Домашняя работа №4

Бредихин Александр

16 марта 2020 г.

Задача 1

Определите, являются ли задачи выполнимости и тавтологичности булевой формулы в ДНФ $\mathcal{P}, \mathcal{NP}c$ или $co\mathcal{NP}c$.

Выролнимые ДНФ

Пусть L – язык выполнимых ДНФ. Покажем, что $L \in \mathcal{P}$, то есть существует характеристическая функккция $\chi_L(x)$, которая за полиномиальное время проверяет принадлежит слово x языку или нет.
Из дискретного анализа знаем, что ДНФ выполнима, когда выполним хотя бы один из конъюктов. Чтобы конъюкт был выполним нужно, чтобы в нём одновременно не встречалось переменной и её отрицания.
Характеристическая функция $\chi_L(x)$ работает следующим образом: циклом проходит по ДНФ, по каждому конъюкту. Если в одном из них нет переменной и её отрицания, то ДНФ выполнима и $\chi_L(x) = 1$. Если после прохождения всей ДНФ функция ничего не вернула, то значит ДНФ не выполнима и $\chi_L(x) = 0$.
$\chi_L(x)$ работает за полиномиальное от длины ДНФ время ($\mathcal{O}(n)$). Размер ДНФ, то есть количество конъюктов в нём конечное число, как и переменных в крнъюкте, значит $\chi_L(x)$ – полиномиальная.
Так как $L \in \mathcal{P} \longrightarrow L \notin \mathcal{NP}c, \quad L \notin co\mathcal{NP}c$ (так как $\mathcal{NP}$ уже нельзя свести к $\mathcal{P}$, значит уже не полная)
Ответ: $L \in \mathcal{P}, \quad L \notin \mathcal{NP}c, \quad L \notin co\mathcal{NP}c$

Тавтологичные ДНФ

Пусть L – язык тавтологичных ДНФ, докажем, что $L \in co\mathcal{NP}c$, то есть, что язык $L^* = coL = \{f : \exists x : f(x) = 0\}$ является $\mathcal{NP}c$.
Рассмотрим $SAT \in \mathcal{NP}c$ – язык выполнимых КНФ и покажем сводимость $SAT \leqslant_p L^*$. Рассмотрим такую функцию $g(x)$: она применяет закон де Моргана к отрицанию КНФ, то есть меняет все конъюкции на

дизъюнкции и наоборот. Также меняет переменную на её отрицание и наоборот, отрицание переменной на саму переменную. В итоге получим $g(x)$ – ДНФ.

- Если $x \in SAT$, то по определению существует набор $\exists x : f(x) = 1$, тогда $g(x) = 0$. Получается, $g(x)$ – ДНФ и нетавтологична (так как есть набор, где она принимает значение 0), значит $g(x) \in L^*$.
- Если $f \notin SAT$, то $\forall x : f(x) = 0$ (по определению SAT), тогда $\forall x : g(x) = 1$. Получаем, $g(x)$ – ДНФ и тавтологична а значит $g(x) \notin L^*$

Функция $g(x)$ полиномиальна (аналогично рассужденям для разрешимых ДНФ, проходит по КНФ один раз), поэтому мы доказали сводимость $SAT \leqslant_p L^*$, следовательно: $L \in co\mathcal{NP}c$
Ответ: $L \in co\mathcal{NP}c$

Задача 2

$EXACTLY3SAT \leq_p 3SAT$ Построим такую функцию сводимости f:

- если в дизъюнкте 3 литерала или больше, то он не изменяется и остаётся таким же.
- если в дизъюнкте меньше трёх литералов (то есть дизъюнкты вида $(x \vee y)$ или (x)), то функция f заменяет их на дизъюнкты из 4 литералов: $(x \vee y \vee a \vee b)$, где a, b - произвольные переменные.

Если $x \in EXACTLY3SAT$, то каждый дизъюнкт x состоит из трёх литералов и $f(x) = x$. Для x есть выполняющий набор, следовательно $f(x) \in 3SAT$ (по определению)

Если $x \notin EXACTLY3SAT$, то возможны случаи:

1) все дизъюнкты x состоят из 3х литералов, но не существует выполняющего набора.
2) есть дизъюнкт, где больше 3х литералов
3) есть дизъюнкт, где меньше 3х литералов

Для 1го случая $f(x) = x$ (так как f не меняет дизъюнкты с 3 литералами), так как для x нет выполняющего набра, то для $f(x)$ тоже, значит, $f(x) \notin 3SAT$.
Для 2го случая дизъюнкт, где больше 3х литералов не изменится и останется в $f(x)$, значит $f(x) \notin 3SAT$.
Для 3го случая дизъюнкты, где меньше 3х литералов перейдут в дизъюнкты с 4 литералами, следовательно, в $f(x)$ будут дизъюнкты с больше чем тремя литералами, то есть $f(x) \notin 3SAT$.

Функция f - полнимиальная (работает за 1 проход по входному x), следовательно $EXACTLY3SAT \leq_p 3SAT$.

$3SAT \leq_p EXACTLY3SAT$
Рассмотрим такую функцию $f = f(x)$:

- если в дизъюнкте x 3 литерала, то f не изменяет его.
- если в дизъюнкте x 2 литерала, то есть $(x \vee y)$, то $f(x) = (x \vee y \vee z) \wedge (x \vee y \vee \neg z)$. Заметим, что первоначальный дизъюнкт равен 1 тогда и только тогда, когда $f(x)$ равен 1 (от добавленной переменной z ничего не звиисит).
- если в дизъюнкте 1 литерал, то есть (x), то $f(x) = (x \vee y) \wedge (x \vee \neg y)$ а затем применяет пункт 2 к полученным 2м дизъюнктам и получает равносильные дизъюнкты с 3 литералами в каждом.

Во всех трёх случаях из принципа работы $f(x)$ следует, что если $x \in 3SAT \Leftrightarrow f(x) \in EXACTLY3SAT$. f – полиномиальна от длины входного x, значит, $3SAT \leq_p EXACTLY3SAT$.

Задача 3

Докажите, что задача $VERTEX\text{-}COVER \in \mathcal{NP}c$

Покажем, что задача $VERTEX\text{-}COVER \in \mathcal{NP}$: в качестве сертификата выберем само вершинное покрытие $V^* \subseteq V$. Предикат проверяет, что $|V^*| = k$ а затем для каждого ребра проверяется, что хотя бы одна из его вершин принадлежит V^* (это происходит за полиномиальное время, так как количество рёбер - конечное число).

Теперь, покажем, что задача $VERTEX\text{-}COVER$ – полная, для этого построим сводимость $CLIQUE \leq_p VERTEX - COVER$.

Рассмотрим такую функцию сводимости f: $f((G,k)) = (G^*, k^*)$, где G^* – дополнение к графу G (то есть в нём есть все рёбра, которых нет в G и наоборот: нет рёбер, которые есть в G). $k^* = n - k$ (n – всего количество вершин в G).

Пусть $(G,k) \in CLIQUE$. Пусть M - множество вершин размером k, образующие клику, N - все оставшиеся вершины. Тогда у $f((G,k))$ у каждого ребра хотя бы одна вершина принадлежит N (по определению дополнения графа, с учётом того, что в нём есть клика - M), следовательно, вершины N образуют вершинное покрытие у $f((G,k))$ (по определению вершинного покрытия) и его размер $n - k \longrightarrow f((G,k)) \in VERTEX - COVER$.

Пусть $(G,k) \notin CLIQUE$. От противного: пусть в $f((G,k))$ есть вершинное покрытие размером $n - k$. Тогда можно рассмотреть множество вершин, не входящих в него - M, тогда все вершины в M не связаны друг с другом (иначе вершинное покрытие было бы другое), но тогда в (G,k) эти вершины образовали бы клику размером k (по определению дополнению графа). Получили противоречие, следовательно, $f((G,k)) \notin VERTEX - COVER$.

Функция f – полиномиальная, так как строит дополнение графа (один раз проходит по матрице смежности). Значит, мы показали сводимость $CLIQUE \leq_p VERTEX - COVER$. Из семинара $CLIQUE \in \mathcal{NP}c \longrightarrow VERTEX\text{-}COVER \in \mathcal{NP}c$

Задача 4

Докажите, что задача ПРОТЫКАЮЩЕЕ-МНОЖЕСТВО $\in \mathcal{NP}c$.

Пусть L – ПРОТЫКАЮЩЕЕ-МНОЖЕСТВО. Покажем, что $L \in \mathcal{NP}$:
Верификатор получает на вход множество B из k элементов и проверяет пересечение со всеми множествами A_i, если все пересечения непустые, то возвращается 1, иначе 0. Верефикатор полиномеален, так как множеств A_i - конечное число и в каждом из них конечное число переменных.

Покажем, что $L \in \mathcal{NP}c$, для этого построим сводимость $SAT \leq_p L$ (где SAT предполагает КНФ).
Зададим функцию сводимости $f = f(x_1, \cdots, x_n)$, где x_i - переменная SAT, следующим образом: она по SAT строит семейство подмножеств A_i.

Сначала строим множества вида $A_i = \{x_i, \neg x_i\}$ для каждой переменной из SAT, затем для каждого дизъюнкта строим A_i состоящие из всех логических переменных в данном дизъюнкте (то есть если там было отрицание, то ставим отрицание и т.д.)

Пусть $y \in SAT$, следовательно существует её выполняющий набор x. Тогда множество B которое состоит из таких элементов: если в выполняющем наборе $x_i = 1$, то и в B лежит x_i, если в выполняющем наборе $x_i = 0$, то в B лежит $\neg x_i$. (то есть в B ровно k элементов, количество переменных в SAT).
B является протыкающим множеством для A_i. Докажем это от противного: пусть есть A_j с которым пустое пересечение. Пусть это множество построено на основе дизъюнкта F. Рассмотрим этот дизъюнкт: если в F содержится x_i, то в A_j содержится $\neg x_i$ и наоборот (иначе бы было пересечение). Из взятия элементов в A_j получаем, что все x_i в дизъюнкте должны равняться 0, следовательно весь дизъюнкт равен 0, тогда получаем противоречие, что x - выполняющий набор, значит, B – протыкающие множество для A_i.

Пусть $y \notin SAT$ (предполагаем, что мы работаем на множестве КНФ, то есть не рассматриваем y, которые не принадлежит КНФ, только те, для которых не находится выполняющего набора), покажем, что для A_i нет протыкающего множества. От противного, пусть B – протыкающее множество для A_i. Понятно, что в B есть либо x_i либо $\neg x_i$ (иначе не было бы пересечений с множествами вида $A_i = \{x_i, \neg x_i\}$. Для кадого дизъюнкта есть хотя бы одна логическая переменная из B (иначе не было бы пересечений со множествами 2го вида), но тогда по построению значение это переменной равно 1, следовательно каждый из дизъюнктов равняется 1, получается, что y – выполним. Противоречие. Следовательно, для A_i нет протыкающего набора.
Построение A_i полиномиально, так как в SAT конечное число переменных и дизъюнктов.

Задача 5

Покажите, что $VERTEX\text{-}COVER \leqslant_p SET\text{-}COVER$.

Построим функцию сводимости f следующим образом:
введём обозначения: U – множество элементов, а S это семейство подмножеств U. Пусть k это такое количество подмножеств из S, таких что их объединение это U.

$(G = (V, E), k) \in VERTEX\text{-}COVER$. Тогда, пусть $U = E$ и функция f в S добавляет для всех вершин из V рёбра такие, что они инцинденты с этими вершинами, то есть $S_v = \{e \in E : e \text{ инцидентно } v\}\ \forall v \in V$.
Покажем, что $(G = (V, E), k) \in VERTEX\text{-}COVER \Leftrightarrow f((G, k)) = (U, S, k) \in SET\text{-}COVER$

Пусть $(G = (V, E), k) \in VERTEX\text{-}COVER$, значит существует A – вершинное покрытие графа G размер которого k, тогда множество $f(G, k) = S_v : v \in A$ образует *setcover* для U, так как если мы предположим, что некоторый элемент из $U \notin S_v$, то в A не будет вершины, которая бы покрывала это ребро и A, следовательно получили не *vertexcover*, также размер размер S_v равен k, так как в A k вершин. Следовательно, $f(G, k) = S_v : v \in A$ – *setcover*.

В обратную сторону, пусть $(U, S, k) \in SET\text{-}COVER$, тогда $A\{v : S_v$ входит в set-cover $U\}$ будет являться vertex-cover размера k для G: $f((G, k)) = (U, S, k)$. По построению: все элементы из U входят в какое-то множество $S_v \longrightarrow$ все рёбра G покрыты вершинами из A.

Построили f - полиномиальную, так как количество рёбер и вершин в G конечно, следовательно $VERTEX\text{-}COVER \leqslant_p SET\text{-}COVER$.

Задача 7

Докажите, что $\Sigma_k \cup \Pi_k \subset \Sigma_{k+1} \cap \Pi_{k+1}$.

Для решения задачи нужно показать 4 вложения:

1) $\Sigma_k \subset \Sigma_{k+1}$

2) $\Sigma_k \subset \Pi_{k+1}$

3) $\Pi_k \subset \Pi_{k+1}$

4) $\Pi_k \subset \Sigma_{k+1}$

Из этого и будет значить утверждение задачи.
Покажем 1ое и 2ое вложения, 3ие и 4ое делаются аналогично. По определению:

$$\Sigma_k = x \in A \Leftrightarrow \exists y_1 \forall y_2 \exists y_3 \ldots \forall y_k : V(x, y_1, y_2, \ldots, y_k) = 1$$

$$\Sigma_{k+1} = x \in A \Leftrightarrow \exists y_1 \forall y_2 \exists y_3 \ldots \forall y_k \exists y_{k+1} V(x, y_1, y_2, \ldots, y_{k+1}) = 1$$

$$\Pi_{k+1} = x \in A \Leftrightarrow \forall y_1 \exists y_2 \exists y_3 \ldots \exists y_k \forall y_{k+1} : V(x, y_1, y_2, \ldots, y_{k+1}) = 1$$

(делаем аналогично контрольной с семинара, только для общего случая с k. Почему в одном случае фиктивная переменная – последняя, а вдругом первая, обсуждалось на семинаре)
Для 1го: $\Sigma_k \subset \Sigma_{k+1}$. Пусть $A \in \Sigma_k$, т.е $x \in A \Leftrightarrow \exists y_1 \forall y_2 \exists y_3 \ldots \forall y_k : V(x, y_1, y_2, \ldots, y_k) = 1$. Тогда $x \in A \Leftrightarrow \exists y_1 \forall y_2 \exists y_3 \ldots \forall y_k \exists y_{k+1} : V(x, y_1, y_2, \ldots, y_k) = 1$, где y_{k+1} фиктивная переменная, и предикат V ее не использует. По определению $A \in \Sigma_{k+1}$. Значит $\Sigma_k \subset \Sigma_{k+1}$.

Для 2го: $\Sigma_k \subset \Pi_{k+1}$. Пусть $A \in \Sigma_k$, т.е $x \in A \Leftrightarrow \exists y_1 \forall y_2 \exists y_3 \ldots \forall y_k : V(x, y_1, y_2, \ldots, y_k) = 1$. Тогда $x \in A \Leftrightarrow \exists y_0 \forall y_1 \exists y_2 \ldots \forall y_k : V(x, y_1, y_2, \ldots, y_k) = 1$, где y_0 фиктивная переменная, и предикат V ее не использует. По определению $A \in \Pi_{k+1}$. Значит $\Sigma_k \subset \Pi_{k+1}$.

Аналогично 3) и 4)

Задача 9

Докажите, что полиномиальная иерархия «схлопывается», если существует $\mathcal{PH}c$ задача.
Под схлопыванием имеется в виду $\exists k : \mathcal{PH} = \Sigma_k = \Pi_k$.

Пусть язык $A \in PH$ – полный, тогда он лежит и в PH и поэтому лежит в Σ_k для некоторого k (по определению PH). Так как $A \in PH$ – полный, то $\forall B \in PH \longrightarrow B \leq_p A$, значит, B также лежит в Σ_k. Поэтому $PH = \Sigma_k$ для некоторого k.
По определению $\mathcal{PH} == \cup\Pi_k = \Sigma_k$, поэтому для любого n верно $\Pi_{k+n} \subseteq \Sigma_k$,. Из семинара $\Sigma_k \subseteq \Pi_{k+n}$ для любого n. В итоге получаем, что $\Pi_k = \Sigma_k = \mathcal{PH}$ (что и требовалось доказать).