Моделирование и анализ информационных систем. Т. 26, № 3 (2019), с. 332–350
Modeling and Analysis of Information Systems. Vol. 26, No 3 (2019), pp. 332–350

DOI: 10.18255/1818-1015-2019-3-332-350

УДК 519.71

Формальная верификация диаграмм троичных цифровых сигналов

Куцак Н. Ю., Подымов В. В.

Поступила в редакцию 28 июня 2019
После доработки 2 сентября 2019
Принята к публикации 4 сентября 2019

Аннотация. В работе исследуется задача формальной верификации (математически строгой проверки правильности) диаграмм цифровых сигналов, используемых на практике на ранних стадиях разработки микроэлектронных цифровых устройств (цифровых схем). Отправной точкой разработки схемы, согласно современным методам проектирования, является её описание на каком-либо высокоабстрактном языке описания аппаратуры (hardware description language, HDL). Обязательным этапом разработки HDL-кода схемы является отладка этого кода, схожая по устройству и важности с отладкой программ. Один из популярных способов отладки HDL-кода основан на получении и проверке правильности диаграммы сигналов, то есть совокупности графиков сигналов: функций, описывающих изменение значений в выделенных местах схемы в реальном времени. В работе предлагаются математические средства автоматизации проверки правильности таких диаграмм, основанные на понятиях и методах верификации систем относительно формул темпоральных логик и учитывающие такие характерные особенности сигналов в HDL и соответствующих свойств правильности диаграмм в неформальном смысле, как реальное время, троичность и наличие точек фронтов. Троичность сигнала означает, что наряду с основными логическими значениями 0 и 1 сигнал может принимать и неопределённое значение: одно из значений 0 и 1, но неизвестно или неважно, какое именно. Точкой фронта называется момент изменения значения сигнала. В работе предлагаются понятия, утверждения и алгоритмы, предназначенные для формализации и решения задачи верификации диаграмм сигналов: определения сигналов и диаграмм, учитывающие упомянутые характерные особенности сигналов; темпоральная логика, предназначенная для описания свойств диаграмм сигналов, и соответствующая постановка задачи верификации диаграмм; метод решения предлагаемой задачи верификации, основанный на сведении к задачам преобразования и анализа сигналов; соответствующий алгоритм верификации диаграмм с обоснованием корректности и “приемлемой” оценкой сложности.

Ключевые слова: формальная верификация, цифровой сигнал, темпоральная логика, троичная логика

Для цитирования: Куцак Н. Ю., Подымов В. В., "Формальная верификация диаграмм троичных цифровых сигналов", *Моделирование и анализ информационных систем*, **26**:3 (2019), 332–350.

Об авторах:
Куцак Нина Юрьевна, orcid.org/0000-0002-0832-3635, студент бакалавриата,
Московский государственный университет имени М.В. Ломоносова, факультет ВМК,
Ленинские горы, 1, стр. 52, г. Москва, ГСП-1, 119991 Россия, e-mail: nina_svetik@mail.ru

Подымов Владислав Васильевич, orcid.org/0000-0002-2041-7634, канд. физ.-мат. наук, научный сотрудник,
Московский государственный университет имени М.В. Ломоносова, факультет ВМК,
Ленинские горы, 1, стр. 52, г. Москва, ГСП-1, 119991 Россия, e-mail: valdus@yandex.ru

Благодарности:
Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-01-00854.

Введение

Данная работа представляет собой попытку применения методов формальной верификации [1] (математически строгой проверки правильности выполнения систем) для формализации и автоматизации одного из этапов разработки цифровых микроэлектронных устройств (цифровых схем) [2]. Отправной точкой проектирования цифровой схемы, согласно современным подходам, является разработка её функционала на каком-либо языке описания аппаратуры (hardware description language, HDL) [2] на высоком уровне абстракции, не учитывающем многие физические и технологические особенности схем. Обязательным этапом разработки HDL-кода схемы является отладка этого кода, схожая с отладкой программ, но основанная на понятиях и типах данных, характерных для схем. Основным таким понятием является цифровой сигнал: функция, описывающая изменение логических значений (1 и 0; истина и ложь; высокий и низкий уровни напряжения в заданном месте схемы) в реальном времени. Сигналы в рамках HDL могут принимать и другие значения, например: неопределённое значение, то есть одно из значений 0, 1, но неизвестно или неважно, какое именно; значение высокого импеданса, то есть физически изолированная точка схемы; арифметические значения в двоичной записи для совокупностей сигналов. В данной работе рассматриваются сигналы, принимающие три значения: 0, 1 и $*$. Значение $*$ трактуется как неопределённость в упомянутом смысле, а также как полноценное независимое третье значение сигнала. Соответствующим двояким образом трактуется и троичность сигналов.

Один из популярных способов отладки HDL-описания схемы устроен следующим образом. Разрабатывается показательное семейство наборов значений входных сигналов, то есть тестовое покрытие. Выполняется симуляция схемы на элементах покрытия подходящим программным средством: вычисление значений выходных сигналов согласно особой семантике языка, реализованной в средстве. В результате симуляции вычисляется диаграмма сигналов: совокупность графиков, описывающих изменение значений сигналов в выделенных местах схемы в действительном (реальном) модельном времени. Полученная диаграмма изучается экспертом на предмет правильности: соответствия поведения схемы, представленного в диаграмме, ожидаемому. Основной целью работы является разработка математических средств, пригодных для автоматизации такой проверки правильности диаграмм.

Для наглядности рассмотрим в качестве примера D-триггер [2]: однобитовую схемную ячейку памяти, используемую практически во всех нетривиальных цифровых схемах. D-триггер содержит два входных сигнала (in, clk) и один выходной сигнал (out), и его функционирование можно коротко описать так: каждый раз, когда значение clk изменяется с 0 на 1 (то есть наступает так называемый передний фронт сигнала), в триггере сохраняется текущее значение in; значение out всегда совпадает с последним сохранённым значением. Пример диаграммы, которую можно получить в результате программной симуляции правильного HDL-кода D-триггера, приведён на рисунке 1. В этой диаграмме по горизонтали отложена шкала реального времени, и по строкам изображены графики сигналов in, clk и out. Нижний, средний и верхний уровни строк соответствуют значениям 0, $*$ и 1. Вертикальные линии соответствуют мгновенным изменениям значений сигналов (фронтам). Отметим, что неопределённое значение сигнала out на рисунке 1 возникает по трём причинам:

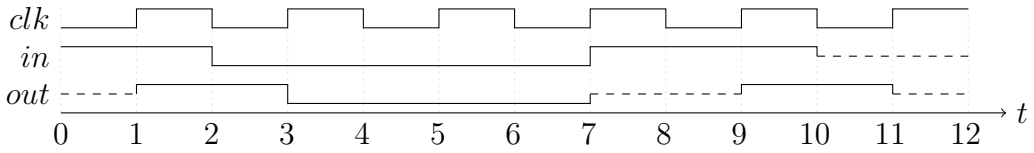

Рис. 1. Диаграмма сигналов D-триггера
Fig. 1. A waveform of a D flip-flop

до первого переднего фронта сигнала clk значение, сохранённое в триггере, произвольно; если значение сигнала in в момент переднего фронта clk не определено, то и сохраняемое значение не определено; если сигнал in в момент переднего фронта clk изменяет своё значение, то может сохраниться как значение до изменения, так и после (это известный схемный эффект, называемый метастабильностью [2]).

Отправной точкой формальной верификации диаграммы сигналов является запись свойства правильности на формальном языке. Как видно из рассмотренного примера, в подходящем формальном языке требуется иметь средства рассуждения о взаимосвязи логических значений во времени. Такие средства содержатся в языках темпоральных логик [1]. Наиболее популярные темпоральные логики, как правило, принадлежат одному из двух широких классов: логики дискретного времени, в которых время описывается множеством целых чисел, и логики реального времени, в которых время описывается множеством действительных чисел. При использовании дискретных логик для верификации схема обычно заменяется конечным автоматом, выполняющим переходы в моменты передних фронтов выбранного (тактового) сигнала. В исследованиях встречается широкий спектр вариаций такой замены, и с основными идеями таких вариаций можно ознакомиться, например, в [2–5] (в том числе с использованием троичности — в [6]). Такая замена без потери полноты описания поведения возможна только для синхронных схем [2]: изменяющих своё состояние только по указанным фронтам единственного тактового сигнала. Для остальных схем (асинхронных) применение такого подхода сопряжено с дополнительным анализом схемы и потерей точности описания её поведения. Темпоральные логики реального времени, основанные на понятиях сигнала, наиболее близких к используемому на практике в диаграммах, предлагаются в [7, 8]. В этих работах рассматриваются двоичные сигналы, и кроме того, в предлагаемых языках отсутствуют средства рассуждения о фронтах сигналов, и из-за этого предлагаемые языки практически непригодны для верификации диаграмм сигналов: значение $*$ часто встречается в диаграммах, и неопределённость либо произвольность — в рассуждениях о правильности диаграмм, и даже в таких простых схемах, как D-триггер, требуются средства рассуждения о фронтах сигналов.

В работе предлагаются: формальный язык (темпоральная логика), предназначенный для записи свойств диаграмм троичных сигналов и содержащий, в числе прочего, средства записи высказываний о моментах фронтов сигналов; сопутствующий набор понятий, включая строгие определения троичного сигнала и диаграммы; постановку и конструктивное алгоритмическое решение задачи верификации диаграмм относительно формул предлагаемой логики. Текст работы имеет следующую структуру. В разделе 1 обсуждаются понятия и обозначения, не относящиеся непосредственно к цифровым сигналам и предлагаемому языку. В разделе 2 вводятся

x	$\neg x$
0	1
$*$	$*$
1	0

$x \vee y$		y		
		0	$*$	1
	0	0	$*$	1
x	$*$	$*$	$*$	1
	1	1	1	1

$x \leftrightarrow y$		y		
		0	$*$	1
	0	1	$*$	0
x	$*$	$*$	$*$	$*$
	1	0	$*$	1

$x \Leftrightarrow y$		y		
		0	$*$	1
	0	1	0	0
x	$*$	0	1	0
	1	0	0	1

$x \sqsubseteq y$		y		
		0	$*$	1
	0	1	0	0
x	$*$	1	1	1
	1	0	0	1

Рис. 2. Таблицы значений троичных функций
Fig. 2. Value tables of three-valued functions

основные определения и обозначения, относящиеся к троичным сигналам и диаграммам. В разделе 3 предлагаются синтаксис и семантика формул логики, предназначенной для записи свойств правильности диаграмм и для ясности названной логикой троичных сигналов, и строгая постановка задачи верификации диаграмм. В разделе 4 вводится альтернативная семантика формул, позволяющая переформулировать задачу верификации диаграмм как задачу преобразования и анализа сигналов. Соответствующий решающий алгоритм с обоснованием корректности и грубой оценкой сложности приведён в разделе 5. Наконец, в разделе 6 обсуждается набор операций, выразимых в логике троичных сигналов, и приводятся примеры формул, выражающих правильность диаграмм несложных "реальных" схем.

1. Общие обозначения

Записями $\mathbb{N}$, $\mathbb{N}_0$ и $\mathbb{R}$ обозначим соответственно множества всех натуральных чисел, всех целых неотрицательных чисел и всех действительных чисел. В работе используются следующие виды *интервалов* (конечные интервалы действительных чисел): $(x, y) = \{z \mid z \in \mathbb{R}, x < z < y\}$; $[x, y) = \{z \mid z \in \mathbb{R}, x \leq z < y\}$; $(x, y] = \{z \mid z \in \mathbb{R}, x < z \leq y\}$; $[x, y] = \{z \mid z \in \mathbb{R}, x \leq z \leq y\}$. Также в работе используются *диапазоны* целых неотрицательных чисел: $[x..y] = \{z \mid z \in \mathbb{N}_0, x \leq z \leq y\}$.

Рассмотрим произвольную функцию $f : X \to Y$. Записью $f^{-1}(y)$ обозначим множество $\{x \mid x \in X, f(x) = y\}$. Записью $f\langle Z\rangle \sim v$, где $Z \subseteq X$ и $\sim$ — равенство ($=$) или неравенство ($\neq$), обозначим следующий факт: для каждого элемента z множества Z верно $f(z) \sim y$. Будем говорить, что значение функции f *постоянно* на множестве Z, $Z \subseteq X$, если существует значение y, $y \in Y$, такое что $f\langle Z\rangle = y$.

Записью $\mathfrak{T}$ обозначим множество $\{0, 1, *\}$. Это множество будет использоваться в двух смыслах. В широком смысле, $\mathfrak{T}$ — множество значений, которыми оперируют троичные функции [9]. В узком смысле, $\mathfrak{T}$ — множество истинностных значений троичной логики Клини [10, 11], согласно которой 0 трактуется как *ложь*, 1 — как *истина*, и $*$ — как *неопределённое* значение: либо истина, либо ложь, но неизвестно или неважно, что именно. *Троичной функцией* (местности n, где $n \in \mathbb{N}$) называется функция вида $\mathfrak{f} : \mathfrak{T}^n \to \mathfrak{T}$. На рисунке 2 изображены таблицы значений троичных функций, использующихся в разделах 3 и 6: отрицание ($\neg$), дизъюнкция ($\vee$) и равносильность ($\leftrightarrow$) логики Клини; равносильность алгебры троичных функций ($\Leftrightarrow$); функция $\sqsubseteq$, означающая, что левый аргумент можно доопределить до правого.

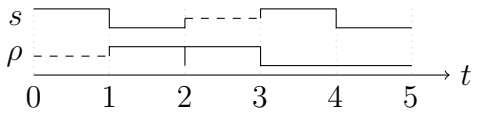

Рис. 3. График сигнала (s) и заготовки, не являющейся сигналом (ρ)
Fig. 3. Plots of a signal (s), and a non-signal preform (ρ)

2. Троичные цифровые сигналы

Далее полагаются заданными действительные чи́сла $\mathbf{a}$ и $\mathbf{b}$, задающие область определения $(\mathbf{a}, \mathbf{b})$ рассматриваемых сигналов. Чи́сла интервала $[\mathbf{a}, \mathbf{b}]$ назовём *моментами времени*, а также *точками* (временно́й оси). Точки интервалов $[\mathbf{a}, \mathbf{b})$, $(\mathbf{a}, \mathbf{b}]$ и $(\mathbf{a}, \mathbf{b})$ будем называть соответственно *левыми*, *правыми* и *внутренними*.

Записью $\mathfrak{T}_\updownarrow$ обозначим множество $\mathfrak{T} \cup \{\updownarrow\}$, где $\updownarrow$ — *фронтальное* значение, $\updownarrow \notin \mathfrak{T}$. *Сигнальной функцией* назовём отображение вида $\chi : (\mathbf{a}, \mathbf{b}) \to \mathfrak{T}_\updownarrow$. Будем говорить, что функция χ имеет значение v *справа от левой точки* ℓ, если существует точка t, такая что $\ell < t$ и $\chi\langle(\ell, t)\rangle = v$, и имеет значение v *слева от правой точки* r, если существует точка t, такая что $t < r$ и $\chi\langle(t, r)\rangle = v$. Значения χ справа и слева от точки t обозначим записями $\chi(t+0)$ и $\chi(t-0)$ соответственно. Сигнальную функцию ρ назовём *заготовкой* троичного цифрового сигнала, если множество $\rho^{-1}(\updownarrow)$ конечно и на каждом интервале $\mathcal{I}$, таком что $\rho\langle\mathcal{I}\rangle \neq \updownarrow$, значение ρ постоянно. Пусть $\rho^{-1}(\updownarrow) = \{t_1, \ldots, t_k\}$, где $t_1 < \cdots < t_k$. Точку t_i назовём *точкой i-го фронта* заготовки ρ. Записью $|\rho|$ обозначим общее число точек фронтов ρ: $|\rho| = k$. Точки $\mathfrak{t}_i^\rho$, $i \in [0..k+1]$, определим так: $(\mathfrak{t}_0^\rho, \mathfrak{t}_1^\rho, \ldots, \mathfrak{t}_k^\rho, \mathfrak{t}_{k+1}^\rho) = (\mathbf{a}, t_1, \ldots, t_k, \mathbf{b})$. Записями $\mathfrak{I}_i^\rho$ и $\mathfrak{v}_i^\rho$, $i \in [0..k]$, обозначим соответственно интервал $(\mathfrak{t}_i^\rho, \mathfrak{t}_{i+1}^\rho)$ и значение из $\mathfrak{T}$, такое что $\rho\langle\mathfrak{I}_i^\rho\rangle = \mathfrak{v}_i^\rho$. Отметим, что каждое значение $\mathfrak{v}_i^\rho$ существует и единственно, так как значение функции ρ на каждом интервале $\mathfrak{I}_i^\rho$ постоянно и множество $\rho^{-1}(\updownarrow)$ конечно.

Пример 1. На рисунке 3 изображены графики заготовок s и ρ на интервале $(0, 5)$, определяемых так: $|s| = 4$, $(\mathfrak{t}_0^s, \ldots, \mathfrak{t}_5^s) = [0..5]$, $\mathfrak{I}_i^s = (i, i+1)$, где $i \in [0..4]$, и $(\mathfrak{v}_0^s, \ldots, \mathfrak{v}_4^s) = (1, 0, *, 1, 0)$; $|\rho| = 3$, $(\mathfrak{t}_0^\rho, \ldots, \mathfrak{t}_4^\rho) = (0, 1, 2, 3, 5)$, $\mathfrak{I}_i^\rho = (i, i+1)$, где $i \in [0..2]$, $\mathfrak{I}_3^\rho = (3, 5)$ и $(\mathfrak{v}_0^\rho, \mathfrak{v}_1^\rho, \mathfrak{v}_2^\rho, \mathfrak{v}_3^\rho) = (*, 1, 1, 0)$. Значения 0, $*$ и 1 соответствуют нижнему, среднему (пунктирному) и верхнему уровням графиков. Вертикальные линии соответствуют значению $\updownarrow$.

Утверждение 1. *Для любых заготовки ρ, точки t и индекса i, $i \in [0..|\rho|]$, справедливо следующее:*

1. $[\mathbf{a}, \mathbf{b}] \setminus (\mathfrak{I}_0^\rho \cup \cdots \cup \mathfrak{I}_{|\rho|}^\rho) = \{\mathfrak{t}_0^\rho, \ldots, \mathfrak{t}_{|\rho|+1}^\rho\}$.
2. *Если* $t \in \mathfrak{I}_i^\rho$, *то* $\rho(t-0) = \rho(t) = \rho(t+0) = \mathfrak{v}_i^\rho$.
3. *Если* $t = \mathfrak{t}_i^\rho$, *то* $\rho(t+0) = \mathfrak{v}_i^\rho$.
4. *Если* $t = \mathfrak{t}_{i+1}^\rho$, *то* $\rho(t-0) = \mathfrak{v}_i^\rho$.

Доказательство. Пункт 1 следует из определений $\mathfrak{t}_0^\rho, \ldots, \mathfrak{t}_{|\rho|+1}^\rho$ и $\mathfrak{I}_0^\rho, \ldots, \mathfrak{I}_{|\rho|}^\rho$. Если $t \in [\mathfrak{t}_i^\rho, \mathfrak{t}_{i+1}^\rho)$, то $\rho(t+0) = \rho\langle(t, \mathfrak{t}_{i+1}^\rho)\rangle = \rho\langle(\mathfrak{t}_i^\rho, \mathfrak{t}_{i+1}^\rho)\rangle = \mathfrak{v}_i^\rho$. Если $t \in (\mathfrak{t}_i^\rho, \mathfrak{t}_{i+1}^\rho]$, то $\rho(t-0) = \rho\langle(\mathfrak{t}_i^\rho, t)\rangle = \rho\langle(\mathfrak{t}_i^\rho, \mathfrak{t}_{i+1}^\rho)\rangle = \mathfrak{v}_i^\rho$. Если $t \in (\mathfrak{t}_i^\rho, \mathfrak{t}_{i+1}^\rho)$, то $\rho(t) = \rho\langle(\mathfrak{t}_i^\rho, \mathfrak{t}_{i+1}^\rho)\rangle = \mathfrak{v}_i^\rho$. □

Следствие. *Для любых заготовки ρ, левой точки ℓ и внутренней точки t, такой что $t \neq \updownarrow$, существуют единственные индексы i, j диапазона $[0..|\rho|]$, такие что $\ell \in [\mathfrak{t}^\rho_i, \mathfrak{t}^\rho_{i+1})$ и $t \in (\mathfrak{t}^\rho_j, \mathfrak{t}^\rho_{j+1})$.*

Для обозначения индексов i, j последнего следствия будем использовать соответственно записи $[\ell + 0]$ и $[t]$ на месте индекса m в задании точек $\mathfrak{t}^\rho_m$, значений $\mathfrak{v}^\rho_m$ и интервалов $\mathfrak{I}^\rho_m$. Троичным цифровым *сигналом* назовём заготовку s, такую что $\mathfrak{v}^s_{i-1} \neq \mathfrak{v}^s_i$ для всех i, $i \in [1..|s|]$. *Диаграммой* сигналов над конечным множеством *переменных* Var назовём отображение $D : \mathsf{Var} \to \mathfrak{S}$, где $\mathfrak{S}$ — множество всех сигналов. Множество Var далее полагаем заданным по умолчанию.

Пример 2. Заготовка ρ из примера 1 не является сигналом, так как $\mathfrak{v}^\rho_1 = \mathfrak{v}^\rho_2 = 1$. Заготовка s из того же примера является сигналом.

Упорядочим множество $\mathfrak{T}$: $0 < * < 1$. *Точкой переднего* (*заднего*) *фронта* сигнала s назовём точку фронта $\mathfrak{t}^s_i$, такую что $\mathfrak{v}^s_{i-1} < \mathfrak{v}^s_i$ ($\mathfrak{v}^s_{i-1} > \mathfrak{v}^s_i$). Тот факт, что t является точкой переднего фронта сигнала s, будем записывать в следующем виде: $s(t) = \uparrow$. Для произвольной точки t записью $next_\uparrow(s, t)$ обозначим точку t' переднего фронта, *следующего* за t в s: $t < t'$; $s(t') = \uparrow$; $s\langle(t, t')\rangle \neq \uparrow$. *Тактом* сигнала s назовём интервал (ℓ, r), такой что: $\ell < r$; $\ell = \mathbf{a}$ или $s(\ell) = \uparrow$; $r = \mathbf{b}$ или $s(r) = \uparrow$; $s\langle(\ell, r)\rangle \neq \uparrow$. Такт (ℓ, r) назовём *тактом точки* t и обозначим записью $C(s, t)$, если $t \in [\ell, r)$.

3. Формулы и задача верификации

В данном разделе предлагается *логика троичных сигналов*, включающая в себя синтаксис и семантику формул, предназначенных для описания свойств диаграмм, и постановку задачи верификации диаграмм. Синтаксис *формул* (над множеством переменных Var) зададим следующей формой Бэкуса-Наура:

$$\varphi \ ::= \ 1 \ \mid \ * \ \mid \ x \ \mid \ \mathfrak{f}(\varphi_1, \ldots, \varphi_k) \ \mid \ (\varphi_1 \oplus \varphi_2) \ \mid \ (\circlearrowleft \varphi_1),$$

где $\varphi, \varphi_1, \varphi_2, \ldots, \varphi_k$ — формулы, $x \in \mathsf{Var}$, $\mathfrak{f}$ — k-местная троичная функция, $\oplus \in \{\mathbf{U}, \mathbf{C}, \mathbf{X}\}$ — двуместный темпоральный оператор и $\circlearrowleft$ — одноместный *оператор отражения*. Перечисленные функции и операторы будем называть *сигнальными операциями*. В записи формул иногда будем использовать инфиксную нотацию для троичных функций и опускать внешнюю пару скобок, а также другие пары скобок согласно приоритетам операций: наиболее приоритетны одноместные операции; затем $\mathbf{U}$, $\mathbf{C}$ и $\mathbf{X}$; затем остальные троичные функции с обычными приоритетами.

Заметим, что сигнал s может трактоваться как описание изменения истинностного значения формулы в реальном времени: $s(t \pm 0)$ — как истинность, ложность или неопределённость до и после точки t; $s(t)$ — как обозначение постоянства (стабильности) значения в точке t, если $s(t) \in \mathfrak{T}$, и непостоянства (нестабильности), если $s(t) = \updownarrow$. При этом сигнал однозначно задаётся спектром истинностных значений справа от всех внутренних точек, что обосновывается следующим утверждением.

Утверждение 2. *Для любых сигнала s, внутренней точки t и правой точки r и для сигнальной функции s^{+0}, определяемой тождеством $s^{+0}(t) = s(t + 0)$, верно следующее:*

1. *Если $s(t - 0) = s(t + 0)$, то $s(t) = s^{+0}(t)$, а иначе $s(t) = \updownarrow$.*

2. Существует точка ℓ, такая что $\ell < r$ и $s(r-0) = s^{+0}\langle(\ell, r)\rangle$.

Доказательство. Пункт 1 следует из утверждения 1 и определения сигнала.
Пункт 2. Пусть $\mathfrak{I}^s_{[r-0]} = \mathfrak{I}^s_i$. По утверждению 1, для любой точки t' интервала $\mathfrak{I}^s_i$ верно $s^{+0}(t') = s(t'+0) = \mathfrak{v}^s_i = s(r-0)$. Значит, $s^{+0}\langle(\mathfrak{t}^s_i, r)\rangle = s^{+0}\langle\mathfrak{I}^s_i\rangle = s(r-0)$, и при этом $\mathfrak{t}^s_i < r$. □

Отразим упомянутую выше трактовку сигналов и свойства, сформулированные в утверждении 2, в *логической семантике* формул. Сопоставим каждой формуле φ, диаграмме D и левой точке ℓ значение $\varphi[D, \ell+0]$ множества $\mathfrak{T}$, которое будем называть *значением формулы* φ на диаграмме D *справа от левой точки* ℓ. В определении будем использовать вспомогательные виды значений φ на D:

- Значение *слева от правой точки* r:
$$\varphi[D, r-0] = \begin{cases} v, & \text{если } \exists \ell \in [\mathbf{a}, r) : \forall t \in (\ell, r) : \varphi[D, t+0] = v \in \mathfrak{T}; \\ * & \text{в остальных случаях.} \end{cases}$$
- Значение *во внутренней точке* t:
$$\varphi[D, t] = \begin{cases} \varphi[D, t+0], & \text{если } \varphi[D, t-0] = \varphi[D, t+0]; \\ \updownarrow & \text{в остальных случаях.} \end{cases}$$
- Значение *на интервале* $\mathcal{I}$: $\varphi[D, \mathcal{I}] \sim v \Leftrightarrow$ для любой точки t интервала $\mathcal{I}$ верно $\varphi[D, t] \sim v$, где $\sim$ — равенство $(=)$ или неравенство $(\neq)$.

В описании семантики формул понадобятся обобщения понятий переднего фронта и такта с сигналов на формулы. Для формулы φ, диаграммы D и внутренней точки t записью $\varphi[D, t] = \uparrow$ обозначим следующий факт: $\varphi[D, t-0] < \varphi[D, t+0]$. Содержательное прочтение: формула φ *становится достовернее* на D в t или, по-другому, t — *точка переднего фронта* формулы φ на D. Записью $next_{\uparrow}(\varphi, D, t)$, где t — произвольная точка, обозначим передний фронт t' формулы φ, *следующий* за t на D: $t < t'$; $\varphi[D, t'] = \uparrow$; $\varphi[D, (t, t')] \neq \uparrow$. *Тактом* формулы φ на D назовём интервал (ℓ, r), такой что: $\ell < r$; $\ell = \mathbf{a}$ или $\varphi[D, \ell] = \uparrow$; $r = \mathbf{b}$ или $\varphi[D, r] = \uparrow$; $\varphi[D, (\ell, r)] \neq \uparrow$. Записью $C(\varphi, D, t)$ обозначим такт (ℓ, r) формулы φ на D, такой что $t \in [\ell, r)$.

Отражением точки t, *сигнала* s и *диаграммы* D назовём соответственно точку $t^{\circlearrowleft}$, сигнал $s^{\circlearrowleft}$ и диаграмму $D^{\circlearrowleft}$, определяемые тождествами $t^{\circlearrowleft} = (\mathbf{a} + \mathbf{b} - t)$, $s^{\circlearrowleft}(t) = s(t^{\circlearrowleft})$ и $D^{\circlearrowleft}(x) = D(x)^{\circlearrowleft}$.

Утверждение 3. *Для любого сигнала s существует единственный сигнал $s^{\circlearrowleft}$.*

Доказательство. Единственность следует из того, что для любого сигнала s и любой внутренней точки t значение $s(t^{\circlearrowleft})$ определено однозначно.
Существование. Рассмотрим такую заготовку ρ: $\rho^{-1}(\updownarrow) = \{t^{\circlearrowleft} \mid t \in s^{-1}(\updownarrow)\}$; $\mathfrak{v}^{\rho}_i = \mathfrak{v}^s_{|s|-i}$, $i \in [0..|s|]$. Верны соотношения $\mathfrak{v}^{\rho}_{i-1} = \mathfrak{v}^s_{|s|-i+1} \neq \mathfrak{v}^s_{|s|-i} = \mathfrak{v}^{\rho}_i$, $i \in [1..|\rho|]$, а значит, ρ — сигнал. Рассмотрим произвольную внутреннюю точку t. Если $\rho(t) = \updownarrow$, то $t \in \rho^{-1}(\updownarrow)$, а значит, $t^{\circlearrowleft} \in \{t^{\circlearrowleft} \mid t \in \rho^{-1}(\updownarrow)\} = \{t^{\circlearrowleft\circlearrowleft} \mid t \in s^{-1}(\updownarrow)\} = s^{-1}(\updownarrow)$, то есть $\rho(t) = \updownarrow = s(t^{\circlearrowleft})$. Если $\rho(t) \neq \updownarrow$ и $\mathfrak{I}^{\rho}_{[t]} = \mathfrak{I}^{\rho}_i$, то $t^{\circlearrowleft} \in (\mathfrak{t}^{\rho}_{i+1}{}^{\circlearrowleft}, \mathfrak{t}^{\rho}_i{}^{\circlearrowleft}) = (\mathfrak{t}^s_{|s|-(i+1)}, \mathfrak{t}^s_{|s|-i}) = \mathfrak{I}^s_{|s|-i}$, а значит, $\rho(t) = \rho\langle\mathfrak{I}^{\rho}_i\rangle = \mathfrak{v}^{\rho}_i = \mathfrak{v}^s_{|s|-i} = s\langle\mathfrak{I}^s_{|s|-i}\rangle = s(t^{\circlearrowleft})$. Таким образом, ρ — сигнал, такой что для любой внутренней точки t верно $\rho(t) = s(t^{\circlearrowleft})$, то есть $\rho = s^{\circlearrowleft}$. □

Семантику формул (значение $\varphi[D, \ell+0]$) определим следующими правилами:

- $1[D, \ell+0] = 1$.

- $*[D, \ell + 0] = *$.
- $x[D, \ell + 0] = D(x)(\ell + 0)$, если $x \in \mathsf{Var}$.
- $\mathfrak{f}(\varphi_1, \ldots, \varphi_k)[D, \ell + 0] = \mathfrak{f}(\varphi_1[D, \ell + 0], \ldots, \varphi_k[D, \ell + 0])$.
- $(\varphi \mathbf{U} \psi)[D, \ell + 0] = \begin{cases} 1, & \text{если } \exists t \in (\ell, \mathbf{b}) : \psi[D, t] = (\varphi \vee \psi)[D, (\ell, t)] = 1; \\ *, & \text{если условие выше неверно и} \\ & \quad \exists t \in (\ell, \mathbf{b}) : \psi[D, t] \neq 0 \text{ и } (\varphi \vee \psi)[D, (\ell, t)] \neq 0; \\ 0 & \text{в остальных случаях.} \end{cases}$
- $(\varphi \mathbf{C} \psi)[D, \ell + 0] = \begin{cases} 1, & \text{если } \varphi[D, C(\psi, D, \ell)] = 1; \\ 0, & \text{если } \exists t \in C(\psi, D, \ell) : \varphi[D, t] = 0; \\ * & \text{в остальных случаях.} \end{cases}$
- $(\varphi \mathbf{X} \psi)[D, \ell + 0] = \begin{cases} v, & \text{если } \exists t = next_{\uparrow}(\psi, D, \ell) \text{ и } \varphi[D, t] = v \in \mathfrak{T}; \\ * & \text{в остальных случаях.} \end{cases}$
- $(\circlearrowleft \varphi)[D, \ell + 0] = \varphi[D^{\circlearrowleft}, \ell^{\circlearrowleft} - 0]$.

Содержательное прочтение темпоральных операторов: $\varphi \mathbf{U} \psi$ — ψ станет истинным, а до тех пор будет истинно φ; $\varphi \mathbf{C} \psi$ — φ истинно на текущем такте формулы ψ; $\varphi \mathbf{X} \psi$ — φ будет истинным в момент следующего переднего фронта формулы ψ; $\circlearrowleft \varphi$ — формула φ истинна, если поменять ролями будущее и прошлое (отразить временну́ю ось и все сигналы относительно текущей точки). Строгая семантика и содержательная трактовка оператора $\mathbf{U}$ совмещает в себе семантику и трактовку одноимённого оператора двоичных логик реального времени [1, 7] и троичных логик дискретного времени [12, 13]. Известные нам темпоральные логики реального времени не содержат операторов, сколь-нибудь схожих с операторами $\mathbf{C}$ и $\mathbf{X}$. Известные нам темпоральные логики дискретного времени не содержат операторов, схожих с $\mathbf{C}$, и нередко содержат одноместный оператор $\mathbf{X}$ (“в следующий момент времени”; в некоторых системах обозначений — $\circ$) [1,13], отдалённо похожий на оператор $\mathbf{X}$ логики троичных сигналов, но ввиду отсутствия реального времени и точек фронтов существенно отличающийся и трактовкой, и строгим определением.

Запись $D \models \varphi$ (*формула φ выполняется на диаграмме D*) будем использовать как синоним записи $\varphi[D, \mathbf{a} + 0] = 1$. *Задача верификации*, исследуемая в работе, формулируется так: для заданных диаграммы D и формулы φ проверить справедливость соотношения $D \models \varphi$.

4. Сигнальная семантика формул

Решение задачи верификации основано на подходе к заданию семантики формул, согласно которому каждым формуле φ и диаграмме D сопоставляется сигнал, описывающий изменение значения формулы с течением реального времени. Для произвольных формулы φ и диаграммы D определим функцию $\varphi[[D]] : (\mathbf{a}, \mathbf{b}) \to \mathfrak{T}_{\updownarrow}$ тождеством $\varphi[[D]](t) = \varphi[D, t]$. *Сигнальная семантика* формул определяется этой функцией. Далее в разделе обосновывается корректность сигнальной семантики: доказывается, что функция $\varphi[[D]]$ является сигналом и что значения сигнала $\varphi[[D]]$ и формулы φ на D слева от правой точки и справа от левой точки всегда равны. Предлагаемое решение задачи верификации основано на сведе́нии проверки соотношения $\varphi \models D$ к вычислению и анализу сигнала $\varphi[[D]]$.

Записью $\Delta(\chi_1, \chi_2)$, где χ_1, χ_2 — сигнальные функции, обозначим множество всех внутренних точек t, таких что $\chi_1(t) \neq \chi_2(t)$. Функции χ_1, χ_2 назовём *почти равными*, если множество $\Delta(\chi_1, \chi_2)$ конечно.

Лемма 1. *Для любых почти равных заготовок ρ_1, ρ_2, левой точки ℓ и правой точки r верны равенства $\rho_1(\ell + 0) = \rho_2(\ell + 0)$ и $\rho_1(r - 0) = \rho_2(r - 0)$.*

Доказательство. По определению значения заготовки справа, существуют точки r_1 и r_2, такие что $\ell < r_1$, $\ell < r_2$ и $\rho_1(\ell + 0) = \rho_1\langle(\ell, r_1)\rangle$ и $\rho_2(\ell + 0) = \rho_1\langle(\ell, r_2)\rangle$. Рассмотрим точку r, равную наименьшей из точек r_1, r_2. Множество $\Delta = (\ell, r) \cap \Delta(\rho_1, \rho_2)$ конечно, так как заготовки ρ_1, ρ_2 почти равны. Рассмотрим наименьшую точку t множества Δ. Так как $(\ell, t) \cap \Delta = \emptyset$, $\ell < t$ и $(\ell, t) \subseteq (\ell, r_1) \cap (\ell, r_2)$, верно $\rho_1(\ell + 0) = \rho_1\langle(\ell, t)\rangle = \rho_2\langle(\ell, t)\rangle = \rho_2(\ell + 0)$.

Обоснование равенства $\rho_1(r - 0) = \rho_2(r - 0)$ аналогично. □

Лемма 2. *Для любой заготовки ρ существует единственный почти равный сигнал s.*

Доказательство. Существование. Пусть $m_1 < \cdots < m_k$ — все индексы диапазона $[1..|\rho|]$, такие что $\mathfrak{v}^\rho_{m_j-1} \neq \mathfrak{v}^\rho_{m_j}$. Рассмотрим заготовку s следующего вида: $s^{-1}(\updownarrow) = \{\mathfrak{t}^\rho_{m_1}, \ldots, \mathfrak{t}^\rho_{m_k}\}$; $\mathfrak{v}^s_0 = \mathfrak{v}^\rho_0$; $\mathfrak{v}^s_i = \mathfrak{v}^\rho_{m_i}$, $i \in [1..k]$. По заданию s, для каждого i, $i \in [1..k]$, справедлива цепочка соотношений (*): $\mathfrak{v}^\rho_{m_{i-1}} = \mathfrak{v}^\rho_{m_{i-1}+1} = \cdots = \mathfrak{v}^\rho_{m_i-1} \neq \mathfrak{v}^\rho_{m_i}$. Из (*) следует, что $\mathfrak{v}^s_{i-1} = \mathfrak{v}^\rho_{m_{i-1}} \neq \mathfrak{v}^\rho_{m_i} = \mathfrak{v}^s_i$ для всех i, $i \in [1..|s|]$, а значит, s — сигнал. Также из (*) следует, что для любой точки t любого интервала $\mathfrak{I}^\rho_j$, $j \in [0..|\rho|]$, верно $s(t) = \rho(t)$. По утверждению 1, $\Delta(s, \rho) \subseteq (\mathbf{a}, \mathbf{b}) \setminus (\mathfrak{I}^\rho_0 \cup \cdots \cup \mathfrak{I}^\rho_{|\rho|}) = \rho^{-1}(\updownarrow)$. Значит, множество $\Delta(s, \rho)$ конечно, то есть сигнал s почти равен заготовке ρ.

Единственность. Рассмотрим произвольные различные сигналы s_1, s_2: существует внутренняя точка t, такая что $s_1(t) \neq s_2(t)$. Покажем, что сигналы s_1, s_2 не являются почти равными. Предположим от противного, что $s_1(t - 0) = s_2(t - 0)$ и $s_1(t + 0) = s_2(t + 0)$. Если $s_1(t - 0) = s_1(t + 0)$, то, по утверждению 2, $s_1(t) = s_1(t + 0) = s_2(t + 0) = s_2(t)$ (противоречие). Иначе $s_1(t - 0) \neq s_1(t + 0)$ и, по утверждению 2, $s_1(t) = s_2(t) = \updownarrow$ (противоречие). Значит предположение неверно, то есть верно хотя бы одно из неравенств $s_1(t - 0) \neq s_2(t - 0)$, $s_1(t + 0) \neq s_2(t + 0)$. Тогда из леммы 1 следует, что сигналы s_1, s_2 не являются почти равными. □

Опираясь на лемму 2, обозначим (существующий и единственный) сигнал, почти равный заготовке ρ, записью $\rho^\updownarrow$. Для заданных формулы φ и диаграммы D функцию $\varphi[[D]]$ назовём *корректной*, если для любых левой точки ℓ и правой точки r верны равенства $\varphi[[D]](\ell + 0) = \varphi[D, \ell + 0]$ и $\varphi[[D]](r - 0) = \varphi[D, r - 0]$. В формулировках следующих далее лемм 3–10 для краткости опущено общее начало “для любых диаграммы D, формулы φ, заготовки ρ и сигнала s верно следующее”.

Лемма 3. *Если для любой левой точки ℓ верно $s(\ell+0) = \varphi[D, \ell+0]$, то $s = \varphi[[D]]$ — корректный сигнал.*

Доказательство. Рассмотрим произвольную правую точку r. По утверждению 2, существует точка t, такая что $t < r$ и $s(r - 0) = s^{+0}\langle(t, r)\rangle$. Значит, для любой точки t' интервала (t, r) верно $s(r - 0) = s(t' + 0) = \varphi[D, t' + 0]$. По определению значения формулы слева, $s(r - 0) = \varphi[D, r - 0]$.

Рассмотрим произвольную внутреннюю точку t. По условию и по доказанному, $s(t+0) = \varphi[D, t+0]$ и $s(t-0) = \varphi[D, t-0]$. По утверждению 2 и определению значения формулы в точке, $s(t) = \varphi[D, t]$. □

Лемма 4. *Если для любой левой точки ℓ верно $\rho(\ell{+}0) = \varphi[D, \ell{+}0]$, то $\rho^{\updownarrow} = \varphi[[D]]$ — корректный сигнал.*

Доказательство. $\rho^{\updownarrow}$ — сигнал, почти равный ρ. По лемме 1, для любой левой точки ℓ верно $\rho^{\updownarrow}(\ell+0) = \rho(\ell+0) = \varphi[D, \ell+0]$. Значит, сигнал $\rho^{\updownarrow}$ подходит под условие леммы 3. □

Лемма 5. *Если $\varphi \in \{1, *\} \cup \mathsf{Var}$, то $\varphi[[D]]$ — корректный сигнал.*

Доказательство. Случай 1: $\varphi = v \in \{0, 1\}$. Рассмотрим сигнал s, всюду принимающий значение v. Для любой левой точки ℓ верно $s(\ell+0) = v = \varphi[D, \ell+0]$.
Случай 2: $\varphi = x \in \mathsf{Var}$. Рассмотрим сигнал $s = D(x)$. Для любой левой точки ℓ верно $s(\ell+0) = D(x)(\ell+0) = \varphi[D, \ell+0]$.
Итог: по лемме 3, в обоих случаях $s = \varphi[[D]]$ — корректный сигнал. □

Для троичной функции $\mathfrak{f}$ местности k и сигналов $s_1, \ldots, s_k$ записью $\mathfrak{f}(s_1, \ldots, s_k)$ обозначим такую заготовку ρ:

$$\rho^{-1}(\updownarrow) = s_1^{-1}(\updownarrow) \cup \cdots \cup s_k^{-1}(\updownarrow); \quad \mathfrak{v}_i^{\rho} = \mathfrak{f}(s_1(\mathfrak{t}_i^{\rho}+0), \ldots, s_k(\mathfrak{t}_i^{\rho}+0)),\ i \in [0..|\rho|].$$

Лемма 6. *Если $\mathfrak{f}$ — троичная функция, $\varphi = \mathfrak{f}(\psi_1, \ldots, \psi_k)$ и $s_1 = \psi_1[[D]], \ldots, s_k = \psi_k[[D]]$ — корректные сигналы, то $\mathfrak{f}(s_1, \ldots, s_k)^{\updownarrow} = \varphi[[D]]$ — корректный сигнал.*

Доказательство. Пусть $\rho = \mathfrak{f}(s_1, \ldots, s_k)$. По лемме 4, достаточно показать, что для любой левой точки ℓ верно $\rho(\ell+0) = \varphi[D, \ell+0]$.

Пусть $\mathfrak{I}^{\rho}_{[\ell+0]} = \mathfrak{I}^{\rho}_i$. По утверждению 1 и заданию ρ, верны равенства $\rho(\ell{+}0) = \mathfrak{v}_i^{\rho} = \mathfrak{f}(s_1(\mathfrak{t}_i^{\rho}{+}0), \ldots, s_k(\mathfrak{t}_i^{\rho}{+}0)) = \mathfrak{f}(s_1\langle\mathfrak{I}_i^{\rho}\rangle, \ldots, s_k\langle\mathfrak{I}_i^{\rho}\rangle) = \mathfrak{f}(s_1(\ell{+}0), \ldots, s_k(\ell{+}0))$. По условию леммы, верны равенства $\mathfrak{f}(s_1(\ell{+}0), \ldots, s_k(\ell{+}0)) = \mathfrak{f}(\psi_1[[D]](\ell{+}0), \ldots, \psi_k[[D]](\ell{+}0)) = \mathfrak{f}(\psi_1[D, \ell+0], \ldots, \psi_k[D, \ell+0]) = \mathfrak{f}(\psi_1, \ldots, \psi_k)[D, \ell+0] = \varphi[D, \ell+0]$. □

Для сигналов s_1, s_2 записью $\mathbf{U}(s_1, s_2)$ обозначим такую заготовку ρ:

$$\rho^{-1}(\updownarrow) = s_1^{-1}(\updownarrow) \cup s_2^{-1}(\updownarrow);$$
$$\mathfrak{v}_i^{\rho} = \begin{cases} 1, & \text{если } \exists j \in [0..|s_2|] : \mathfrak{t}_i^{\rho} < \mathfrak{t}_{j+1}^{s_2}, \mathfrak{v}_j^{s_2} = 1 \text{ и } s_1\langle(\mathfrak{t}_i^{\rho}, \mathfrak{t}_j^{s_2})\rangle = 1; \\ *, & \text{если условие выше не выполнено и} \\ & \quad \exists j \in [0..|s_2|] : \mathfrak{t}_i^{\rho} < \mathfrak{t}_{j+1}^{s_2}, \mathfrak{v}_j^{s_2} \neq 0 \text{ и } s_1\langle(\mathfrak{t}_i^{\rho}, \mathfrak{t}_j^{s_2})\rangle \neq 0; \\ 0 & \text{в остальных случаях, } i \in [0..|\rho|]. \end{cases}$$

Лемма 7. *Если $\varphi = (\psi_1 \mathbf{U} \psi_2)$ и $s_1 = \psi_1[[D]]$, $s_2 = \psi_2[[D]]$ — корректные сигналы, то $\mathbf{U}(s_1, s_2)^{\updownarrow} = \varphi[[D]]$ — корректный сигнал.*

Доказательство. Пусть $\rho = \mathbf{U}(s_1, s_2)$. По лемме 4, достаточно показать, что для любой левой точки ℓ верно $\rho(\ell+0) = \varphi[D, \ell+0]$. Пусть, для ясности, $\mathfrak{I}^{\rho}_{[\ell+0]} = \mathfrak{I}^{\rho}_i$. По утверждению 1, достаточно показать, что $\mathfrak{v}_i^{\rho} = \varphi[D, \ell+0]$.
Случай 1: $\mathfrak{v}_i^{\rho} = 1$. Тогда для некоторого j, $j \in [0..|s_2|]$, верно $\mathfrak{t}_i^{\rho} < \mathfrak{t}_{j+1}^{s_2}$, $\mathfrak{v}_j^{s_2} = 1$ и $s_1\langle(\mathfrak{t}_i^{\rho}, \mathfrak{t}_j^{s_2})\rangle = 1$.
Подслучай (a): $\ell \geq \mathfrak{t}_j^{s_2}$. По заданию множества $\rho^{-1}(\updownarrow)$ и выбору индекса i, верны неравенства $\mathfrak{t}_j^{s_2} \leq \ell < \mathfrak{t}_{i+1}^{\rho} \leq \mathfrak{t}_{j+1}^{s_2}$. Рассмотрим точку $t = (\ell + \mathfrak{t}_{j+1}^{s_2})/2$. По утверждению 1,

верно $s_2(t) = s_2\langle(\ell, t)\rangle = 1$. По заданию s_2, верно $\psi_2[D, t] = \psi_2[D, (\ell, t)] = 1$. По логической семантике дизъюнкции и последнему равенству, верно $(\psi_1 \vee \psi_2)[D, (\ell, t)] = 1$. Значит, $\varphi[D, \ell + 0] = 1$.
Подслучай (б): $\ell < \mathfrak{t}_j^{s_2}$. Тогда $s_1\langle(\ell, \mathfrak{t}_j^{s_2})\rangle = s_2\langle(\mathfrak{t}_i^{\rho}, \mathfrak{t}_j^{s_2})\rangle = 1$. По заданию s_1, верно $\psi_1[D, (\ell, \mathfrak{t}_j^{s_2})] = 1$. Рассмотрим точку $t = (\mathfrak{t}_j^{s_2} + \mathfrak{t}_{j+1}^{s_2})/2$. По утверждению 1, верно $s_2(t) = s_2\langle(\mathfrak{t}_j^{s_2}, t)\rangle = 1$. По заданию s_2, верно $\psi_2[D, t] = \psi_2[D, (\mathfrak{t}_j^{s_2}, t)] = 1$. Из полученных равенств $\psi_1[D, (\ell, \mathfrak{t}_j^{s_2})] = \psi_2[D, (\mathfrak{t}_j^{s_2}, t)] = 1$ следует равенство $(\psi_1 \vee \psi_2)[D, (\ell, t)] = 1$. Значит, с учётом соотношения $\psi_2[D, t] = 1$, верно $\varphi[D, \ell + 0] = 1$.
Случай 2: $\mathfrak{v}_i^{\rho} \neq 0$. Тогда, аналогично случаю 1, верно $\varphi[D, \ell] \neq 0$.
Случай 3: $\varphi[D, \ell + 0] = 1$. Тогда существует точка t, такая что $\ell < t$ и $\psi_2[D, t] = (\psi_1 \vee \psi_2)[D, (\ell, t)] = 1$. Пусть $\mathfrak{I}_{[\ell+0]}^{s_2} = \mathfrak{I}_m^{s_2}$ и $\mathfrak{I}_{[t]}^{s_2} = \mathfrak{I}_k^{s_2}$. Тогда $\mathfrak{v}_k^{s_2} = s_2(t) = 1$, и так как $\ell < t$, то верно $m \leq k$. Рассмотрим наименьший индекс j диапазона $[m..k]$, такой что $\mathfrak{v}_j^{s_2} = 1$. По выбору индексов i и m и неравенству $m \leq j$, верно $\mathfrak{t}_i^{\rho} \leq \ell < \mathfrak{t}_{j+1}^{s_2}$.

Предположим, что существует точка t' интервала $(\ell, \mathfrak{t}_j^{s_2})$, такая что $s_1(t') \neq 1$. Тогда, по утверждению 2, существует точка t'' интервала $(\ell, t']$, такая что $s_1(t''+0) \neq 1$. По выбору индекса j, верно $s_2\langle(\ell, \mathfrak{t}_j^{s_2})\rangle \neq 1$, а значит, $s_2(t'' + 0) \neq 1$. Пусть $s_{12} = (\psi_1 \vee \psi_2)[[D]]$. По лемме 6, s_{12} — корректный сигнал, а значит, $s_{12}(t'' + 0) = \vee(s_1(t'' + 0), s_2(t'' + 0)) \neq 1$. При этом, согласно полученному в начале случая, $s_{12}(t'' + 0) = s_{12}\langle(t'', t)\rangle = s_{12}\langle(\ell, t)\rangle = 1$, что противоречит последнему неравенству. Следовательно, предположение неверно: $s_1\langle(\ell, \mathfrak{t}_j^{s_2})\rangle = 1$ и, по утверждению 1 и выбору индекса i, $s_1\langle(\mathfrak{t}_i^{\rho}, \mathfrak{t}_j^{s_2})\rangle = 1$.

Итог рассуждений случая 3: существует индекс j, такой что $\mathfrak{t}_i^{\rho} \leq \mathfrak{t}_j^{s_2}$, $\mathfrak{v}_j^{s_2} = 1$ и $s_1\langle(\mathfrak{t}_i^{\rho}, \mathfrak{t}_j^{s_2})\rangle = 1$. Значит, по заданию ρ, верно $\mathfrak{v}_i^{\rho} = 1$.
Случай 4: $\varphi[D, \ell + 0] \neq 0$. Тогда, аналогично случаю 3, верно $\mathfrak{v}_i^{\rho} \neq 0$.
Итог: верны равносильности $\mathfrak{v}_i^{\rho} = 1 \Leftrightarrow \varphi[D, \ell + 0] = 1$ и $\mathfrak{v}_i^{\rho} \neq 0 \Leftrightarrow \varphi[D, \ell + 0] \neq 0$. Значит, так как $\mathfrak{v}_i^{\rho} \in \{0, 1, *\}$, верно и равенство $\mathfrak{v}_i^{\rho} = \varphi[D, \ell + 0]$. □

Для сигналов s_1, s_2 записью $\mathbf{C}(s_1, s_2)$ обозначим такую заготовку ρ:

$$\rho^{-1}(\updownarrow) = s_1^{-1}(\updownarrow) \cup s_2^{-1}(\updownarrow);$$
$$\mathfrak{v}_i^{\rho} = \begin{cases} 1, & \text{если } s_1\langle C(s_2, \mathfrak{t}_i^{\rho})\rangle = 1; \\ 0, & \text{если } \exists t \in C(s_2, \mathfrak{t}_i^{\rho}) : s_1(t) = 0; \\ * & \text{в остальных случаях, } i \in [0..|\rho|]. \end{cases}$$

Лемма 8. *Если* $\varphi = (\psi_1 \mathbf{C} \psi_2)$ *и* $s_1 = \psi_1[[D]]$, $s_2 = \psi_2[[D]]$ *— корректные сигналы, то* $\mathbf{C}(s_1, s_2)^{\updownarrow} = \varphi[[D]]$ *— корректный сигнал.*

Доказательство. Пусть $\rho = \mathbf{C}(s_1, s_2)$. Аналогично доказательству леммы 7, достаточно показать, что если $\mathfrak{I}_{[\ell+0]}^{\rho} = \mathfrak{I}_i^{\rho}$, то $\mathfrak{v}_i^{\rho} = \varphi[D, \ell + 0]$. Для обоснования этого равенства достаточно заметить следующее. По заданию s_1, для любой внутренней точки t верно $s_1(t) = \psi_1[D, t]$. По заданию s_2 и определениям передних фронтов и тактов сигналов и формул, $C(s_2, \mathfrak{t}_i^{\rho}) = C(s_2, \ell) = C(\psi_2, D, \ell)$. □

Для сигналов s_1, s_2 записью $\mathbf{X}(s_1, s_2)$ обозначим такую заготовку ρ:

$$\rho^{-1}(\updownarrow) = s_1^{-1}(\updownarrow) \cup s_2^{-1}(\updownarrow);$$
$$\mathfrak{v}_i^{\rho} = \begin{cases} v, & \text{если } \exists t = next_{\uparrow}(s_2, \mathfrak{t}_i^{\rho}) \text{ и } v = s_1(t) \neq \updownarrow; \\ * & \text{в остальных случаях, } i \in [0..|\rho|]. \end{cases}$$

Лемма 9. *Если* $\varphi = (\psi_1 \mathbf{X} \psi_2)$ *и* $s_1 = \psi_1[[D]]$, $s_2 = \psi_2[[D]]$ *— корректные сигналы, то* $\mathbf{X}(s_1, s_2)^{\updownarrow} = \varphi[[D]]$ *— корректный сигнал.*

Доказательство. Пусть $\rho = \mathbf{X}(s_1, s_2)$. Аналогично доказательству леммы 7, достаточно показать, что если $\mathfrak{I}^{\rho}_{[\ell+0]} = \mathfrak{I}^{\rho}_i$, то $\mathfrak{v}^{\rho}_i = \varphi[D, \ell{+}0]$. Для обоснования этого равенства достаточно заметить следующее. По заданию s_1, для любой внутренней точки t верно $s_1(t) = \psi_1[D, t]$. По заданию s_2 и определениям передних фронтов и следующих передних фронтов сигналов и формул, значения $next_{\uparrow}(s_2, \mathfrak{t}^{\rho}_i)$, $next_{\uparrow}(s_2, \ell)$ и $next_{\uparrow}(\psi_2, D, \ell)$ либо все не определены, либо все определены и равны. □

Лемма 10. *Если $\varphi = (\circlearrowleft\psi)$ и $s = \psi[[D^{\circlearrowleft}]]$ — корректный сигнал, то $s^{\circlearrowleft} = \varphi[[D]]$ — корректный сигнал.*

Доказательство. По лемме 3, достаточно показать, что для любой левой точки ℓ верно $s^{\circlearrowleft}(\ell + 0) = \varphi[D, t + 0]$. По условию леммы и определениям отражения сигнала и точки и значений сигнала справа и слева, верна цепочка равенств $s^{\circlearrowleft}(\ell + 0) = s(\ell^{\circlearrowleft} - 0) = \psi[[D^{\circlearrowleft}]](\ell^{\circlearrowleft} - 0) = \psi[D^{\circlearrowleft}, \ell^{\circlearrowleft} - 0] = \varphi[D, \ell + 0]$. □

Теорема 1. *Для любых формулы φ и диаграммы D функция $\varphi[[D]]$ является корректным сигналом.*

Доказательство. Применим индукцию по построению формулы. База индукции: $\varphi \in \{1, *\} \cup \mathsf{Var}$ — обосновывается леммой 5. Индуктивный переход: $\varphi = (\psi_1 \oplus \psi_2)$, где $\oplus \in \{\mathbf{U}, \mathbf{C}, \mathbf{X}\}$, или $\varphi = (\circlearrowleft\psi)$ — обосновывается леммами 6–10. □

5. Алгоритм верификации диаграмм сигналов

Заготовку ρ назовём *рациональной*, если все числа множества $\rho^{-1}(\updownarrow) \cup \{\mathbf{a}, \mathbf{b}\}$ рациональны. *Рациональной диаграммой* назовём диаграмму, все сигналы области значений которой рациональны. В алгоритмах работы с сигналами рассматриваются только рациональные точки, заготовки, сигналы и диаграммы. Такое ограничение типично для моделей с реальным временем [1,8] и связано с тем, что: множество действительных чисел континуально; разнообразие входных данных алгоритма и множество рациональных чисел счётны; любое действительное число можно приблизить рациональным с любой заданной точностью. Отметим, что в алгоритмах можно использовать и более широкие (но всё равно счётные) множества чисел по сравнению с рациональными, однако на практике это обычно не требуется, и в описании алгоритмов это не столь важно.

В качестве конечного представления $\overline{\rho}$ заготовки ρ в алгоритмах будем использовать пару $\langle T, V\rangle$, где $T = (\mathfrak{t}^{\rho}_1, \ldots, \mathfrak{t}^{\rho}_{|\rho|})$ и $V = (\mathfrak{v}^{\rho}_0, \mathfrak{v}^{\rho}_1, \ldots, \mathfrak{v}^{\rho}_{|\rho|})$. В связи с устройством такого представления ρ будем в алгоритмах использовать записи $|\rho|$, $\mathfrak{t}^{\rho}_i$ и $\mathfrak{v}^{\rho}_j$, где $i \in [0..|\rho| + 1]$ и $j \in [0..|\rho|]$, понимая под этим размер набора T, соответствующие точки и значения представления и точки $\mathbf{a}$, $\mathbf{b}$. Диаграмму D представим в виде конечного отображения $\overline{D}$, сопоставляющего каждой переменной x пару $\overline{s}$. Записью $|D|$ обозначим общее число точек фронтов образов D: $|D| = \sum_{x \in Var} |D(x)|$. Записью $|\varphi|$, где φ — формула, обозначим общее число сигнальных операций в φ.

Алгоритм верификации (проверки соотношения $D \models \varphi$) опишем в процедурном стиле. Результат выполнения процедуры π на входных данных $o_1, \ldots, o_m$ обозначим записью $\pi(o_1, \ldots, o_m)$. *Проверками* будем называть процедуры с двумя возможными результатами: 0 (неуспех) и 1 (успех). *Сложностью* процедуры в дальнейших

оценках будем считать общее число сравнений и присваиваний значений множества $\mathfrak{T}_{\updownarrow}$ и точек. Обсуждаемые далее оценки сложности не являются оптимальными, но достаточны для обоснования полиномиальной разрешимости исследуемой задачи.

Алгоритм отождествляется с основной процедурой П, описанной после всех вспомогательных процедур. В описаниях процедур полагается, что: ρ — рациональная заготовка; $s, s_1, s_2, \ldots, s_k$ — рациональные сигналы; ℓ, r и t — рациональные левая, правая и внутренняя точки соответственно; $v \in \mathfrak{T}$.

Процедура π_{+0}: $\pi_{+0}(\overline{s}, \ell) = s(\ell + 0)$. Устройство процедуры:
- Перебором вычислить индекс i диапазона $[0..|s|]$, такой что $\mathfrak{t}^s_i \le \ell < \mathfrak{t}^s_{i+1}$.
- Выдать результат: $\pi_{+0}(\overline{s}, \ell) = \mathfrak{v}^s_i$.

Корректность процедуры обосновывается утверждением 1.
Сложность процедуры: $O(|s|)$.

Процедура π_{-0}: $\pi_{-0}(\overline{s}, r) = s(r - 0)$. Устройство процедуры:
- Перебором вычислить индекс i диапазона $[0..|s|]$, такой что $\mathfrak{t}^s_i < r \le \mathfrak{t}^s_{i+1}$.
- Выдать результат: $\pi_{-0}(\overline{s}, r) = \mathfrak{v}^s_i$.

Корректность процедуры обосновывается утверждением 1.
Сложность процедуры: $O(|s|)$.

Процедура π_{val}: $\pi_{val}(\overline{s}, t) = s(t)$. Устройство процедуры:
- Вычислить значения $v_- = \pi_{-0}(\overline{s}, t)$ и $v_+ = \pi_{+0}(\overline{s}, t)$.
- Выдать результат: если $v_- = v_+$, то $\pi_{val}(\overline{s}, t) = v_+$; иначе $\pi_{val}(\overline{s}, t) = \updownarrow$.

Корректность процедуры обосновывается утверждением 2 и корректностью процедур π_{-0}, π_{+0}. *Сложность процедуры*: $O(|s|)$, определяется вызовами π_{-0}, π_{+0}.

Процедура π_{clean}: $\pi_{clean}(\overline{\rho}) = \overline{\rho^{\updownarrow}}$. Устройство процедуры:
- Перебором вычислить все индексы $i_1, \ldots, i_k$ диапазона $[1..|\rho|]$, такие что $\mathfrak{v}^\rho_{i_j - 1} \ne \mathfrak{v}^\rho_{i_j}$, в порядке возрастания.
- Выдать результат: $\pi_{clean}(\overline{\rho}) = \langle (\mathfrak{t}^\rho_{i_1}, \ldots \mathfrak{t}^\rho_{i_k}), (\mathfrak{v}^\rho_0, \mathfrak{v}^\rho_{i_1}, \ldots, \mathfrak{v}^\rho_{i_k}) \rangle$.

Корректность процедуры обосновывается в доказательстве леммы 2.
Сложность процедуры: $O(|\rho|)$.

Проверка $\pi_\forall$: $\pi_\forall(\overline{s}, \ell, r, v) = 1 \Leftrightarrow s\langle(\ell, r)\rangle = v$. Устройство проверки:
- Если $r \le \ell$, то выдать результат: $\pi_\forall(\overline{s}, \ell, r, v) = 1$. Иначе продолжить проверку.
- Перебором вычислить индекс i диапазона $[0..|s|]$, такой что $\mathfrak{t}^s_i \le \ell < \mathfrak{t}^s_{i+1}$.
- Выдать результат: $\pi_\forall(\overline{s}, \ell, r, v) = 1 \Leftrightarrow r \le \mathfrak{t}^s_{i+1}$ и $\mathfrak{v}^s_i = v$.

Корректность проверки обосновывается утверждением 1: проверка успешна в том и только том случае, если $(\ell, r) = \emptyset$ или для некоторого i верно $(\ell, r) \subseteq \mathfrak{I}^s_i$ и $v = \mathfrak{v}^s_i$.
Сложность проверки: $O(|s|)$.

Проверка $\pi_\exists$: $\pi_\exists(\overline{s}, \ell, r, v) = 1 \Leftrightarrow \exists t \in (\ell, r) : s(t) = v$. Устройство проверки:
- Если $r \le \ell$, то выдать результат: $\pi_\exists(\overline{s}, \ell, r, v) = 0$. Иначе продолжить проверку.
- Перебором вычислить индекс i диапазона $[0..|s|]$, такой что $\mathfrak{t}^s_i \le \ell < \mathfrak{t}^s_{i+1}$.
- Перебором вычислить индекс j диапазона $[i..|s|]$, такой что $\mathfrak{t}^s_j < r \le \mathfrak{t}^s_{j+1}$.
- Выдать результат:
  $\pi_\exists(\overline{s}, \ell, r, v) = 1 \Leftrightarrow$ хотя бы одно из значений $\mathfrak{v}^s_k$, $k \in [i..j]$, равно v.

Корректность проверки обосновывается утверждением 1: проверка успешна в том и только том случае, если $(\ell, r) \neq \emptyset$ и интервал (ℓ, r) пересекается хотя бы с одним интервалом $\mathfrak{I}_k^s$, таким что $\mathfrak{v}_k^s = 1$. *Сложность проверки*: $O(|s|)$.

Проверка $\pi_\uparrow$**:** $\pi_\uparrow(\overline{s}, t) = 1 \Leftrightarrow s(t) = \uparrow$. Устройство проверки:

- Вычислить значения $v_- = \pi_{-0}(\overline{s}, t)$ и $v_+ = \pi_{+0}(\overline{s}, t)$.
- Выдать результат: $\pi_\uparrow(\overline{s}, t) = 1 \Leftrightarrow v_- < v_+$.

Корректность проверки обосновывается определением точки переднего фронта сигнала, утверждением 2 и корректностью процедур π_{-0}, π_{+0}.
Сложность проверки: $O(|s|)$, определяется вызовами процедур π_{-0} и π_{+0}.

Процедура π_{next}**:** $\pi_{next}(\overline{s}, \ell) = \begin{cases} next_\uparrow(s, \ell), & \text{если это значение существует;} \\ \mathbf{b} & \text{иначе.} \end{cases}$

Устройство процедуры:

- Перебором вычислить наименьший индекс i диапазона $[1..|s|]$,
  такой что $\ell < \mathfrak{t}_i^s$ и проверка $\pi_\uparrow(\overline{s}, \mathfrak{t}_i^s)$ успешна.
  Если перебором такой индекс не обнаружен, то положить $i = |s| + 1$.
- Выдать результат: $\pi_{next}(\overline{s}, \ell) = \mathfrak{t}_i^s$.

Корректность процедуры обосновывается определением точки следующего фронта и корректностью проверки $\pi_\uparrow$.
Сложность процедуры: $O(|s|^2)$, определяется $|s|$ вызовами проверки $\pi_\uparrow$.

Процедура π_{cycle}**:** $\pi_{cycle}(\overline{s}, \ell) = \langle t_1, t_2 \rangle$ — пара точек, такая что $(t_1, t_2) = C(s, \ell)$.
Устройство процедуры:

- Перебором вычислить наибольший индекс i диапазона $[1..|s|]$,
  такой что $\mathfrak{t}_i^s \leq \ell$ и проверка $\pi_\uparrow(\overline{s}, \mathfrak{t}_i^s)$ успешна.
  Если такого индекса не существует, то положить $i = 0$.
- Вычислить индекс $j = \pi_{next}(\overline{s}, \ell)$.
- Выдать результат: $\pi_{cycle}(\overline{s}, \ell) = \langle \mathfrak{t}_i^s, \mathfrak{t}_j^s \rangle$.

Корректность процедуры обосновывается определением такта точки t и корректностью проверки $\pi_\uparrow$ и процедуры π_{next}.
Сложность процедуры: $O(|s|^2)$, определяется $|s|$ вызовами процедуры $\pi_\uparrow$.

Процедура $\pi_\circlearrowleft$**:** $\pi_\circlearrowleft(\overline{s}) = \overline{s^\circlearrowleft}$. Устройство процедуры:

- Выдать результат: $\pi_\circlearrowleft(\overline{s}) = \langle (\mathfrak{t}_{|s|}^{s\,\circlearrowleft}, \mathfrak{t}_{|s|-1}^{s\,\circlearrowleft}, \ldots, \mathfrak{t}_1^{s\,\circlearrowleft}), (\mathfrak{v}_{|s|}^s, \mathfrak{v}_{|s|-1}^s, \ldots, \mathfrak{v}_0^s) \rangle$.

Корректность процедуры обосновывается в доказательстве утверждения 3.
Сложность процедуры: $O(|s|)$.

Процедура $\pi_{\circlearrowleft'}$**:** $\pi_{\circlearrowleft'}(\overline{D}) = \overline{D^\circlearrowleft}$. Устройство процедуры:

- Для каждой переменной x вычислить представление $\overline{s_x} = \pi_\circlearrowleft(\overline{D}(x))$.
- Выдать результат: $\pi_{\circlearrowleft'}(\overline{D})$ — отображение, сопоставляющее каждой переменной x представление $\overline{s_x}$.

Корректность процедуры обосновывается определением отражения диаграммы и корректностью процедуры $\pi_\circlearrowleft$.
Сложность процедуры: $O(|D|)$, определяется сложностью процедуры $\pi_\circlearrowleft$.

Спектр процедур $\pi_\mathfrak{f}$**:** $\pi_\mathfrak{f}(\overline{s_1}, \ldots, \overline{s_k}) = \overline{\mathfrak{f}(s_1, \ldots, s_k)}$, где $\mathfrak{f}$ — k-местная троичная функция. Устройство каждой такой процедуры:

- Перебором точек, содержащихся в $\overline{s_1}, \ldots, \overline{s_k}$, вычислить набор $(t_1, \ldots, t_m)$ всех таких точек без повторений в порядке возрастания. Положить $t_0 = \mathbf{a}$.
- Для каждого индекса i диапазона $[0..m]$ вычислить значение $v_i = \mathfrak{f}(\pi_{+0}(\overline{s_1}, t_i), \ldots, \pi_{+0}(\overline{s_k}, t_i))$.
- Выдать результат: $\pi_{\mathfrak{f}}(\overline{s_1}, \ldots, \overline{s_k}) = \langle (t_1, \ldots, t_m), (v_0, \ldots, v_m) \rangle$.

Корректность процедуры обосновывается определением заготовки $\mathfrak{f}(s_1, \ldots, s_k)$ и корректностью процедуры π_{+0}. *Сложность процедуры*: $O(n^2)$, где $n = |s_1| + \cdots + |s_k|$, определяется $O(n)$ вызовами процедуры π_{+0}.

Процедура $\pi_{\mathbf{U}}$: $\pi_{\mathbf{U}}(\overline{s_1}, \overline{s_2}) = \overline{\mathbf{U}(s_1, s_2)}$. Устройство процедуры:

- Перебором точек, содержащихся в $\overline{s_1}$, $\overline{s_2}$, вычислить набор $(t_1, \ldots, t_m)$ всех таких точек без повторений в порядке возрастания. Положить $t_0 = \mathbf{a}$.
- Для каждого индекса i диапазона $[0..m]$ вычислить значение v_i:
  - перебором проверить, существует ли индекс j диапазона $[0..|s_2|]$, такой что $t_i < \mathfrak{t}^{s_2}_{j+1}$, $\mathfrak{v}^{s_2}_j = 1$ и проверка $\pi_\forall(s_1, t_i, \mathfrak{t}^{s_2}_j, 1)$ успешна: если существует, то $v_i = 1$, иначе продолжить вычисление v_i;
  - перебором проверить, существует ли индекс j диапазона $[0..|s_2|]$, такой что $t_i < \mathfrak{t}^{s_2}_{j+1}$, $\mathfrak{v}^{s_2}_j \neq 0$ и проверка $\pi_\exists(s_1, t_i, \mathfrak{t}^{s_2}_j, 0)$ неуспешна: если существует, то $v_i = *$, иначе $v_i = 0$.
- Выдать результат: $\pi_{\mathbf{U}}(\overline{s_1}, \overline{s_2}) = \langle (t_1, \ldots, t_m), (v_0, \ldots, v_m) \rangle$.

Корректность процедуры обосновывается определением заготовки $\mathbf{U}(s_1, s_2)$ и корректностью процедур $\pi_\forall$, $\pi_\exists$. *Сложность процедуры*: $O(n^3)$, где $n = |s_1| + |s_2|$, определяется $O(n^2)$ вызовами процедур $\pi_\forall$, $\pi_\exists$.

Процедура $\pi_{\mathbf{C}}$: $\pi_{\mathbf{C}}(\overline{s_1}, \overline{s_2}) = \overline{\mathbf{C}(s_1, s_2)}$. Устройство процедуры:

- Перебором точек, содержащихся в $\overline{s_1}$, $\overline{s_2}$, вычислить набор $(t_1, \ldots, t_m)$ всех таких точек без повторений в порядке возрастания. Положить $t_0 = \mathbf{a}$.
- Для каждого индекса i диапазона $[0..m]$ вычислить значение v_i:
  - вычислить пару точек $\langle t^i_1, t^i_2 \rangle = \pi_{cycle}(\overline{s_2}, t_i)$;
  - если проверка $\pi_\forall(\overline{s_1}, t^i_1, t^i_2, 1)$ успешна, то $v_i = 1$, а иначе продолжить вычисление v_i;
  - если проверка $\pi_\exists(\overline{s_1}, t^i_1, t^i_2, 0)$ успешна, то $v_i = 0$, иначе $v_i = *$.
- Выдать результат: $\pi_{\mathbf{C}}(\overline{s_1}, \overline{s_2}) = \langle (t_1, \ldots, t_m), (v_0, \ldots, v_m) \rangle$.

Корректность процедуры обосновывается определением заготовки $\mathbf{C}(s_1, s_2)$ и корректностью процедур π_{cycle}, $\pi_\forall$, $\pi_\exists$. *Сложность процедуры*: $O(n^3)$, где $n = |s_1| + |s_2|$, определяется $O(n)$ вызовами процедуры π_{cycle}.

Процедура $\pi_{\mathbf{X}}$: $\pi_{\mathbf{X}}(\overline{s_1}, \overline{s_2}) = \overline{\mathbf{X}(s_1, s_2)}$. Устройство процедуры:

- Перебором точек, содержащихся в $\overline{s_1}$, $\overline{s_2}$, вычислить набор $(t_1, \ldots, t_m)$ всех таких точек без повторений в порядке возрастания. Положить $t_0 = \mathbf{a}$.
- Для каждого индекса i диапазона $[0..m]$ вычислить значение v_i:
  - вычислить точку $t'_i = \pi_{next}(\overline{s_2}, t_i)$ и, если $t'_i \neq \mathbf{b}$, значение $v'_i = \pi_{val}(\overline{s_1}, t'_i)$;
  - если $t'_i \neq \mathbf{b}$ и $v'_i \neq \updownarrow$, то $v_i = v'_i$, а иначе $v_i = *$.
- Выдать результат: $\pi_{\mathbf{X}}(\overline{s_1}, \overline{s_2}) = \langle (t_1, \ldots, t_m), (v_0, \ldots, v_m) \rangle$.

Корректность процедуры обосновывается определением заготовки $\mathbf{X}(s_1, s_2)$ и корректностью процедур π_{next}, π_{val}. *Сложность процедуры*: $O(n^3)$, где $n = |s_1| + |s_2|$, определяется $O(n)$ вызовами процедуры π_{next}.

Процедура $\pi_{[]}$: $\pi_{[]}(\varphi, \overline{D}) = \overline{\varphi[[D]]}$. Устройство процедуры:

- В зависимости от вида формулы φ выдать результат:
  - если $\varphi = v \in \{1, *\}$, то $\pi_{[]}(\varphi, \overline{D}) = \langle((), (v)\rangle$;
  - если $\varphi = x \in \mathsf{Var}$, то $\pi_{[]}(\varphi, \overline{D}) = \overline{D}(x)$;
  - если $\varphi = \mathfrak{f}(\psi_1, \ldots, \psi_k)$, где $\mathfrak{f}$ — троичная функция, то $\pi_{[]}(\varphi, \overline{D}) = \pi_{clean}(\pi_{\mathfrak{f}}(\pi_{[]}(\psi_1, \overline{D}), \ldots \pi_{[]}(\psi_k, \overline{D})))$;
  - если $\varphi = (\psi_1 \oplus \psi_2)$, где $\oplus \in \{\mathbf{U}, \mathbf{C}, \mathbf{X}\}$, то $\pi_{[]}(\varphi, \overline{D}) = \pi_{clean}(\pi_{\oplus}(\pi_{[]}(\psi_1, \overline{D}), \pi_{[]}(\psi_2, \overline{D})))$.
  - если $\varphi = (\circlearrowleft\psi)$, то $\pi_{[]}(\varphi, \overline{D}) = \pi_{\circlearrowleft}(\pi_{[]}(\psi, \pi_{\circlearrowleft'}(\overline{D}))$.

Корректность процедуры обосновывается индукцией согласно доказательству теоремы 1, леммами 5–10 и корректностью процедур $\pi_{\mathfrak{f}}$, $\pi_{\mathbf{U}}$, $\pi_{\mathbf{C}}$, $\pi_{\mathbf{X}}$, $\pi_{\circlearrowleft}$, $\pi_{\circlearrowleft'}$ и π_{clean}.
Сложность процедуры: $O(|\varphi| \cdot |D|^3)$, определяется сложностями используемых процедур, способом организации рекурсии и тем фактом, что все точки вычисляемых представлений содержатся в образах $\overline{D}$ и $\overline{D^{\circlearrowleft}}$.

Проверка Π**:** $\Pi(\varphi, \overline{D}) = 1 \Leftrightarrow D \models \varphi$. Устройство проверки:

- Вычислить сигнал, определяемый сигнальной семантикой: $\overline{s} = \pi_{[]}(\varphi, \overline{D})$.
- Выдать результат: $\Pi(\varphi, \overline{D}) = 1 \Leftrightarrow \mathfrak{v}_0^s = 1$.

Корректность проверки обосновывается корректностью процедуры $\pi_{[]}$ и:

- определением выполнимости формул: $D \models \varphi \Leftrightarrow \varphi[D, \mathbf{a} + 0] = 1$;
- теоремой 1, согласно которой вычисляемый сигнал s корректен;
- определением корректного сигнала: $\varphi[D, \mathbf{a} + 0] = s(\mathbf{a} + 0)$;
- утверждением 1: $s(\mathbf{a} + 0) = \mathfrak{v}_0^s$.

Сложность проверки: $O(|\varphi| \cdot |D|^3)$, определяется вызовом процедуры $\pi_{[]}$.
Корректностью и сложностью процедуры Π обосновывается следующая теорема.

Теорема 2. *Задача верификации рациональных диаграмм относительно формул логики троичных сигналов полиномиально разрешима.*

Пример 3. Положим, что $(\mathbf{a}, \mathbf{b}) = (0, 11)$ и $\mathsf{Var} = \{a, b, c, d\}$. Рассмотрим формулу

$$\varphi = (((a\mathbf{C}b) \vee c)\mathbf{U}\circlearrowleft(d\mathbf{X}b))$$

и диаграмму D, значениями которой являются сигналы, изображённые в верхних четырёх строках рисунка 4. Принцип прочтения рисунка обозначен в примере 1. Этапы проверки соотношения $D \models \varphi$ согласно алгоритму Π устроены так:

1. Последовательно вычисляются сигналы, изображённые на рисунке 4 и соответствующие подформулам формулы φ, включая саму формулу φ. При вычислении сигнала, соответствующего подформуле $\circlearrowleft(d\mathbf{X}b)$, используются сигналы $D^{\circlearrowleft}(b)$ и $D^{\circlearrowleft}(d)$. Эти сигналы изображены в пятой и шестой строках рисунка 4.
2. Для сигнала $s = \varphi[[D]]$ проверяется равенство $\mathfrak{v}_0^s = 1$.
   В данном примере равенство не выполнено ($\mathfrak{v}_0^s = *$), а значит, $D \not\models \varphi$.

6. Выразительные возможности формул

При помощи оператора $\mathbf{U}$ обычным образом [1] можно определить другие темпоральные операторы. В будущем φ станет истинным: $\mathbf{F}\varphi = 1\mathbf{U}\varphi$. Всегда в будущем истинно φ: $\mathbf{G}\varphi = \neg\mathbf{F}\neg\varphi$. Используя оператор $\circlearrowleft$, можно определить ана-

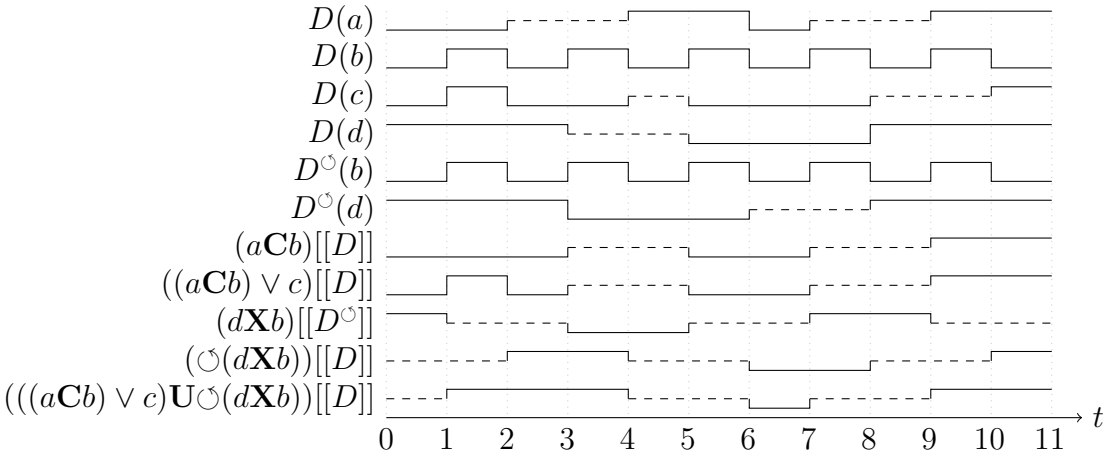

Рис. 4. Пример выполнения основного этапа алгоритма верификации диаграмм
Fig. 4. An execution example for the main stage of the verification algorithm

логи имеющихся темпоральных операторов, рассуждающие о прошедшем времени [1,8,14]. В прошлом было истинным ψ, и с тех пор истинно φ: $\varphi\mathbf{U}^{-}\psi = \circlearrowleft(\circlearrowleft\varphi\mathbf{U}\circlearrowleft\psi)$. В прошлом φ было истинным: $\mathbf{F}^{-}\varphi = 1\mathbf{U}^{-}\varphi$. В прошлом φ всегда было истинным: $\mathbf{G}^{-}\varphi = \neg\mathbf{F}^{-}\neg\varphi$. Комбинируя имеющиеся операции, можно определить и другие операторы, полезные для записи свойств диаграмм. Во время следующего заднего фронта формулы ψ истинно φ: $\varphi\mathbf{X}\neg\psi$. Во время предыдущего переднего фронта формулы ψ истинно φ: $\varphi\mathbf{X}^{-}\psi = \circlearrowleft(\circlearrowleft\varphi\mathbf{X}\circlearrowleft\psi)$. Формула φ истинна на следующем такте формулы ψ: $\varphi\mathbf{C}_{\mathbf{x}}\psi = (\varphi\mathbf{C}\psi)\mathbf{X}\psi$. Значение φ изменяется только в моменты передних фронтов формулы ψ: $\varphi\mathbf{S}\psi = \mathbf{G}(\varphi \Leftrightarrow \varphi\mathbf{C}\psi)$.

Далее приведено два простых, но показательных примера, демонстрирующих применение логики троичных сигналов для записи свойств правильности “реальных” диаграмм. Отдельно отметим, что в рамках логик, предлагаемых во всех известных нам работах, в том числе всех упомянутых в тексте, невозможно точно и полно выразить даже такие несложные свойства.

D-триггер. Функционирование D-триггера и пример соответствующей правильной диаграммы его выполнения обсуждаются во введении к работе. Свойство правильности диаграммы выполнения триггера можно записать в виде двух формул:

$$out\mathbf{S}clk \quad \text{и} \quad \mathbf{G}(in\mathbf{X}^{-}clk \sqsubseteq out).$$

Содержательное прочтение последней формулы: если значение in в момент последнего переднего фронта clk определено, то оно равно текущему значению out. Этой формулой учитываются, в числе прочего, произвольность значения out до первого переднего фронта сигнала clk в диаграмме и эффект метастабильности [2]: если в момент переднего фронта clk значение in изменяется (фронтально), то сохраняется произвольное (неопределённое) значение.

Счётчик чётности. Рассмотрим схему с входными сигналами in, clk и выходным сигналом out, функционирующую так: если в момент переднего фронта сигнала clk сигнал in имеет значение 1, то значение out изменяется на противоположное; в остальные моменты значение out не изменяется. Свойство правильности диаграмм выполнения такой схемы может быть записано двумя формулами:

$$out\mathbf{S}clk \quad \text{и} \quad \mathbf{G}(\neg(out \leftrightarrow in\mathbf{X}clk) \sqsubseteq out\mathbf{C}_{\mathbf{x}}clk).$$

Содержательное прочтение последней формулы: если текущее значение *out* и значение *in* в момент следующего переднего фронта сигнала *clk* определены, то значение *out* на следующем такте сигнала *clk* равно сумме по модулю два этих двух значений.

Заключение

В работе предложена система понятий, утверждений и алгоритмов, нацеленная на формализацию и автоматическую проверку свойств правильности диаграмм троичных цифровых сигналов и включающая в себя определения троичного цифрового сигнала и диаграммы, логический язык описания свойств диаграмм (логику троичных сигналов), постановку задачи верификации диаграмм относительно формул этой логики и конструктивное алгоритмическое решение этой задачи. В определениях учтён ряд особенностей диаграмм, возникающих на практике при отладке кода схем на языках описания аппаратуры: неопределённые значения, мгновенные фронты сигналов и действительное модельное время. Предложенная логика похожа на известные темпоральные логики, но при этом содержит особые операторы ($\mathbf{C}$, $\mathbf{X}$, $\circlearrowleft$ и другие), предназначенные для формализации свойств поведения схемных сигналов и для единообразного расширения логики операторами прошедшего времени. Операторы, аналогичные $\mathbf{C}$, $\mathbf{X}$ и производным от них, нехарактерны для известных нам логик как дискретного, так и реального времени. Устройством и "естественностью" оператора $\mathbf{X}$ подчёркивается промежуточное положение логики троичных сигналов между логиками дискретного времени и реального времени.

Список литературы / References

[1] Baier C., Katoen, J. P., *Principles of model checking*, The MIT Press, Cambridge, USA, 2008.

[2] Harris S., Harris D., *Digital design and computer architecture, second edition*, Morgan Kaufmann Publishers Inc., San Francisco, USA, 2012.

[3] Meinel C., Theobald T., *Algorithms and data structures in VLSI design: OBDD — foundations and applications*, Springer-Verlag, Berlin, Germany, 1998.

[4] Kern C., Greenstreet M. R., "Formal verification in hardware design: a survey", *ACM Transactions on Design Automation of Electronic Systems*, **4**:2 (1999), 123–193.

[5] Kropf T., *Introduction to formal hardware verification*, Springer-Verlag, Berlin, Germany, 1999.

[6] Bryant R. E., Seger C.J. H., "Formal verification of digital circuits using symbolic ternary system models", *Computer-Aided Verification*, CAV 1990, Lecture Notes in Computer Science, **531**, Springer-Verlag, Berlin, Germany, 1991, 33–43.

[7] Baldor K., Niu J., "Monitoring dense-time, continuous-semantics, metric temporal logic", *Runtime Verification*, RV 2012, Lecture Notes in Computer Science, **7687**, Springer-Verlag, Berlin, Germany, 2013, 245–259.

[8] Basin D., Klaedtke F., Zălinescu E., "Algorithms for monitoring real-time properties", *Acta Informatica*, **55**:4 (2018), 309–338.

[9] Яблонский С. В., *Введение в дискретную математику*, Наука, Москва, 1986; [Yablonsky S. V., *Vvedenie v diskretnuju matematiku*, Nauka, Moscow, Russia, 1986, (in Russian).]

[10] Kleene S. C., "On notation for ordinal numbers", *The Journal of Symbolic Logic*, **3**:4 (1938), 150–155.

[11] Kleene S. C., *Introduction to metamathematics*, North-Holland Pub. Co., Amsterdam, Netherlands, 1952.

[12] Bruns G., Godefroid P., "Model checking partial state spaces with 3-valued temporal logics", *Computer-Aided Verification*, CAV 1999, Lecture Notes in Computer Science, **1633**, Springer-Verlag, Berlin, Germany, 1991, 274–287.

[13] Chechik M., Devereux B., Gurfinkel A., "Model-checking infinite state-space systems with fine-grained abstractions using SPIN", *Model Checking Software*, SPIN 2001, Lecture Notes in Computer Science, **2057**, Springer-Verlag, Berlin, Germany, 2001, 16–36.

[14] Laroussinie F., Markey N., Schnoebelen P., "Temporal logic with forgettable past", *Proceedings of the 17th Annual IEEE Symposium on Logic in Computer Science*, IEEE Computer Society, Washington, DC, USA, 2002, 383–392.

Kutsak N. Yu., Podymov V. V., "Formal Verification of Three-Valued Digital Waveforms", *Modeling and Analysis of Information Systems*, **26**:3 (2019), 332–350.

DOI: 10.18255/1818-1015-2019-3-332-350

Abstract. We investigate a formal verification problem (mathematically rigorous correctness checking) for digital waveforms used in practical development of digital microelectronic devices (digital circuits) at early design stages. According to modern methodologies, a digital circuit design starts at high abstraction levels provided by hardware description languages (HDLs). One of essential steps of an HDL-based circuit design is an HDL code debug, similar to the same step of program development in means and importance. A popular way of an HDL code debug is based on extraction and analysis of a waveform, which is a collection of plots for digital signals: functional descriptions of value changes related to selected circuit places in real time. We propose mathematical means for automation of correctness checking for such waveforms based on notions and methods of formal verification against temporal logic formulae, and focus on such typical featues of HDL-related digital signals and corresponding (informal) properties, such as real time, three-valuededness, and presence of signal edges. The three-valuededness means that at any given time, besides basic logical values 0 and 1, a signal may have a special undefined value: one of the values 0 and 1, but which one of them is either not known, or not important. An edge point of a signal is a time point at which the signal changes its value. The main results are mathematical notions, propositions, and algorithms which allow to formalize and solve a formal verification problem for considered waveforms, including: definitions for signals and waveforms which the mentioned typical digital signal features; a temporal logic suitable for formalization of waveform correctness properties, and a related verification problem statement; a solution technique for the verification problem, which is based on reduction to signal transfromation and analysis; a corresponding verification algorithm together with its correctness proof and "reasonable" complexity bounds.

Keywords: formal verification, digital signal, temporal logic, three-valued logic

On the authors:
Nina Yu. Kutsak, orcid.org/0000-0002-0832-3635, bachelor student,
Lomonosov Moscow State University, Faculty of Computational Mathematics and Cybernetics,
1-52, Leninskiye Gory, Moscow, GSP-1, 119991 Russia, e-mail: nina_svetik@mail.ru

Vladislav V. Podymov, orcid.org/0000-0002-2041-7634, PhD in Mathematics, researcher,
Lomonosov Moscow State University, Faculty of Computational Mathematics and Cybernetics,
1-52, Leninskiye Gory, Moscow, GSP-1, 119991 Russia, e-mail: valdus@yandex.ru

Acknowledgments:
The reported study was funded by RFBR according to the research project № 18-01-00854.