Нижние экспоненциальные оценки для модальных логик

Pavel Hrubeš
в изложении
Ариста Кожевникова

ПОМИ РАН

18 апреля 2008

Модальная логика

Расширим язык классической логики при помощи $\Box$ (“всегда”). Для построения модальных формул, к правилам построения формул классической логики, добавим следующие:

- Если A — формула, то $\Box A$ — формула.

Можно определить $\Diamond$ (“иногда”):

$$\Diamond A = \neg\Box\neg A.$$

Модальная логика

Расширим язык классической логики при помощи $\Box$ (“всегда”). Для построения модальных формул, к правилам построения формул классической логики, добавим следующие:

- Если A — формула, то $\Box A$ — формула.

Можно определить $\Diamond$ (“иногда”):

$$\Diamond A = \neg\Box\neg A.$$

Аксиоматизация минимальной модальной логики K

Система Фреге:

$A \to (B \to A)$, $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,
$A \wedge B \to B$, $A \wedge B \to A$, $(A \to (B \to C)) \to (A \wedge B \to C)$,
$A \to A \vee B$, $B \to A \vee B$, $(B \to A) \to ((C \to A) \to (B \vee C \to A))$,
$\bot \to A$, $\neg\neg A \to A$

Правила обобщения и modus ponens:

$$\frac{A}{\Box A} \quad \text{и} \quad \frac{A \quad A \to B}{B}$$

Схема аксиом дистрибутивности:

$$\Box(A \to B) \to (\Box A \to \Box B).$$

Аксиоматизация минимальной модальной логики K

Система Фреге:

$A \to (B \to A)$, $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,
$A \wedge B \to B$, $A \wedge B \to A$, $(A \to (B \to C)) \to (A \wedge B \to C)$,
$A \to A \vee B$, $B \to A \vee B$, $(B \to A) \to ((C \to A) \to (B \vee C \to A))$,
$\bot \to A$, $\neg\neg A \to A$

Правила обобщения и modus ponens:

$$\frac{A}{\Box A} \quad \text{и} \quad \frac{A \quad A \to B}{B}$$

Схема аксиом дистрибутивности:

$$\Box(A \to B) \to (\Box A \to \Box B).$$

Аксиоматизация минимальной модальной логики K

Система Фреге:

$A \to (B \to A)$, $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,
$A \wedge B \to B$, $A \wedge B \to A$, $(A \to (B \to C)) \to (A \wedge B \to C)$,
$A \to A \vee B$, $B \to A \vee B$, $(B \to A) \to ((C \to A) \to (B \vee C \to A))$,
$\bot \to A$, $\neg\neg A \to A$

Правила обобщения и modus ponens:

$$\frac{A}{\Box A} \quad \text{и} \quad \frac{A \quad A \to B}{B}$$

Схема аксиом дистрибутивности:

$$\Box(A \to B) \to (\Box A \to \Box B).$$

Семантика Крипке для K

Пусть R — отношение на наборах значений переменных, пара (R, x), где x — набор значений переменных, выполняет формулу A, $(R, x) \models A$.

$(R, x) \models p$, если переменная p имеет значение 1 в x;

$(R, x) \models \neg A$, если $(R, x) \not\models A$;

$(R, x) \models A \wedge B$, если $(R, x) \models A$ и $(R, x) \models B$;

...

$(R, x) \models \Box A$, если $(R, y) \models A$ для всех $(x, y) \in R$.

Семантика Крипке для K

Пусть R — отношение на наборах значений переменных, пара (R, x), где x — набор значений переменных, выполняет формулу A, $(R, x) \models A$.
$(R, x) \models p$, если переменная p имеет значение 1 в x;
$(R, x) \models \neg A$, если $(R, x) \not\models A$;
$(R, x) \models A \wedge B$, если $(R, x) \models A$ и $(R, x) \models B$;
...
$(R, x) \models \Box A$, если $(R, y) \models A$ для всех $(x, y) \in R$.

Семантика Крипке для K

Пусть R — отношение на наборах значений переменных, пара (R, x), где x — набор значений переменных, выполняет формулу A, $(R, x) \models A$.
$(R, x) \models p$, если переменная p имеет значение 1 в x;
$(R, x) \models \neg A$, если $(R, x) \not\models A$;
$(R, x) \models A \wedge B$, если $(R, x) \models A$ и $(R, x) \models B$;
...
$(R, x) \models \Box A$, если $(R, y) \models A$ для всех $(x, y) \in R$.

Другие модальные логики

- S:
  Отношение R — рефлективно (т.е. $(x, x) \in R$) $\Leftrightarrow$
  $\mathsf{K} + \Box A \to A$
- K4:
  Отношение R — транзитивно
  (т.е. $(x, y), (y, z) \in R \Rightarrow (x, y) \in R$) $\Leftrightarrow \mathsf{K} + \Box A \to \Box\Box A$
- K5: Отношение R — транзитивно и симметрично
  (т.е. $(x, y) \in R \Rightarrow (y, x) \in R$) $\Leftrightarrow \mathsf{K4} + \neg\Box A \to \Box\neg\Box A$

Другие модальные логики

- S:
  Отношение R — рефлективно (т.е. $(x, x) \in R$) $\Leftrightarrow$
  $\mathsf{K} + \Box A \to A$
- K4:
  Отношение R — транзитивно
  (т.е. $(x, y), (y, z) \in R \Rightarrow (x, y) \in R$) $\Leftrightarrow \mathsf{K} + \Box A \to \Box\Box A$
- K5: Отношение R — транзитивно и симметрично
  (т.е. $(x, y) \in R \Rightarrow (y, x) \in R$) $\Leftrightarrow \mathsf{K4} + \neg\Box A \to \Box\neg\Box A$

Другие модальные логики

- S:
  Отношение R — рефлективно (т.е. $(x, x) \in R$) $\Leftrightarrow$
  $\mathsf{K} + \Box A \to A$
- K4:
  Отношение R — транзитивно
  (т.е. $(x, y), (y, z) \in R \Rightarrow (x, y) \in R$) $\Leftrightarrow \mathsf{K} + \Box A \to \Box\Box A$
- K5: Отношение R — транзитивно и симметрично
  (т.е. $(x, y) \in R \Rightarrow (y, x) \in R$) $\Leftrightarrow \mathsf{K4} + \neg\Box A \to \Box\neg\Box A$

Интерполяция булевой схемой

Схема $C(\overline{p})$ интерполирует $A(\overline{p})$ и $B(\overline{p}, (\overline{r})$

1. для любого набора значений σ переменных $\overline{p}$, если $A(\sigma) = 1$, тогда $C(\sigma) = 1$;
2. если $C(\sigma) = 1$, тогда для всех θ $B(\sigma, \theta) = 1$.

Основная Теорема

Пусть A — монотонная формула, зависящая от переменных $\overline{p}$, пусть B — формула без модальностей и пусть

$$A(\Box\overline{p}) \to \Box B$$

имеет K-доказательство с применением n схем аксиом дистрибутивности. Тогда существует булева схема размера $O(n^2)$ интерполирующая A и B.

Интерполяция булевой схемой

Схема $C(\overline{p})$ интерполирует $A(\overline{p})$ и $B(\overline{p}, (\overline{r})$

1. для любого набора значений σ переменных $\overline{p}$, если $A(\sigma) = 1$, тогда $C(\sigma) = 1$;
2. если $C(\sigma) = 1$, тогда для всех θ $B(\sigma, \theta) = 1$.

Основная Теорема

Пусть A — монотонная формула, зависящая от переменных $\overline{p}$, пусть B — формула без модальностей и пусть

$$A(\Box\overline{p}) \to \Box B$$

имеет K-доказательство с применением n схем аксиом дистрибутивности. Тогда существует булева схема размера $O(n^2)$ интерполирующая A и B.

Идеи доказательства

1. Преобразовать K-доказательство в доказательство, в котором играют роль только применения аксиомы дистрибутивности.
2. Применение аксиомы дистрибутивности очень похоже на правило резолюции:

$$\frac{\Box A \qquad \Box(\neg A \vee B)}{\Box B},$$

построить по множеству применений аксиомы дистрибутивности монотонную булеву схему.

Идеи доказательства

1. Преобразовать K-доказательство в доказательство, в котором играют роль только применения аксиомы дистрибутивности.
2. Применение аксиомы дистрибутивности очень похоже на правило резолюции:

$$\frac{\Box A \qquad \Box(\neg A \vee B)}{\Box B},$$

построить по множеству применений аксиомы дистрибутивности монотонную булеву схему.

Упрощение доказательств: теория K_5^0

Расширим классическую систему Фреге правилами:

$$\frac{A}{\Box A}, \qquad \frac{A \Leftrightarrow B}{\Box A \Leftrightarrow \Box B}$$

и схемой аксиом

$$\Box((A \wedge \Box C) \vee (B \wedge \Box \neg C)) \Leftrightarrow (\Box A \wedge \Box C) \vee (\Box B \wedge \Box \neg C).$$

В K_5^0 нет аксиомы дистрибутивности + формулы с модальностями не зависят от настоящего мира.

Модели K_5^0

Пусть $\mathfrak{G}$ — набор множеств наборов значений переменных, x — набор значений переменных. Определим отношение $\langle \mathfrak{G}, x \rangle \models A$ индукцией по длине формулы A:

1. для переменных и классических связок стандартным образом;
2. $\langle \mathfrak{G}, x \rangle \models \Box A$, тогда и только тогда $\{u : u \models A\} \in \mathfrak{G}$.

Утверждение 1

K_5^0 не противоречива и полна для K_5^0-моделей, т.е. $K_5^0 \vdash A$ тогда и только тогда для любой K_5^0-модели M, $M \models A$.

Модели K_5^0

Пусть $\mathfrak{G}$ — набор множеств наборов значений переменных, x — набор значений переменных. Определим отношение $\langle \mathfrak{G}, x \rangle \models A$ индукцией по длине формулы A:

1. для переменных и классических связок стандартным образом;
2. $\langle \mathfrak{G}, x \rangle \models \Box A$, тогда и только тогда $\{u : u \models A\} \in \mathfrak{G}$.

Утверждение 1

K_5^0 не противоречива и полна для K_5^0-моделей, т.е. $\mathsf{K}_5^0 \vdash A$ тогда и только тогда для любой K_5^0-модели M, $M \models A$.

Свойства K_5^0

Утверждение 2

Для любой формулы A существует такая формула A' модальной глубины 1, что

$$K_5^0 \models A \Leftrightarrow A'.$$

Свойства K_5^0

Утверждение 3

Пусть A — K-тавтология.

1. Пусть Γ — множество применений аксиомы дистрибутивности возникающих в K-доказательстве A, тогда следующие — K_5^0-тавтология:

$$\bigwedge \Gamma \to A. \tag{1}$$

2. Пусть для любого Γ: $|\Gamma| < k$ формула (1) — не K_5^0-тавтология, тогда любое K-доказательстве A содержит по крайней мере k аксиом дистрибутивности.

Свойства K_5^0

Утверждение 4

Для модальной формулы A обозначим через A' — формулу, получаемую из A удалением всех $\Box$ в A а через A^* — формулу, получаемую из A удалением всех $\Box$ в области действия другого $\Box$. Тогда:

1. Если A — K-тавтология, тогда A' — тавтология.
2. Если A — K-тавтология, тогда A^* — K-тавтология. Более того, если A имеет K-доказательство S с n применями аксиомы дистрибутивности, тогда A^* имеет K-доказательство S^*:
    1. S^* содержит n применений аксиомы дистрибутивности;
    2. все модальная глубина всех формул в S^* равна 1.

Свойства K_5^0

Утверждение 5

Доказательство S K-тавтологии A с n применениями аксиомы дистрибутивности можно преобразовать в доказательство S^* с n применениями аксиомы дистрибутивности, каждое из которых имеет модальную глубину 1.

Блок-схема

Определение

Направленный граф с метками M называется блок-схемой, если

1. Метки на вершинах уникальны и существуют вершины с метками $p_1, \ldots, p_n$ и 1.
2. Для любого ребра (a, b) в M существует вершина a': (a', b) — ребро в M и оба ребра имеют метку $\wedge\{a, a'\}$. Такая пара называется $\wedge$-гейтом, будем говорить $b = a \wedge a'$.

Выражение $b = a \vee a'$ можно записать при помощи двух $\wedge$-гейтов: $b = a \wedge 1$ и $b = a' \wedge 1$. Более того

Утверждение 6

Если функция f вычисляется блок-схемой размера n, то существует булева схема размера $O(n^2)$, вычисляющая f.

Блок-схемы для дистрибутивностей

Обозначим $[A] := u : u \models A$. Построим блок-схему M для множества применений аксиомы дистрибутивности Γ:

1. добавим все $[p_i]$ в M и 1 для всего множества наборов значений переменных;
2. для $\Box(A \to B) \wedge \Box A \to \Box B$ добавим (если их ещё нет) вершины $[-A \cup B], [A], [B]$ в M и $\wedge$-гейт $[B] = [-A \cup B] \wedge [A]$.

Свойства блок-схем для дистрибутивностей

Утверждение 7

Пусть M — блок-схема для некоторого множества применений аксиомы дистрибутивности Г, пусть M содержит вершину $[A]$ и пусть σ — набор значений для p_i такой, что $[A]$ получает значение 1 в M. Тогда

$$K \vdash \bigvee_{p_i|_\sigma = 1} \Box p_i \to \Box A.$$

Утверждение 8

Пусть M — блок-схема для некоторого множества применений аксиомы дистрибутивности Г, пусть M содержит вершину $[A]$ и пусть σ — набор значений для p_i такой, что $[A]$ получает значение 0 в M. Тогда существует такая модель M, что $M \models \Box p_i$ и $M \not\models \Box A$.

Свойства блок-схем для дистрибутивностей

Утверждение 7

Пусть M — блок-схема для некоторого множества применений аксиомы дистрибутивности Γ, пусть M содержит вершину $[A]$ и пусть σ — набор значений для p_i такой, что $[A]$ получает значение 1 в M. Тогда

$$K \vdash \bigvee_{p_i|_\sigma = 1} \Box p_i \to \Box A.$$

Утверждение 8

Пусть M — блок-схема для некоторого множества применений аксиомы дистрибутивности Γ, пусть M содержит вершину $[A]$ и пусть σ — набор значений для p_i такой, что $[A]$ получает значение 0 в M. Тогда существует такая модель M, что $M \models \Box p_i$ и $M \not\models \Box A$.

Другие модальные логики

Аналогичные оценки можно доказать и для других модальных логик (кроме K5). Более того, можно доказать их экспоненциальную отделимость друг от друга.

Спасибо за внимание!