Бескванторная линейная вероятностная логика (в измеримом случае)

Дмитрий Ярцев

9 октября 2020

Сигнатура языка

- $\Phi = \{p_1, p_2, ...\}$ — бесконечное множество элементарных высказываний (элементарных событий);
- $\wedge^2, \vee^2, \neg^1$ — символы пропозициональной логики;
- w^1 — символ для перехода к вероятности события;
- $\geqslant^2, +^2$ — символы логики неравенств;
- $true = p \vee \neg p$, $false = \neg true$.
- Пропозициональные формулы (события) — замыкание Φ под действием логических связок.

Термы и формулы с весами

- Базовый терм с весом — это выражение вида $w(\varphi)$, где φ — пропозициональная формула;
- Терм с весом (далее просто "терм") — это выражение вида $a_1 w(\varphi_1) + a_2 w(\varphi_2) + \ldots + a_k w(\varphi_k)$, где a_i — целые числа, $k \geqslant 1$;
- Базовая формула с весом — это выражение вида $t \geqslant c$, где t — терм, c — целое число;
- Формула с весом (или просто "формула") — это булева комбинация базовых формул.

Замечание: мы иногда будем допускать не только целые, но и любые рациональные коэффициенты. Так можно делать, поскольку любое неравенство с рациональными весами равносильно некоторому неравенству с целыми весами.

Некоторые сокращения

Мы будем использовать некоторые интуитивные сокращения, а именно:

- $w(\varphi) - w(\psi) \geqslant a$ означает $w(\varphi) + (-1)w(\psi) \geqslant a$;
- $w(\varphi) \geqslant w(\psi)$ означает $w(\varphi) - w(\psi) \geqslant 0$;
- $w(\varphi) \leqslant c$ означает $-w(\varphi) \geqslant -c$;
- $w(\varphi) < c$ означает $\neg(w(\varphi) \geqslant c)$, аналогично для $>$;
- $w(\varphi) = c$ означает $(w(\varphi) \leqslant c) \wedge (w(\varphi) \geqslant c)$;
- и т.п.

Оценочная семантика

Вероятностной структурой называется четвёрка $M = (X, \mathcal{F}, \mu, \pi)$, где $(X, \mathcal{F}, \mu)$ — вероятностное пространство, а функция $\pi : X \to \{true, false\}^{\Phi}$ предписывает каждому состоянию пространства X, какие переменные в нём истинны.
Оценку π можно естественным образом распространить на всё множество пропозициональных формул. Свяжем теперь с каждой переменной p множество $p^M = \{x \in X \mid \pi(x)(p) = true\}$, а с каждой пропозицональной формулой φ — множество $\varphi^M = \{x \in X \mid \pi(x)(\varphi) = true\}$.
Вероятностная структура называется измеримой, если все множества p^M измеримы, т.е. лежат в $\mathcal{F}$. Нетрудно понять, что тогда измеримы и все множества φ^M. В дальнейшем нас будут интересовать лишь измеримые структуры.

Семантическое следование

Будем говорить, что $M \vDash a_1 w(\varphi_1) + a_2 w(\varphi_2) + \ldots + a_k w(\varphi_k) \geqslant c$ (формула $a_1 w(\varphi_1) + a_2 w(\varphi_2) + \ldots + a_k w(\varphi_k) \geqslant c$ выполняется в структуре M), если

$$a_1 \mu(\varphi_1^M) + a_2 \mu(\varphi_2^M) + \ldots + a_k \mu(\varphi_k^M) \geqslant c.$$

Отношение $\vDash$ естественным образом продолжается на все формулы с весом, а именно

$$M \vDash \neg f \Leftrightarrow M \nvDash f,$$

$$M \vDash f \wedge g \Leftrightarrow M \vDash f \text{ и } M \vDash g.$$

Говорят, что формула общезначима, если она выполняется в каждой структуре, и выполнима, если она выполнена в какой-нибудь структуре.

Аксиомы вероятностной логики

Система аксиом AX_{MEAS} включает в себя следующее:

- Taut. Все пропозициональные тавтологии, в которые подставили все возможные наборы формул с весом;
- Ineq. Все тавтологии логики линейных неравенств, в которые подставили все возможные наборы термов с весом;
- Вероятностные аксиомы (схемы аксиом):
  - W1. $w(\varphi) \geqslant 0$ — неотрицательность;
  - W2. $w(true) = 1$ — вероятность истины равна 1;
  - W3. $w(\varphi \wedge \psi) + w(\varphi \wedge \neg\psi) = w(\varphi)$ — **конечная** аддитивность;
  - W4. Для всех пропозициональных тавтологий вида $\varphi \leftrightarrow \psi$ $w(\varphi) = w(\psi)$ — дистрибутивность.

Единственное правило вывода в логике — это MP.

Замечание: поскольку аддитивность конечная, а не счётная, у логики существуют нестандартные модели, не являющиеся вероятностными структурами.

Пример — вывод формулы $w(false) = 0$:

1. $w(true \wedge true) + w(true \wedge false) = w(true)$ — W3;
2. $w(true \wedge true) = w(true)$ — W4;
3. $w(true \wedge false) = w(false)$ — W4;
4. $w(true) + w(false) = w(true)$ — Ineq + 1-3 + MP;
5. $w(false) = 0$ — Ineq + 4 + MP;

Альтернативное определение полноты

Формула f называется противоречивой, если $\neg f$ выводима.

Теорема

Система аксиом, в которой верен закон исключённого третьего, полна (т.е. каждая общезначимая формула в ней выводима) тогда и только тогда, когда каждая непротиворечивая формула выполнима.

Доказательство. $\Rightarrow$: если формула f невыполнима, то $\neg f$ — тавтология. Значит, $\neg f$ выводима, а f противоречива.
$\Leftarrow$: если формула f невыводима, то $\neg f$ — непротиворечива. Значит, $\neg f$ выполнима, а f — не тавтология.

Теорема о полноте

Теорема

AX_{MEAS} корректна и полна в измеримых вероятностных структурах, то есть:

1. *Все формулы, выводимые в AX_{MEAS}, истинны во всех измеримых вероятностных структурах;*
2. *Каждая непротиворечивая в AX_{MEAS} формула выполнена в некоторой измеримой вероятностной структуре.*

Доказательство. Корректность очевидна, поскольку все аксиомы и MP верны в ИВС.

Доказательство полноты

Рассмотрим непротиворечивую формулу f. Рассмотрим её ДНФ $g_1 \vee g_2 \vee \ldots \vee g_r$, где все g_i являются конъюнкциями базовых формул с весом и их отрицаний. Можно считать $f = g_1 \vee \ldots \vee g_r$, так как эквивалентность $f \leftrightarrow g_1 \vee \ldots \vee g_r$ всегда выводима, а эквивалентность сохраняет непротиворечивость.
Поскольку формула f непротиворечива, одна из формул g_i тоже непротиворечива: если выводимы все формулы $\neg g_i$, то выводима и их конъюнцкия $\neg(g_1 \vee \ldots \vee g_r)$. В то же время f выполняется в каждой модели, где выполняется одна из g_i, поэтому достаточно построить модель для случая, когда f — конъюнкция базовых формул с весом и их отрицаний.

n-атомы

Назовём *n*-атомом (или просто атомом) пропозициональный терм вида $p_1' \wedge p_2' \wedge \ldots \wedge p_n'$, где каждый член p_i' — это либо элементарное высказывание p_i, либо его отрицание.

Лемма

Пусть пропозициональная формула φ содержит в себе переменные $p_1, \ldots, p_n$, из которых можно составить атомы $\psi_1, \ldots, \psi_{2^n}$. Тогда формула $w(\varphi) = w(\varphi \wedge \psi_1) + \ldots + w(\varphi \wedge \psi_{2^n})$ выводима.

Доказательство. Простая индукция с использованием аксиомы аддитивности.

Следствие: пусть пропозициональная формула φ содержит переменные $p_1, \ldots, p_n$. Рассмотрим множество $At_n(\varphi)$ атомов δ, для которых тавтологична импликация $\delta \to \varphi$. Тогда формула $w(\varphi) = \sum_{\delta \in At_n(\varphi)} w(\delta)$ выводима.

Продолжение доказательства

Воспользовавшись леммой, перепишем каждый терм внутри f в виде $a_1 w(\delta_1) + a_2 w(\delta_2) + ... + a_{2^n} w(\delta_{2^n})$, где в формулу f входят переменные $p_1, ..., p_n$, из которых всевозможным образом составлены атомы $\delta_1, ..., \delta_{2^n}$.
Рассмотрим формулу f', для получения которой припишем к f конъюнкты
$w(\delta_j) \geqslant 0, w(\delta_1) + ... + w(\delta_{2^n}) \geqslant 1, -w(\delta_1) - ... - w(\delta_{2^n}) \geqslant -1$.
Поскольку новые конъюнкты выводимы, выводима и эквивалентность $f' \leftrightarrow f$.

Промежуточный итог

Итак, нам удалось найти формулу, которая выводимо эквивалентна исходной и при этом соответствует системе неравенств с целыми коэффициентами

$$\begin{cases} w(\delta_1) \geqslant 0 \\ \dots \\ w(\delta_{2^n}) \geqslant 0 \\ w(\delta_1) + \dots + w(\delta_{2^n}) \geqslant 1 \\ -w(\delta_1) - \dots - w(\delta_{2^n}) \geqslant -1 \\ a_{1,1} w(\delta_1) + \dots + a_{1,2^n} w(\delta_{2^n}) \geqslant c_1 \\ \dots \\ a_{r,1} w(\delta_1) + \dots + a_{r,2^n} w(\delta_{2^n}) \geqslant c_r \\ -a'_{1,1} w(\delta_1) - \dots - a'_{1,2^n} w(\delta_{2^n}) > -c'_1 \\ \dots \\ -a_{s,1} w(\delta_1) + \dots + a_{s,2^n} w(\delta_{2^n}) > -c'_s. \end{cases}$$

Промежуточный итог

Она выполнима тогда и только тогда, когда выполнима система неравенств

$$\begin{cases} x_1 \geqslant 0 \\ \ldots \\ x_{2^n} \geqslant 0 \\ x_1 + \ldots + x_{2^n} \geqslant 1 \\ -x_1 - \ldots - x_{2^n} \geqslant -1 \\ a_{1,1}x_1 + \ldots + a_{1,2^n}x_{2^n} \geqslant c_1 \\ \ldots \\ a_{r,1}x_1 + \ldots + a_{r,2^n}x_{2^n} \geqslant c_r \\ -a'_{1,1}x_1 - \ldots - a'_{1,2^n}x_{2^n} > -c'_1 \\ \ldots \\ -a_{s,1}x_1 + \ldots + a_{s,2^n}x_{2^n} > -c'_s. \end{cases} \tag{1}$$

Окончание доказательства

Либо эта система выполнима, либо её отрицание является аксиомой *Ineq*, откуда следовала бы выводимость $\neg f'$. Второй случай невозможен, поэтому всегда имеет место первый. Решения системы естественным образом соответствуют распределениям на вероятностных пространствах, поэтому f' и эквивалентная ей f всегда выполнимы, ч.т.д.

Теорема о маленькой модели

Назовём длиной формулы f число $|f|$ символов, необходимых для её записи (коэффициенты считаются за 1 символ). Тогда справедлива следующая

Теорема

Если формула f выполнима в измеримой структуре, то она выполнена в некоторой ИВС, где состояний не более $|f|$, а любое множество состояний измеримо.

Вспомогательная лемма (почти без доказательства)

Лемма

Если система из r линейных уравнений имеет решение в неотрицательных числах, то она имеет такое неотрицательное решение, где положительны значения не более r переменных.

Доказательство. Множество векторов, удовлетворяющих одному линейному уравнению — это аффинная гиперплоскость в пространстве наборов переменных. Тогда все решения системы тоже образуют непустое аффинное подпространство. Возможны два случая.

Два случая

Случай 1: это пространство состоит из одной точки. Поскольку каждая новая гиперплоскость уменьшает размерность пространства решений не более, чем на 1, в пересечении уже участвовало не меньше уравнений, чем было переменных.
Случай 2: это пространство размерности хотя бы 1. Тогда оно пересекает границу ортанта, т.е. одну из переменных можно обнулить, оставив остальные неотрицательными. Ведя индукцию по числу переменных, мы докажем теорему.

Следствие для неравенств

Следствие: если система из r линейных равенств и/или неравенств имеет неотрицательное решение, то она имеет такое неотрицательное решение, где отличны от нуля значения не более r переменных.

Доказательство. Заменим каждое (не)равенство $h(x_1, \ldots, x_k) = (\geqslant, >)c$ на $h(x_1, \ldots, x_k) = h(x_1^*, \ldots, x_k^*)$, где $(x_1^*, \ldots, x_k^*)$ — какое-то решение системы. У новой системы уравнений есть решение с не более, чем r не-нулями, оно же будет решением старой системы, т.к. все правые части константы.

Доказательство теоремы о маленькой модели

Рассмотрим выполнимую формулу f. Запишем её в ДНФ. Отметим, что каждый дизъюнкт — это конъюнкция не более, чем $|f| - 1$, базовых формул и их отрицаний. Поскольку f выполнима, у её ДНФ есть выполнимый дизъюнкт g. Построим по формуле g линейную систему, как (1), но без ограничения на неотрицательность и заменой следующих двух неравенств на одно уравнение. У этой системы будет неотрицательное решение, а тогда неотрицательными можно оставить не более $r + s + 1 \leqslant |f|$ переменных. Такое решение соответствует ИВС, где атомов не более $|f|$, а измеримыми можно считать все их множества.

Размеры чисел и формул

Будем называть длиной целого числа его длину в двоичной записи, размером обыкновенной дроби — сумму длин её числителя и знаменателя, а символом $||f||$ — наибольшую из длин всех коэффициентов, входящих в формулу f. Тогда теорему о маленькой модели можно усилить.

Теорема

Если формула f выполнима в измеримой структуре, то она выполнена в некоторой структуре, где состояний не более $|f|$, любое множество состояний измеримо, а мера каждого состояния — рациональное число размера $O(|f| \cdot ||f|| + |f| \log(|f|))$.

Усиление вспомогательной леммы

Лемма

Если система из r линейных уравнений с целыми коэффициентами длины не более l имеет неотрицательное решение, то она имеет такое неотрицательное решение, где не более r переменных положительны, причём они также рациональны и имеют размер $O(rl + r\log r)$.

Доказательство. Можно считать, что система невырождена. Рассуждая, как в доказательстве слабой версии, сведём задачу к случаю, когда решение единственно. Получилась квадратная система размера не более $r \times r$ с коэффициентами длины не более l. Её решение находится по методу Крамера и состоит из отношений двух определителей.

Все определители — это суммы $r!$ слагаемых длины не более rl, поэтому длина определителя есть $O(rl + \log(r!))$. Тогда размер частного двух таких определителей тоже есть $O(rl + r\log r)$.

Следствие для неравенств тоже верно, но мы воспользуемся им без доказательства.

Последняя лемма

Лемма

Рассмотрим формулу f и две ИВС $M = (X, \mathcal{F}, \mu, \pi)$, $M' = (X, \mathcal{F}, \mu, \pi')$, отличающиеся только оценками. Предположим, что $\pi(s)(p) = \pi'(s)(p)$ для каждого состояния s и элементарного высказывания p, входящего в формулу f. Тогда $M \models f \Leftrightarrow M' \models f$.

Доказательство. Для базовых формул эта лемма верна по определению, а ещё её истинность сохраняется при применении логических связок.

Задача о выполнимости формулы с весом

Теорема

Задача о выполнимости формулы с весом в измеримой вероятностной структуре NP-полна.

Доказательство. NP-трудность очевидна: пропозициональная формула φ выполнима тогда и только тогда, когда выполнима формула с весом $w(\varphi) > 0$. Докажем принадлежность NP. Если формула f выполнима в ИВС, то можно недетерминированно угадать число атомов в малой модели (их не больше $|f|$), меры всех атомов (это рациональные числа размера $O(|f| \cdot ||f|| + |f| \log(|f|))$ и значения оценки во всех атомах для всех переменных, входящих в f (число пар (состояние, переменная из f) тоже полиномиально зависит от длины входа $\Omega(|f| + ||f||)$). Задачу проверки истинности формулы f в данной ИВС можно решить за полиномиальное время от размера формулы и структуры (для базовых формул — полным перебором атомов, где они истинны, для более сложных — поочерёдно интерпретируя связки). Так мы научились недетерминированно решать задачу за полиномиальное время.

Спасибо!
Вопросы?