Определения

Содержание слова

Содержание слова $w \in \Sigma^*$ - это $S(w) = \{a \in \Sigma \mid |w|_a > 0\}$

Централизатор

$Z(\rho) = \{e : \mathcal{M} \twoheadrightarrow \mathcal{M} \mid \rho \circ e = e \circ \rho\}$

Лемма 3

$\forall e \in Z(\rho) : \forall x \in \mathcal{M} : |e(x)| = |x|$

Доказательство

λ - пустое слово.

$$x\ \rho^{|x|}\ \lambda \to e(x)\ \rho^{|x|}\ e(\lambda),$$

Рис. 1: Иллюстрация к лемме 3

Если $e(x)\rho^{|x|-1}e(\lambda)$, то т.к $e^{-1} \in Z(\rho)$, то $x\rho^{|x|-1}\lambda$ - противоречие ($\bigotimes$).

так как $e \in Z(\rho)$ $|e(x)| \leq |e(\lambda)| + |x|$ - разность длин $e(x)$ и $e(\lambda)$ не более $|x|$.

Рис. 2: * Здесь должно быть равенство вместо $\leq$

$\Rightarrow |e(x)| \geq |x|$
$e(x)\rho^{|e(x)|}\lambda \Rightarrow$ подействуем e^{-1}:

$$x\rho^{|e(x)|}e^{-1}(\lambda)$$

Если бы $x\rho^{|e(x)|-1}e^{-1}(\lambda)$, то $e(x)\rho^{|e(x)|-1}\lambda$ - противоречие ($\bigotimes$).
Т.е $|x| = |e(x)| + |e^{-1}(\lambda)| \Rightarrow |x| \geq |e(x)|$
$\blacksquare$
Итак, $e \in Z(\rho) \Rightarrow \forall k\ e(\Sigma^k) = \Sigma^k$.

Пример 1

- Если удалить символ из x, а потом применить θ, то получим такой же результат, как если бы мы применили θ, а затем удалили символ из x $\Rightarrow$
$$\theta \circ \rho = \rho \circ \theta \Rightarrow \theta \in Z(\rho)$$

Пример 1

$$\Theta(x) = \overleftarrow{x}$$

$$\Theta(a_1, a_2, \ldots, a_t) = a_t, a_{t-1}, \ldots, a_2, a_1$$

Пример 2 (шифр простой замены)

$$\Pi \in S_\Sigma$$

$$\Pi(a_1 a_2 \ldots a_t) = \Pi(a_1)\Pi(a_2)\ldots\Pi(a_t)$$

Это ШПЗ - Шифр простой замены. Не распространяет искажений типа “пропуск”, то есть $\Pi \circ \rho = \rho \circ \Pi$. Рассмотрим $e \in Z(\rho)$.

Замечание

$(\theta \circ \Pi) \circ \rho = \rho \circ (\theta \circ \Pi)$ (по стабильности относительно $\subseteq$)

$\theta \circ \Pi \in Z(\rho)$

Пусть $e : \mathcal{M} \twoheadrightarrow \mathcal{M} : \forall k : e(\Sigma^k) = \Sigma^k$. Тогда:

$$e(\Sigma) = \Sigma \Rightarrow e : \Sigma \twoheadrightarrow \Sigma$$

Определим $\alpha : \mathcal{M} \twoheadrightarrow \mathcal{M}$:

$$\alpha(x_1, \cdots, x_k) = e(x_1)e(x_2)\cdots e(x_k)$$

* по сути задали шифр простой замены, индуцированный функцией e

e - биекция $\Rightarrow e^{-1}$ - биекция

$\alpha^{-1} \circ e : \mathcal{M} \twoheadrightarrow \mathcal{M}$

$((\alpha^{-1} \circ e)(x_1, \cdots, x_k)) = e(e^{-1}(x_1), e^{-1}(x_2), \cdots e^{-1}(x_k))$

$\forall x_i \in \Sigma : (\alpha^{-1} \circ e)(x_i) = x_i$

Лемма 4

Если $e \in Z(\rho)$, то $\forall x \in \mathcal{M} : S((\alpha^{-1} \circ e)(x)) = S(x)$

Доказательство

- $e \in Z(\rho)$
- $\alpha \in Z(\rho) \Rightarrow \alpha^{-1} \in Z(\rho)$
- $\Rightarrow \alpha^{-1} \circ e \in Z(\rho) \Rightarrow$ по лемме 3 сохраняет длину

$\measuredangle(\alpha^{-1} \circ e)(a_1, a_2, \cdots, a_k) = b_1 b_2 \cdots b_k$

$b_1 b_2 \cdots b_k \rho^{k-1} b_i (\forall i)$

$\Rightarrow \forall i : b_i \in S((\alpha^{-1} \circ e)(a_1 \cdots a_k))$

$\measuredangle(\alpha^{-1} \circ e)^{-1} \circ (\alpha^{-1} \circ e)(a_1, \cdots, a_k) = (a_1, \cdots, a_k)$
* т.к $(\alpha^{-1} \circ e)$ - тождественная функция на алфавите, то

$$(a_1, \cdots, a_k)\rho^{k-1}(\alpha^{-1} \circ e)(b_i) = b_i \Rightarrow (a_1, \cdots, a_k)\rho^{k-1}b_i$$

т.е $b_i \in S(a_1 \cdots a_k)$
Получаем, что $S((\alpha^{-1} \circ e)(a_1, \cdots, a_k)) \subseteq S(a_1 \cdots a_k)$
* в силу $(\alpha^{-1} \circ e)(a_1, a_2, \cdots, a_k) = b_1 b_2 \cdots b_k$
$(\alpha^{-1} \circ e)^{-1}(b_1 \cdots b_k) = a_1 \cdots a_k \rho^{k-1} a_i (\forall i)$
* т.к $(\alpha^{-1} \circ e)$ - тождественная функция на алфавите, то

$$(\alpha^{-1} \circ e) \circ (\alpha^{-1} \circ e)^{-1}(b_1 \cdots b_k)\rho^{k-1}(\alpha^{-1} \circ e)a_i(\forall i) = a_i$$

Получаем, что $S(a_1 \cdots a_k) \subseteq S((\alpha^{-1} \circ e)(a_1, \cdots, a_k))$
■

Теорема Глухова (Главная часть билета)

$e : \mathcal{M} \twoheadrightarrow \mathcal{M}$, $L \geq 3$ (т.е длина слов не менее 3)
Тогда:

$$e \in Z(\rho), \text{ т.е } \rho \circ e = e \circ \rho \Leftrightarrow e = \begin{cases} \Pi \text{ (из примера)} \\ \theta \circ \Pi = \Pi \circ \theta, \theta = \theta^{-1} \end{cases}$$

Доказательство ($\Leftarrow$)

Доказано, т.к проверили, что $\Pi, \theta, \Pi \circ \theta \in Z(\rho)$

Доказательство ($\Rightarrow$)

Берём $e \in Z(\rho)$. Пусть $\Pi = \alpha_e$.
Нужно показать, что:

- либо $e = \Pi \Rightarrow \Pi^{-1} \circ e = \epsilon$
- либо $e = \Pi \circ \sigma \Rightarrow \theta^{-1} \circ \Pi^{-1} \circ e = \epsilon$

$\measuredangle \Pi^{-1} \circ e$, действующая на Σ^2:
* в силу лемм 3 и 4, т.е отображение сохраняет длину и содержание

$$(\Pi^{-1} \circ e)(ab) = \begin{cases} ab \\ ba \end{cases}$$

- если получаем ab, то оставляем его
- если получаем ba, то применяем θ

Т.е можно выбрать $\varphi = \begin{cases} \text{либо } \Pi^{-1} \circ e \\ \text{либо } \theta \circ \Pi^{-1} \circ e \end{cases}$ так, чтобы $\varphi(ab) = ab$ для конкретных букв a и b.

Анализ действия на тройки букв

$\measuredangle \forall a, b, c \in \Sigma$:

1. $\Pi^{-1} \circ e(ab) = \begin{cases} \text{либо } ab \\ \text{либо } ba \end{cases}$
2. $\Pi^{-1} \circ e(ac) = \begin{cases} \text{либо } ac \\ \text{либо } ca \end{cases}$
3. $\Pi^{-1} \circ e(bc) = \begin{cases} \text{либо } bc \\ \text{либо } cb \end{cases}$

Возможны случаи:

1. Во всех 3 местах сохраняется порядок букв
2. Во всех 3 местах инвертируется порядок букв
3. В 2 местах сохраняется порядок, в одном - инвертируется
4. В 2 местах инвертируется порядок, в одном - сохраняется

Допустим, что мы находимся в случае 3 или 4.
Без ограничения общности считаем:

- $\Pi^{-1} \circ e(ab) = ab \Rightarrow \Pi^{-1} \circ e(ba) = ba$
- $\Pi^{-1} \circ e(bc) = bc \Rightarrow \Pi^{-1} \circ e(cb) = cb$
- $\Pi^{-1} \circ e(ac) = ca \Rightarrow \Pi^{-1} \circ e(ca) = ac$

Теперь подействуем $\Pi^{-1} \circ e$ на abc:

$$\Pi^{-1} \circ e(abc) = w, \text{ где } S(w) = \{a, b, c\}, |w| = 3$$

Т.к $\Pi^{-1} \circ e \in Z(\rho)$ и $abc\rho ab \Rightarrow w\rho(\Pi^{-1} \circ e)(ab) = ab \Rightarrow$ **a стоит до b в слове w**

Аналогично:

- $abc\rho bc \Rightarrow w\rho bc \Rightarrow$ **b стоит до c в слове w**
- $abc\rho ac \Rightarrow w\rho ca \Rightarrow$ **c стоит до a в слове w**

Приходим к противоречию ($\bigotimes$).
$\Rightarrow$ **Не может быть случаев 3 и 4**
$\Rightarrow$ **Значит это либо случай 1, либо 2**

Т.е $\forall a, b, c \in \Sigma$ можно выбрать $\varphi_{\{a,b,c\}} = \begin{cases} \text{либо } \Pi^{-1} \circ e \\ \text{либо } \theta \circ \Pi^{-1} \circ e \end{cases}$ так, что $\varphi_{\{a,b,c\}}(x, y) = xy$ ($\forall x, y \in \{a, b, c\}$), т.е ($\varphi_{\{a,b,c\}}|_{\{a,b,c\}} = \epsilon$).

Индукция по алфавиту

Возьмем $a_1, a_2, a_3, a_4 \in \Sigma$ и составим:

- $\varphi_{\{a_1,a_2,a_3\}}$
- $\varphi_{\{a_1,a_2,a_4\}}$

Покажем, что они одинаковые:

$\varphi_{\{a_1,a_2,a_3\}}$ и $\varphi_{\{a_1,a_2,a_4\}}$ действуют тождественно на $a_1 a_2 \Rightarrow$ они совпадают.

Заметим, что $\{a_1, a_2, a_3, a_4\}^2 \subseteq \{a_1, a_2, a_3\}^2 \cup \{a_1, a_2, a_4\}^2$.

Теперь проведем индукцию по k:

- База: для $k = 3$ доказано
- Шаг: предположим верно для k, докажем для $k + 1$

Переход к словам большей длины

Воспользуемся определением множества $\mathrm{sub}(w)$ и предложением:

Определение множества sub(w)

Для $w \in \Sigma^*$: $\mathrm{sub}(w) = \{v \in \Sigma^* \mid w\rho v\} \setminus \{w\}$

Предложение

Предположение(о Sub): $\quad |\mathrm{w}| \geq 3$

$$\mathrm{Sub(w)} = \mathrm{Sub(v)} \Rightarrow w = v$$

Проведем индукцию по k, чтобы показать, что $\varphi|_{\Sigma^k} = \epsilon$.

$\measuredangle w \in \Sigma^{k+1}$. Покажем, что $\varphi(w) = w$.

$\measuredangle \mathrm{sub}(w) \subseteq \Sigma^k$.

$|x| = k$, $x \in \mathrm{sub}(w) \Leftrightarrow w\rho x \Leftrightarrow$ (т.к $\varphi \in Z(\rho)$) $\varphi(w)\rho\varphi(x) = x$ (по П.И.)

Получаем, что $\varphi(w)\rho x \Leftrightarrow x \in \mathrm{sub}(\varphi(w))$

Т.е $\mathrm{sub}(w) = \mathrm{sub}(\varphi(w)) \Rightarrow$ (по предложению, т.к $k + 1 \geq 3$) $\varphi(w) = w$

$\blacksquare$

Вывод

Если хотим обеспечить нераспространение искажений, то придётся ограничиваться слабыми шифрами перестановки и многоалфавитной замены. Т.е можно вообще забить на это всё.