

# Вероятностные разделения в TFNP

Докладчик:

Киселёв Фёдор Алексеевич

24 сентября 2025 г.

# Часть 1: Основные определения

# Задачи поиска

---

## Определение

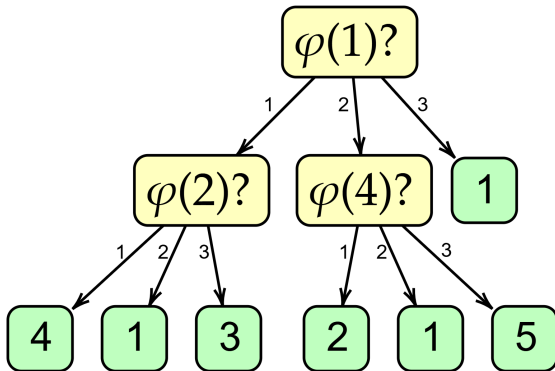
*Задачей поиска* называется последовательность  $R = \{R_N\}_{N=1}^{\infty}$ , где  $R_N \subset \Sigma_N^{l(N)} \times O_N$ .  $\Sigma_N$  называется *алфавитом*  $R_N$ ,  $l(N)$  - *длиной входов*  $R_N$ ,  $O_N$  - *множеством ответов*  $R_N$ . Говорим, что  $o \in O_N$  является *корректным ответом* на вход  $x \in \Sigma_N^{l(N)}$ , если  $(x, o) \in R_N$ .

Все интересующие нас задачи поиска будут *тотальными*, то есть для каждого входа будет существовать корректный ответ.

# Модель вычислений

- Все вычисления производятся семействами решающих деревьев
- Вычисления считаются эффективными, если глубина всех используемых деревьев ограничена одной  $f \in \text{poly}(\log N)$

Пример: решающее дерево, обращающееся к некоторой  $\varphi : [4] \rightarrow [3]$



# Задачи поиска

---

## Определение

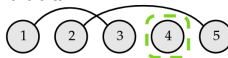
Задачей поиска называется последовательность  $R = \{R_N\}_{N=1}^{\infty}$ , где  $R_N \subset \Sigma_N^{l(N)} \times O_N$ .  $\Sigma_N$  называется алфавитом  $R_N$ ,  $l(N)$  - длиной входов  $R_N$ ,  $O_N$  - множеством ответов  $R_N$ . Говорим, что  $o \in O_N$  является корректным ответом на вход  $x \in \Sigma_N^{l(N)}$ , если  $(x, o) \in R_N$ . Задача поиска лежит в TFNP, если она *тотальна* (для каждого входа существует корректный ответ) и корректность ответа легко проверяется: для каждого  $N$  и  $o \in O_N$  существует решающее дерево  $T_{N,o}$  малой глубины, для которого  $(x, o) \in R_N \Leftrightarrow T_{N,o}(x) = 1$ .

Далее все рассматриваемые задачи лежат в TFNP.

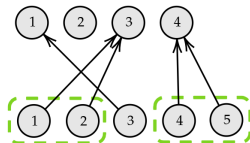
# Рассматриваемые задачи поиска

- PPA: задача поиска одинокого элемента в частичном разбиении  $[2N + 1]$  на пары.
- PPP: задача поиска коллизии в отображении  $\varphi : [N] \rightarrow [N - 1]$ .
- PLS: задача поиска вершины-стока в графе, где все все переходы по рёбрам ведут в вершину со строго бóльшим номером.

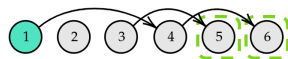
PPA:



PPP:



PLS:



 : корректные ответы

 : отображение (необратимое)

 : выделенный источник

# Рассматриваемые задачи поиска

- PPADS: задача поиска вершины-стока в графе на  $N$  вершинах с исходящими и входящими степенями не больше 1 и с выделенной вершиной-исток.
- PPAD: аналогично PPADS, но в качестве ответа также принимается любой исток, кроме выделенного.

PPADS:



PPAD:



 : корректные ответы

 : отображение (обратимое)

 : выделенный исток

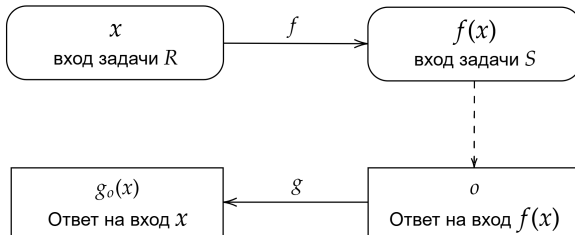
# Сведение

## Определение

Сведением  $R_N$  к  $S_M$  называется пара функций  $(f(x), g(o, x))$ , заданных наборами решающих деревьев. Сведение успешно на входе  $x$ , являющемся входом  $R_N$ , если:

$$\forall o : [(f(x), o) \in S_M \Rightarrow (x, g_o(x)) \in R_N].$$

Глубиной сведения будем называть максимальную глубину среди всех использованных в нём деревьев.



# Обычная и вероятностная сводимости

---

## Определение

Задача поиска  $R$  сводится к задаче поиска  $S$ , если для каждого  $N$  существует  $M$  и сведение  $R_N$  к  $S_M$  глубины не более  $\text{poly}(\log N)$ , успешное на всех входах.

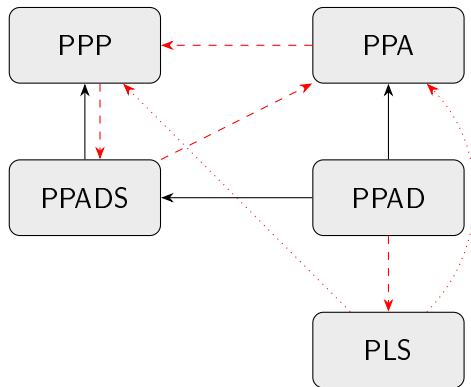
## Определение

Задача поиска  $R$  *вероятностно сводится* к задаче поиска  $S$ , если существует  $t = t(N) \leq \text{poly}(\log N)$  такое, что для любого  $N$  и распределения  $\mathcal{X}$  на входах  $R_N$  найдётся  $M$  и сведение  $R_N$  к  $S_M$  глубины не более  $t$ , успешное на входе  $x \sim \mathcal{X}$  с вероятностью хотя бы  $\frac{1}{\text{poly}(\log N)}$ .

Обычная и вероятностная сводимости транзитивны.

# Диаграмма сводимостей

- $A \longrightarrow B$ :  $A$  сводится к  $B$ .
- $A \dashrightarrow B$ :  $A$  не сводится к  $B$  даже вероятно.
- Точечные стрелки обозначают предполагаемые отсутствия вероятностной сводимости.



## Часть 2: Общий метод доказательства отсутствия вероятностной сводимости

# Центральная теорема

---

## Теорема (Центральная теорема, неформально)

Пусть  $R, S$  - задачи поиска. Пусть выполнены следующие условия:

1.  $R$  не сводится к  $S$ .
2. Для  $R$  выполняется ряд свойств. В частности, существует некоторое хорошее «рекурсивное» распределение входов.

Тогда  $R$  не сводится вероятностно к  $S$ .

Отметим, что второй пункт теоремы накладывает ограничения только на  $R$ .  
Далее мы продемонстрируем идею доказательства теоремы для  $R = \text{PPP}$ .

# Частичные назначения

## Определение

*Частичным назначением* (partial assignment) длины  $l$  над алфавитом  $\Sigma$  называется строка  $\rho \in (\Sigma \cup \{*\})^l$ . *Размером*  $\rho$  будем называть величину  $|\rho| = |\{i : \rho_i \neq *\}|$ . Мы говорим, что  $\rho_2$  *продолжает*  $\rho_1$  (обозначается  $\rho_1 \nearrow \rho_2$ ), если  $\rho_2$  можно получить из  $\rho_1$  заменой некоторых  $*$  на элемент  $\Sigma$ .  $\rho_1$  и  $\rho_2$  *совместимы* относительно  $X \subset \Sigma^l$ , если существует  $x \in X$ , продолжающий их обоих.

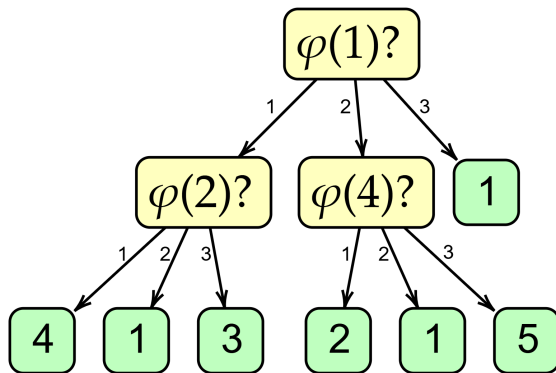
## Определение

Пусть фиксированы задача поиска  $R$  и какое-то  $N$ . Частичными назначениями над входами  $R$  при таком  $N$  будем называть частичные назначения с алфавитом  $\Sigma_N$  и длиной  $l(N)$ . Частичное назначение называется *раскрывающим ответ*  $o \in O_N$ , если для любого продолжения  $\rho$  до входа  $x$  выполнено  $(x, o) \in R_N$ .

# Решающие деревья и частичные назначения

Каждому пути от корня решающего дерева до листа соответствует некоторое частичное назначение. Значение в листе при это не имеет значения.

Пример: решающее дерево, обращающееся к некоторой  $\varphi : [4] \rightarrow [3] = [3]^4$ . Самому левому листу соответствует частичное назначение  $11 **$ .

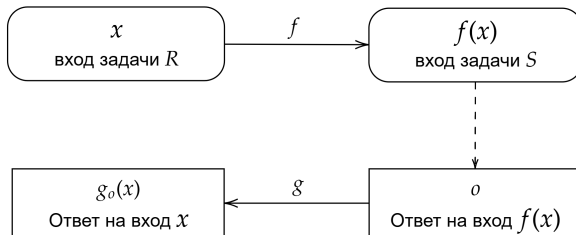


# Требования к сведению

---

Можно добиться, чтобы сведение  $R$  к  $S$  удовлетворяло следующим требованиям:

1. Внимательность:  $g_o$  в начале работы запускает проверку, что  $(f(x), o) \in S$ . В листьях  $g_o$ , которые раскрывают ответ, выдаём любой из раскрываемых ответов.
2. В листьях  $g_o$ , которые не раскрывают ответ, сдаёмся.



# Структура плохих входов

Будем называть *плохими* входы, на которых сведение не успешно. Следующая лемма описывает структуру плохих входов.

## Лемма

Пусть дано сведение  $R_N$  к  $S_M$ , имеющее глубину  $h$  и приведённое к хорошему виду. Тогда для любого плохого  $x$  найдётся такое нераскрывающее частичное назначение  $\rho$ , что:

- $|\rho| \leq h$ ;
- $\rho \nearrow x$ ;
- Все входы  $\{x' \in \Sigma_N^{l(N)} \mid \rho \nearrow x'\}$  также будут плохими.

Из этого в частности следует, что множество плохих входов представляется в виде  $\bigcup_{\rho \in B} \{x' \in \Sigma_N^{l(N)} \mid \rho \nearrow x'\}$  для некоторого  $B$ , состоящего из частичных перестановок размера не более  $h$ .

## Сужения

---

Вернёмся к частному случаю  $R_N = \text{PPP}_N$ . Ограничимся множеством входов  $X_N$ , задающих биекцию  $[N] \rightarrow [N-1] \cup \{\perp\}$ . Для таких входов единственный корректный ответ — точка, в которой функция принимает значение  $\perp$ .

## Сужения

Положим  $k := N - N^{\frac{1}{4}}$  и рассмотрим  $\mathcal{P}_k$  - нераскрывающие частичные назначения размера  $k$ . Возьмём произвольное  $\kappa \in \mathcal{P}_k$ . Тогда можно заметить, что задача поиска  $\perp$  в  $PPP_N$  при условии, что вход продолжает  $\kappa$ , в некотором смысле эквивалентна решению  $PPP_{N-k}$ . То есть  $PPP_N \upharpoonright \kappa \simeq PPP_{N-k} = PPP_{N^{1/4}}$ . Кроме того,  $\kappa$  можно использовать, чтобы по любому сведению  $PPP_N$  к  $S_M$  получить сведение  $PPP_{N^{1/4}}$  к  $S_M$ . При этом глубина сведения не увеличивается, поэтому если изначальное сведение было полилогарифмической по  $N$  глубины, то полученное будет полилогарифмической по  $N^{\frac{1}{4}}$  глубины. При этом будет наблюдаться связь:

$$\begin{aligned} x' &\text{ — плохой вход сведения } PPP_{N^{1/4}} \text{ к } S_M \Leftrightarrow \\ x' \cup \kappa &\text{ — плохой вход сведения } PPP_N \text{ к } S_M \end{aligned}$$

Учитывая то, что при достаточно большом  $N$  для сведения  $PPP_{N^{1/4}}$  к  $S_M$  найдётся плохой вход  $x'$ , получаем следующую лемму:

### Лемма

Каждое  $\kappa \in \mathcal{P}_k$  совместимо относительно  $X_N$  с каким-то  $\rho \in B$ .

## Вероятность провала сведения

---

Заметим, что чтобы сгенерировать случайный  $x \in X_N$ , можно взять случайный  $\kappa \in \mathcal{P}_k$ , а затем дополнить  $\kappa$  случайным образом до биекции  $[N] \rightarrow [N-1] \cup \{\perp\}$ . Тогда если мы покажем, что с большой вероятностью случайное  $\kappa$  не просто совместимо с каким-то  $\rho \in B$ , а даже продолжает какой-то  $\rho \in B$ , то с не меньшей вероятностью случайный  $x \in X_N$  будет продолжать какой-то  $\rho \in B$ , а значит будет плохим.