

May - Ozerov (2015)

В основе - алгоритм реш-я задачи NN (Nearest Neighbors)

А почему?

Мотивировка

$$e_q = \tilde{H}(e_1 + e_2) + \tilde{z}$$

$$\pi(H), \pi(\tilde{e})$$

$$\begin{cases} H e^t = s \\ wt(e) = w \end{cases} \Leftrightarrow \begin{cases} \tilde{H} e_1 = \tilde{H} e_2 + e_q + \tilde{s} \\ wt(e_1) = wt(e_2) = p/2 \\ wt(e_q) = w - p \end{cases} \quad (1)$$

$$\tilde{H} = \begin{matrix} & \begin{matrix} 1 & 0 & & \end{matrix} \\ \begin{matrix} 0 & 1 & & \end{matrix} & & & \end{matrix} \quad \begin{matrix} n-k & k & & \end{matrix}$$

$$\tilde{z} = \begin{matrix} n-k & k/2 & k/2 \\ w-p & p/2 & p/2 \end{matrix}$$

$$\tilde{e} = e_q + e_1 + e_2$$

$$e_q \in \mathbb{F}_2^{n-k} \times \mathbb{F}_2^{k/2} \times \mathbb{F}_2^{k/2}$$

$$e_1 \in \mathbb{F}_2^{n-k} \times \mathbb{F}_2^{k/2} \times \mathbb{F}_2^{k/2}$$

Осн. идея: $[m] = \{1, 2, \dots, m\}$ т.з. - s.t. w.o.p.

$|m|$ - длина в-ров L и R

Определим константу λ т.з. $|L| = |R| = 2^{\lambda m}$

$|$ перес-ка P хорошая (good), т.е. $\exists Q$ и $\exists (e_1^*, e_2^*)$ - реш.(1)

Определим $0 < \gamma < \frac{1}{2}$ т.з. $w-p = \gamma m \Leftrightarrow \gamma = \frac{w-p}{m}$

$| u^* = \tilde{H} e_1^*, v^* = \tilde{H} e_2^* + \tilde{s}$

Постановка задачи (m, γ, λ) -NN

$| m \in \mathbb{N}, 0 < \gamma < \frac{1}{2}, 0 < \lambda < 1$
Дано: 2 списка $L, R \subset \mathbb{F}_2^m : |L| = |R| = 2^{\lambda m}$
(with uniform and pairwise indep. vector)

Если $\exists (u^*, v^*) \in L \times R$ т.з. $\Delta(u^*, v^*) = \gamma m$
то мы должны вывести список $C \ni (u^*, v^*)$

(?) Все ли реш-я будут в C ?
Или хотя бы одно?

Наивный способ: считаем $\Delta(u, v)$ для каждой пары $(u, v) \in L \times R \Rightarrow$ сложность $\tilde{O}(|L|^2) = \tilde{O}(2^{2\lambda m})$

Идея алг-ма - составить экспоненциально много пар подписков L', R'

Каждый подписок сост-ся с использованием случайного разбиения $A \subset [m], |A| = \frac{m}{2}$



Мы отбираем в L', R' только такие эл-ты из L, R , к-рые имеют опр-ный вес Хэмминга $h \cdot \frac{m}{2}$ на позициях, вход-х в A , для нек-рого $0 < h < \frac{1}{2}$, зависящего только от λ .

Как выбрать h ? Т.обр., чтобы мат.отстояние длины списков L', R' полиномиально завис. от m

Сколько списков L', R' нужно? Столько, чтобы w.o.p.

$\exists$ пара подписков L^*, R^* , содержащих (u^*, v^*) .
т.е. $(u^*, v^*) \in L^* \times R^*$
Поиск реш-я в L', R' происходит полным перебором.
Все найд-е пара (u^*, v^*) сох-ся в C .