Лекция 14

Иерархия для эвристических вероятностных вычислений

(Конспект: А. Банкевич, В. Вальтман)

Предупреждение: конспект не проверен лектором

При попытке построения иерархии для языков из класса **BPP** возникает естественная проблема, состоящая в том, что не любая машина Тьюринга задает язык из **BPP**, поскольку для этого необходимо, чтобы 3/4 ответов машины были одинаковы. То есть диагонализирующая машина D не может просто так взять и повторить ответ машины M, которую она симулирует: если окажется, что M не из **BPP**, D не будет иметь права ее моделировать, поскольку тогда сама она выпадет из **BPP**. С другой стороны, непонятно, как проверить, лежит ли M в **BPP**, значит D не сможет угадать, надо ли симулировать M (чтобы получить ответ, отличный от ответа **BPP** машины) или нет (чтобы не выпасть из **BPP**).

На данный момент иерархия для **BPP** не доказана, но если этот класс немного расширить, то уже что-то можно сказать. Здесь будет в сильно упрощенной формулировке доказан результат, полученный в 2006 году.

Определение 14.1. Язык L принадлежит классу $\mathrm{heur}_\delta\mathbf{BPP}$ тогда и только тогда, когда существует полиномиальная по времени недетерминированная машина Тьюринга M: $\forall n$ на доле δ входов длины n выполнено:

- если $x \in L$ то хотя бы 3/4 ветвей приняли вход .
- если $x \notin L$ то хотя бы 3/4 ветвей не приняли вход .

На остальных $(1-\delta)2^n$входах машина может работать как угодно.

То есть машина работает как **BPP**, но иногда ошибается и не может мичего ответить.

Аналогично определяется $\mathrm{heur}_\delta\mathbf{BPTime}(f(n))$.

Целесообразно рассматривать только классы для $1/2 < \delta < 1$. При $\delta = 1$, очевидно, получаем класс **BPP**.

Теорема 14.1. $\mathrm{heur}_\delta\mathbf{BPTime}(n^k) \subsetneq \mathrm{heur}_\delta\mathbf{BPP}$.

Доказательство. Доказательство будем проводить диагонализацией. Зафиксируем очень быстро растущую функцию $h(n) = 2^{2^{2^n}}$, а так же функцию $\theta : \{0,1\}^* \to [0,1]; \theta(x) = \delta + z(x) \cdot (1 - 2\delta)$. $z(x)$ это число $\overline{0,x}$, рассматриваемое как вещественное число в 2-ичное системе счисления. (то есть каждому двоичному слову сопоставляем число от $1-\delta$ до δ так, что значения функции при заданной длине слова равномерно заполняют этот отрезок). Для начала опишем диагонализирующую машину N.

Пусть процедура $A(x, M)$ делает следующее: запускает машину M на входе x и некоторой случайной подсказке c раз и принимает вход если большая часть запусков M приняла вход , где c — константа, зависящая от δ.

Тогда диагонализировать будем так:

- N вычисляет i: $H(i) \le |x| < H(i+1)$. После чего строит запись M_i — машины Тьюринга, кодируемой числом i, причем если эта машина не обладает встроенным будильником, заканчивающим работу машины через $f(|x|)$ шагов, отвергаем вход.

- при $|x| = H(i+1) - 1$. N принимает вход, если большая часть ответов M_i по всем входам длины $H(i)$ и по всем подсказкам для них отрицательны (в том смысле, что мы перебираем все входы, для каждого входа вычисляем ответ, как MAJORITY по подсказкам, а потом берем MAJORITY по входам). Это можно сделать, не используя случайные биты, поскольку у нас большой запас времени и мы можем посчитать все детерминированно.

- при $H(i) \le |x| < H(i+1) - 1$. Мы запускаем $A(y_k, M_i)$ для k от 1 до c, где y_k — случайные строки длины $|x|+1$ и принимаем вход, если доля положительных ответов процедуры $A > \theta(x)$.

Наша задача, во-первых, показать что $N \in \mathrm{heur}_\delta\mathbf{BPP}$, и, во-вторых, если оказалось, что $M_i \in \mathrm{heur}_\delta\mathbf{BPTime}(n^k)$, то M_i не может задавать тот же язык, что и N.

Из теории вероятности известно, что при полиномиальном числе подкидываний монетки вероятность сильного отклонения реальной доли успехов от вероятности успеха при одном бросании убывает экспоненциально. Более формально это выглядит так (это неравенство называется неравенством Чернова):

$$Pr(|\frac{\sum x_i}{n} - \mu| > \varepsilon) < e^{-\frac{\varepsilon^2 n}{2}}$$

где μ — вероятность выпадения единицы. Возьмем n таким, что $e^{-\frac{\varepsilon^2 n}{2}} < \delta - \frac{1}{2}$ и будем считать, что наша машина в этих случаях ошибалась.

Для каждого запуска A есть некая независимая вероятность p того, что A примет вход, поскольку каждый раз A работает на новом, независимо выбираемом наборе случайных битов. Таким образом, несколько раз запустив A, мы получим, что доля положительных ответов A с большой вероятностью не сильно отличается от p (не более, чем на ε). Таким образом с большой вероятностью сравнение доли положительных ответов с $\theta(x)$ будет давать все время один и тот же ответ, если выполнено, что $|\theta(x) - p| > \varepsilon$. Но мы выбрали ε таким, что последнее неравенство выполнено на доле входов, большей, чем δ. Таким образом, наш язык лежит в $\mathrm{heur}_\delta\mathbf{BPP}$.

Теперь докажем, что наш язык не лежит в $\mathrm{heur}_\delta\mathbf{BPTime}(f(n))$. Действительно, пусть M_i лежит в $\mathrm{heur}_\delta\mathbf{BPTime}(f(n))$ и принимает наш язык. Докажем, что все ответы N на входах длины от $H(i)$ до $H(i+1)-1$ одинаковы. Доказываем по индукции. Для $|x| = H(i+1)-1$ это очевидно по построению. Пусть теперь все ответы N на входах длины от m до $H(i+1)-1$ $(m > H(i))$ одинаковы, докажем, что и ответы на входах длины $m-1$ тоже такие же. Мы предположили, что машина M_i задает тот же язык, что и N. Значит, по крайней мере на $\delta 2^m$ входах длины m M_i говорит то же, что и N. Но по построению машины N, если M_i отвечает одинаково хотя бы на доле δ длины m, то N отвечает так на все входы длины $m-1$. Значит, переход индукции доказан. Таким образом, и на длине $H(i)$ N отвечает точно так же, как и на больших длинах. Но этого не может быть, так как на длине входа $H(i+1)-1$ N отвечает не так, как M_i отвечает на большинстве входов длины $H(i)$. $\square$