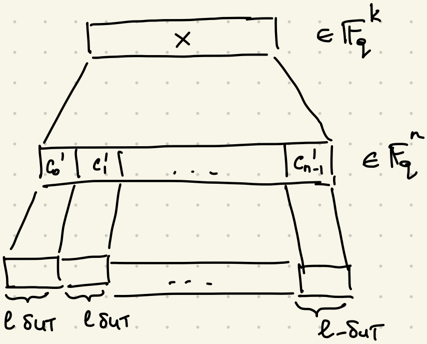
Лекция №10

Коды конкатенации

Идея:



$\mathbb{F}_q = \mathbb{F}_{2^\ell}$

Код конкатенации. Положим $C_{out} \subseteq \mathbb{F}_{q_{out}}^{n_{out}}$ – $[n_{out}, k_{out}, d_{out}]$ – внешний код

$C_{in} \subseteq \mathbb{F}_{q_{in}}^{n_{in}}$ – $[n_{in}, k_{in}, d_{in}]$ – внутренний код

$q_{out} = q_{in}^{k_{in}}$ $\qquad \mathbb{F}_{q_{out}} \cong \mathbb{F}_{q_{in}}^{k_{in}}$

Код конкатенации $C_{in} \circ C_{out} \subseteq \mathbb{F}_{q_{in}}^{n_{in} \cdot n_{out}}$ – это линейный код с ф-цей кодирования $Enc()$, заданной следующим образом:

1. $x \in \left(\mathbb{F}_{q_{out}}^{k_{out}}\right) \cong \left(\mathbb{F}_{q_{in}}^{k_{in}}\right)^{k_{out}}$
2. кодируем x с помощью $Enc_{out}(x) \to C' \in \mathbb{F}_{q_{out}}^{n_{out}} \cong \left(\mathbb{F}_{q_{in}}^{k_{in}}\right)^{n_{out}}$
3. кодируем C_i' $1 \le i \le n_{out}$ с помощью $Enc_{in}()$:

$$c = Enc_{in}(c_1') \,\|\, Enc_{in}(c_2') \ldots \,\|\, Enc_{in}(c_{n_{out}}')$$

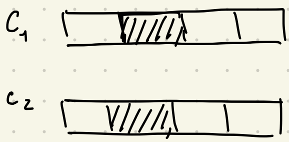
Пар-ры кода:

1) размерность: $k_{in} \cdot k_{out} = k$
2) длина: $n_{in} \cdot n_{out} = n$

$\Bigg\}$ скорость $R = \frac{k}{n} = \underbrace{R_{out}}_{\frac{k_{out}}{n_{out}}} \cdot R_{in}$

Предложение 1 Min. расстояние $C_{in} \circ C_{out} \geq d_{in} d_{out}$

Δ $\exists\ c_1, c_2 \in C_{in} \circ C_{out}$



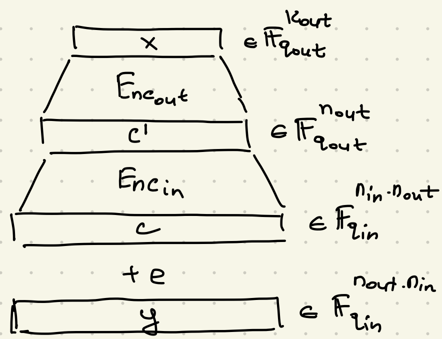
1. Как min. d_{out} блоков c_1, c_2 кодирует разные символы в $\mathbb{F}_{q_{in}}^{k_{in}}$
2. каждый эл-т одного из таких блоков кодируется в слово из C_{in} с min. расстоянием d_{in}.

Пример 1. C_{out} – код Рида – Соломона

2. C_{in} – "хороший" бинарный код, порождённый "случайной" матрицей $G \in \mathbb{F}_2^{k \times n}$.

II Декодирование $C_{in} \circ C_{out}$

Попытка №1.



Алгоритм #1

1. Декодировать каждое $y_i \in \mathbb{F}_{q_{in}}^{n_{in}}$, $i \leq n_{out}$ с помощью Dec_{in}:

$$w_i' = \underset{c \in C_{in}}{\arg\min}\ \Delta(y_i, c) \in \mathbb{F}_{q_{in}}^{n_{in}}$$

2. Получить для всех w_i' соответствующее сообщение m_i', то есть такое, что $w_i' = Enc_{in}(m_i')$

$$m_i' \in \mathbb{F}_{q_{in}}^{k_{in}} \cong \mathbb{F}_{q_{out}}, \quad i \leq n_{out}$$

3. Декодировать $(m_1', .., m_{out}')$ с помощью Dec_{out}.

Лемма 1 Алгоритм №1 может декодировать $< \frac{d_{in} \cdot d_{out}}{4}$ ошибок.

Замечание "хороший" алгоритм декодирования для $C_{in} \circ C_{out}$ должен декодировать $\left\lfloor \frac{d_{in} \cdot d_{out} - 1}{2} \right\rfloor$ ошибок.

◁ Назовём блок $y_i \in \mathbb{F}_{q_{in}}^{n_{in}}$ "плохим", если в нём больше, чем $\lfloor \frac{d_{in}-1}{2} \rfloor$ ошибок.

Так как всего у нас $wt(e)$ ошибок, то максимум $\frac{wt(e)}{\lfloor \frac{d_{in}-1}{2} \rfloor}$ блоков "плохие". Декодер Dec_{in} не может корректно декодировать такие блоки y_i на шаге 1. $\Rightarrow$ В таком случае, Dec_{out} получит на вход слово $\notin C_{out}$. D_{out} может исправить максимум $\lfloor \frac{d_{out}-1}{2} \rfloor$ таких слов. В итоге, # плохих блоков $\leq \lfloor \frac{d_{out}-1}{2} \rfloor$.

В итоге, $\frac{wt(e)}{\lfloor \frac{d_{in}-1}{2} \rfloor} \leq \lfloor \frac{d_{out}-1}{2} \rfloor \Rightarrow wt(e) \leq \lfloor \frac{d_{out}-1}{2} \rfloor \lfloor \frac{d_{in}-1}{2} \rfloor < \frac{d_{in} \cdot d_{out}-1}{4}$. ▶

Попытка №2

Замечание: Когда мы декодируем y_i на шаге 1, мы получаем помимо $w_i' \in C_{in}$, расстояние $\Delta(y_i, w_i')$. Суть алгоритма 2: каждому w_i' приписывается "уровень доверия" (confidence level), зависящий от $\Delta(y_i, w_i')$. В случае, если $\Delta(y_i, w_i')$ – большое, то считаем y_i – удалённым символом ("$*$").

Лемма 2 (Возможности декодирования кода RS): Мы можем декодировать $RS_{\mathbb{F}_q, \mathbb{F}_q^*}[n, k]$ с $wt(e)$ ошибками и $\leq$ удалёнными символами, если $2 \cdot wt(e) + s < n-k+1$.

Алгоритм №2

Вход: $y = (y_1 \dots y_{n_{out}}) \in (\mathbb{F}_{q_{in}}^{n_{in}})^{n_{out}}$

1. Для $i = 1 \dots n_{out}$.

   1.1. $w_i = \underset{c \in C_{in}}{\arg\min}\, \Delta(y_i, c) \in \mathbb{F}_{q_{in}}^{n_{in}}$

   1.2. С вероятностью $\min\left(1, \frac{2\Delta(y_i, w_i)}{d_{in}}\right)$
   $w_i = "*"$ $\quad // m_i' = "*"$

   иначе
   m_i' – сообщение, т.ч. $Enc_{in}(m_i') = w_i$

2. $X = Dec_{out}(m_1', m_2', \dots, m_{out}')$

Лемма 3 $\mathbb{E}\left[\,|w_i| = \text{"*"} + 2|w_i \ne C_{out}|\,\right] < d_{out}$

("декодирование на шаге 2 алг-ма 2 пройдёт успешно в среднем").

$\triangleleft$ $e_i = \Delta(y_i, c_i)$

$$wt(e) = \sum_{i \le n_{out}} e_i < \frac{d_{in}\, d_{out}}{2}$$

Обозначим для $1 \le i \le n_{out}$: $Z_i^{erasure} = \begin{cases} 1, & w_i = \text{"*"} \\ 0, & \text{иначе} \end{cases}$, $Z_i^{error} = \begin{cases} 1, & w_i \ne \text{"*"},\ w_i \ne C_{out} \\ 0, & \text{иначе} \end{cases}$

Утверждение: $\mathbb{E}\left[2Z_i^{error} + Z_i^{erasure}\right] \le \frac{2e_i}{d_{in}}$ (1)

Из (1) $\Rightarrow$ Лемма 3, т.к. $\mathbb{E}\left[\sum_{i=1}^{n_{out}} Z_i^{erasure} + 2\sum_{i=1}^{n_{out}} Z_i^{error}\right]$

$$= \sum_{i \le n_{out}} \mathbb{E}\left[Z_i^{erasure} + 2Z_i^{error}\right] \underset{(1)}{\le} \sum_{i \le n_{out}} \frac{2e_i}{d_{in}} < \frac{2}{d_{in}} \cdot \frac{d_{in} \cdot d_{out}}{2} = d_{out}$$

Случай 1 $w_i = c_i$

$$Z^{error} = 0$$

$$\mathbb{E}\left[Z^{erasure}\right] = 1 \cdot \Pr\left[w_i = \text{"*"}\right] + 0 \cdot \Pr\left[w_i \ne \text{"*"}\right]$$

$$= 1 \cdot \min\left(1, \frac{2\Delta(y_i, w_i)}{d_{in}}\right) \le \frac{2\Delta(y_i, w_i)}{d_{in}} = \frac{2\Delta(y_i, c_i)}{d_{in}} =$$

$$= \frac{2e_i}{d_{in}} .$$

Случай 2 $w_i \ne c_i$

$$\mathbb{E}\left[Z^{erasure}\right] = \min\left(1, \frac{2\Delta(y_i, w_i)}{d_{in}}\right) = \frac{2}{d_{in}} \min\left(\frac{d_{in}}{2}, \Delta(y_i, w_i)\right)$$

$$Z^{error} = 1 - Z^{erasure} \quad \text{(по опр-ию)}$$

$$\mathbb{E}\left[Z^{error}\right] = \mathbb{E}\left[1 - Z^{erasure}\right] = 1 - \mathbb{E}\left[Z^{erasure}\right] \Rightarrow$$

$$\Rightarrow \mathbb{E}\left[2 \cdot Z^{error} + Z^{erasure}\right] = 2\left(1 - \mathbb{E}\left[Z^{erasure}\right]\right) + \mathbb{E}\left[Z^{erasure}\right]$$

$$= 2 - \mathbb{E}\left[Z^{erasure}\right]$$

$\forall\ 2-\mathbb{E}[Z^{erasure}] = 2 - \frac{2}{d_{in}} \min\left(\frac{d_{in}}{2}, \Delta(y_i, w_i)\right)$ $\begin{cases} d_{in} \le \Delta(c_i, w_i) \le \\ \le \Delta(c_i, y_i) + \Delta(w_i, y_i) \end{cases}$

- $\min = \Delta(y_i, w_i) \Rightarrow 2 - \frac{2}{d_{in}} \Delta(y_i, w_i) \le 2\left(1 - \frac{d_{in} - e_i}{d_{in}}\right) = 2\left(1 - 1 + \frac{e_i}{d_{in}}\right) =$

$= \frac{2e_i}{d_{in}}.$

- $\min = \frac{d_{in}}{2}$; $e_i \geqslant \frac{d_{in}}{2}$ (иначе внутр. декодер сработал бы корректно)

$$\frac{d_{in}}{2} + e_i \geqslant d_{in}$$

$$\shortparallel$$

$$\min\{\} + e_i \geqslant d_{in} \Rightarrow \min\{\} \geqslant d_{in} - e_i \Rightarrow$$

$$2 - \frac{2}{d_{in}} \cdot \min\{\} \le 2 - \frac{2}{d_{in}} (d_{in} - e_i) = \frac{2e_i}{d_{in}}$$