PCP-теорема и вопросы аппроксимируемости NP-трудных задач комбинаторной оптимизации

По работам С.Ароры и И.Динур

М.Ю. Хачай[1]
mkhachay@imm.uran.ru

[1]Институт математики и механики им. Н.Н.Красовского УрО РАН
С.Ковалевской, 16, Екатеринбург, 620990, Россия

2013

Аннотация

Неформально

PCP-теорема утверждает, что для произвольного языка $L \in NP$ найдется формат представления доказательства (принадлежности этому языку), которое может быть проверено (верифицировано) вероятностным способом так, что процедура верификации потребует прочтения не более чем фиксированного числа битов (символов) этого доказательства.

- Известно, что PCP-теорема может быть эквивалентным образом переформулирована в терминах неэффективной аппроксимируемости подходящей NP-трудной задачи комбинаторной оптимизации.

Аннотация

Неформально

PCP-теорема утверждает, что для произвольного языка $L \in NP$ найдется формат представления доказательства (принадлежности этому языку), которое может быть проверено (верифицировано) вероятностным способом так, что процедура верификации потребует прочтения не более чем фиксированного числа битов (символов) этого доказательства.

- Известно, что PCP-теорема может быть эквивалентным образом переформулирована в терминах неэффективной аппроксимируемости подходящей NP-трудной задачи комбинаторной оптимизации.

Аннотация

Неформально

PCP-теорема утверждает, что для произвольного языка $L \in NP$ найдется формат представления доказательства (принадлежности этому языку), которое может быть проверено (верифицировано) вероятностным способом так, что процедура верификации потребует прочтения не более чем фиксированного числа битов (символов) этого доказательства.

- Известно, что PCP-теорема может быть эквивалентным образом переформулирована в терминах неэффективной аппроксимируемости подходящей NP-трудной задачи комбинаторной оптимизации.
- Лекция посвящена обзору комбинаторного подхода [Dinur, 2006] к доказательству PCP-теоремы, базирующегося на этой взаимосвязи.

Содержание

Определения и обозначения

класс NP

Язык $L \in NP$, если существует детерминированный алгоритм $Ver : (x, \pi) \mapsto \{true, false\}$, время работы которого ограничено сверху $poly(|x|)$, при этом:

- если $x \in L$, то $\exists \pi = \pi(x)$, $Ver(x, \pi) = true$,
- если $x \notin L$, то $Ver(x, \pi) = false$ для произвольного π.

класс PCP

Язык $L \in PCP[p, q]$, если существует полиномиальный стохастический алгоритм $Ver : (x, \pi) \mapsto \{true, false\}$, параметризуемый $O(p)$ случайными битами и читающий $O(q)$ битов «доказательства» π так, что:

- если $x \in L$, то найдется $\pi = \pi(x)$, $Pr(Ver(x, \pi) = true) = 1$,
- в пр. сл., $Pr(Ver(x, \pi) = true) \leq 1/2$ для произвольного π.

Определения и обозначения

класс NP

Язык $L \in NP$, если существует детерминированный алгоритм $Ver : (x, \pi) \mapsto \{true, false\}$, время работы которого ограничено сверху $poly(|x|)$, при этом:

- если $x \in L$, то $\exists \pi = \pi(x)$, $Ver(x, \pi) = true$,
- если $x \notin L$, то $Ver(x, \pi) = false$ для произвольного π.

класс PCP

Язык $L \in PCP[p, q]$, если существует полиномиальный стохастический алгоритм $Ver : (x, \pi) \mapsto \{true, false\}$, параметризуемый $O(p)$ случайными битами и читающий $O(q)$ битов «доказательства» π так, что:

- если $x \in L$, то найдется $\pi = \pi(x)$, $Pr(Ver(x, \pi) = true) = 1$,
- в пр. сл., $Pr(Ver(x, \pi) = true) \leq 1/2$ для произвольного π.

PCP-теорема

Theorem 1 (Arora, Safra 1998)

Справедливо соотношение: $NP \subseteq PCP[\log n, 1]$

- новый, робастный взгляд на понятие «доказательство»;
- исторический аспект, $PCP[r, q] \subseteq IP = PSPACE$

Constraint satisfaction problem (CSP)

Определение

Пусть $V = \{v_1, \ldots, v_n\}$ — множество переменных, и Σ — конечный алфавит. Назовем *q-арным ограничением* кортеж $c = (C, i_1, \ldots, i_q)$, в котором $C \subset \Sigma^q$ — допустимое множество и $i_1, \ldots, i_q \in \{1, \ldots, n\} = \mathbb{N}_n$.
Набор значений переменных $a : V \to \Sigma$ удовлетворяет ограничению c, если $(a(v_{i_1}), \ldots, a(v_{i_q})) \in C$.

CSP

Задано: множество ограничений $\mathcal{C} = \{c_1, \ldots, c_n\}$ над множеством переменных V и алфавитом Σ.
Существует ли набор значений переменных, удовлетворяющий каждому элементу множества $\mathcal{C}$?

Труднорешаемость задачи CSP

- Задача CSP — NP-полна
- Являясь обобщением задач 3SAT и 3-COLOR

Труднорешаемость задачи CSP

- Задача CSP — NP-полна
- Являясь обобщением задач 3SAT и 3-COLOR

Труднорешаемость задачи CSP

- Задача CSP — NP-полна
- Являясь обобщением задач 3SAT и 3-COLOR

Example 2 (Сведение задачи 3-COLOR)

Пусть $G = (V_G, E_G)$ — граф, подлежащий раскраске.
Определим $V = V_G$, $\Sigma = \{1, 2, 3\}$,
зададимся множеством

$$C = \{(i, j) \in \Sigma \times \Sigma : \ i \neq j\},$$

каждому ребру $E_G \ni e = \{v_p, v_t\} \mapsto c_e = (C, p, t)$

Труднорешаемость задачи CSP

- Задача CSP — NP-полна
- Являясь обобщением задач 3SAT и 3-COLOR
- Пусть зафиксировано множество $\mathcal{C} = \{c_1, \ldots, c_n\}$. Сопоставим $a \mapsto UNSAT_a(\mathcal{C})$ долю неудовлетворенных ограничений.

$$UNSAT(\mathcal{C}) = \min_a UNSAT_a(\mathcal{C}).$$

Труднорешаемость задачи CSP

- Задача CSP — NP-полна
- Являясь обобщением задач 3SAT и 3-COLOR
- Пусть зафиксировано множество $\mathcal{C} = \{c_1, \ldots, c_n\}$. Сопоставим $a \mapsto UNSAT_a(\mathcal{C})$ долю неудовлетворенных ограничений.

$$UNSAT(\mathcal{C}) = \min_a UNSAT_a(\mathcal{C}).$$

Theorem 2 (Слабая аппроксимируемость задачи max-CSP)

Существуют целые числа $q > 1$ и $s > 1$ и алфавит Σ, $|\Sigma| = s$ такие, что для множества $\mathcal{C}$ q-арных ограничений над алфавитом Σ NP-трудно различить случаи $UNSAT(\mathcal{C}) = 0$ и $UNSAT(\mathcal{C}) \geq 1/2$.

Эквивалентность теорем 1 и 2

Схема доказательства.

(=>) Пусть $L \in NP$. По теореме 1, найдется случайный алгоритм Ver, параметризуемый $c \log n$ случайными битами, читающий условие x и $q = O(1)$ битов доказательства π и принимающий решение о том, $x \in L$ или нет.

Дерандомизация:

$$\{0,1\}^{c \log n} \ni r \overset{Ver}{\mapsto} i_1^{(r)}, \ldots, i_q^{(r)}, \; C^{(r,x)} \doteq \{b \in \{0,1\}^q : \; Ver(b, x|r) = true\}.$$

Пусть $x \overset{?}{\in} L$ — условие исходной задачи, $n = |x|$. Положим $\Sigma = \{0,1\}$ и сопоставим каждому биту π булеву переменную (б.о.о. полагаем, что их не более $q2^{c \log n}$). Построим систему ограничений $\mathcal{C}_x = \{c_{r,x} = (C^{(r,x)}, i_1^{(r)}, \ldots, i_q^{(r)}), r \in \{0,1\}^{c \log n}\}$. Видно, что $Pr(Ver(b, x|r) = false) = UNSAT(\mathcal{C}_x)$, откуда $UNSAT(\mathcal{C}_x) = 0$, если $x \in L$ и $UNSAT(\mathcal{C}_x) \geq 1/2$, в противном случае. □

Эквивалентность теорем 1 и 2

Схема доказательства.

(<=) Допустим, существует полиномиальная сводимость произвольного NP-полного языка к системе ограничений с условием т. 2.

Построим алгоритм Ver:

1. Ver детерминистски сопоставляет условию исходной задачи подобную систему ограничений
2. Ver ожидает, что π — набор значений переменных в $\mathcal{C}$.
3. Ver случайным образом выбирает одно из ограничений, подставляет в него q битов π и проверяет истинность.

□

Определения и обозначения

Всюду ниже мы ограничимся системами бинарных ограничений вида (C, i, j), которые удобно описывать в терминах графов.

$G = ((V, E), \Sigma, \mathcal{C})$ называется *окрашенным графом*, если

1. (V, E) — мультиграф
2. вершины $v \in V$ «окрашиваются в цвета» из Σ,
3. $E \ni e \mapsto c(e) \subset \Sigma \times \Sigma$, $\mathcal{C} = \{c(e)\}_{e \in E}$. Ограничение $c(e)$ удовлетворяется парой (a, b), если $(a, b) \in c(e)$.

Пусть $\sigma : V \to \Sigma$ — раскраска

$$\sigma \mapsto UNSAT_\sigma(G) = Pr\{(\sigma(u), \sigma(v)) \notin c(e) \colon (u, v) = e \in E\}$$

$$UNSAT(G) = \min_\sigma UNSAT_\sigma(G),\ size(G) = |V| + |E|\ (|\Sigma| = const).$$

Идея

Пусть $\Sigma = \mathbb{N}_3$.
Задача: «для заданного окрашенного графа $G = ((V, E), \Sigma, \mathcal{C})$ выяснить, справедливо ли равенство $UNSAT(G) = 0$»
(3-COLOR) — NP-полна.

Заметим, что для данного графа G,

$$UNSAT(G) > 0 \iff UNSAT(G) \geq 1/|E|$$

Основная проблема — указать в правой части величину, не зависящую от G.

Формулировка

Theorem 3 (Main)

Существует алфавит Σ_0, обладающий следующими свойствами. Для произвольного алфавита Σ найдутся $C > 0$ и $0 < \alpha < 1$, такие что произвольному окрашенному графу $G = ((V, E), \Sigma, \mathcal{C})$ за полиномиальное время может быть сопоставлен граф $G' = ((V', E'), \Sigma_0, \mathcal{C}')$, для которого

1. $size(G') \leq C \times size(G)$,
2. *если* $UNSAT(G) = 0$, *то* $UNSAT(G') = 0$ *(полнота),*
3. $UNSAT(G') \geq \min(2 \times UNSAT(G), \alpha)$ *(непротиворечивость).*

Основные леммы

Доказательство т. 3 состоит из трех основных фаз:

предварительная обработка обеспечивает приведение графа к специальному виду (лемма 4)

возведение в степень усиливает непротиворечивость (лемма 5)

композиция обеспечивает сокращение алфавита путем незначительного снижения непротиворечивости (лемма 6).

Предварительная обработка (графа)

Lemma 4

Существуют константы $0 < \lambda < d$ *и* $\beta_1 > 0$ *такие, что произвольному окрашенному графу* G *может быть сопоставлен граф* $G' = prep(G)$:

1. G' — *d-регулярный, с петлями при каждой вершине, и* $\lambda(G') \leq \lambda < d$.
2. G' *имеет тот же алфавит, что и* G *и* $size(G') = O(size(G))$.
3. $\beta_1 UNSAT(G) \leq UNSAT(G') \leq UNSAT(G)$.

Предварительная обработка (графа)

Lemma 4

Существуют константы $0 < \lambda < d$ *и* $\beta_1 > 0$ *такие, что произвольному окрашенному графу* G *может быть сопоставлен граф* $G' = prep(G)$:

1. G' — d-регулярный, с петлями при каждой вершине, и $\lambda(G') \leq \lambda < d$.
2. G' имеет тот же алфавит, что и G и $size(G') = O(size(G))$.
3. $\beta_1 UNSAT(G) \leq UNSAT(G') \leq UNSAT(G)$.

Преобразование исходного графа производим в 2 этапа

$$G \mapsto prep_1(G) \mapsto prep_2(prep_1(G)) \ (= prep(G)).$$

Графы-расширители

Пусть $G = (V, E)$ — d-регулярный граф, сопоставим

$$V \supseteq S \mapsto E(S) = |(S \times (V \setminus S)) \cap E|$$

величину разреза, порождаемого S. *Реберным расширением (edge expansion)* графа G называется число

$$h(G) = \min_{S \subseteq V, |S| \leq |V|/2} \frac{E(S)}{|S|}.$$

Семейство d-регулярных графов $\{X_n\}$ порядка n называется *семейством расширителей с параметром h*, если $h(X_n) \geq h$.

$prep_1(G)$

Построение

Пусть $G = ((V, E), \Sigma, \mathcal{C})$ — окрашенный граф. Зафиксируем параметры d_0 и h_0 и определим граф $G' = ((V', E'), \Sigma, \mathcal{C}') = prep_1(G)$ по правилам:

$prep_1(G)$

Построение

Пусть $G = ((V, E), \Sigma, \mathcal{C})$ — окрашенный граф. Зафиксируем параметры d_0 и h_0 и определим граф $G' = ((V', E'), \Sigma, \mathcal{C}') = prep_1(G)$ по правилам:

1. вершины: $V \ni v \mapsto [v] = \{(v, e) |\ e \in E, v \in e\}, \quad V' = \bigcup_{v \in V} [v]$.

$prep_1(G)$

Построение

Пусть $G = ((V, E), \Sigma, \mathcal{C})$ — окрашенный граф. Зафиксируем параметры d_0 и h_0 и определим граф $G' = ((V', E'), \Sigma, \mathcal{C}') = prep_1(G)$ по правилам:

1. вершины: $V \ni v \mapsto [v] = \{(v, e) |\ e \in E, v \in e\}, \quad V' = \bigcup_{v \in V} [v]$.
2. ребра: каждому $v \in V$ сопоставим d_0-регулярный граф X_v с вершинами $[v]$ и $h(X_v) \geq h_0$. Положим $E' = E_1 \cup E_2$, где

$$E_1 = \bigcup_{v \in V} E(X_v) \text{ и } E_2 = \{\{(v, e), (v' e)\} |\ e = \{v, v'\} \in E\}.$$

$prep_1(G)$

Построение

Пусть $G = ((V, E), \Sigma, \mathcal{C})$ — окрашенный граф. Зафиксируем параметры d_0 и h_0 и определим граф $G' = ((V', E'), \Sigma, \mathcal{C}') = prep_1(G)$ по правилам:

1. вершины: $V \ni v \mapsto [v] = \{(v, e) |\ e \in E, v \in e\}, \quad V' = \bigcup_{v \in V} [v]$.
2. ребра: каждому $v \in V$ сопоставим d_0-регулярный граф X_v с вершинами $[v]$ и $h(X_v) \geq h_0$. Положим $E' = E_1 \cup E_2$, где

$$E_1 = \bigcup_{v \in V} E(X_v) \text{ и } E_2 = \{\{(v, e), (v'e)\} |\ e = \{v, v'\} \in E\}.$$

3. ограничения: $\mathcal{C}' = \{c(e')\}_{e' \in E'}$, где

$$c(e') = \begin{cases} \{(a, a) |\ a \in \Sigma\}, & \text{если } e' \in E_1, \\ c(e), & \text{если } e' = \{(v, e), (v', e)\} \in E_2. \end{cases}$$

Обоснование $prep_1(G)$

Предложение

$G' = prep_1(G)$ — (d_0+1)-регулярный окрашенный граф, $|V'| \leq 2|E|$ и для некоторого $c = c(d_0, h_0) > 0$,

$$c \times UNSAT(G) \leq UNSAT(G') \leq UNSAT(G).$$

Более того, для произвольной раскраски $\sigma' : V' \to \Sigma$,
раскраска $\sigma : V \to \Sigma$, определенная правилом

$$\sigma(v) = \arg\max_{a \in \Sigma} \{Pr(\sigma'(v,e) = a) \mid (v,e) \in [v]\},$$

удовлетворяет соотношению $c \times UNSAT_\sigma(G) \leq UNSAT_{\sigma'}(G')$.

Доказательство

- Регулярность (при $d = d_0 + 1$) и оценка для числа вершин — очевидны.
  Для обоснования $UNSAT(G') \leq UNSAT(G)$:

$$(\sigma : V \to \Sigma) \mapsto (\sigma' : V' \to \Sigma) : \ \sigma'(v, e) = \sigma(v),$$

  поэтому,

$$UNSAT_{\sigma'}(G') = \frac{UNSAT_{\sigma}(G)|E_2|}{|E_1| + |E_2|} \leq UNSAT_{\sigma}(G).$$

- Заметим, что $|E'| \leq d|E|$. Зафиксируем произв. окраску $\sigma' : V' \to \Sigma$ и определим σ по правилу из условия предложения.
  Пусть $F \subseteq E$ и $F' \subseteq E_2$ — подмножества ребер, нарушающих окраску σ и σ', соответственно.
  Зададим

$$V' \supset S = \bigcup_{v \in V} \left\{(v, e) \in [v] \,|\, \sigma'(v, e) \neq \sigma(v)\right\}.$$

Доказательство

Пусть $e = \{v, v'\} \in F$. Тогда для $e' = \{(v, e), (v'e)\}$ либо $e' \in F'$, либо $e \cap S \neq \emptyset$. Поэтому, если $UNSAT_\sigma(G) = |F|/|E| = \alpha$, то $|F'| + |S| \geq |F| = \alpha|E|$. Возможны 2 варианта:

1. $|F'| \geq \frac{\alpha}{2}|E|$. Тогда $|F'| \geq \frac{\alpha}{2d}|E'|$ и $UNSAT_{\sigma'}(G') \geq UNSAT_\sigma(G)/2d$.

Доказательство

Пусть $e = \{v, v'\} \in F$. Тогда для $e' = \{(v, e), (v'e)\}$ либо $e' \in F'$, либо $e \cap S \neq \emptyset$. Поэтому, если $UNSAT_\sigma(G) = |F|/|E| = \alpha$, то $|F'| + |S| \geq |F| = \alpha|E|$. Возможны 2 варианта:

1. $|F'| \geq \frac{\alpha}{2}|E|$. Тогда $|F'| \geq \frac{\alpha}{2d}|E'|$ и $UNSAT_{\sigma'}(G') \geq UNSAT_\sigma(G)/2d$.
2. $|F'| < \frac{\alpha}{2}|E|$, тогда $|S| \geq \frac{\alpha}{2}|E|$. Пусть $S_v = [v] \cap S$.

$$S_v = \dot{\cup}_{a \in \Sigma} S_{v,a}, \; S_{v,a} = \left\{(v, e) \in S_v \mid \sigma'(v, e) = a\right\},$$

при этом $|S_{v,a}| \leq |[v]|/2$ (по выбору σ.) Т.к. X_v — расширитель, $E(S_{v,a}) \geq h_0|S_{v,a}|$. Все ребра, покидающие $S_{v,a}$, нарушают ограничение равенства окраски, следовательно, как мин.

$$\frac{h_0}{2}\Sigma_v|S \cap [v]| = \frac{h_0}{2}|S| \geq \frac{\alpha h_0}{4}|E| \geq \frac{\alpha h_0}{4d}|E'|$$

ребер нарушают σ', т.е. $UNSAT_{\sigma'}(G') \geq \frac{h_0}{4d} UNSAT_\sigma G$.

$prep_2(G)$ I

Построение

Пусть $G = ((V, E), \Sigma, \mathcal{C})$ — окрашенный граф. Сопоставим ему граф $G' = prep_2(G) = ((V, E'), \Sigma, \mathcal{C}')$ по правилу:

1. вершины: остаются прежними
2. ребра: пусть $X = (V, E_1)$ — d_0'-регулярный расширитель с условием $\lambda(X) < \lambda_0 < d_0'$ и $E_2 = \{\{v, v\} \mid v \in V\}$. Тогда $E' = E \cup E_1 \cup E_2$ (доп. кратные ребра).
3. ограничения: на ребрах E наследуются из G, на всех остальных — отсутствуют.

$prep_2(G)$ II

Предложение

Существуют глобальные константы $d'_0 > \lambda_0 > 0$ такие, что для произвольного d-регулярного G граф $G' = prep_2(G)$ обладает свойствами:

1. G' — $(d + d'_0 + 1)$-регулярный, с петлей при каждой вершине, $\lambda(G') \leq d + \lambda_0 + 1 < deg(G')$;
2. $size(G') = O(size(G))$.
3. для произвольной $\sigma : V \to \Sigma$,

$$\frac{d}{d + d'_0 + 1} UNSAT_\sigma(G) \leq UNSAT_\sigma(G') \leq UNSAT_\sigma(G).$$

Степень графа

Пусть $G = ((V, E), \Sigma, \mathcal{C})$ — окрашенный граф и $t \in \mathbb{N}$.
Определим G^t :

- множество вершин остается прежним
- вершины u и v соединены k кратными дугами, если в графе G их соединяет ровно k маршрутов $(u = u_0), u_1, \ldots, u_{t-1}, (u_t = v)$ длины t.
- алфавит: $\Sigma^{d^{\lceil t/2 \rceil}}$. Пусть

$$\Gamma(u) = \{u' \in V : (u = u_0, u_1, \ldots, u_{\lceil t/2 \rceil} = u') - (\text{полу})\text{маршрут в } G\},$$

Ясно, что $|\Gamma(u)| \leq d^{\lceil t/2 \rceil}$. Значение $a \in \Sigma^{d^{\lceil t/2 \rceil}}$ может рассматриваться как отображение $a : \Gamma(u) \to \Sigma$ (мнение u об окраске соседей).

- Ограничение, ассоц. с дугой $\langle u, v \rangle$ удовлетворяется парой (a, b), $a, b \in \Sigma^{d^{\lceil t/2 \rceil}}$, если $\exists \sigma : \Gamma(u) \cup \Gamma(v) \to \Sigma$, удовлетворяющее каждое ограничение $c(e)$, $e \in E \cap (\Gamma(u) \times \Gamma(v))$ и

$$\forall u' \in \Gamma(u), v' \in \Gamma(v),\ \sigma(u') = a_{u'}, \sigma(v') = b_{v'}.$$

Степень графа

Пусть $G = ((V, E), \Sigma, \mathcal{C})$ — окрашенный граф и $t \in \mathbb{N}$.
Определим G^t :

- множество вершин остается прежним
- вершины u и v соединены k кратными дугами, если в графе G их соединяет ровно k маршрутов $(u = u_0), u_1, \ldots, u_{t-1}, (u_t = v)$ длины t.
- алфавит: $\Sigma^{d^{\lceil t/2 \rceil}}$. Пусть

$$\Gamma(u) = \{u' \in V : (u = u_0, u_1, \ldots, u_{\lceil t/2 \rceil} = u') - (\text{полу})\text{маршрут в } G\},$$

Ясно, что $|\Gamma(u)| \leq d^{\lceil t/2 \rceil}$. Значение $a \in \Sigma^{d^{\lceil t/2 \rceil}}$ может рассматриваться как отображение $a : \Gamma(u) \to \Sigma$ (мнение u об окраске соседей).

- Ограничение, ассоц. с дугой $\langle u, v \rangle$ удовлетворяется парой (a, b), $a, b \in \Sigma^{d^{\lceil t/2 \rceil}}$, если $\exists \sigma : \Gamma(u) \cup \Gamma(v) \to \Sigma$, удовлетворяющее каждое ограничение $c(e)$, $e \in E \cap (\Gamma(u) \times \Gamma(v))$ и

$$\forall u' \in \Gamma(u), v' \in \Gamma(v),\ \sigma(u') = a_{u'}, \sigma(v') = b_{v'}.$$

Степень графа

Пусть $G = ((V, E), \Sigma, \mathcal{C})$ — окрашенный граф и $t \in \mathbb{N}$.
Определим G^t :

- множество вершин остается прежним
- вершины u и v соединены k кратными дугами, если в графе G их соединяет ровно k маршрутов $(u = u_0), u_1, \ldots, u_{t-1}, (u_t = v)$ длины t.
- алфавит: $\Sigma^{d^{\lceil t/2 \rceil}}$. Пусть

$$\Gamma(u) = \{u' \in V : (u = u_0, u_1, \ldots, u_{\lceil t/2 \rceil} = u') - \text{(полу)маршрут в } G\},$$

Ясно, что $|\Gamma(u)| \leq d^{\lceil t/2 \rceil}$. Значение $a \in \Sigma^{d^{\lceil t/2 \rceil}}$ может рассматриваться как отображение $a : \Gamma(u) \to \Sigma$ (мнение u об окраске соседей).

- Ограничение, ассоц. с дугой $\langle u, v \rangle$ удовлетворяется парой (a, b), $a, b \in \Sigma^{d^{\lceil t/2 \rceil}}$, если $\exists \sigma : \Gamma(u) \cup \Gamma(v) \to \Sigma$, удовлетворяющее каждое ограничение $c(e)$, $e \in E \cap (\Gamma(u) \times \Gamma(v))$ и

$$\forall u' \in \Gamma(u), v' \in \Gamma(v),\ \sigma(u') = a_{u'}, \sigma(v') = b_{v'}.$$

Степень графа

Пусть $G = ((V, E), \Sigma, \mathcal{C})$ — окрашенный граф и $t \in \mathbb{N}$.
Определим G^t :

- множество вершин остается прежним
- вершины u и v соединены k кратными дугами, если в графе G их соединяет ровно k маршрутов $(u = u_0), u_1, \ldots, u_{t-1}, (u_t = v)$ длины t.
- алфавит: $\Sigma^{d^{\lceil t/2 \rceil}}$. Пусть

$$\Gamma(u) = \{u' \in V : (u = u_0, u_1, \ldots, u_{\lceil t/2 \rceil} = u') - \text{(полу)маршрут в } G\},$$

Ясно, что $|\Gamma(u)| \leq d^{\lceil t/2 \rceil}$. Значение $a \in \Sigma^{d^{\lceil t/2 \rceil}}$ может рассматриваться как отображение $a : \Gamma(u) \to \Sigma$ (мнение u об окраске соседей).

- Ограничение, ассоц. с дугой $\langle u, v \rangle$ удовлетворяется парой (a, b), $a, b \in \Sigma^{d^{\lceil t/2 \rceil}}$, если $\exists \sigma : \Gamma(u) \cup \Gamma(v) \to \Sigma$, удовлетворяющее каждое ограничение $c(e)$, $e \in E \cap (\Gamma(u) \times \Gamma(v))$ и

$$\forall u' \in \Gamma(u), v' \in \Gamma(v),\ \sigma(u') = a_{u'}, \sigma(v') = b_{v'}.$$

Степень графа (прод.)

Lemma 5 (Об усилении)

Пусть фиксированы числа $0 < \lambda < d$ *и* $|\Sigma|$. *Найдется число* $\beta_2 = \beta_2(\lambda, d, |\Sigma|) > 0$ *такое, что для каждого* $t \in \mathbb{N}$ *и для каждого* d*-регулярного окрашенного графа* $G = ((V, E), \Sigma, \mathcal{C})$ *с петлями при каждой вершине и* $\lambda(G) \leq \lambda$,

$$UNSAT(G^t) \geq \beta_2 \sqrt{t} \min\left(UNSAT(G), \frac{1}{t}\right).$$

Тестер набора истинности

Определение

Тестером набора истинности с алфавитом Σ_0 и вероятностью отказа $\varepsilon > 0$ называется алгоритм $\mathcal{P}$, принимающий на вход булеву формулу Φ над множеством булевых переменных X и генерирующий окрашенный граф $G = ((V, E), \Sigma_0, \mathcal{C})$ так, что $X \subset V$ и справедливы следующие условия. Пусть $V' = V \setminus X$ и $a : X \to \{0, 1\} \subset \Sigma_0$.

- если $a \in SAT(\Phi)$, найдется продолжение $b : V' \to \Sigma_0$, такое, что $UNSAT_{a \cup b}(G) = 0$;
- если $a \notin SAT(\Phi)$, то для произвольного $b : V' \to \Sigma_0$, $UNSAT_{a \cup b}(G) \geq \varepsilon rdist(a, SAT(\Phi))$.

Суперпозиция (прод.)

Lemma 6

Допустим существование тестера $\mathcal{P}$ набора истинности с алфавитом $\Sigma_0 = O(1)$ и вероятностью отказа $\varepsilon > 0$. Тогда найдется число $\beta_3 = \beta_3(\mathcal{P})$ такое, что произвольному окрашенному графу $G = ((V, E), \Sigma, \mathcal{C})$ за линейное время может быть сопоставлен граф G' : $size(G') = c(\mathcal{P}, |\Sigma|)size(G)$ над Σ_0 такой, что

$$\beta_3 UNSAT(G) \leq UNSAT(G') \leq UNSAT(G).$$

Доказательство теоремы 3

- Как показано выше, для заданного графа G NP-трудно различить случаи $UNSAT(G) = 0$ и $UNSAT(G) \geq 1/|E|$ (даже при $|\Sigma| = 3$).
- Положим $G_0 = G$ и G_i — результат применения лемм 5 и 6 к G_{i-1}. Тогда $\Sigma_i = \Sigma_0$, $size(G_i) \leq C^i size(G_0) = poly(n)$.
- Полнота — очевидна, $UNSAT(G_0) = 0 \Rightarrow UNSAT(G_i) = 0$.
- Пусть теперь $UNSAT(G_0) \geq 1/|E_0|$, и пусть $k \geq \log(|E_0|)$. Если $\exists i < k$, $UNSAT(G_i) \geq \alpha/2$, то для всех $j > i$, $UNSAT(G_j) \geq \alpha$.
- В противном случае,

$$UNSAT(G_i) \geq \min(2^i UNSAT(G_0), \alpha) = 2^i UNSAT(G_0),$$

следовательно, $UNSAT(G_k) \geq 2^k UNSAT(G_0) \geq 1 > \alpha$, по выбору k.

Доказательство теоремы 3

- Как показано выше, для заданного графа G NP-трудно различить случаи $UNSAT(G) = 0$ и $UNSAT(G) \geq 1/|E|$ (даже при $|\Sigma| = 3$).
- Положим $G_0 = G$ и G_i — результат применения лемм 5 и 6 к G_{i-1}. Тогда $\Sigma_i = \Sigma_0$, $size(G_i) \leq C^i size(G_0) = poly(n)$.
- Полнота — очевидна, $UNSAT(G_0) = 0 \Rightarrow UNSAT(G_i) = 0$.
- Пусть теперь $UNSAT(G_0) \geq 1/|E_0|$, и пусть $k \geq \log(|E_0|)$. Если $\exists i < k$, $UNSAT(G_i) \geq \alpha/2$, то для всех $j > i$, $UNSAT(G_j) \geq \alpha$.
- В противном случае,

$$UNSAT(G_i) \geq \min(2^i UNSAT(G_0), \alpha) = 2^i UNSAT(G_0),$$

следовательно, $UNSAT(G_k) \geq 2^k UNSAT(G_0) \geq 1 > \alpha$, по выбору k.

Доказательство теоремы 3

- Как показано выше, для заданного графа G NP-трудно различить случаи $UNSAT(G) = 0$ и $UNSAT(G) \geq 1/|E|$ (даже при $|\Sigma| = 3$).
- Положим $G_0 = G$ и G_i — результат применения лемм 5 и 6 к G_{i-1}. Тогда $\Sigma_i = \Sigma_0$, $size(G_i) \leq C^i size(G_0) = poly(n)$.
- Полнота — очевидна, $UNSAT(G_0) = 0 \Rightarrow UNSAT(G_i) = 0$.
- Пусть теперь $UNSAT(G_0) \geq 1/|E_0|$, и пусть $k \geq \log(|E_0|)$. Если $\exists i < k$, $UNSAT(G_i) \geq \alpha/2$, то для всех $j > i$, $UNSAT(G_j) \geq \alpha$.
- В противном случае,

$$UNSAT(G_i) \geq \min(2^i UNSAT(G_0), \alpha) = 2^i UNSAT(G_0),$$

следовательно, $UNSAT(G_k) \geq 2^k UNSAT(G_0) \geq 1 > \alpha$, по выбору k.

Доказательство теоремы 3

- Как показано выше, для заданного графа G NP-трудно различить случаи $UNSAT(G) = 0$ и $UNSAT(G) \geq 1/|E|$ (даже при $|\Sigma| = 3$).
- Положим $G_0 = G$ и G_i — результат применения лемм 5 и 6 к G_{i-1}. Тогда $\Sigma_i = \Sigma_0$, $size(G_i) \leq C^i size(G_0) = poly(n)$.
- Полнота — очевидна, $UNSAT(G_0) = 0 \Rightarrow UNSAT(G_i) = 0$.
- Пусть теперь $UNSAT(G_0) \geq 1/|E_0|$, и пусть $k \geq \log(|E_0|)$. Если $\exists i < k$, $UNSAT(G_i) \geq \alpha/2$, то для всех $j > i$, $UNSAT(G_j) \geq \alpha$.
- В противном случае,

$$UNSAT(G_i) \geq \min(2^i UNSAT(G_0), \alpha) = 2^i UNSAT(G_0),$$

следовательно, $UNSAT(G_k) \geq 2^k UNSAT(G_0) \geq 1 > \alpha$, по выбору k.

Доказательство теоремы 3

- Как показано выше, для заданного графа G NP-трудно различить случаи $UNSAT(G) = 0$ и $UNSAT(G) \geq 1/|E|$ (даже при $|\Sigma| = 3$).
- Положим $G_0 = G$ и G_i — результат применения лемм 5 и 6 к G_{i-1}. Тогда $\Sigma_i = \Sigma_0$, $size(G_i) \leq C^i size(G_0) = poly(n)$.
- Полнота — очевидна, $UNSAT(G_0) = 0 \Rightarrow UNSAT(G_i) = 0$.
- Пусть теперь $UNSAT(G_0) \geq 1/|E_0|$, и пусть $k \geq \log(|E_0|)$. Если $\exists i < k$, $UNSAT(G_i) \geq \alpha/2$, то для всех $j > i$, $UNSAT(G_j) \geq \alpha$.
- В противном случае,

$$UNSAT(G_i) \geq \min(2^i UNSAT(G_0), \alpha) = 2^i UNSAT(G_0),$$

следовательно, $UNSAT(G_k) \geq 2^k UNSAT(G_0) \geq 1 > \alpha$, по выбору k.

Литература


Arora, S., and Safra, S. Probabilistic checking of proofs: A new characterization of NP. J. ACM 1998. 45, 1, 70–122.


Arora, S., Lund, C., Motvany, R., Sudan, M., and Szegedy, M. Proof verification and intractability of approximation problems. J. ACM 1998. 45, 3, 501–555.


Dinur I. The PCP Theorem by Gap Amplification. J. ACM 2007. 54, 3