Полные задачи в эвристических классах. Часть 1.

Дмитрий Ицыксон

ПОМИ РАН

21 марта 2008

План

1. **P**, **NP**, **BPP**, задача об ограниченной остановке
2. **HeurP**, **HeurNP**, **HeurBPP**
3. Полная задача для класса **HeurNP**
4. Полная задача для класса **HeurBPP**

Классические классы

- Класс **P** состоит из языков L, которые распознаются детерминированными полиномиальными по времени Машинами Тьюринга M:

$$\forall x \; M(x) = L(x)$$

- Класс **NP** состоит из языков L, которые распознаются недетерминированными полиномиальными по времени Машинами Тьюринга M:

$$\forall x \; M(x) = L(x)$$

- Класс **BPP** состоит из языков L, которые распознаются вероятностными с двусторонней ограниченной ошибкой полиномиальными по времени Машинами Тьюринга M:

$$\forall x \, \Pr\{M(x) = L(x)\} \geq \frac{3}{4}$$

Полнота

- Сводимость по Тьюрингу. Язык L сводится к языку L', если сущесвтует детерминированная полиномиальная машина Тьюринга с оракулом $M^{L'}$, которая распознает язык L.
- Язык L называется полным в классе **C**, если $L \in \mathbf{C}$ и все языки из **C** сводятся к L.
- Задача об ограниченной остановке .

$$BH = \{(M, x, 1^t) | \text{НМТ } M \text{ принимает } x \text{ за } \leq t \text{ шагов}\}$$

BH является **NP**-полным языком.

Почему не получается построить **BPP**-полную задачу?

- Рассмотрим язык

$$BH' = \{(M, x, 1^t) | \Pr\{M \text{ принимает } x \text{ за } \leq t \text{ шагов}\} \geq \frac{1}{2}\};$$

- Это **BPP**-трудный язык;
- Непонятно, содержится ли он в **BPP**;
- Среди M много некорректных **BPP**-машин, но неизвестно способа перечислить только корректные **BPP**-машины.

Распределения на входах

- $D_n : \{0,1\}^n \to \mathbb{R}_+, \sum_{x \in \{0,1\}^n} D_n(x) = 1$;
- $D = \{D_n\}_{n=1}^{n=\infty}$;
- Распределение D называется **P**-Samplable (моделируемым за полиномиальное время), если существует такой полиномиальный по времени вероятностный алгоритм (самплер) S, если его выходы на входе 1^n распределены согласно D_n;
- Распределенная задача: (L, D), где L — язык, D — распределение;
- Мы рассматриваем только **P**-Samplable распределения.

Эвристические классы сложности

- Класс **HeurP** состоит из задач (L, D), для которых существует детерминированная Машина Тьюринга $M(x, \delta)$, полиномиальная по времени относительно $\frac{|x|}{\delta}$:
$$\Pr_{x \leftarrow D_n} \{M(x, \delta) \neq L(x)\} < \delta$$
- Класс **HeurNP** состоит из задач (L, D), для которых существует недетерминированная Машина Тьюринга $M(x, \delta)$, полиномиальная по времени относительно $\frac{|x|}{\delta}$:
$$\Pr_{x \leftarrow D_n} \{M(x, \delta) \neq L(x)\} < \delta$$
- Класс **HeurBPP** состоит из задач (L, D), для которых существует вероятностная Машина Тьюринга $M(x, \delta)$, полиномиальная по времени относительно $\frac{|x|}{\delta}$:
$$\Pr_{x \leftarrow D_n} \{\Pr\{M(x, \delta) \neq L(x)\} \geq \frac{1}{4}\} < \delta$$

Эвристические сведения

Определение. Сведением (L, D) к (L', D') называется алгоритм алгоритм с оракулом $T^\bullet(x, \delta)$:

- Алгоритм $T^\bullet(x, \delta)$ работает время $poly(\frac{|x|}{\delta})$
- Запрос к оракулу — это 2 параметра (y, ϵ), $\epsilon > \frac{1}{poly(\frac{|x|}{\delta})}$
- Если для некоторого алгоритма $F(y, \epsilon)$ выполняется

$$\forall n \Pr_{y \leftarrow D'_n}\{F(y, \epsilon) \neq L'(y)\} < \epsilon,$$

тогда

$$\forall n \Pr_{x \leftarrow D_n}\{T^F(x, \delta) \neq L(x)\} < \delta.$$

Лемма. Если (L, D) сводится к (L', D') и $(L', D') \in$ **HeurP**, то $(L, D) \in$ **HeurP**

HeurNP-полная задача: попытка 1

- $BH = \{(M, x, 1^t) | \text{НМТ } M \text{ принимает } x \text{ за } \leq t \text{ шагов}\}$
- Попытка сведения: если машина $M(x, \delta)$ решала (L, D) в **HeurNP**, то запрос к оракулу $(M_\delta, x, 1^{p(|x|)})$.
- А если оракул ошибается ровно на этом входе?
- Какое распределение на входах?
- Идея: ввести распределение так, чтобы вероятность $(M_\delta, x, 1^{p(|x|)})$ была бы не более, чем полиномиально меньше вероятности x.

HeurNP-полная задача: попытка 2

- $\widetilde{BH} = \{(M, S, 1^s, x, 1^t) |$ НМТ M принимает x за $\leq$ t шагов$\}$, где S — это сэмплер, s — это число шагов, которое разрешается делать сэмплеру.
- Распределение получим с помощью сэмплера $\tilde{\mathcal{R}}$.

1. Сгенерировать случайную строку вида (M, S, s, y, r) длины n.
2. Запустить S на входе $1^{|y|}$ на не более, чем $|s|$ шагов. Результат работы строка x.
3. Выдать $(M, S, 1^{|s|}, x, 1^{|r|})$

HeurNP-полная задача

Теорема. $(\widetilde{BH}, \tilde{R})$ — **HeurNP**-полная задача.

Доказательство.

Пусть $(L, D) \in HeurNP$, где D генерируется сэмплером S, который работает время $q(n)$, а L решается НМТ $M(x, \delta)$ за время $p(n)$. Делаем запрос оракулу $(M_{\frac{\delta}{2}}, S, 1^{q(|x|)}, x, 1^{p(|x|)})$ и параметром $\epsilon = \frac{\delta}{2^{|M_{\frac{\delta}{2}}|+|S|+1} poly(|x|)}$. $\square$

Литература

- Andrej Bogdanov and Luca Trevisan. Average-case complexity. *Foundation and Trends in Theoretical Computer Science*, 2(1):1–106, 2006.
- Dmitry Itsykson. A complete problem for **HeurBPP** with polynomial-time samplable distributions. http://logic.pdmi.ras.ru/~dmitrits/papers/heurbpp.ps