Дискретная математика

Модальная логика

Константин Чухарев

Осень 2026

Модальная логика

> *Невозможное — это то, чего никогда не будет.*
>
> ***— Традиционное определение***

Миры и достижимость

Модальная логика — логика *миров* и их взаимной достижимости. Формула истинна в одном мире и ложна в другом.

Определение 1 (Фрейм и модель)

- *Фрейм* — пара $F = (W, R)$: непустое множество миров W и отношение *достижимости* $R \subseteq W \times W$.
- *Модель* — тройка $M = (W, R, V)$, где $V : \mathrm{AP} \to \mathcal{P}(W)$ — оценка: $w \in V(p)$ означает, что атом p истинен в w.

Модальные операторы

Определение 2 (Операторы $\Box$ и $\Diamond$)

- $\Box B$ — «необходимо B»: B истинно во *всех* достижимых мирах.
- $\Diamond B$ — «возможно B»: B истинно в *некотором* достижимом мире.

Операторы двойственны: $\Box A \equiv \neg\Diamond\neg A$, $\Diamond A \equiv \neg\Box\neg A$. «Необходимо» — «невозможно не», «возможно» — «не необходимо не».

Пустые миры

Если из мира w не достижим ни один мир:

- $\Box B$ выполнено *вакуумно* — нет мира, опровергающего B;
- $\Diamond B$ ложно — нет мира, подтверждающего B.

Свойство серийности (ниже) устраняет пустые миры.

Минимальная нормальная модальная логика K задаётся аксиомой $\Box(p \to q) \to (\Box p \to \Box q)$ и правилом необходимости: из A выводится $\Box A$.

Свойства отношения и аксиомы

Центральный факт: каждая аксиома ровно выражает одно свойство отношения достижимости — на уровне фреймов.

Теорема 1 (Соответствие свойства и аксиомы)

Свойство R		Аксиома
серийность: $\forall u \exists v : R(u, v)$	$\leftrightarrow$	D: $\Box p \to \Diamond p$
рефлексивность: $\forall w : R(w, w)$	$\leftrightarrow$	T: $\Box p \to p$
симметричность: $R(u, v) \to R(v, u)$	$\leftrightarrow$	B: $p \to \Box \Diamond p$
транзитивность: $R(u, v) \wedge R(v, w) \to R(u, w)$	$\leftrightarrow$	4: $\Box p \to \Box \Box p$
евклидовость: $R(u, v) \wedge R(u, w) \to R(v, w)$	$\leftrightarrow$	5: $\Diamond p \to \Box \Diamond p$

Пример: аксиома T

Пример (Почему T соответствует рефлексивности)

Если R рефлексивно, то $R(w, w)$, и из $\Box p$ в w следует p в w. Обратно, если R не рефлексивно, возьмём $V(p) = W \setminus \{w\}$: $\Box p$ истинно в w вакуумно, но p ложно.

Системы модальной логики

Из аксиом собирают именованные системы:

- $S_4 = K + T + 4$ — логика рефлексивных и транзитивных фреймов;
- $S_5 = K + T + 5$ — логика фреймов, где R — отношение эквивалентности.

Соответствие — на уровне фреймов, а не моделей: $\Box p \to p$ может быть истинна в модели, где R не рефлексивно (мир без достижимых миров, $V(p) = \{w\}$). Оно выполняется, когда мы квантуем по всем оценкам на фрейме.

Другие модальности

Пара $\Box/\Diamond$ — не только «необходимо/возможно»: чтение зависит от того, что считать мирами и достижимостью.

- **Алетические**: необходимость и возможность. Лейбниц: необходимо — истинно во всех возможных мирах. Аксиома T: необходимое истинно.
- **Эпистемические**: знание Kp. T: знание истинно, 4 и 5 — интроспекция (рациональный агент).
- **Деонтические**: обязанность Op, разрешение Pp. D: $Op \to Pp$, но $Op \to p$ неверно.
- **Доксастические**: убеждение Bp. D есть, T нет: убеждения бывают ложными.

Темпоральная логика — то же чтение для времени: $\Box$ = «всегда», $\Diamond$ = «когда-нибудь». Дальше разбираем именно её: время как модальность доведено до инженерного инструмента (model checking).

Пример: время как модальность

Для реактивных систем:

- «мир» — состояние программы;
- «достижимость» — шаг выполнения.

Определение 3 (Модель Крипке)

Тройка $M = (S, R, L)$:

- S — конечное множество *состояний*;
- $R \subseteq S \times S$ — отношение *переходов* (обычно тотальное);
- $L : S \to \mathcal{P}(\mathrm{AP})$ — *разметка*: атомарные утверждения, истинные в состоянии.

Пути и светофор

Путь — бесконечная последовательность $\pi = s_0, s_1, s_2, \ldots$ с $(s_i, s_{i+1}) \in R$.

Пример (Светофор)

- Состояния G, Y, R.
- Переходы $G \to Y \to R \to G$.
- Разметка $L(G) = \{\text{green}\}$, $L(Y) = \{\text{yellow}\}$, $L(R) = \{\text{red}\}$.

LTL: линейная темпоральная логика

Определение 4 (Синтаксис LTL)

Формулы о *путях*:

- атомарные p;
- $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$;
- $\bigcirc\, \varphi$ («в следующем состоянии»);
- $\varphi U \psi$ («до тех пор, пока»).

Производные операторы:

- $\Diamond\varphi \equiv \text{true}\ U\varphi$ — «когда-нибудь»;
- $\Box\varphi \equiv \neg\Diamond\neg\varphi$ — «всегда».

Семантика LTL

Определение 5 (Семантика LTL)

На пути $\pi = s_0, s_1, \ldots$:

- $\pi \vDash \bigcirc \varphi$ тогда и только тогда, когда $\pi^1 \vDash \varphi$;
- $\pi \vDash \varphi U \psi$ тогда и только тогда, когда существует $j \geq 0$: $\pi^j \vDash \psi$ и $\forall i < j : \pi^i \vDash \varphi$.

Пример (Свойства в LTL)

- Светофор: $\square(\text{green} \rightarrow \diamondsuit\ \text{red})$ — «после зелёного когда-нибудь красный».
- Ответ на запрос: $\square(\text{request} \rightarrow \diamondsuit\ \text{response})$.
- Взаимная блокировка: $\square\neg(\text{crit}_1 \wedge \text{crit}_2)$.

CTL: логика ветвящегося времени

Определение 6 (Синтаксис CTL)

Кванторы пути перед темпоральным оператором — A («на всех путях») и E («существует путь»):

- $A \bigcirc \varphi$, $E \bigcirc \varphi$;
- $A(\varphi U \psi)$, $E(\varphi U \psi)$.

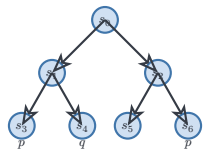
$A\Diamond$ resp — «ответ гарантирован при любом ходе системы». $E\Diamond$ resp — «существует ход, приводящий к ответу».

Пример (Свойства в CTL)

- «Всегда возможно перезапуск» — $A\Box E\Diamond$ restart: в каждом состоянии любого пути есть продолжение к перезапуску.
- Взаимное исключение — $A\Box\neg(\mathrm{crit}_1 \wedge \mathrm{crit}_2)$.

Дерево вычислений

Корень s_0 — текущее состояние, от него отходят *все* преемники по R. Каждая ветвь вниз — один возможный путь, одно будущее. Точка ветвления — момент выбора следующего хода.



A — «на *всех* ветвях из корня», E — «существует ветвь». Кванторы CTL пробегают по ветвям этого дерева.

LTL против CTL

Выразительные силы LTL и CTL несравнимы:

- $A\Box E\Diamond$ restart выразимо в CTL, но не в LTL — LTL не умеет говорить «существует путь» внутри пути;
- справедливость $A(\Box\Diamond p \to \Diamond q)$ выразима в LTL, но не в CTL.

Пример (Неподвижные точки CTL)

- $E(\varphi U \psi) \equiv \psi \vee (\varphi \wedge E \bigcirc E(\varphi U \psi))$ — наименьшая неподвижная точка.
- $E\Box\varphi \equiv \varphi \wedge E \bigcirc E\Box\varphi$ — наибольшая.
- $A(\varphi U \psi) \equiv \psi \vee (\varphi \wedge A \bigcirc A(\varphi U \psi))$.

Model checking: разметка состояний

Определение 7 (Labeling-алгоритм)

Проверка $E(\varphi U \psi)$ в модели $M = (S, R, L)$ через пре-образ $\mathrm{pre}_\exists(X) = \{s : \exists s' \in R(s), s' \in X\}$:

- $Y := \{s : s \vDash \psi\}$;
- повторять, пока не стабилизируется: $Y := Y \cup (\{s : s \vDash \varphi\} \cap \mathrm{pre}_\exists(Y))$.

Итог Y — в точности состояния с $E(\varphi U \psi)$.

Для $A\Box\varphi$ — пре-образ «по всем преемникам»: $\mathrm{pre}_\forall(X) = \{s : \forall s' \in R(s), s' \in X\}$.

- Живость ($\Diamond$, U) — наименьшие неподвижные точки; безопасность ($\Box$) — наибольшие.
- Безопасность опровергается конечным префиксом, живость — только бесконечным путём.

LTL через автоматы Бюхи

Model checking LTL сложнее CTL: формула говорит обо всех путях, прямой labeling не работает.

Три шага:

1. Построить автомат Бюхи $A_{\neg\varphi}$ для отрицания свойства — принимает ровно пути, где $\neg\varphi$ истинна.
2. Построить синхронное произведение $M \times A_{\neg\varphi}$.
3. Искать путь, бесконечно часто попадающий в принимающие состояния.

Нет пути — свойство выполняется. Есть путь — контрпример.

BDD и инструменты

Практическая трудность — взрыв пространства состояний: n булевых переменных дают 2^n состояний.

Современные model checker'ы (NuSMV, SPIN) справляются с 10^{20} состояниями благодаря *символьной верификации*: множества состояний представляются BDD (бинарными решающими диаграммами), а операции над множествами — операциями над BDD.

Пример (Взаимное исключение)

Два процесса конкурируют за критическую секцию.

Требование — $A\Box\neg(\text{crit}_1 \wedge \text{crit}_2)$: никогда не бывает, что оба в критической секции.

Найденный путь с обоими в критической секции — контрпример, диагностика гонки.

Что мы поняли?

- Модальная логика — логика миров и достижимости: $\Box$ и $\Diamond$ читаются через отношение R.
- Каждой аксиоме соответствует свойство отношения: D — серийность, T — рефлексивность, B — симметричность, 4 — транзитивность.
- Модели Крипке — модальные модели, где миры — состояния, достижимость — шаг выполнения.
- LTL говорит о путях, CTL — о ветвлении будущего; их выразительные силы несравнимы.
- Model checking проверяет CTL разметкой через неподвижные точки, LTL — через автоматы Бюхи.
- Взрыв состояний сдерживается символьными представлениями (BDD).

Вопросы для самопроверки

- Чем фрейм отличается от модели Крипке? Что добавляет оценка V?
- Какое свойство отношения соответствует аксиоме T: $\Box p \to p$? Докажите в одну сторону.
- Почему $\Box p \to p$ может быть истинна в модели, где R не рефлексивно?
- Запишите в LTL «после запроса всегда рано или поздно ответ».
- Чем $A\Diamond$ resp отличается от $E\Diamond$ resp?
- Почему $A\Box E\Diamond$ restart не выразимо в LTL?
- Что такое наименьшая и наибольшая неподвижная точка в model checking CTL?