

1 Билет 1

Утверждение 1.1. Пусть M – одноленточная МТ, которая распознает язык бинарных палиндромов. Тогда существует константа $C : \exists n_0 : \forall n > n_0$ существует вход длины n , на котором $M(x)$ делает $\geq Cn^2$ шагов.

Доказательство. В начале очевиден принцип несжимаемости, нельзя инъективно перевести строки из $\{0, 1\}^n$ в $\{0, 1\}^*$ так, чтобы все образы по длине были меньше чем n .

Будем доказывать для входов, длина которых кратна 3. По $x \in \{0, 1\}^n$ строим вход $x0^n x^{rev}$ и скормливаем МТ все такие входы. Возьмем все перегородки после нулей, их всего n , существует перегородку, через которую МТ прошла $\leq \frac{T(x)}{n}$ раз.

Теперь строим отображение $f : \{0, 1\}^n \rightarrow \{0, 1\}^*$, переводим строку x в протокол работы МТ на строке $x0^n rev(x)$. Для этого выпишем набор состояний, в которые переодила МТ, переходя через "хорошую" перегородку и номер этой перегородки.

Утверждается, что такая f – инъекция, чтобы доказать, предположите обратное и рассмотрите работу на строке $x0^n y^{rev}$.

Пусть $|x| = n$, тогда $f(x) \leq \log n + \frac{T(x)}{n}C$, но при этом существует $|y| = n$, такой что $f(y) \geq n$. Получаем, что

$$n \leq \log n + \frac{T(x)}{n}C$$

$T(x) = \omega(n^2)$ на таких входах.

Для некратных 3 входов делаем также, но по-середине пишем вместо n нулей, на один ноль больше или меньше – это не влияет на оценки. ■

2 Билет 2

Определение 2.1. k – ленточная машина Тьюринга. (Добавляется куча лент и функция перехода теперь действует по всем лентам).

Утверждение 2.1. Для любой k – ленточной МТ, которая на входе x работает время $T(x)$, существует 1 ленточная МТ, которая работает $O(T(x)^2)$.

Доказательство. Будем хранить в одном символе МТ символы всех лент (а также спец символы, помеченные головкой). На каждом шаге будем идти вправо и делать все изменения, которые нужны на лентах. ■

Определение 2.2. Универсальная МТ – эмулирует МТ по описанию.

Утверждение 2.2. Для любой k -ленточной МТ существует универсальная k -ленточная МТ с линейным замедлением.

Доказательство. Понятно как получить квадратичное замедление, нужно положить описание в начало, например, первой ленты. Далее постоянно возвращаться, чтобы узнать, какой шаг сделать. Если же хотим линейного – давайте возить описание с собой, это будет давать $O(1)$ действий из-за его константного размера, при этом эмуляция будет работать за линейное время. ■

Утверждение 2.3. k ленточную МТ можно эмулировать на 2-ленточной с логарифмическим замедлением.

Доказательство. TODO ■

3 Билет 3

Основная модель вычислений – многоленточная МТ.

Определение 3.1. $f : \mathbb{N} \rightarrow R_+$, тогда $L \in DTime[f(n)]$, если существует многоленточная МТ, такая что

1. $\forall x \in L \Rightarrow M(x) = 1$.
2. $\forall x \notin L \Rightarrow M(x) = 0$.
3. $\forall x$ МТ работает $O(f(|x|))$ шагов.

Определение 3.2. $P = \cup_{i \geq 0} DTime[n^i]$.

Определение 3.3. Про семейство схем, распознающих язык.

Определение 3.4. $L \in Size[f(n)]$, если есть последовательность схем, распознающих L и для достаточно больших n выполнено $|C_n| \leq f(n)$.

Определение 3.5. $P/Poly = \cup_{i \geq 0} Size[n^i]$.

Пример 3.1. Неразрешимый язык может лежать в $P/Poly$. Например $1^H = \{1^n | n \in H\}$, для некоторого языка тоже является разрешимым и лежит в $P/Poly$, так как на каждую длину мы можем предоставить схему.

Утверждение 3.1. Существует такой алгоритм A , который получает на вход T, n, t и

1. A работает $poly(n + T + |t|)$ шагов.
2. Если МТ t на всех входах из $\{0, 1\}^*$ выдает ответ за $\leq T$ шагов, то алгоритм A выдает схему C , которая имеет n входов и 1 выход и распознает на входах длины n также как t .

Доказательство. Будем возвращать схему размера $T \times T \cdot O(1)$.

На уровне i будет T ячеек, в каждой из которых будет вычисляться некоторая информация: символ, написанный в этой ячейке, есть ли тут головка в момент i , а также, если есть головка, то состояние, в которой МТ сейчас находится. Понятно, что для пересчета этих параметров нужно обратиться к нескольким соседним ячейкам предыдущей строки. Для того, чтобы узнать ответ, посмотрим, принималось ли где-нибудь состояние q_{yes} . ■

Утверждение 3.2. $P \subseteq P/Poly$.

Замечание 3.1. Таким образом хотели доказывать, что $P \neq NP$, взять, к примеру, SAT и показать, что он не лежит в $P/Poly$, однако доказывать нижние оценки на схемы пока что не научились.

4 Билет 4

Определение 4.1. $L \subseteq \Sigma^*$, система доказательств для языка L – это такой алгоритм Π , который обладает следующими свойствами:

1. (Полнота) $\forall x \in L \Rightarrow \exists w : \Pi(x, w) = 1$
2. (Корректность) $\forall x \notin L \Rightarrow \forall w \Pi(x, w) \neq 1$ (Ну или равно 0).

3. P всегда останавливается

Определение 4.2. Система доказательств P называется эффективной, если $P(x, w)$ работает за $\leq poly(|x| + |w|)$ шагов.

Замечание 4.1. Системы доказательств существуют для перечислимых языков, как мы знаем из предыдущей главы курса. Также можно доказать, что для всех перечислимых языков существует и эффективная система доказательств (TCS12), искусственно увеличивая подсказку.

Определение 4.3. класс NP состоит языков, для которых существует эффективная система доказательств P , а также полином q , такой что $\forall x \in L \exists w, |w| \leq q(|x|), P(x, w) = 1$, то есть, существует полиномиальная подсказка.

Пример 4.1. Примеры языков из NP .

1. SAT – множество выполнимых пропозициональных формул.
 $SAT \in NP$, но не выяснено, $UNSAT \notin / \in NP$.
2. $HamPath$ – язык графов, в которых есть гамильтонов путь, также лежит в NP .
3. $CLIQUE$ – язык пар (граф, число) такой, что в графе есть клика на числе вершин. Лежит в NP .
4. $Composite$ – язык составных натуральных чисел, лежит в NP , а также, известно, что $Primes \in NP$ (TCS11) и, более того, человечество умеет показывать $Primes \in P$.

Определение 4.4. Недетерминированные МТ. Вместо одной функции перехода теперь две и машина сама выбирает, в какую идти. (:)).

Говорят, что недетерминированная M принимает слово, если существует последовательность корректных переходов, при которых она придет в состояние q_{yes} на входе этом слове.

Время работы НМ – максимум по всем возможным применениям функции перехода.

Определение 4.5. $NTime[f(n)]$ – множество языков, которые принимаются многоленточными НМТ за $O(f(n))$ шагов, где n – длина входа.

Определение 4.6 (Второе определение NP). $NP = \cup_{c>0} NTime[n^c]$.

Определение 4.7 (МТ с подсказкой). К обычной МТ добавляется лента подсказки, на которую записывается некоторая строка, к которой может обращаться МТ во время работы. Машина принимает слово, если существует подсказка, для которой она придет в состояние q_{yes} . Время работы такой машины – максимум по всем подсказкам.

Теорема 4.1. Следующие условия эквивалентны:

1. $L \in NP$ (на языке систем доказательств)
2. L распознается машиной Тьюринга с подсказкой за полиномиальное время.
3. $L \in \cup_{c>0} Ntime[n^c]$.

Доказательство. (1) \Rightarrow (2): построим МТ с подсказкой. Пусть наша МТ при обращениях к подсказке будет теперь обращаться на ленту с подсказкой вместо ленты входа. Тогда понятно, что подсказки аналогичны друг другу.

(2) \Rightarrow (3) : пусть МТ порождает подсказку, а далее действует детерминированно. Подсказка более чем полиномиального размера не нужна, так как наш алгоритм не успеет ее обработать из-за своего времени работы.

(3) \Rightarrow (1) : подсказка – какую функцию перехода выбирать на каждом шагу. ■

5 Билет 5

Определение 5.1. Язык A сводится по Карпу к языку B , если существует полиномиально вычисляемая $f: \forall x, x \in A \iff f(x) \in B$. Обозначается $A \leq_p B$.

Утверждение 5.1. Свойства сведения

1. $A \leq_p B, B \in P \Rightarrow A \in P$.
2. $A \leq_p B, B \leq_p C \Rightarrow A \leq_p C$.

Определение 5.2. Язык A называется NP -трудным, если $\forall L \in NP, L \leq_p A$. Язык A NP -полный, если $A \in NP$ и A – NP -трудный.

Определение 5.3. $BH = \{(M, x, 1^t) \mid \exists y, M(x, y) \text{ выдает } 1 \text{ за } \leq t \text{ шагов}\}$.

Теорема 5.1. BH – NP -полный.

Доказательство. Проверим, что $BH \in NP$. Подсказка как раз и будет этот y . Запускаем на t шагов и проверяем, приняло или нет. Если тройка лежит в языке, то по определению найдется такая подсказка, что выдаст *yes*. Иначе – нет.

Возьмем $L \in NP$, хотим проверить $L \leq_p BH$. У L есть нмт эффективная система доказательств Π , работающая за $q(|x| + |y|)$, при этом также для лежащих в языке слов есть маленькая подсказка, длины $\leq p(x)$. Давайте сделаем следующее отображение $f(x) = (M, x, 1^{q(|x|+p(|x|))})$. Очевидно, что это корректное сведение. ■

Определение 5.4. $Circuit - SAT$ – язык, в котором лежат схемы, у которых есть выполняющий набор.

Теорема 5.2. $Circuit - SAT$ – NP полный.

Доказательство. $Circuit - SAT \in NP$, подсказка – выполняющий набор.

Возьмем $L \in NP$. Хотим полиномиально свести L к $Circuit - SAT$. Давайте по МТ, решающей L с помощью подсказки и x построим схему, в которой длина входа равна $q(|x|)$, где q – полином, ограничивающий подсказку. Тогда осталось понять, существует ли подсказка, при которой схема даст значение 1, а это инстанс задачи $Circuit - SAT$. ■

Определение 5.5. $3SAT$ – язык из формул, записанных в КНФ так, что каждый дизъюнкт состоит из не более чем 3 литералов.

Теорема 5.3. SAT и $3SAT$ – NP полные.

Доказательство. Будем сводить $Circuit - SAT$ к этим задачам. Можно сводить только к $3SAT$, так как дальше сведение тривиально. Просто запишем кнф формулу для схемы, добавив новые переменные для каждого узла в ней и связав их нужными условиями. ■

6 Билет 6

Определение 6.1. Q – предикат. Он полиномиально ограниченный, если $Q(x, y) = 1 \Rightarrow |y| \leq p(|x|)$ для некоторого полинома p .

Каждый язык $L \in NP$ задается полиномиально ограниченным, полиномиально проверяемым предикатом, таким что $x \in L \iff \exists y Q(x, y) = 1$.

Определение 6.2 (Задача поиска). Q – полиномиально ограниченный, полиномиально проверяемый предикат двуместный предикат. Задача поиска, заданная предикатом Q это задача: по x найти y такой, что $Q(x, y) = 1$. Множество задач поиска для таких предикатов обозначим \widetilde{NP} .

Будем говорить, что задача поиска решается алгоритмом A , если для любого x , для которого существует такой y , что $Q(x, y) = 1$, выполнено $Q(x, A(x)) = 1$. Множество задач поиска, для которых существуют полиномиальные по времени алгоритмы будем обозначать \tilde{P} . Очевидно, что задачи распознавания, соответствующие задачам из \tilde{P} , лежат в P .

Определение 6.3. МТ с оракулом, лента для вопросов к оракулу.

Определение 6.4 ($A \leq_{pT} B$). Вычислительная задача (задача распознавания или NP задача поиска Q) сводится по Куку (= По Тьюрингу за полином) к языку A , если она может быть решена за полином с оракулом A .

Утверждение 6.1 (Свойства сведений по Куку). .

1. если $L_1 \leq_p L_2$, то $L_1 \leq_{pT} L_2$
2. \leq_{pT} транзитивно, даже если цепочка начинается на задаче поиска.
3. Если мы свелись по Куку к задаче из P , то мы сами лежим в P . Аналогично и для задач поиска.

Доказательство. .

1. В начале сведемся, потом сделаем один запрос к оракулу.
2. Пусть начиналось на задаче распознавания. $L \leq_{pT} A \leq_{pT} B$. Давайте всякий раз, когда МТ для L делает запрос к оракулу A будем запускать полиномиальный алгоритм проверки для языка A , который делает запросы к оракулу B . Таким образом обойдемся только оракулом для B . Аналогично и для задач поиска.
3. Будем эмулировать запрос к оракулу, запуская полиномиальный алгоритм.

■

Теорема 6.1. Каждая задача поиска из \widetilde{NP} сводится по Куку к некоторому языку из NP .

Доказательство. В начале введем нестрогий порядок на строках. $x \preceq y$. Сначала сортируем по длине, потом лексико. Пусть Q – полиномиально ограниченный предикат полиномом p . Рассмотрим язык $L = \{(x, a) \mid |a| \leq p(|x|), \exists y \preceq a : Q(x, y) = 1\}$. Тогда такой язык лежит в NP , так как подсказка это нужный y . Задача поиска сводится к этому языку по Куку с помощью бинарного поиска по ответу. Делаем бп, в котором для определения, куда сдвигать границу, обращаемся к оракулу. ■

Утверждение 6.2. Если $P = NP$, то $\tilde{P} = \widetilde{NP}$.

Это из-за того, что все задачи поиска из \widetilde{NP} в таком случае сводятся по Куку к задачам из P , а значит, сами лежат в \tilde{P} .

Утверждение 6.3. Если NP -полный язык L задается предикатом Q , то задача поиска Q сводится по Куку к L .

Задача поиска Q сводится по Куку к какому-то языку из NP . Этот язык сводится по Карпу к L , а значит сводится к нему по Куку и мы получаем утверждение из транзитивности сведения по Куку.

7 Билет 7

Определение 7.1. $DTime^A[f(n)]$ как и раньше, но машина с оракулом. Аналогично, $NTime^A[f(n)]$.
 $P^A = \cup_{c>0} DTime^A[n^c]$.
 $NP^A = \cup_{c>0} NTime^A[n^c]$.

Определение 7.2. $EXP = \cup_{c>0} Dtime[2^{n^c}]$.

Утверждение 7.1. $EXPCOMP = \{(M, x, t), M(x) = 1 \text{ за не более } t \text{ шагов}\}$ – полный язык в классе EXP .

Доказательство. Понятно включение. Действительно, будем просто эмулировать M , это займет не более t шагов, что экспонента от длины входа. Возьмем $L \in EXP$. Покажем $L \leq_p EXPCOMP$. По x как всегда выдадим $(M, x, 2^{|x|^c})$, где c – константа из работы M . Очевидно, сведение корректно. ■

Утверждение 7.2. $P^{EXPCOMP} = NP^{EXPCOMP} = EXP$.

Доказательство. $EXPCOMP$ – EXP полный, поэтому $EXP \subseteq P^{EXPCOMP}$. А также $NP^{EXPCOMP} \subseteq EXP$, так как можно перебрать подсказку, а дальше полином обращений к оракулу решить тоже за экспоненту. ■

Теорема 7.1 (Бэйкер, Гилл, Солвэй). *Существует такой язык B , что $P^B \neq NP^B$.*

Доказательство. B – какой-то язык. $U_B = \{1^n \mid \exists x \in \{0, 1\}^n \cap B\}$. Если $B \in NP$, то $U_B \in NP$. Подсказка – строка нужного размера и подсказка для нее.

Теперь будем строить B так, чтобы $P^B \neq NP^B$.

Рассмотрим нумерацию Машин Тьюринга с оракулом $U_B - M_i$. Будем параллельно достраивать язык B , идя по машинам. Возьмем машину M_k . Посмотрим, что она выдает на входе 1^k . Причем дадим ей поработать максимум $2^k/10$ шагов. Если она выдала 1, то не будем добавлять в языке B слов длины k . Иначе добавим какую-нибудь строку длины k . Это можно сделать, так как все предыдущие машины сделали меньше обращений к оракулу, чем 2^k .

Почему мы обманули все полиномиальные машины? Давайте возьмем какую-нибудь полиномиальную МТ и покажем, что она ошибается. Пусть она работает за $p(n)$. Возьмем ее номер k в нумерации такой, что $2^k/10 > p(k)$. Тогда эта машина ошибается на строке 1^k по построению. ■

8 Билет 8

Теорема 8.1 (Ладнер). *Если $P \neq NP$, то существует $L \in NP$, такой, что, $L \notin P$ и L – не полный в NP .*

Доказательство. Интуиция следующая: хотим немного ослабить язык SAT . Давайте рассматривать

$$SAT_H = \{\varphi 01^{n^{H(n)}} \mid \varphi \in SAT, |\varphi| = n\}$$

Поймем, как определить H . Возьмем нумерацию всех машин Тьюринга M_1, M_2, M_3, \dots

$H(n) = i$, если i – такое минимальное число, что $i < \lfloor \log \log n \rfloor$, что M_i решает SAT_H на всех входах $|x| \leq \log n$ за время $i|x|^i$, или, если такого числа нет, то $\lfloor \log \log n \rfloor$.

Заметим, что $H(n)$ определяется через SAT_H и наоборот.

Но заметим, что чтобы определить $H(n)$ нам не потребуется значений $H(x)$ при $x > \log n$, так как $H(n)$ нужно для дописывания только к строкам длины $n + 1$.

Утверждение 8.1. $H(n)$ вычисляется по значениям $H(1), \dots, H(n-1)$ за $poly(n)$ действий.

Будем вычислять по определению. Переберем

1. $i \leq \log \log n$
2. $x, |x| \leq \log n$, это $2^{\log n} = O(n)$ действий
3. запустим машину i на $(\log \log i)(\log i)^{\log \log i} =$ действий.
4. Сравним результат с реальным: мы можем понять, лежит или нет, так как знаем предыдущие значения H , SAT будем решать перебором за $O(n)$.

Таким образом вычислим $H(n)$ за $O(n^3)$ по предыдущим значениям. Тогда мы сможем вычислить $H(n)$ за $O(n^4)$, вычисляя по очереди все значения.

Утверждение 8.2. $H(n)$ не убывает.

Действительно, если $H(n) = i$, то такое i подошло и для всех предыдущих, либо i – верхняя граница для $H(n)$, но тогда оно точно больше предыдущих.

Утверждение 8.3. $SAT_H \in P \iff H(n) \leq C$.

\Rightarrow : есть МТ, решающая SAT_H за $p(|x|)$. Но эта МТ встречается в нумерации бесконечное число раз. Она там также встречается как M_i при $i|x|^i > p(|x|)$. Но тогда $H(n) \leq i$, так как такая машина нам все решит и мы ее запустим на такое число шагов.

\Leftarrow : Ограниченная неубывающая функция это такая функция, что с некоторого момента она равна j . Но заметим, что тогда M_j решит нам язык за $j|x|^j$, что есть полином. ■

Утверждение 8.4. $SAT_H \in NP$

Действительно, давайте просто давать как подсказку решение для внутренней SAT , при этом определить, верное ли кол-во единиц мы можем, вычислив H .

Утверждение 8.5. $SAT_H \notin P$.

Пусть это не так. Тогда $H(n)$ ограничена. Тогда $SAT \leq_p SAT_H$ и $P = NP$.

Утверждение 8.6. SAT не сводится к SAT_H полиномиально.

Предположим обратное. Покажем тогда, что мы сможем решить SAT за полином. Пусть сведение работает за n^c . Тогда величина формулы, которую выдаст сведение $\leq n^c$, где n – длины формулы, поступившей нам на вход.

$H(n)$ не ограничена, возьмем n_0 такое, что $H(n) > 3c$ при $n > n_0$. Тогда пусть сведение выдало битовую строку, длина которой $m > n_0$ (иначе сделаем полный перебор, который займет $O(1)$) и у которой правильное число единиц на конце (иначе мы это легко проверим за полином).

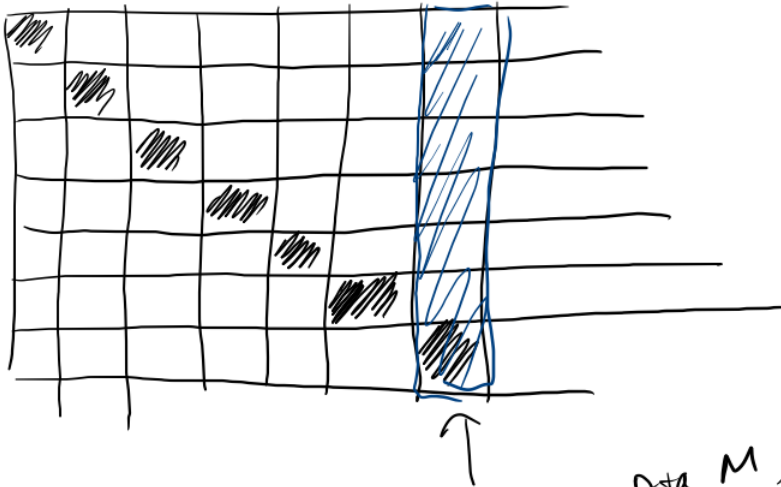
Тогда $m \geq |\varphi| + 1 + |\varphi|^{3c}$, отсюда $|\varphi| \leq m^{1/3c}$, при этом $m \leq n^c$. Получается, $|\varphi| \leq n^{1/3}$. При больших n такое значение хотя бы в 2 раза меньше n . Значит, мы свелись к формуле меньшего размера в 2 раза. Таким образом мы сделаем не более \log полиномиальных сведений и выдадим верный ответ. Отсюда $P = NP$ и противоречие.

9 Билет 9

Пример 9.1. $DTime[n^2] \subsetneq DTime[n^3]$.

Доказательство. Давайте диагонализировать.

$L(n) = 1 - \langle n \rangle(n)$, если $\langle n \rangle(n)$ ок. за $n^{2.5}$ шагов



наша задача M ,
она будет отличаться
от самой себе на
своих входе, т.к.
остатки вбавлять за
 $Cn^2 < n^{2.5}$

Рассмотрим язык $L = \{M \mid M \text{ отвергает } M \text{ за не более } |M|^{2.5}\}$. Пусть он решается квадратичной M за Cn^2 шагов. Тогда давайте найдем эквивалентную ей M' такую, что $|M'|^{2.5} > C|M'|^2$. Тогда получится, что M' не равна себе же в строчке, соответствующей M' .

Как показать, что $L \in DTime[n^3]$? Давайте эмулировать МТ, которая работает $O(n^{2.5})$ с логарифмической задержкой.

Тогда получили нужный язык L . ■

Определение 9.1. $h : \mathbb{N} \rightarrow \mathbb{N}$ – конструктивная по времени, если $n \rightarrow h(n)$ можно вычислить за $O(h(n))$ шагов на ДМТ.

Теорема 9.1 (Об иерархии по времени для детерминированных вычислений). $f, g, h : \mathbb{N} \rightarrow \mathbb{N}$, h – конструктивная по времени.

$f(n) = o(h(n))$, $h(n) \log h(n) = o(g(n))$, тогда $DTime[f(n)] \subsetneq DTime[g(n)]$.

Доказательство. Конструкция такая же, как и в предыдущем утверждении. Конструктивная функция нужна для будильника в МТ. \log – для эмуляции. ■

Утверждение 9.1. $P \subsetneq EXP$.

Доказательство. $P \subseteq DTime[2^n] \subsetneq DTime[2^{n^2}] \subseteq EXP$. ■

Замечание 9.1. Доказательство не работает для НМТ, потому что мы не можем реверснуть ответ за такое же время.

Пример 9.2. $NTime[n^2] \subsetneq NTime[n^3]$.

Доказательство. Определим для M_i из перечисления всех НМТ отрезок $[n_i, n_i^*]$ так, что $n_i^* = 2^{n_i^{2.5}}$.
 $n_{i+1} = n_i^* + 1$.

$[n_1, n_1^*], [n_2, n_2^*], [n_3, n_3^*], \dots$

Определим язык L так:

1. $L(n_i^*) = 1 - M_i(0^{n_i})$, если $M_i(0^{n_i})$ завершилось за менее чем $n_i^{2.5}$ шагов и 0 иначе.
2. $L(n) = M_i(0^{n+1})$ для $n_i \leq n < n_i^*$

Утверждение 9.2. $L \notin NTime[n^2]$.

Пусть это не так, тогда есть M , решающая L за Cn^2 . Возьмем такое ее вхождение, что $\forall n \in [n_i, n_i^*], n^{2.5} > Cn^2$. Тогда:

$$M(0^{n_i}) = L(0^{n_i}) = M(0^{n_i+1}) = L(0^{n_i+1}) = \dots = L(0^{n_i^*}) \neq M(0^{n_i})$$

так как все машины успеют отработать.

Утверждение 9.3. $L \in NTime[n^3]$. Разбираем случаи, если надо проэмулировать, то эмулируем, иначе нам нужно реверснуть выход недетерминированной машины. Мы можем сделать это за $2^{n_i^{2.5}} \cdot n_i^{2.5} < ((n_i^*)^3)$.

■

Теорема 9.2 (Об иерархии по времени для недетерминированных вычислений). . $f, g, h : \mathbb{N} \rightarrow \mathbb{N}$, h – конструктивная по времени. $f(n) = o(h(n))$, $h(n+1) = o(g(n))$, тогда $NTime[f(n)] \subsetneq NTime[g(n)]$.

Утверждение 9.4. $NP \notin NEXP$.

Доказательство. аналогично детерминированному случаю.

■

10 Билет 10

Определение 10.1 (Модель вычислений с ограничением по памяти). МТ с дополнительной лентой входа, она *read-only*, также по ней нельзя уйти правее первого пробела. Также есть лента выхода, по которой нельзя двигаться влево, а только выдавать очередной символ ответа. Затраченная память – максимальный уход вправо на какой-то из рабочих лент.

Определение 10.2. $DSpace[f(n)]$ – класс языков, которые принимают ДМТ, использующие $O(f(n))$ памяти. $NSpace[f(n)]$ – то же самое, но для НМТ.

Определение 10.3. $PSPACE = \cup_{c>0} DTime[n^c]$, $NPSpace = \cup_{c>0} NTime[n^c]$.

Определение 10.4. $L = LOGSPACE = DSPACE[\log(n)]$, $NL = NSPACE[\log n]$.

Утверждение 10.1. $\forall s(n) : DTime[s(n)] \subseteq DSpace[s(n)] \subseteq NSpace[s(n)]$. Причем первое включение работает лишь для некоторых моделей вычислений. В частности, для МТ.

Определение 10.5. $S : \mathbb{N} \rightarrow \mathbb{N}$ – конструктивная по памяти, если $1^{S(n)}$ можно вывести за $O(S(n))$ памяти.

Замечание 10.1. Для хороших функций выполняется также иерархия по памяти. То есть, например, известно, что $DSPACE[n^2] \subsetneq DSPACE[n^3]$, $NSPACE[n^2] \subsetneq NSPACE[n^3]$. (Смотри TCS30, TCS31).

Теорема 10.1. $s(n)$ – конструктивная по памяти и $s(n) \geq \log n$. Тогда

$$NSPACE[s(n)] \subseteq DTIME[2^{O(s(n))}] = \cup_{c>0} DTIME[2^{cs(n)}]$$

Доказательство. Для доказательства используется идея с графом конфигураций. Конфигурация МТ это набор параметров:

1. Положение головок на всех лентах
2. Содержание рабочих лент
3. Состояние

Проблема выяснения того, принимает ли МТ вход x может быть рассмотрена как проблема выяснения существования пути в графе конфигураций. Поймем, сколько есть конфигураций:

$n \cdot (Cs(n))^k$ – положение головок, $2^{c's(n)^k}$ – содержимое рабочих лент. Если $s(n) \geq \log n$, то это число есть $2^{O(s(n))}$. В таком случае мы можем сгенерировать такой граф и проверять наличие пути полиномиальным алгоритмом. Получится время работы $poly(2^{O(s(n))}) = 2^{O(s(n))}$.

Зачем пользовались конструктивностью функции по времени? Для того чтобы сгенерировать конфигурацию нужно отмерить максимальную длину конфигурации и дальше уже перебирать все возможные строчки. Поэтому хочется уметь отмерить за нормальную память.

То есть итоговый алгоритм такой: по M, x строим граф конфигураций и ищем путь из K_0 в K_{accept} . Можно сделать одно состояние K_{accept} , попросив МТ стирать все рабочие ленты перед тем как завершиться. Так мы унифицируем конечные состояния, но, очевидно, не изменим вычислительную мощь (:)). ■

Утверждение 10.2. .

1. $NSPACE \subseteq EXP$
2. $NP \subseteq EXP$

Теорема 10.2 (Савич). $s(n)$ – конструктивная по времени и $s(n) \geq \log n$, тогда $NSPACE[s(n)] \subseteq DSPACE[s(n)^2]$.

Доказательство. Все сводится к тому, чтобы по графу понять, есть ли в нем путь от вершины до другой за память $s(n)^2$, где $s(n)$ – память рассматриваемой НМТ. Воспользуемся предикатом $PATH(u, v, i)$ – есть ли путь от u до v длины не более 2^i и рекурсивным перебором. ■

Утверждение 10.3. $NPSPACE = PSPACE$

$$P \subseteq NP \subseteq NPSPACE = PSPACE \subseteq EXP \subseteq NEXP$$

11 Билет 11

Рассмотрим кванторные пропозициональные формулы: $Q_1x_1, \dots, Q_nx_n\varphi(x_1, \dots, x_n)$. Язык таких истинных формул это $TQBF$. Понятно, что $SAT \leq_p TQBF$ просто дописываниям ко всем переменным квантора существования.

Утверждение 11.1. $TQBF$ лежит в $PSPACE$

Действительно, можно просто сделать перебор рекурсивно и проверить выполнимость.

Утверждение 11.2. $TQBF$ – полный в классе $PSPACE$.

Доказательство. Берем граф конфигураций. Хотим записать формулу $PATH(K_0, K_{accept}, cp(n))$. (время работы не более $2^{cp(n)}$, так как иначе все заиклится).

Будем записывать при помощи следующего выражения:

$PATH(u, v, i) = \exists z \forall A, B ((A = u, B = z) \vee (A = z, B = v)) \rightarrow PATH(A, B, i - 1)$, тогда мы сможем записать всё за полиномиальное количество бит. Остаются детали, как записать в виде формулы утверждения вида $PATH(u, v, 0)$. Мы можем с помощью полиномиального алгоритма проверить такой предикат.

Еще нужно подумать о том, как записать равенство конфигураций, это можно сделать просто побитово. ■

Замечание 11.1. Выяснение вопроса детерминированной победы в конечных играх – задача из $PSPACE$, так как ее можно записать в $TQBF$ в виде $\exists step_{1,1} \forall step_{2,1} \exists step_{1,2} \dots Q(..)$, что означает, что есть ход первого игрока, что при любом ходе второго есть ход первого и тд, что первый игрок выиграл.

12 Билет 12

Определение 12.1 (Логарифмическое сведение). $A \leq_l B$, если существует p , вычисляемая с использованием логарифмической памяти такая что $x \in A \iff p(x) \in B$.

Утверждение 12.1 (Свойства лог сведений). 1. $A \leq_l B \Rightarrow A \leq_p B$.

2. $A \leq_l B, B \leq_l C \Rightarrow A \leq_l C$.

3. $A \leq_l B, B \in L \Rightarrow A \in L$.

Чтобы доказать эти утверждения нужна лемма.

Утверждение 12.2. f, g – вычисляемые с логарифмической памятью. Тогда $f \circ g$ тоже вычислима с логарифмической памятью.

Доказательство. Будем вычислять $f(g(x))$, когда для вычисления f будет требоваться очередной бит входа, будем вычислять i -тый бит выхода $g(x)$ заново и ждать пока выведется бит под номером i . ■

$L \in NL$, а вот есть ли равенство – открытый вопрос.

Определение 12.2 (Определение NL через систему доказательств). У нас появляется лента для подсказки, по которой можно двигаться только вправо (потому что НМТ не может записывать результат выбора на ленту). Это задает такой же класс языков, это можно видеть также как мы видели для разных определений NP .

Определение 12.3. $DPATH = \{(G, u, v) \mid \text{в ор. графе } G \text{ есть путь } u \rightarrow v\}$.

$DPATH \in NL$, подсказкой является собственно путь. Нужно проверить, что первая вершина в нем есть u , последняя v и что есть ребро между соседними, это можно сделать за \log памяти.

Теорема 12.1. $DPATH - NL$ полный (относительно \leq_l).

Доказательство. пусть $A \in NL$, M – нмт, решающая A . Сведение будет следующим. Оно будет генерировать конфигурации, которые составляют максимум \log памяти и выводить ребра между ними, то есть строить граф конфигураций. Далее выведем начальное и конечное состояние и это и будет искомым инстанс задачи $DPATH$. ■

Замечание 12.1. Неизвестно, лежит ли $DPATH$ в L , или нет.

Теорема 12.2. $\overline{DPATH} \in NL$

Доказательство. Нам нужно сертифицировать, что между s, t нет пути, причем сделать такое доказательство, которое можно читать слева направо и использовать логарифмическую память.

U_i – множество вершин, до которых есть путь от s длины не более i .

1. для v можно сертифицировать, что $v \in U_i$, сертификат – просто путь, как в языке $DPATH$.
2. если известно $|U_{i-1}| = k$, то можно сертифицировать, что $u \notin U_i$. Для этого предоставим список вершин из U_{i-1} с сертификатами, что они действительно оттуда. Причем список будет у нас возрастающим, чтобы не было повторяющихся вершин. Проверим, что там правильное число вершин + нет вершины u и также нет ребра между вершинами из списка и u .
3. если известно $|U_{i-1}| = k$, то можно сертифицировать, что $|U_i| = t$. Просто для каждой вершины напомним одно из двух, либо сертификат того, что она лежит в U_i , либо сертификат того, что не лежит, при условии $|U_{i-1}| = k$.
4. Таким образом мы можем сертифицировать, что размер $U_{n-1} = k$ и что $t \notin U_n$. ■

Определение 12.4 (соЯзык). X – класс языков. Тогда $coX = \{\Sigma^* \setminus L \mid L \in X\}$.

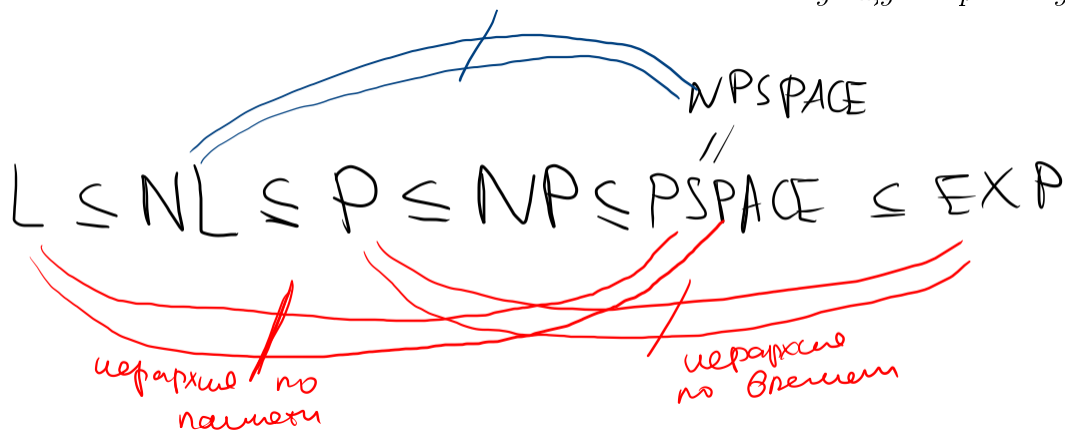
Замечание 12.2. Как мы уже видели, $NP = coNP$ – неизвестно.

Теорема 12.3. $s(n) \geq \log n$ – конструктивная по памяти. Тогда $NSpace[s(n)] = coNSpace[s(n)]$.

Доказательство. $A \in NSPACE[s(n)]$, хотим показать, что $A \in coNSpace[s(n)] \iff \bar{A} \in NSpace[s(n)]$. Причем, если покажем это, то автоматически последует равенство, так как для $A \in coNSpace[s(n)]$ надо показать, что $\bar{A} \in NSpace[s(n)]$, тогда из той стрелочки, которая описана это последует. Рассмотрим M – НМТ, которая распознает A с памятью $s(n)$. $x \in \bar{A} \iff x \notin A \iff$ в графе конфигураций G_x из K_0 нет пути в K_{accept} .

Сертификатом будет тот же самый, сертификат, что и был в теореме выше. Размер графа конфигураций будет $2^{O(s(n))}$, тогда нам потребуется $O(s(n))$ памяти, чтобы проверить сертификат. Причем граф строить полностью не надо, нужно всего лишь уметь проверять, есть ли некоторые ребра в нем. ■

Замечание 12.3. Выяснили на нынешний момент следующую картинку:



13 Билет 13

Определение 13.1. Определение классов $\Sigma_0^P, \Sigma_1^P, \dots$, а также Π_0^P, Π_1^P .

Интуиция про $NP, coNP$ и Σ_1^P, Π_1^P .

Можно развернуть определение: $\forall x, x \in L \iff \exists y_1 |y_1| \leq p(|x|) \forall y_2, \dots, y_i Q(x, y_1, \dots, y_i)$.

Определение 13.2. $PH = \cup_{i \geq 0} \Sigma_i^P$

Утверждение 13.1 (Свойства полиномиальной иерархии). .

$$1. \Sigma_i^P \cup \Pi_i^P \subseteq \Sigma_{i+1}^P \cap \Pi_{i+1}^P.$$

Доказательство. Добавляем фиктивные переменные и кванторы. ■

$$2. PH = \cup_{i \geq 0} \Pi_i^P.$$

$$3. \Sigma_i^P = co\Pi_i^P$$

$$4. \Sigma_i^P = \Pi_i^P \Rightarrow PH = \Sigma_i^P.$$

Доказательство. Доказательство индукцией по $j \geq i$, что $\Sigma_j^P = \Pi_j^P$. Используйте равенство предыдущего уровня для объединения кванторов в один. ■

$$5. \Sigma_i^P \text{ и } \Pi_i^P \text{ замкнуты относительно } \leq_p.$$

Доказательство. Легко видеть, что надо просто взять вычислимый Q из определения и попросить его использовать сведение чтобы охарактеризовать нужным образом язык. ■

$$6. \text{Если в } PH \text{ есть полный язык, то полиномиальная иерархия схлопывается.}$$

Доказательство. Просто все языки, начиная с уровня, на котором лежит полный, будут лежать в этом же уровне. ■

$$7. \text{Теперь введем полные языки на уровнях иерархии. Пусть } \Sigma SAT \text{ это язык, в котором лежат истинные формулы вида } \exists x_1 \forall x_2 \exists x_3, \dots, x_i Q(x_1, \dots, x_i), \text{ где } x_i \text{ — возможно вектор значений. Аналогично, только с противоположными кванторами определяется } \Pi_i.$$

Утверждение 13.2. при $i \geq 1$ выполняется то, что $\Sigma_i SAT$, $\Pi_i SAT$ полны в соответствующих классах на i -том уровне полиномиальной иерархии.

Доказательство. Покажем про $\Sigma_i SAT$. В начале то, что он лежит в Σ_i^P . Характеристика его такова: так как мы не знаем точно сколько там переменных внутри векторчиков, то будем в каждый блок класть столько переменных, чтобы нам хватило. То есть, характеристика следующая: $\exists x_1, |x_1| = |\varphi|, \forall x_2 |x_2| = |\varphi|, \dots, x_i : A(\varphi, x_1, \dots, x_i)$. A – просто полиномиальный алгоритм, который берет и подставляет из наших блоков переменные в φ и проверяет то, что она истинна. Таким образом показали включение.

Теперь полнота. Возьмем некоторый язык $L \in \Sigma_i^P$. Его характеристика имеет вид: $\exists y_1, |y_1| = p(|x|), \dots, y_i Q(x, y_1, \dots, y_i)$. Можно в характеристике сделать все игришки фиксированной длины (в отличии от того что у нас раньше была оценка сверху на длину), так как можно допихать нулей в случае чего.

$Q(x, y_1, \dots, y_i)$ – какой-то полиномиально вычислимый предикат. Давайте переделаем его в схему. Это получится, так как y_1, \dots, y_i и x имеют фиксированную полиномиальную длину. Теперь переделаем схему в формулу при помощи введения дополнительных переменных для всех узлов схемы и обеспечения соответствующих равенств. Получится формула вида $\exists t \varphi(x, y_1, \dots, y_n)$. Если вдруг нам и нужен был квантор существования в конце (i – нечетно), то мы уже победили. Иначе воспользуемся трюком с существованием для отрицания и получим запись с квантором всеобщности. Тогда этот квантор можно совместить с последним квантором из характеристики L .

■

14 Билет 14

Теорема 14.1. $\Sigma_{i+1}^P = NP^{\Pi_i SAT}$

Доказательство. .

\subseteq : $L \in \Sigma_{i+1}^P$ тогда есть следующая характеристика $\exists L' \in \Pi_i^P, \forall x \in L \Leftrightarrow \exists y \in \{0, 1\}^{p(|x|)}, (x, y) \in L'$. Тогда пусть наша НМТ генерирует этот x , потом делает запрос к оракулу при помощи сведения (x, y) к $\Pi_i SAT$.

\supseteq : пусть $L \in NP^{\Pi_i SAT}$ и его решает НМТ M за $p(n)$ с использованием оракула Π_i .

$x \in L \iff \exists z \in \{0, 1\}^{p(n)}, T_1(x, z) \wedge T_2(x, z) \wedge T_3(x, z)$, где

1. z отвечает за недетерминированные выборы НМТ и ответы оракулов.
2. $T_1(x, z)$ проверяет, что мы действительно принимаем x действуя согласно строке z
3. $T_2(x, z)$ проверяет, правда ли, что оракул дал верные положительные ответы. Все вопросы к оракулу выглядят как формулы вида: $\forall x_1, \dots, x_k \varphi(x_1, \dots, x_k)$. Тогда давайте T_2 будет выглядеть так: $\forall r_1 \in \{0, 1\}^{p(n)^2}, \dots, r_k \in \{0, 1\}^{p(n)^2} R(x, z, r_1, \dots, r_k)$, где R поблочно подставляет переменные во все формулы, про которые спрашивал наш алгоритм у оракула и проверяет истинность.
4. T_3 проверяет отрицательные ответы оракула. Для того, чтобы проверить, что φ ложна – нужно проверить, что истинно отрицание φ , то есть, что $\exists x_1, \dots, x_k \neg \varphi(x_1, \dots, x_k) = 1$. Тогда давайте запишем характеристику следующим образом: $\exists x_1 \in \{0, 1\}^{p(n)^2}, \dots, x_k \in \{0, 1\}^{p(n)^2} T'(x, z, x_1, \dots, x_k)$ и T' выдает 1 тогда и только тогда, когда все формулы обнулились.

Теперь вынесем кванторы независимо из T_1, T_2 . Получится нужное чередование.

■

15 Билет 15

Определение 15.1 (Вычисления с неравномерной подсказкой). Языки, принимаемые МТ с неравномерной подсказкой длины $K(n)$ ($P/K(n)$) это такие языки, для которых существует М – МТ с лентой для подсказки и α_n – последовательность подсказок длины $\leq K(n)$ такие, что МТ понимает, лежит ли x в L , используя подсказку $\alpha_{|x|}$.

Замечание 15.1. $P/1$ содержит неразрешимые языки.

Утверждение 15.1. $\cup_c P/n^c = P/poly$.

Доказательство. .

\subseteq : давайте переделаем МТ в схемы, потом встроив туда подсказку. Получим последовательность схем.

\supseteq : в качестве подсказки возьмем схему. ■

Теорема 15.1. Существует функция $f : \{0, 1\}^n \rightarrow \{0, 1\}$ такая, что она не вычислима схемой размера менее $2^n/10^n$.

Доказательство. Схему размера T можно задать за не более чем $4T \log T$ битов. Тогда таких схем не более $2^{4T \log T}$. Пусть $T < 2^n/10n$. Тогда покажем, что $2^{4T \log T} < 2^{2^n}$. Нужно показать: $4T \log T < 2^n$, действительно: $4T \log T < 42^n/(10n) \log(2^n/10n) < 4 * 2^n/10 < 2^n$. ■

16 Билет 16

Теорема 16.1 (Карп-Липтон). Если $NP \in P/poly$, то полиномиальная иерархия схлопывается на втором уровне.

Доказательство. За счет того, что мы умеем сводить задачи распознавания к задачам поиска, у нас существует и семейство схем, которое выдает выполняющие наборы для схем. Пусть это семейство C_n . Причем пусть размеры ограничены полиномом $p(n)$

Хотим показать, что $\Sigma_2^P = \Pi_2^P$. Нам хватит показать, что $\Pi_2 SAT$ лежит в Σ_2^P , так как это со языки друг друга.

Что у нас лежит в $\Pi_2 SAT$? Истинные формулы вида $\forall x \exists y Q(x, y)$. Давайте попробуем написать для этого языка Σ_2^P характеристику.

$\varphi \in \Pi_2 SAT \iff \exists C_1, \dots, C_{|\varphi|} \forall z \in \{0, 1\}^{|\varphi|} T_z(C_{|T_z|}(T_z)) = 1$. Мы легко можем проверить последний предикат за полиномиальное время. Причем из того, что $NP \in P/poly$ будем существовать нужный набор схем в случае, если формула действительно лежит в языке. ■

17 Билет 17

Теорема 17.1 (Первая теорема Каннана). PH не лежит в $Size[n^k]$ ни для какого k .

Доказательство. Давайте построим язык, который будет содержаться в PH , но при этом не решаться схемами размера n^k .

Посмотрим на булевы функции от $(k+1) \log n$ переменных. Тогда по теореме про существование сложной функции, среди таких функций найдется функция, схемная сложность которой более $\frac{2^{(k+1) \log n}}{10(k+1) \log n} = \frac{n^{k+1}}{10(k+1) \log n}$, что больше n^k при больших n .

Будем с помощью кванторов задавать первую такую функцию. Скажем, что $x \in L \rightarrow \forall f (\forall C |C| \leq n^k \iff \exists x C(x) \neq f(x)), \forall g (g \prec f, \exists C |C| \leq n^k \forall x C(x) = g(x)) \rightarrow f(x) = 1$. Мы сможем проверить предикат лексикографической меньшести и равенства функции, так как функцию из $(k+1) \log n$ битов можно задать таблицей истинности полиномиального размера. ■

Теорема 17.2 (Вторая теорема Каннана). *Уже в $\Sigma_2^P \cap \Pi_2^P$ есть язык, который не распознается семейством полиномиальных схем.*

Доказательство. Пусть это не так. Тогда $NP \in \Sigma_2^P \cap \Pi_2^P \leq P/poly$, но тогда из теоремы Карпа-Липтона получим, что полиномиальная иерархия схлопывается на 2 уровне и $PH = \Sigma_2^P$, но это противоречие с первой версией теоремы Каннана. ■