Экспоненциальная нижняя оценка размерности эмбеддингов для ранжирования лемм

Р. А. Хрулев*

Леммы-кандидаты для тактик Lean 4 часто отбирают векторным поиском по скалярному произведению эмбеддингов цели и леммы. Показано, что не существует фиксированной размерности эмбеддингов, достаточной для точного ранжирования лемм: уже на явном семействе лемм-переписываний, шаблон которых состоит из m блоков по m^2 разностей, необходимая размерность растёт экспоненциально по m.

Ключевые слова: поиск лемм, эмбеддинги, автоматическое доказательство теорем, Lean 4, нижние оценки.

Пусть X — состояние доказательства в системе Lean 4 (цель и гипотезы), Λ — библиотека лемм. Тактика (`rw`, `apply`) проверяет, применима ли лемма $\ell \in \Lambda$ к X, получая на вход одновременно и X, и ℓ. Проверять так все леммы на каждом шаге доказательства (т. е. для каждого нового состояния X) дорого, поэтому кандидатов отбирают векторным поиском [1]: эмбеддинг $g(\ell)$ каждой леммы вычисляется заранее, один раз, а на каждом шаге вычисляется только эмбеддинг $f(X)$ текущего состояния; затем тактикой проверяются лишь несколько лемм с наибольшей оценкой $S(X, \ell) = \langle f(X), g(\ell)\rangle = \sum_{k=1}^{d} f_k(X)\, g_k(\ell)$. Здесь f и g — любые отображения в $\mathbb{R}^d$, но, в отличие от тактики, f видит только X, а g — только ℓ. Эмбеддинги *точно ранжируют* набор целей и лемм, если для каждой цели все применимые леммы оцениваются строго выше неприменимых.

Мы доказываем, что точное ранжирование лемм может требовать экспоненциальной размерности. Для этого строится семейство лемм-переписываний, шаблон которых состоит из m блоков по m^2 разностей; лемма применима к цели, если хотя бы в одном из m мест цели пройдены все проверки (разд. 1). Для этого семейства нужно $d \geq 2^{cm} - 1$, где $c > 0$ — абсолютная постоянная (теорема 1).

* *Хрулев Руслан Александрович* — аспирант каф. МаТИС мех.-мат. факультета МГУ; научный руководитель: Боков Григорий Владимирович, e-mail: `ra.khrulev@gmail.com`, ORCID: 0009-0000-3423-775X.

Khrulev Ruslan Aleksandrovich — PhD student, Department of Mathematical Theory of Intelligent Systems, Faculty of Mechanics and Mathematics, Moscow State University; scientific supervisor: Bokov Grigory Vladimirovich.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

1. Модель применимости

Лемма-переписывание имеет вид $\ell:\ \forall a,b,\dots\ Л(a,b,\dots)=П(a,b,\dots)$, где Л — *шаблон*. Вместо переменных шаблона $a,b,\dots$ можно подставлять любые термы, а переменные цели фиксированы. *Сопоставить* шаблон с подтермом t цели — найти подстановку, после которой шаблон совпадает с t; при этом Lean отождествляет некоторые термы, равные по определению. Тактика `rw [ℓ]` ищет такой подтерм и заменяет его правой частью. Например, лемма `sub_self`: $a-a=0$ переписывает цель $(x-y)+(z-z)=w$ в $(x-y)+0=w$, а на цели $(x-y)+(y-x)=w$ не срабатывает. *Повтор переменной в шаблоне — это проверка равенства*: подтермы цели на позициях этой переменной обязаны совпасть. *Место* — подтерм цели, к которому прикладывается шаблон; `rw [ℓ]` срабатывает $\iff$ есть место, где пройдены все проверки.

Определение 1 (семейство $\mathcal{G}_{m,L}$)**.** Все термы имеют тип $\mathbb{Z}$ и строятся из переменных операциями $+,-,\cdot$, причём в произведениях скобки всюду расставлены слева направо: $abc=(ab)c$. Все буквы ниже — переменные. *Лемма* ℓ_Y, $Y\in\{0,1\}^{m\times L}$, имеет шаблон $\prod_{k=1}^{m}\prod_{j=1}^{L}(u_{kj}-v_{kj})$; множители с одним k образуют *блок* k. Все u_{kj} различны; $v_{kj}=u_{kj}$ при $Y_{kj}=1$, а при $Y_{kj}=0$ v_{kj} — новая переменная. Правая часть на применимость не влияет; годится, например, произведение тех же множителей в обратном порядке. *Цель* с таблицей $X\in\{0,1\}^{m\times L}$ имеет вид $P_1+\dots+P_m=w$. Каждое слагаемое P_i (*место* i) устроено как шаблон: это произведение m блоков по L разностей. Блок i в P_i равен $(t_{i1}-t'_{i1})\cdots(t_{iL}-t'_{iL})$, где $t'_{ij}=t_{ij}$ при $X_{ij}=0$, а при $X_{ij}=1$ переменная t'_{ij} отлична от t_{ij}; остальные блоки $k\neq i$ равны $(e-e)\cdots(e-e)$.

В семействе $\mathcal{G}_{m,L}$ сопоставление сводится к буквальному совпадению (вычитание и умножение на $\mathbb{Z}$ при сопоставлении не раскрываются), поэтому вид шаблона в цели имеют только $P_1,\dots,P_m$, и при сопоставлении с P_i j-я разность k-го блока шаблона прикладывается к j-й разности k-го блока P_i. Нетривиальные проверки возникают только в блоке i (пары $(e-e)$ проходят любую проверку), т. е. строка i таблицы Y — требования к месту i.

Пусть даны лемма ℓ_Y и цель с таблицей X. Назовём j-ю разность блока i в месте P_i *препятствием*, если лемма требует равенства её членов ($Y_{ij}=1$: в шаблоне стоит $(u_{ij}-u_{ij})$), а в цели они различны ($X_{ij}=1$: стоит $(t_{ij}-t'_{ij})$, $t'_{ij}\neq t_{ij}$). Поэтому число препятствий в месте i равно $c_i(X,Y)=\sum_{j=1}^{L}X_{ij}Y_{ij}$.

Утверждение 1. *Переписывание* `rw [`ℓ_Y`]` *срабатывает на цели* $X \iff$ *в ней есть место без препятствий, т. е.* $c_i(X,Y) = 0$ *при некотором* i.

Пример: $m = L = 2$, $X = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, $P_1 = (x-y)(z-z)\cdot(e-e)(e-e)$, $P_2 = (e-e)(e-e)\cdot(x-x)(y-z)$. Две леммы:

$Y = \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$, $(a-a)(b-p)\cdot(q-r)(s-h)$, $(c_1,c_2) = (1,0)$: применима;
$Y = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, $(a-a)(b-p)\cdot(q-r)(s-s)$, $(c_1,c_2) = (1,1)$: неприменима.

2. Нижняя оценка

Определение 2. Пусть R — матрица из нулей и единиц. Вещественная матрица B того же размера *согласована по знакам* с R, если $B[X,Y] > 0$ при $R[X,Y] = 1$ и $B[X,Y] < 0$ при $R[X,Y] = 0$. *Знаковый ранг* $\operatorname{sr}(R)$ — минимум $\operatorname{rank} B$ по всем таким матрицам B.

Теорема Разборова–Шерстова ([2])**.** *Для* $X, Y \in \{0,1\}^{m\times L}$ *положим* $H_{m,L}[X,Y] = \bigwedge_{i=1}^{m}\bigvee_{j=1}^{L}(X_{ij}\wedge Y_{ij})$. *Существует* $c > 0$ *такое, что* $\operatorname{sr}(H_{m,m^2}) \geq 2^{cm}$ *при всех достаточно больших* m.

Теорема 1. *Если эмбеддинги* $f(X), g(\ell) \in \mathbb{R}^d$ *точно ранжируют* $\mathcal{G}_{m,m^2}$, *то при всех достаточно больших* m *выполнено* $d \geq 2^{cm} - 1$, *где* c — *постоянная из теоремы Разборова–Шерстова.*

Доказательство. Пусть $L = m^2$, $H = H_{m,L}$. Возьмём по одной цели с каждой таблицей X и все леммы ℓ_Y. Рассмотрим матрицы со строками X и столбцами Y: оценок $S[X,Y] = \langle f(X), g(\ell_Y)\rangle$ и *применимости* A: $A[X,Y] = 1$, если `rw [`ℓ_Y`]` срабатывает на цели X, иначе 0.

Шаг 1. Покажем, что $\operatorname{rank} S \leq d$. Имеем $S = FG^{\top}$, где строки матриц F и G — векторы $f(X)$ и $g(\ell_Y)$ длины d, поэтому $\operatorname{rank} S \leq \operatorname{rank} F \leq d$; здесь существенно, что f не видит лемму, а g — цель.

Шаг 2. Покажем, что $\operatorname{sr}(A) \leq d+1$. Ранжирование точное, поэтому для каждой строки X есть порог θ_X, меньший оценок всех применимых лемм и больший оценок всех неприменимых. Матрица $T[X,Y] = S[X,Y] - \theta_X$ согласована по знакам с A и отличается от S на матрицу ранга не более 1, поэтому $\operatorname{sr}(A) \leq \operatorname{rank} T \leq \operatorname{rank} S + 1 \leq d+1$ по определению 2.

Шаг 3. Покажем, что $\operatorname{sr}(A) = \operatorname{sr}(H) \geq 2^{cm}$. По утверждению 1 $A[X,Y] = 0 \iff c_i(X,Y) \geq 1$ при всех i, т. е. при всех i есть j с $X_{ij}Y_{ij} = 1$, а это и есть $H[X,Y] = 1$. Значит, $A = 1 - H$, и $\operatorname{sr}(A) = \operatorname{sr}(H)$: B согласована по знакам с $A \iff -B$ согласована с H, а $\operatorname{rank}(-B) = \operatorname{rank} B$. Наконец, в $\mathcal{G}_{m,L}$ есть цели и леммы со *всеми* таблицами X и Y, поэтому H — вся матрица H_{m,m^2}, и $\operatorname{sr}(H) \geq 2^{cm}$ по теореме Разборова–Шерстова. Вместе с шагом 2 получаем $d+1 \geq \operatorname{sr}(A) = \operatorname{sr}(H) \geq 2^{cm}$. □

Таким образом, точно ранжировать произвольные леммы эмбеддингами фиксированной размерности нельзя: размерность должна расти экспоненциально по числу блоков в шаблоне леммы. Оценка касается только точного ранжирования. Приближённый поиск, при котором среди нескольких лемм с наибольшей оценкой достаточно найти хотя бы одну применимую, — другая задача и тема дальнейших исследований.

Список литературы

[1] K. Yang et al., “LeanDojo: Theorem proving with retrieval-augmented language models”, *Advances in Neural Information Processing Systems*, NeurIPS, **36**, 2023, 21573–21612. DOI: 10.52202/075280-0944.

[2] A. A. Razborov, A. A. Sherstov, “The sign-rank of AC^0”, *SIAM J. Comput.*, **39**:5 (2010), 1833–1855. DOI: 10.1137/080744037 .

Статья поступила 23 октября 2026 г.

An Exponential Lower Bound on Embedding Dimension for Lemma Ranking

R. A. Khrulev

Lean 4 tactics often take candidate lemmas from vector search by the inner product of goal and lemma embeddings. We show that no fixed embedding dimension suffices to rank lemmas exactly: already on an explicit family of rewrite lemmas whose patterns consist of m blocks of m^2 differences, the required dimension grows exponentially in m.

Keywords: premise selection, embeddings, automated theorem proving, Lean 4, lower bounds.

References

[1] K. Yang et al., “LeanDojo: Theorem proving with retrieval-augmented language models”, *Advances in Neural Information Processing Systems*, NeurIPS, **36**, 2023, 21573–21612. DOI: 10.52202/075280-0944.

[2] A. A. Razborov, A. A. Sherstov, “The sign-rank of AC^0”, *SIAM J. Comput.*, **39**:5 (2010), 1833–1855. DOI: 10.1137/080744037.

Received on October 23, 2026