966 г. Амир Пнуэли был награжден премией Тьюринга.

В LTL максимально упрощены все включенные в нее концепции.

Во-первых, в LTL темпоральными операторами расширена простейшая логика высказываний, формулы которой строятся из конечного числа атомарных предикатов (утверждений) и булевых операций.

Определение 2 *(атомарный предикат).* ***Атомарный предикат (атомарное утверждение)*** *– это утверждение, которое может принимать истинное или ложное значение, от структуры которого мы абстрагируемся.*

Во-вторых, в новую логику включено минимальное число темпоральных операторов, которые определяют характеристики истинности высказываний, упорядоченных во времени. Таких операторов только два, **U** и **X**. Логика LTL не включает темпоральных операторов прошлого. Основания для этого очевидны: прошлое для технических систем менее важно, чем их будущее поведение, начинающееся с момента их включения, запуска.

В качестве интерпретации формул темпоральной логики рассматривается дискретная во времени бесконечная линейная направленная в будущее последовательность "*миров*", в каждом из которых существует своя интерпретация атомарных утверждений. Иными словами, формулы LTL принимают истинное или ложное значение на последовательности миров, и в каждом из миров для всех введенных атомарных утверждений определены свои конкретные истинностные значения. Такой взгляд на изменчивость во времени значения истинности атомарных утверждений (атомарных предикатов) имел еще Аристотель, который говорил, что "утверждения и мнения" могут иметь разные значения истинности в зависимости от моментов, в которые они делаются, отражая изменения в объектах, свойства которых они представляют.

Направленность последовательности миров от прошлого к будущему позволяет проводить рассуждения об относительном времени, в терминах "*до*" и "*после*". На рис. 4 построен пример такой интерпретации. На последовательности "*миров*" w0, w1, w2, ..., wn, ... задано множество атомарных предикатов {p, q, r}. В "*мире*" w0 атомарные предикаты p и q истинны, а r – ложен, в "мире" w1 утверждения q и r истинны, а p – ложно, и т. п. Будем считать, что, начиная с w2, все истинностные значения p, q и r во всех "*мирах*" этой конкретной бесконечной последовательности одинаковы и совпадают с их значениями в w2.

Как происходит переключение от одного мира к следующему, теория не рассматривает, от этого она абстрагируется.

Поскольку в каждом "*мире*" каждый атомарный предикат имеет свое стабильное и неизменное в этом "*мире*" истинностное значение – истину или ложь, *true* или *false*, то и формулы обычной логики высказываний в разных "*мирах*" могут иметь различные истинностные значения, вычисленные по этим интерпретациям своих аргументов. Например, в мире w0 формула $q \Rightarrow r$ ложна, а во всех следующих "*мирах*" данной цепочки миров она истинна. Формула $r \wedge \neg q$ в мире w0 ложна, а в w2 – истинна. Рис. 5 показывает, в каких

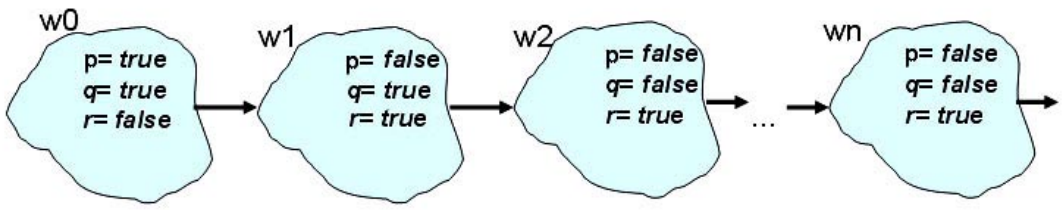

Рис. 4. Возможная интерпретация темпоральной логики LTL – бесконечная последовательность миров

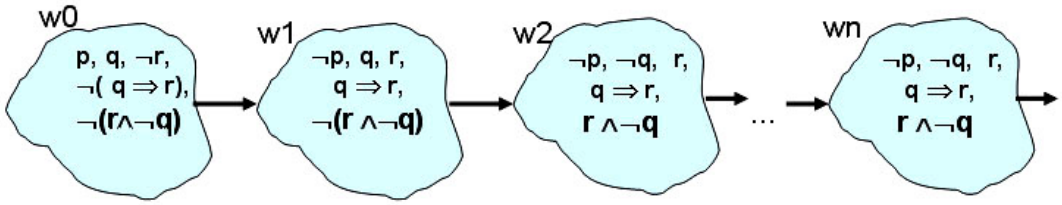

Рис. 5. В каждом мире некоторые пропозициональные формулы истинны, другие – нет

"мирах" упомянутые формулы выполняются, а в каких – нет (они представлены тогда со знаком отрицания '¬').

Очевидно, что на конкретной цепочке миров можно, в принципе, подсчитать и истинность формул, включающих темпоральные операторы. Например, формула r∧¬q истинна, начиная с w2, поэтому в w0 истинна формула q**U**(r∧¬q): действительно, существует такое $i \geq 0$ (равное 2), что до wi истинно q, а начиная с wi истинно r∧¬q (рис. 6).

Определение 3. *Формула линейной темпоральной логики Ф выполняется на последовательности "миров" w0, w1, w2, ..., если Ф истинна в начальном "мире" w0 этой последовательности.*

Такая привязка к начальному моменту времени важна для технических систем: для нас обычно важно знать, будет ли некоторое свойство будущего поведения выполняться в системе, стартующей из *начального* состояния. Это означает, что для приведенной цепочки "*миров*" выполняются формулы p, q, ¬r, ¬(q⇒r), ¬(r∧¬q), q**U**(r∧¬q) и т. д. – именно они истинны в w0.

Итак, линейная темпоральная логика является расширением обычной логики высказываний для рассуждений о бесконечной последовательности "*миров*" (например, дней или лет нашей жизни: "*... в раскаянье бесплодном / Влачил я цепь тяжелых лет ...*"). В последовательности "*миров*" все "*миры*" в цепочке можно считать пронумерованными, и в каждом "*мире*" логические переменные (атомарные предикаты) принимают конкретные истинностные значения – либо истину, либо ложь. Например, сегодня я числюсь студентом и Путин – президент, а завтра я отчислен, Путин уже не президент, а Джейн родит ребенка. Формулы LTL построены из этих атомарных предикатов с помощью булевых операций и темпоральных операторов. Значения истинности обычных булевых формул в каждом конкретном "*мире*" определяются очевидным образом по значениям истинности, которые имеют атомарные предикаты в этом мире. Истинностные значения темпоральных операторов в каждом "*мире*" определяются по значениям истинности их аргументов в цепочке "*миров*", начинающейся с данного конкретного "*мира*".

Темпоральные формулы характеризуют развитие ситуации во времени, они могут использоваться для задания свойств бесконечных процессов. Так, формула **X**p истинна, если в следующем "*мире*" (например, на следующий день) утверждение p будет истинным. Формула p**U**q истинна в текущем "*мире*", если q уже истинно в этом "*мире*", или p

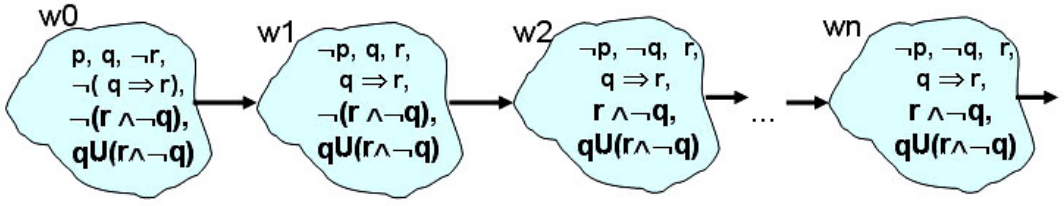

Рис. 6. В каждом мире некоторые темпоральные формулы истинны, другие – нет

истинно в этом "*мире*" и будет истинным во всех будущих "*мирах*", до тех пор пока не станет истинным q. В логике LTL через темпоральный оператор U можно определить темпоральные операторы **F** и **G**. Эти операторы называются "выводимыми" в логике LTL.

Например, формула **F**p истинна в текущем "*мире*" данной цепочки "*миров*", если когда-нибудь в будущем в этой цепочке станет истинным p (возможно, неоднократно). Можно строить и композицию темпоральных операторов. Формула **GF**p истинна в текущем "*мире*", если в любом будущем "*мире*" верно, что в дальнейшем станет истинным p. В "*мирах*", которые идут после тех, в которых p стало истинным, тоже выполняется **F**p, поэтому **GF**p определяет, что в будущем p будет истинным бесконечно много раз. Формула **FG**p истинна, если когда-нибудь в будущем p станет истинным и останется истинным навсегда (свойство стабилизации).

При записи формул темпоральной логики будем считать, что все темпоральные операторы имеют одинаковый приоритет, больший, чем приоритет любой логической операции. Поэтому, например, формулу p**U**q∨Gq,будем понимать, как (p**U**q)∨(**G**q). При сомнениях для более ясной записи и выделения структуры формул рекомендуется использовать скобки.

Пример 4. Рассмотрим несколько примеров формализации высказываний естественного языка. Такую формализацию зачастую можно выполнить по-разному, поскольку высказывания естественного языка не всегда однозначны.

a) Формализуем известное латинское изречение "*Dum spiro, spero"* (*пока живу, надеюсь)*. Его нельзя представить простой импликацией "*Если я жив, то я надеюсь"* (формально: *Я_жив* ⇒ *Я_надеюсь*), поскольку формула p⇒q показывает связь двух атомарных утверждений p и q только в текущий момент. Утверждение "*Пока живу, надеюсь"* говорит, что я буду надеяться *всегда*, пока буду жив. Поэтому более точно его смысл передает такая формула LTL:

G(*Я_жив* ⇒ *Я_надеюсь*).

"*Сейчас и всегда в будущем, если я буду жив, я буду надеяться*.

Подобно этому, утверждение "*Пока сердце бьется, я буду бороться*!" формализуется так:

G(*Сердце_бьется* ⇒ *Я_борюсь*).

b) Несколько другой смысл имеет утверждение "*Мы будем бороться, пока не победим*". Его можно формализовать так:

Мы_боремся **U** *Мы_победили.*

В соответствие с этой формулой, борьба может продолжаться и после победы, что обычно и случается. Эта формализация предполагает уверенность говорящего в будущей победе. Если такой уверенности нет, то утверждение следует формализовать так:

(*Мы_боремся* **U** *Мы_победили*) ∨ **G** *Мы_боремся.*

В этой формуле нашла отражение мысль: *мы все равно будем бороться, даже если и не победим*. В темпоральной логике иногда используется оператор **W**, так называемый "слабый Until", имеющий именно эту семантику:

p**W**q ≡ (p**U**q)∨**G**p.

С использованием слабого Until утверждение "*Мы будем бороться, пока не победим*" формализуется так:

Мы_боремся **W** *Мы_победили*

Эта формула утверждает, что мы боремся сейчас, будем бороться и дальше, пока не победим, и даже если победы не будет, мы все равно будем бороться.

c) Англоязычные документы часто снабжаются припиской: "*Not valued until signed*" – "*не действителен до тех пор, пока не подписан*". Эту фразу точно передает формула:

Документ_не_действителен **W** *Документ_подписан.*

Здесь используется слабый Until, поскольку нет гарантий того, что документ будет действительно подписан. Если гарантировано, что документ будет подписан (например, паспорт обязательно подписывается владельцем при получении), то эту фразу можно формально представить оператором Until:

Документ_не_действителен **U** *Документ_подписан.*

Эта формула утверждает, что пока документ не подписан, он не действителен, но ничего не говорит о том, что будет после подписания.

d) Если обозначить буквой p утверждение "*Я твоя!*", то **G**p означает *"Я твоя навеки!"*.

e) Утверждение *"Мы придем к победе коммунистического труда!"* формально запишется так:

F *Коммунистический_труд_победил!*

f) Строфе из песни В.Бахнова *"Сегодня он играет джаз, а завтра Родину продаст"*, если ее понимать буквально, соответствует формула:

Он_играет_джаз $\Rightarrow$ **X***Он_продает_Родину.*

Но, по-видимому, поэт имел в виду более общий смысл:

G(*Он_играет_джаз* $\Rightarrow$ **X***Он_продает_Родину*) -

"*если когда-нибудь парень начнет играть джаз, то на следующий день он пойдет продавать Родину*".

Однако, возможно, поэт хотел этой фразой передать еще более общую мысль: "*если когда-нибудь парень начнет играть джаз, то потом, рано или поздно, он обязательно продаст Родину*". В этом случае он мог бы сказать точно и прямо (хотя и не совсем в рифму):

G(*Он_играет_джаз* $\Rightarrow$ **XF***Он_продает_Родину*).

g) Пусть p означает "*Я люблю Машу*", а q –"*Я люблю Дашу*". Тогда:

Fp – *"Я когда-нибудь обязательно полюблю Машу";*

Gq – *"Я люблю Дашу и буду любить ее всегда";*

G($\neg$p$\vee\neg$q) – *"Я однолюб, и никогда не буду любить и Машу, и Дашу одновременно";*

q**U**p – *"В будущем я полюблю Машу, а до той поры я буду любить Дашу";*

FGp – *"Когда-нибудь я полюблю Машу навечно";*

GFq– *"Я буду бесконечно влюбляться в Дашу"*.

h) Рекламный слоган "*Раз Персил – всегда Персил*" не совсем ясен простому человеку. Что значит – "*Раз Персил*"?

По-видимому, рекламодатели хотели сказать, что если только кто-нибудь попробует Персил, то с этого момента он уже не сможет от Персила отказаться, то есть будет им пользоваться всегда. Но тогда абсолютно точно смысл этого слогана выражает следующая формула логики LTL:

G(*Персил* $\Rightarrow$ **G***Персил*).

Очевидно, что подобными точными формулами и надо рекламировать товары.

Итак, темпоральные формулы могут конечным образом характеризовать свойства бесконечных процессов, имеющих поведение по времени, разворачивающихся во времени в последовательности "*миров*", или состояний, если снабдить "*миры*" (каждую статическую ситуацию в дискретной последовательности таких ситуаций) конечным набором атомар-

ных утверждений, принимающих только два значения – *истина* или *ложь* в каждом из "*миров*". Атомарные утверждения сами не включают время, в каждом "*мире*" их истинностное значение статично, неизменно. Но в другом "*мире*" эти значения могут быть другими.

Введенные выше последовательности "*миров*" можно считать моделью функционирования технических систем. Каждый "*мир*" может представлять состояние системы, а переходы – изменения состояний. Как внешнее воздействие, так и реакцию системы можно включить в ее состояние. В качестве атомарных предикатов могут использоваться любые утверждения, имеющие значение *истина* или *ложь* в состояниях системы, например: "*переменная x положительна*" (x>0), "*очередь заявок к ресурсу пуста*" (q=0), "*подтверждение посылки сообщения получено*" (*request =true*). Имя состояния, в котором может находиться дискретная система (например, метка оператора), также может быть атомарным предикатом. Атомарный предикат, принимающий истинное значение, когда модуль M находится в состоянии s, можно записать как 'M@s', или, если имя модуля очевидно, то '@s'.

Темпоральная логика оказалось очень эффективной для спецификации требований к поведению реагирующих систем, особенно для параллельных и распределенных систем, в которых именно упорядоченность событий выражает свойства их корректного поведения. Например, требование взаимного исключения параллельных процессов формулируется просто: $\mathbf{G}\neg(@crint_1 \wedge @crint_2)$ – "*два процесса никогда одновременно не будут находиться в своих критических интервалах*".

Пример 5. Рассмотрим примеры записи некоторых требований к вычислениям реагирующих систем с помощью формул LTL.

$\mathbf{G}(q \Rightarrow \mathbf{XG}\neg q)$ – *q встретится в будущем не более одного раза,*

$\mathbf{F}q \wedge \mathbf{G}(q \Rightarrow \mathbf{XG}\neg q)$ – *q встретится в будущем точно один раз,*

$\mathbf{G}(p \Rightarrow p\mathbf{U}q)$ – *всегда если запрос p будет подан, реакция q на него обязательно будет получена, а до ее получения запрос p не сбросится.*

$\mathbf{F}q \Rightarrow (\neg p)\mathbf{U}q$ – *событие p не выполнится до наступления события q.*

Литература

1. *H. Reichenbach.* Elements of symbolic logic. New York: Macmillan, 1947.
2. *A. Prior.* Past, present and future // Oxford University Press, 1967.
3. *A. Pnueli.* The temporal logic of program // Proc. of the 18th Anny. Symp. on Foundation of Computer Science, 1977.

Abstract

Linear temporal logic (LTL) is presented and its formulas are explained by numerous examples. It is demonstrated how behavior properties of discrete dynamic systems, in particular reactive systems, may be presented in LTL. The paper is a brief exposition of a chapter from the author's book «Model checking. Verification of parallel and distributed programs», to be published at BHV St. Petersburg Publishing office.

Карпов Юрий Глебович,
доктор технических наук,
профессор, заведующий кафедрой
«Распределённые вычисления и
компьютерные сети»
Санкт-Петербургского
Политехнического Университета,

karpov@dcn.infos.ru