Сложность в среднем

$D = \{D_n\}_{n=1}^{\infty}$ анс. распр. D_n – это распр. $\{0,1\}^n$

(L, D) – распр. задача $L \subseteq \{0,1\}^*$

D – анс. распределение

Опр $\mathrm{Heur}_{\delta(n)} P = \{(L,D) \mid \exists$ полин по врем. алгоритм A:

$\delta: \mathbb{N} \to [0,1]$ $\forall n \Pr_{x \leftarrow D_n}[A(x) \neq L(x)] < \delta(n)\}$

Теорема $\exists$ такой анс. распр D :

$\forall$ разрешимого L $(L,D) \in \mathrm{Heur}_{1/n^3} P \Leftrightarrow L \in P$.

Д-во $\sum_x 2^{-KP(x)} \leq 1$ $\quad D_n(x) = \frac{2^{-KP(x)}}{\sum_{y \in \{0,1\}^n} 2^{-KP(y)}}$

Пусть L – разреш. если $(L,D) \in \mathrm{Heur}_{1/n^3} P$. Пусть A – полин. алг!

$\forall n \Pr_{x \leftarrow D_n}[A(x) \neq L(x)] < 1/n^3$

$\{x \mid A(x) \neq L(x)\}$ конечное.

Положим

$n - \max_{x \in \{0,1\}^n} : A(x) \neq L(x)$

$D_n(x) \leq \frac{1}{n^3}$ (т.к. $D_n(x) = 2^{-KP(x)}$) $\Rightarrow$ $KP(x) \geqslant 3\log n$

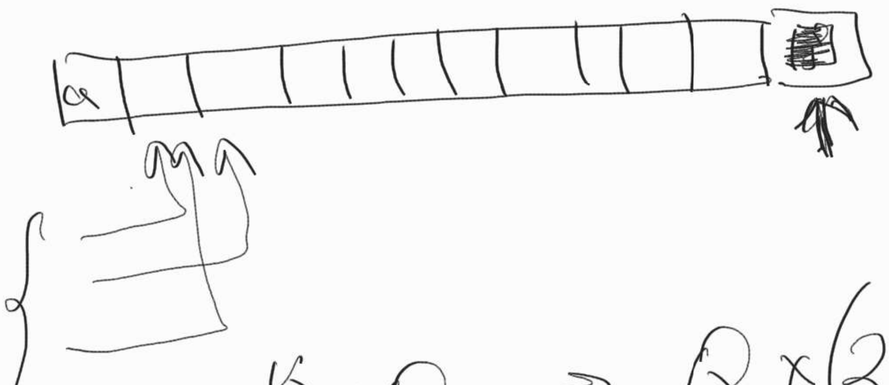
x – некот. лекс. первая строка из $\{0,1\}^n$: $A(x) \neq L(x)$

$KP(x) \le \log n + 2\log\log n + O(1)$

n $\qquad$ $\underbrace{0011001101}$

$3\log n \le \log n + 2\log\log n + O(1)$ — может выполняться только для маленьких числа n. !!! ...

Конечные автоматы с k головками.



Q

q_0

F

k

$\delta: \Sigma^k \times Q \to Q \times (2^{[k]} \setminus \emptyset)$

Принимаем слово, если все головки дошли до конца и мы в приним. состоянии

$\{ x \# x \mid x \in \{0,1\}^* \}$

Теорема $\forall k \ge 1$ $\exists$ язык, кот. распознается автоматом с $k+1$ головкой, но не

расп. с k головками

Д-во

$m \geq 1$

$L_m = \{ w_1 \# w_2 \# \dots \# w_m \# w_m \# w_{m-1} \dots \# w_1 \mid w_1, w_2, \dots, w_m \in \{0,1\}^* \}$

Утв. А может с k головками распознать L_m, если $m \leq \binom{k}{2} = \frac{k(k-1)}{2}$

$(k-1) + (k-2) + \dots + 1 = \frac{k(k-1)}{2}$

Утв Если $m > \frac{k(k-1)}{2}$, тогда любой L_m не распознается автоматами с k головками.

Пара головок проверяет слово w_i, если в некоторый момент эти головки указывают на разные части w_i

Всегда $\exists i \in [m]$ w_i не проверено никакой парой.

$N \in \mathbb{N}$ фикс. больше.

$KS(w_1 w_2 \dots w_m) \geq m - N$

$\in \{0,1\}^{kN}$

$w = w_1 \# w_2 \ldots \# w_m \# w_m \# \ldots \# w_1$

Пусть i — такое, что w_i не проверено никакой парой головок.

Протокол работы автомата на w:

каждый раз, когда какая-то головка пришла в w_i или ушла из w_i мы запишем

(положение всех головок, q)

k, m — константы

$O(\log N)$ битов — P

Покажем, что по P можно восстановить w_i.

Перебираем все строки $w \in \{0,1\}^N$ вместо w_i и смотрим, какой получаем протокол.

w': протокол получается такой же.

w_i w'

w_i w_i

w' w'

$mN \leq (m-1)N + O(r \log N)$

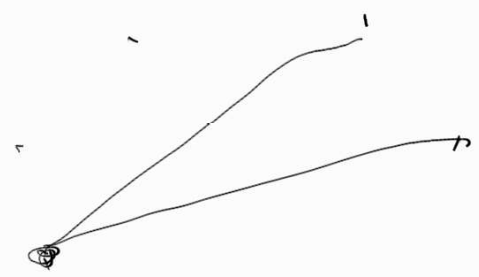
Конструктивный вариант Л.Л.Л.

$A_1, A_2, \dots, A_n$ — события.

$P_r[A_i] = p$

$P_r[\overline{A_1}\,\overline{A_2}\dots\overline{A_n}] = (1-p)^n > 0$

$A_1, A_2, \dots, A_n$



A_i зависит от $\{A_j \mid (i,j) \in E\}$

ЛЛЛ (Симметр. вершина)

$A_1, A_2, \dots, A_n$. G — граф зависимостей.

$G \leq d$, $\forall i\ P_r[A_i] \leq p$.

если $4pd \leq 1$. Тогда $P_r[\overline{A_1}\,\overline{A_2}\dots\overline{A_n}] > 0$

Пример φ – это ф-ла в к-КНФ в каждом дизъюнкте входит m разл. перем. $\exists$ каждый дизъюнкт имеет общую перем. с $\leq \frac{2^m}{4}$ дизъюнктами.

Тогда φ – выполнима.

Д-во $\forall$ случ. присв каждой перем. A_i – i-й дизъюнкт не вып.

$\Pr[A_i] = 2^{-m}$ Граф зав. $(i,j) \in E \iff C_i$ и C_j имеют общую переменную. $d \leq \frac{2^m}{4}$

$4pd \leq 1 \xrightarrow{\text{ЛЛ}} \Pr[\overline{A_1}\overline{A_2}\dots\overline{A_n}] > 0.$

Мозер Тардош ~ 2008

Теорема $\exists$ вероятн. алгоритм кот. с вер. $\geq 1/2$ находит вып. набор ф-ла в к-КНФ (в каждом дизъюнкте k разл. пер.), в кот. N дизъюнктов, и переменных, каждый дизъюнкт имеет общие перем. с $\leq \frac{2^k}{8}$ дизъюнктами. за $O(n+N)$ шагов. каждый шаг poly$(|\varphi|)$.

$\varphi = C_1 \wedge C_2 \wedge \ldots \wedge C_N$

C – д-т φ $S(C)$ – упор. мн-во дизъюнктов, имеющ. общ. что пер. с C.

Алгоритм

- Выбрать знач. всех перем. случайно
- Для всех i от 1 до N
  Если C_i не вып., то
  $Fix(C_i)$

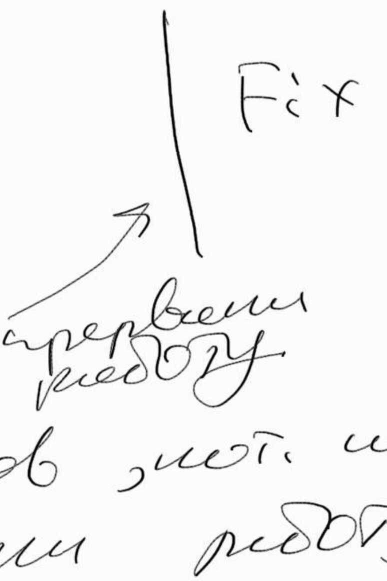
$Fix(C)$

- Выбрать новое знач. для всех пер. C.
- Для всех $C_i \in S(C)$
  Если C_i не вып., то
  $Fix(C_i)$

Утв. Если $Fix(C)$ завершился, то C выполнен.

Утв. Если д-т C' была выполнен до запуска $Fix(C)$, то после завершения тоже.

Утв. Если алгоритм закончил работу, то все дизъюнкты выполнены.



Посл-ть случ. битов, исп. до того, как прервали работу можно восст. по знач. пер. в посл. момент.

и посл-ти дизъюнктов, к кот. прим. Fix.

Пусть мы применяли Fix к рез.

$n + m \cdot k$ случ. битов использовали

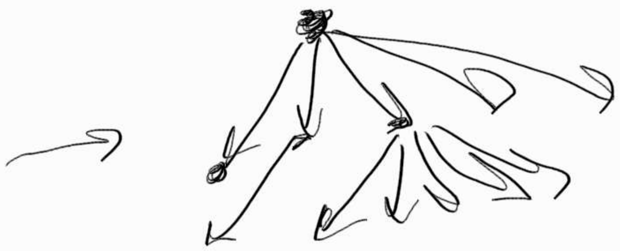
Закодируем их иначе

– значения всех переменных и битов в посл-ий момент

Надо как-то закодир. список дизъюнктов, к кот. применялось Fix.

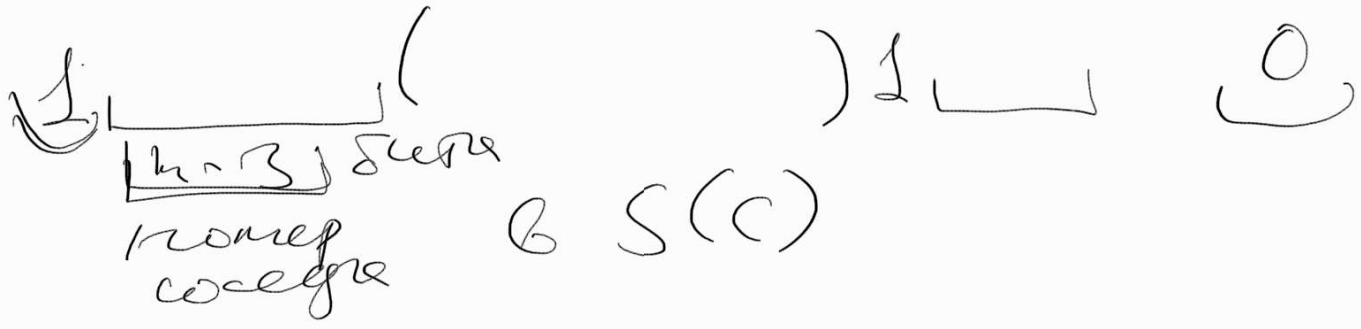
$\{0,1\}^N$ – для каждого дизъюнкта говорим применяли ли мы к нему Fix на верхнем уровне

$\frac{2^m}{\sigma}$



1 идем вниз по дереву

0 идем вверх по дереву.



m-1 бита

k (m-1) битов.

$N + k(m-1) + n <<$

$n + k \cdot m$

$k >> 10 N$

$N + k(m-1) + n \leq n + km - 1$

$k \geq N + 1$

MCSP