

## 1 Определения

**Определение 1** (Искажение типа "Пропуск"). Бинарное отношение  $\alpha : \mathcal{M} \times \mathcal{M}$  называется искажением типа "Пропуск", если:

$$(u, v) \in \alpha \Leftrightarrow v \text{ получено из } u \text{ вычеркиванием одной буквы}$$

Определим также бинарное отношение  $\rho : \mathcal{M} \times \mathcal{M}$ :

$$(u, v) \in \rho \Leftrightarrow \begin{cases} \text{либо } (u, v) \in \alpha \\ \text{либо } u = v \end{cases}$$

**Определение 2** (Шифр, не распространяющий искажений). Шифр  $(\mathcal{M}, E)$  не распространяет искажений типа "пропуск", если:

$$\forall e \in E, \forall \vec{x}, \vec{y} \in \mathcal{M}, \forall k \leq |\vec{x}| : \vec{x} \rho^k \vec{y} \Rightarrow e(x) \rho^k e(y)$$

- $e$  - биекция  $\mathcal{M} \rightarrow \mathcal{M}$  (функция шифрования/расшифрования)
- $\vec{x}, \vec{y}$  - криптограммы (настоящая и испорченная)
- Если при передаче пропало не более  $k$  букв, то после расшифрования пропадёт тоже не более  $k$  букв

## 2 Леммы

**Лемма 1.** Для любого отображения  $e : \mathcal{M} \rightarrow \mathcal{M}$  и бинарного отношения  $\rho \subseteq \mathcal{M} \times \mathcal{M}$ :

$$\forall x, y : x \rho y \Rightarrow e(x) \rho e(y) \Leftrightarrow (\rho \circ e \subseteq e \circ \rho)$$

*Доказательство.* ( $\Rightarrow$ ) Пусть  $(x, y) \in \rho \circ e$ . Тогда:

- $\exists z : (x \rho z) \text{ и } (zeu)$
- Из  $(x \rho z) \Rightarrow e(x) \rho e(z)$
- Из  $(zeu) \Rightarrow y = e(z)$  (так как  $e$  - функция)

Следовательно,  $(e(x), y) \in \rho$  и  $(x, e(x)) \in e$ , поэтому  $(x, y) \in e \circ \rho$ .

■ □

*Доказательство.* ( $\Leftarrow$ )  $x \rho y \rightarrow x \rho y e e(y) \rightarrow x (\rho \circ e) e(y) \rightarrow x (e \circ \rho) e(y) \rightarrow \exists z, x e z, z \rho e(y) \Rightarrow e(x) \rho e(y)$  ■ □

**Определение 3** (Стабильность). Отношение  $\alpha$  стабильно относительно операции  $\star$ , если:

$$\forall (x, y) \in \alpha \Rightarrow \begin{cases} (x \star z, y \star z) \in \alpha \\ (z \star x, z \star y) \in \alpha \end{cases}$$

где  $\alpha$  - рефлексивное, транзитивное бинарное отношение.

*Доказательство свойства стабильности.* Пусть  $\alpha \subseteq \beta$  и  $\gamma$  - отношения.

Покажем  $\alpha \circ \gamma \subseteq \beta \circ \gamma$ :

Если  $(x, y) \in \alpha \circ \gamma$ , то  $\exists z$  :

- $(x, z) \in \alpha \Rightarrow (x, z) \in \beta$
- $(z, y) \in \gamma$

Следовательно,  $(x, y) \in \beta \circ \gamma$ .

Аналогично доказывается левая стабильность.

■ □

**Замечание 1.** Следующие условия эквивалентны:

1.  $\forall e \in E, \forall \vec{x}, \vec{y} \in \mathcal{M}, \forall k \leq |\vec{x}| : \vec{x} \rho^k \vec{y} \Rightarrow e(x) \rho^k e(y)$
2.  $\forall x, y : x \rho y \rightarrow e(x) \rho e(y)$

*Доказательство.*  $(\Rightarrow)$  Очевидно.

■ □

*Доказательство.*  $(\Leftarrow)$  По лемме 1:

$$\forall x, y : x \rho y \rightarrow e(x) \rho e(y) \Leftrightarrow \rho \circ e \subseteq e \circ \rho$$

Покажем по индукции, что  $\forall k \leq |x| : \rho^k \circ e \subseteq e \circ \rho^k$ :

- База ( $k = 1$ ): следует из леммы
- Шаг:  $\rho^{k+1} \circ e = (\rho \circ \rho^k) \circ e = \rho \circ (\rho^k \circ e) \subseteq \rho \circ (e \circ \rho^k) = (\rho \circ e) \circ \rho^k \subseteq (e \circ \rho) \circ \rho^k = e \circ \rho^{k+1}$

■ □

**Определение 4** (Централизатор).

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

называется централизатором отношения  $\rho$ .

**Лемма 2**  $Z(\rho) = \{e : \mathcal{M} \rightarrow \mathcal{M} \mid \rho \circ e \subseteq e \circ \rho\}$  - централизатор.  $Z(\rho) \leq S_{\mathcal{M}}$  - группа всех биекций на множестве (с операцией суперпозиции  $\circ$ )

*Устойчивость операций.* Пусть  $e, f \in Z(\rho)$ . Покажем:

1.  $e \circ f \in Z(\rho)$
  2.  $e^{-1} \in Z(\rho)$
- 1)  $\rho \circ (e \circ f) = (\rho \circ e) \circ f \subseteq (e \circ \rho) \circ f = e \circ (\rho \circ f) \subseteq e \circ (f \circ \rho) = (e \circ f) \circ \rho$   
 2) Так как  $|\mathcal{M}| < \infty$ , то  $e^{-1} = e^{k-1}$  для некоторого  $k$ . Поскольку  $Z(\rho)$  замкнуто относительно композиции,  $e^{-1} \in Z(\rho)$ .

■ □

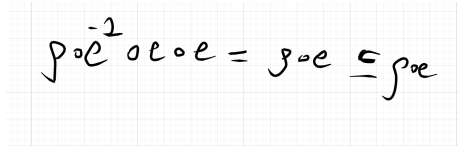
**Следствие 1.**

$$\forall x, y \in \mathcal{M} : (x\rho y) \rightarrow e(x)\rho e(y) \Leftrightarrow e \circ \rho = \rho \circ e$$

*Доказательство.* ( $\Leftarrow$ ) Следует из леммы 1.

( $\Rightarrow$ ) Из леммы 1:  $\rho \circ e \subseteq e \circ \rho$ . Так как  $e \in Z(\rho)$ , то  $e^{-1} \in Z(\rho)$ , следовательно:

$$\rho \circ e^{-1} \subseteq e^{-1} \circ \rho \Rightarrow e \circ \rho \subseteq \rho \circ e$$


$$\rho \circ e^{-1} \circ e \circ e = \rho \circ e \subseteq \rho \circ e$$

Таким образом,  $Z(\rho) = \{e : \mathcal{M} \rightarrow \mathcal{M} \mid \rho \circ e = e \circ \rho\}$ .

■ □