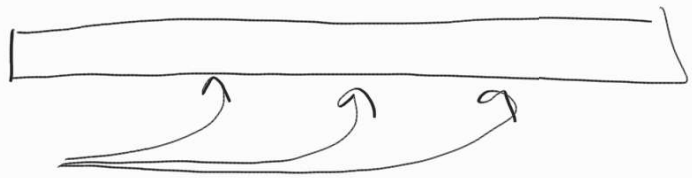
§ Вероятностно-проверяемые доказательства
Probabilistically checkable proofs.



Приближ. алгоритмы

Примеры приближ. алгоритмов

MAX-3-SAT 3-КНФ: в каждой дизъюнкте 3 различных переменных

Найти набор значений, на которых выполняется как можно большее число дизъюнктов.

φ $val(\varphi)$ — макс. число дизъюнктов, на которых можно одновр. выполнить.

$\delta < 1$

δ-приближ. алг. — полиномиальный по времени алгоритм, который находит набор, на котором выполняется $\geq \delta \cdot val(\varphi)$ дизъюнктов.

$\frac{7}{8}$-приближ. алгоритм

Для каждой переменной выбираем случайное значение

$\varphi = C_1 \wedge C_2 \wedge \dots \wedge C_m$

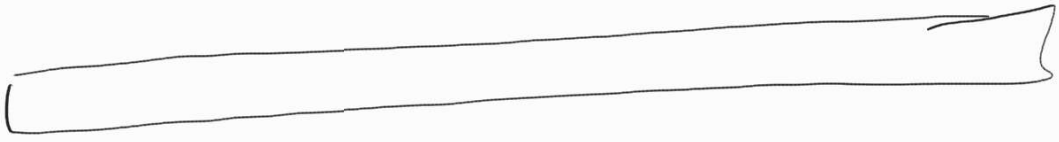
$X_i = \begin{cases} 1, & \text{если } C_i \text{ выполнен} \\ 0, & \text{иначе} \end{cases}$

x	y	z
0	0	0

$E[\sum X_i] = \sum_i E[X_i] = \frac{7}{8} m$

$\frac{7}{8} m \geq \frac{7}{8} val(\varphi)$

$PCP(r(n), q(n))$



$q(n)$

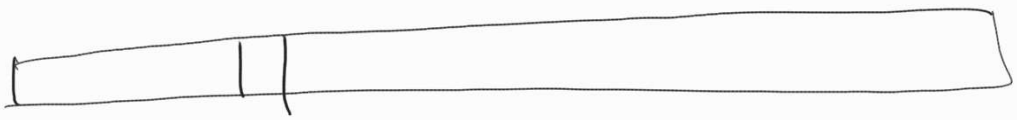
$r(n)$

Опр. $L \in PCP(r(n), q(n))$, если $\exists$ полин. по времени вероят. алгоритм V у которого есть оракульный доступ к строке π длины $2^{O(r(n))} \cdot q(n)$ и обладает след. св-ми:

1) На входе x V исп. $O(r(|x|))$ случ. бит и делает $O(q(|x|))$ неадаптивных запросов к π.
2) Если $x \in L$, то $\exists \pi$: $Pr[V^{\pi}(x) = 1] = 1$
3) Если $x \notin L$, то $\forall \pi'$ $Pr[V^{\pi'}(x) = 1] \leq \frac{1}{2}$

Пример $GNI \in PCP[poly(n), 1]$

(G_0, G_1)



H $\quad 2^{\frac{n(n-1)}{2}}$

$\pi_H = 0$, если $H \simeq G_0$

$\pi_H = 1$, если $H \simeq G_1$

$i \leftarrow \{0,1\}$

$\sigma \leftarrow S_n$

$\pi_{\sigma(G_i)} = i$ $\longrightarrow$ принимаем

иначе отвергаем.

Если $G_0 \cong G_1$, то $\sigma(G_1)$ и $\sigma(G_0)$ — изоморф. ор. ребер

Теорема (PCP1 теорема)

$NP = PCP(\log n, 1)$

Д-во $PCP(\log n, 1) \subseteq NP$

$\forall L \in PCP(\log n, 1)$

$\forall x \in L$ П

CSP Constraint satisfaction problem

q-CSP q-КНФ

$$\begin{cases} f_1(x) = 1 \\ f_2(x) = 1 \\ \vdots \\ f_m(x) = 1 \end{cases}$$

$f_i : \{0,1\}^n \to \{0,1\}$

f_i: зависит только от q битов.

И $val(И)$ — макс. кол-во условий, кот. можно одноврем. выполнить.

m — число условий

Max-q-CSP : найти набор значений переменных, которые выполняют как можно больше условий

ρ-GAP-q-CSP $q \in \mathbb{N}$, $\rho \in (0,1)$

Отличить 2 случая

$val(\mathcal{U}) = m$ — 1

$val(\mathcal{U}) < \rho \cdot m$ — 0

Теорема (PCP2) $\exists\ \rho \in (0,1)$ $\exists q \in \mathbb{N}$: ρ-GAP-q-CSP является NP-трудной!

ρ-GAP-q-CSP $\in NP$ $\forall$ языка $\exists$ полиномиал. по врем. алг. A:

$x' \xrightarrow{A} \mathcal{U}$ — m условий в q-CSP

$x \in L \Rightarrow val(\mathcal{U}) = m$

$x \notin L \Rightarrow val(\mathcal{U}) < \rho \cdot m$

Сл-ие PCP2 $\exists\ \rho \in (0,1)$ $\exists q \in \mathbb{N}$, если $P \neq NP$, нет полином. по времени ρ-прибл. алгоритма к MAX-q-CSP.

Д-во (следствие) q и ρ — какие?

Из PCP2.

Пусть A ρ-прибл. алгоритм для MAX-q-CSP.

$\forall L \in NP$ $\exists$ полином. вып. отобр. f:

$x \in L \Rightarrow val(f(x)) = m$

$x \notin L \Rightarrow val(f(x)) < \rho \cdot m$

$A(f(x)) \longrightarrow$ $val(f(x)) = m \Rightarrow$

найдр, кот. $\text{вып} \geq \beta \cdot m$

$\nearrow$ решил задачу

$val(f(x)) < \beta \cdot m$

прост нет.

$P = NP.$

$PCP_1 \Longleftrightarrow PCP_2$ $\exists s, q:$

$s\text{-GAP-}q\text{-CSP}$

NP трудна

$NP = PCP(\log n, 1)$

Д-во $\Leftarrow$

$\forall L \in NP$

L и

s - поле вых ф-ции

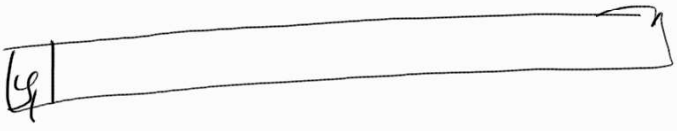
$s\text{-GAP-}q\text{-CSP}$

x $\rightsquigarrow$ $\begin{cases} f_1(y) = 1 \\ f_2(y) = 1 \\ \vdots \\ f_m(y) = 1 \end{cases}$

$|x| = n$

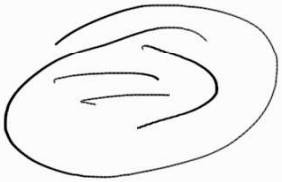
$y \in \{0,1\}^{P(n)}$

Д-во для x — решение системы



$x \in L$ $\quad P_r[V^{\pi}(x)=1]=1$

$x \notin L$ $\quad P_r[V^{\pi}(x)=1] < s$



$L \in NP = PCP(\log n, 1)$

$\exists V^{\pi} \quad |\pi| = p(n)$ – полином

V делает q запросов

и g-бу.

$c \cdot \log n$ — след. битов

r_1 — — — . $\pi_{i_1} \to \pi_{i_q}$

$2^{c\log n}$

r_2 — — — $\pi_{i_1} \quad \pi_{i_q}$

$r_{c\log n}$ — — — .

Применительно СДП — биты

дан ва π.

$2^{c\log n}$ — m ограничений

Огранич., соотв. r_j:

$V^{\pi}_{r_j}(\pi_{i_1}, \ldots, \pi_{i_q})$

$x \in L \Rightarrow val(\varphi) = m$

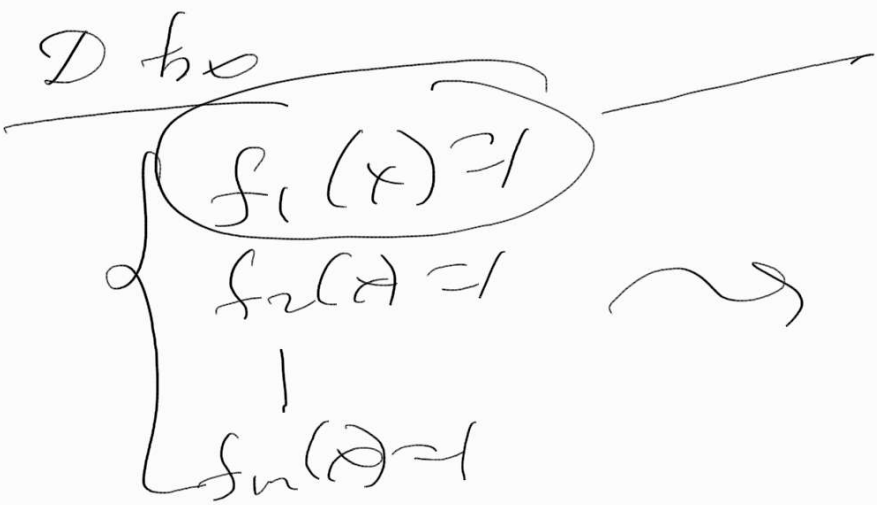
$x \notin L \Rightarrow val(\varphi) \leq \frac{m}{2}$

$\frac{1}{2}$-GAP-q-CSP

PCP2 $\exists p, q$ p-GAP-q CSP
является NP-трудной

Утв. $\exists p, q$: p-GAP-q-SAT
явл. NP-трудным

Док-во



$\rightsquigarrow$

закодируем в q КНФ

m' дизъюнктов

$m \leq m' \leq 2^q m$

$m \geq \frac{m'}{2^q}$

$\phi_{ыр}$ → $\phi_{ин}$

q-ESP → q-КНФ

$val(\varphi) = \frac{s}{m} \cdot m$

$\Rightarrow val(\varphi') \leq$

$m' - (1-s)m$

$\leq m' - \frac{1-s}{2q} m' =$

$= m' \left(1 - \frac{1-s}{2q}\right)$

Упр. $\exists s$: s-GAP-3-SAT

NP-трудно.

Факт. $\left(\frac{7}{8}+\varepsilon\right)$-GAP-3-SAT

$\forall \varepsilon > 0$

NP-трудно

Сл-ие Если $\exists$ полин.

$\left(\frac{\pi}{3}+\varepsilon\right)$ приближ. дает MAX-3-SAT

$\Rightarrow$ $P = NP$.

$NP \subseteq PCP(poly(n), 1)$

Коды Уолша – Адамара

$C: \{0,1\}^n \to \{0,1\}^m$

Кодовое расст. $d = \min\limits_{\substack{x \in \{0,1\}^n \\ y \in \\ x \neq y}} \Delta(C(x), C(y))$

$\longrightarrow d$

$WH: \{0,1\}^n \to \{0,1\}^{2^n}$

$WH(a) = (\langle a, r \rangle)_{r \in \{0,1\}^n}$

$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i \mod 2$

$x, y \in \{0,1\}^n$

кв-ва кодов WH

1) $WH(a+b) = WH(a) + WH(b)$

2) $\Delta(WH(a), WH(b)) = \Delta(WH(a+b), 0)$

$=$

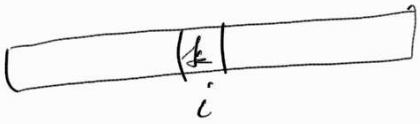
$WH(a)$ $WH(b)$ 2^{n-1}

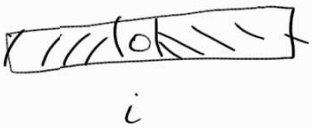
$WH(b)$ $WH(b)$

$WH(a+b)$ 0

$a \neq b$ $a+b \neq 0^n$

Утв. $x \in \{0,1\}^n \setminus 0^n$ $wt(x)$ состоит из 2^{n-1} нулей и 2^{n-1} единиц.





Random subsum principle

$x \in \{0,1\}^n$, $x \neq 0^n$

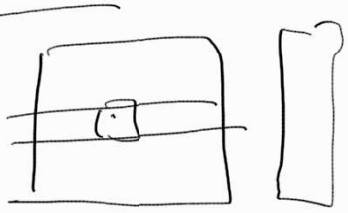
Тогда $Pr_r[\langle x, r \rangle = 1] = \frac{1}{2}$

$r \in \{0,1\}^n$

$\mathbb{F}_2$ $AB = C$ A, B, C матр $n \times n$

$ABr = Cr$ $AB \neq C$

$AB - C$



Код Уолша – Адамара

$\Longleftrightarrow$ линейные ф-ции

$WH(a) = \langle a, r \rangle$ $r \in \{0,1\}^n$

таблица всех ф-ций $f_a : \{0,1\}^n \to \{0,1\}$

$$f_a(x) = \langle a, x \rangle$$

Локальное декодирование кодов Уолша – Адамара.

$$\tilde{f} : \{0,1\}^n \to \{0,1\}$$

$$\Pr_{x \in \{0,1\}^n}\left[f(x) \neq \tilde{f}(x) \right] \leq \delta < \frac{1}{4}$$

$f(x)$ – линейная ф-ция.

$$\Pr\left[f(a) \neq \tilde{f}(r) + \tilde{f}(r+a) \right] \leq$$

$$\leq \Pr\left[\tilde{f}(r) \neq f(r) \right] + \Pr\left[\tilde{f}(r+a) \neq f(r+a) \right]$$

$$< \delta + \delta = 2\delta < \frac{1}{2}$$
