1 Основные определения

Определение 1. *Отображение* $e : X \to X$ *называется* изометрией *относительно метрики* ρ *на* X*, если*

$$\forall a, b \in X : \rho(e(a), e(b)) = \rho(a, b)$$

- *Любая инъективная функция на конечном множестве является биекцией, следовательно изометрия на конечном множестве — это биекция.*

2 Важные примеры изометрий на Σ^r относительно расстояния Хэмминга

Пример 1 (Шифр перестановки)**.** *Для перестановки* $\sigma \in S_r$ *определим:*

$$\sigma(a_1, \cdots, a_r) = (a_{\sigma(1)}, \cdots, a_{\sigma(r)})$$

- σ *— перестановка длины* r
- *В качестве ключа выступает* σ
- σ *— изометрия, которая не распространяет искажений типа "замена"*
- *Для расшифровки применяем обратную перестановку*

Пример 2 (Шифр многоалфавитной замены)**.** *Пусть* $\tau = (\tau_1, \tau_2, \cdots, \tau_r) \in (S_\Sigma)^r$*, тогда:*

$$\tau(a_1, \cdots, a_r) = (\tau_1(a_1), \cdots, \tau_r(a_r))$$

- *Это шифр многоалфавитной замены (ШМЗ)*
- *Для расшифровки применяем к каждой букве свою обратную перестановку*
- *Это изометрия*

3 Теорема Маркова

Теорема 1. *Отображение* e *является изометрией* Σ^r *тогда и только тогда, когда существуют* σ *и* τ *из примеров 1 и 2 такие, что* $e = \sigma \circ \tau$*.*

То есть e *— это суперпозиция перестановки и многоалфавитной замены.*

Доказательство (⇐). Поскольку τ и σ — изометрии, их композиция также является изометрией:

$$\rho(e(x), e(y)) = \rho(\tau(\sigma(x)), \tau(\sigma(y))) = \rho(\sigma(x), \sigma(y)) = \rho(x, y)$$

Первое равенство: по определению композиции.
Второе: поскольку τ сохраняет расстояния.
Третье: поскольку σ сохраняет расстояния.
■ □

Доказательство (⇒). Рассмотрим произвольный вектор $\vec{a} = (a_1, \ldots, a_r) \in \Sigma^r$.

Определим множество:

$$\vec{a_i} = \{(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_r) \mid b \in \Sigma\}$$

Пусть $e(\vec{a}) = \vec{c}$.

3.1 Шаг 1

Покажем, что существует $j \in \{1, \ldots, r\}$ такое, что $e(\vec{a_j}) = \vec{c_j}$.

Предположим противное: существует $\vec{d} \in e(\vec{a_j}) \setminus \{\vec{c}\}$. Тогда найдется $\vec{b} \in \vec{a_j}$ такое, что $\vec{d} = e(\vec{b})$.

Имеем:

$$\rho(\vec{d}, \vec{c}) = \rho(e(\vec{b}), e(\vec{a})) = \rho(\vec{b}, \vec{a}) = 1$$

(Если бы $\rho(\vec{b}, \vec{a}) = 0$, то $\vec{d} = \vec{c}$ — противоречие.)

Следовательно, $\vec{d} \in \vec{c_j}$ для некоторого j. Покажем, что этот индекс j один и тот же для всех $\vec{d}$.

Возьмем $\vec{d_1} \neq \vec{d_2} \in e(\vec{a_j})$. Существуют $\vec{b_1}, \vec{b_2} \in \vec{a_j}$ такие, что:

$$\rho(\vec{d_1}, \vec{d_2}) = \rho(\vec{b_1}, \vec{b_2}) = 1$$

(если бы $\rho(\vec{b_1}, \vec{b_2}) = 0$, то $\vec{d_1} = \vec{d_2}$).

Значит, индекс j должен быть одинаков для $\vec{d_1}$ и $\vec{d_2}$, иначе $\rho(\vec{d_1}, \vec{d_2}) > 1$.

Таким образом, $e(\vec{a_j}) \subseteq \vec{c_j}$. Поскольку e инъективна и мощности множеств равны ($|\Sigma|$), получаем равенство:

$$e(\vec{a_j}) = \vec{c_j}$$

3.2 Шаг 2

Определим окрестность слова $\vec{x}$ радиуса t:

$$O_t(\vec{x}) = \{\vec{y} \in \Sigma^r \mid \rho(\vec{x}, \vec{y}) \leq t\}$$

Из шага 1 следует, что e переводит единичную окрестность $\vec{a}$ в единичную окрестность $\vec{c}$.

Существуют $\tau = (\tau_1, \ldots, \tau_r) \in (S_\Sigma)^r$ и $\sigma \in S_r$ такие, что для всех $\vec{x} \in O_1(\vec{a})$:

$$e(\vec{x}) = (\tau_1(a_{\sigma(1)}), \ldots, \tau_r(a_{\sigma(r)})) = (\sigma \circ \tau)(\vec{a})$$

где $\sigma(j) = i$.

Определим $\varphi = e \circ \tau^{-1} \circ \sigma^{-1}$. На $O_1(\vec{a})$ имеем $\varphi = \epsilon$ (тождественное отображение).

Докажем по индукции по t, что $\varphi = \epsilon$ на $O_t(\vec{a})$.

3.2.1 База индукции ($t = 1$)

Уже доказано.

3.2.2 Шаг индукции

Пусть $\vec{x} \in O_t(\vec{a})$. Если $\rho(\vec{x}, \vec{a}) < t$, применяем предположение индукции.

Рассмотрим случай $\rho(\vec{x}, \vec{a}) = t \geq 2$. Выберем $\vec{y}$ такое, что $\rho(\vec{y}, \vec{a}) = t - 2$ и $\rho(\vec{y}, \vec{x}) = 2$.

Рассмотрим пересечение окрестностей:

$$O_1(\vec{x}) \cap O_1(\vec{y}) = \{\vec{u}, \vec{v}\}$$

где:

$$\vec{u} = (x_1, \ldots, x_\alpha, \ldots, y_\beta, \ldots, x_r)$$
$$\vec{v} = (y_1, \ldots, y_\alpha, \ldots, x_\beta, \ldots, y_r)$$

По неравенству треугольника:

$$\rho(\vec{u}, \vec{a}) \leq \rho(\vec{u}, \vec{y}) + \rho(\vec{y}, \vec{a}) \leq 1 + (t - 2) = t - 1$$

Аналогично для $\vec{v}$.

По предположению индукции:

$$\varphi(\vec{u}) = \vec{u}, \quad \varphi(\vec{v}) = \vec{v}, \quad \varphi(\vec{y}) = \vec{y}$$

Поскольку φ — изометрия:

$$\rho(\varphi(\vec{x}), \vec{u}) = \rho(\vec{x}, \vec{u}) = 1$$

$$\rho(\varphi(\vec{x}), \vec{v}) = \rho(\vec{x}, \vec{v}) = 1$$

Следовательно:

$$\varphi(\vec{x}) \in O_1(\vec{u}) \cap O_1(\vec{v}) = \{\vec{x}, \vec{y}\}$$

Но $\varphi(\vec{x}) \neq \varphi(\vec{y})$, так как $\vec{x} \neq \vec{y}$. Значит, $\varphi(\vec{x}) = \vec{x}$.

Таким образом, $\varphi = \epsilon$ на всем Σ^r, откуда:

$$e = \sigma \circ \tau$$

■ □