Б. А. Погорелов, М. А. Пудовкина, Натуральные метрики и их свойства. Ч. 2. Метрики типа Хемминга,
Матем. вопр. криптогр., 2012, том 3, выпуск 1, 71–95

https://www.mathnet.ru/mvk49

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2012 Т. 3 № 1 С. 71–95

УДК 519.719.1

Натуральные метрики и их свойства. Ч. 2. Метрики типа Хемминга

Б. А. Погорелов[1)], М. А. Пудовкина[2)]

[1)] Академия криптографии Российской Федерации, Москва
[2)] Национальный исследовательский ядерный университет (МИФИ), Москва

Получено 22.IV.2010

Описываются «ближайшие» к метрике Хемминга натуральные надметрики и подметрики, строятся ее аналоги. Рассматриваются натуральные метрики на векторных пространствах, группа изометрий которых содержит группу сдвигов. С помощью $(n+1)$-значных подметрик 2^n-значных надметрик метрики Хемминга строится класс кодов, эквивалентных коду с метрикой Хемминга относительно линейной группы.

Ключевые слова: дискретные пространства, метрика Хемминга, подметрики, надметрики

Natural metrics and their properties. P.2. Hamming-type metrics

B. A. Pogorelov[1)], M. A. Pudovkina[2)]

[1)] *Academy of Cryptography of Russian Federation, Moscow*
[2)] *National Nuclear Research University, Moscow*

Abstract. Natutal overmetrics and submetrics «nearest» to the Hamming metrics are described, analogues of the Hamming metrics are constructed. Natural metrics on the vector spaces with isometry group containing the shift group are considered. By means of $(n + 1)$-valued submetrics of 2^n-valued overmetrics of the Hamming metrics a class of codes which are equivalent to a code with the Hamming metrics relatively to the linear group.

Key words: discrete spaces, Hamming metrics, submetrics, overmetrics

Citation: *Mathematical Aspects of Cryptography*, 2012, vol. 3, no. 1, pp. 71–95 (Russian).

Первая часть работы (см. [5]) была посвящена описанию общих свойств конечных целочисленных метрик. Введены понятия натуральной метрики (т. е. метрики с множеством значений $0,1,...,d$) и ее обобщения — канонической метрики, приведены их свойства.

В этой части работы рассматривается одна из наиболее часто встречающихся в приложениях метрик — метрика Хемминга. Описываются «ближайшие» к ней натуральные надметрики и подметрики. Путем последовательного перехода к подметрикам и надметрикам строятся аналоги метрики Хемминга. Полученные метрики позволяют «разложить» определенные классы булевых функций (например, аффинные, бент-функции) на подклассы функций, находящихся на фиксированном множестве «хеммингових» расстояний относительно данного класса. Рассматриваются натуральные метрики на векторных пространствах, группа изометрий которых содержит группу сдвигов. Их частным случаем являются метрики Хемминга. Описываются все максимальные метрики множества M_n^+, являющиеся надметриками метрики Хемминга. В последнем параграфе с помощью $(n+1)$-значных подметрик 2^n-значных надметрик метрики Хемминга строится класс кодов, эквивалентных исходному коду с метрикой Хемминга относительно линейной группы.

Обозначения:

- $\mathbb{N}$ ($\mathbb{N}_0$) — множество всех натуральных чисел (соответственно, целых неотрицательных);
- $\mathbb{R}$ — множество всех действительных чисел;
- χ_t — метрика Хемминга на t-мерном векторном пространстве $V_t = V_t(2)$ над полем $GF(2)$ (t определяется контекстом);
- $\varepsilon_{j,t} = (0,...,0,\underset{j}{1},0,...,0)$, $\varepsilon_{j,t} \in V_t$, $j \in \{1,...,t\}$;
- $(A_1,...,A_m)$ — разбиение множества A на непустые множества $A_1,...,A_m$;
- $I = \{(x,x) \mid x \in X\}$;
- Δ_t — множество всех векторов из V_n веса Хемминга $t \in \{0,...,n\}$;
- $\mathrm{Isom}\,\mu$ — группа изометрий метрики μ;
- F_n — множество всех двоичных функций от n переменных;
- AF_m — множество всех аффинных функций из множества F_m;
- $\overline{\mathbf{X}}^{(2)}$ — множество всех разбиений множества $(X \times X) \setminus \{(\alpha,\alpha) \mid \alpha \in X\}$ на симметричные подмножества множества $X \times X$;
- $\mu^{i\uparrow}$ – $(d+1+i)$-значная надметрика $(d+1)$-значной метрики μ;

- $\mu_j^{i\uparrow}$ – j-я $(d+1+i)$-значная надметрика метрики μ;
- $\mu^{i\downarrow}$ – $(d+1-i)$-значная подметрика метрики μ;
- $\mu_j^{i\downarrow}$ – j-я $(d+1-i)$-значная подметрика метрики μ;
- $\mu^{\uparrow} = \mu^{1\uparrow}$, $\mu^{\downarrow} = \mu^{1\downarrow}$;
- $A + B = \{\alpha + \beta \mid \alpha \in A, \beta \in B\}$, $A, B \subset V_n$.

Если размерность t пространства V_t понятна из контекста, то у метрики χ_t и вектора $\varepsilon_{j,t}$ символ «t» будем опускать.

При задании метрики будем опускать всегда выполняющееся условие $\mu(\alpha,\alpha) = 0$.

Напомним понятия надметрики и подметрики метрики (см., [5]). Пусть μ — конечная целочисленная метрика на множестве X. Метрика $\rho_\mu : X \times X \to \mathbb{N}_0$, удовлетворяющая для любых $\alpha, \beta, \gamma, \delta \in X$ условиям:

1) если $\mu(\alpha,\beta) = \mu(\gamma,\delta)$, то $\rho_\mu(\alpha,\beta) = \rho_\mu(\gamma,\delta)$;

2) $\rho_\mu(\alpha,\beta) \le \mu(\alpha,\beta)$;

называется *подметрикой* метрики μ.

Метрика $\rho_\mu : X \times X \to \mathbb{N}_0$ называется *надметрикой* метрики μ, если для любых $\alpha, \beta, \gamma, \delta \in X$ она удовлетворяет условиям:

1) если $\rho_\mu(\alpha,\beta) = \rho_\mu(\gamma,\delta)$, то $\mu(\alpha,\beta) = \mu(\gamma,\delta)$;

2) $\mu(\alpha,\beta) \le \rho_\mu(\alpha,\beta)$.

Очевидно, что метрика μ является подметрикой своей надметрики ρ_μ.

§ 5. Надметрики метрики Хемминга

Опишем $(n+2)$-значные надметрики метрики Хемминга χ на V_n.

Утверждение 5.1. *Пусть* $n \ge 2$. *Тогда* $(n+2)$*-значные натуральные надметрики метрики Хемминга* χ *на* V_n *исчерпываются следующим списком*:

$$\chi_r^{\uparrow}(\alpha,\alpha') = \begin{cases} 1, & \text{если } \alpha + \alpha' = \varepsilon_r, \\ 2, & \text{если } \alpha + \alpha' \in \Delta_1 \setminus \{\varepsilon_r\}, \\ t, & \text{если } \alpha + \alpha' \in \Delta_{t-1}, t \ge 3, \end{cases} \qquad r \in \{1,\dots,n\}.$$

При этом $\mathrm{Isom}\chi_r^{\uparrow} = S_2 \uparrow G < S_2 \uparrow S_n$, $G \cong S_{n-1}$.

Доказательство. Для произвольных чисел $i \in \{1,...,n\}$, $j \in \{i+1,...,n+1\}$ и разбиений $\Delta_i = \Delta_i' \cup \Delta_i''$ рассмотрим функцию $\rho_{\Delta_i'}^{(i,j)} : V_n \to \{1,...,n+1\}$:

$$\rho_{\Delta_i'}^{(i,j)}(\alpha,\alpha') = \begin{cases} t, \text{ если } \alpha+\alpha' \in \Delta_t,\ t \in \{1,...,j-1\} \setminus \{i\}, \\ i, \text{ если } \alpha+\alpha' \in \Delta_i', \\ j, \text{ если } \alpha+\alpha' \in \Delta_i'', \\ t, \text{ если } \alpha+\alpha' \in \Delta_{t-1},\ t \in \{j+1,...,n+1\}. \end{cases}$$

Из определения надметрики (см. [5]) следует, что в случае существования она имеет вид $\rho_{\Delta_i'}^{(i,j)}$.

Согласно утверждению 4.2 работы [5], для надметрики $\rho_{\Delta_i'}^{(i,j)}$ метрики χ при $i>1$ должны выполняться соотношения

$$\Delta_i' = \left(\bigcup_{t=1}^{i-1}(\Delta_t + \Delta_{i-t})\right) \setminus \left(\bigcup_{t=0}^{i-1}\Delta_t\right).$$

Однако $\Delta_i' \subset \Delta_i$ и для любого $i>1$ имеет место равенство

$$\Delta_i = \left(\bigcup_{t=1}^{i-1}(\Delta_t + \Delta_{i-t})\right) \setminus \left(\bigcup_{t=0}^{i-1}\Delta_t\right).$$

Поэтому при любых $i>1$, $j \in \{i+1,...,n+1\}$ функция $\rho_{\Delta_i'}^{(i,j)}$ не является метрикой.

Пусть $i=1$. Если $j>2$ и $\rho_{\Delta_1'}^{(1,j)}$ — надметрика, то по утверждению 4.2

$$(\Delta_1' + \Delta_{j-1}) \setminus \left(\bigcup_{c=0}^{j-1}\Delta_c \setminus \Delta_1'\right) \subset \Delta_1'' \subset \Delta_1.$$

Это невозможно, так как в множестве $(\Delta_1' + \Delta_{j-1}) \setminus \left(\bigcup_{c=0}^{j-1}\Delta_c \setminus \Delta_1'\right)$ существует вектор веса j. Значит, функция $\rho_{\Delta_1'}^{(1,j)}$ не является метрикой.

Пусть $(i,j)=(1,2)$, $|\Delta_1'| \geq 2$ и $\varepsilon_c, \varepsilon_t \in \Delta_1'$ для некоторых c, $t \in \{1,...,n\}$, $c \neq t$. Если $\rho_{\Delta_1'}^{(1,j)}$ — надметрика, то опять из утверждения 4.2 работы [5] получаем, что

$$(\Delta_1' + \Delta_1') \setminus (\Delta_0 \cup \Delta_1') \subseteq \Delta_1'',$$

но $\varepsilon_c + \varepsilon_t \in (\Delta_1' + \Delta_1') \setminus (\Delta_0 \cup \Delta_1')$ и $\varepsilon_c + \varepsilon_t \in \Delta_2$. Таким образом, если $|\Delta_1'| \geq 2$, то $\rho_{\Delta_1'}^{(1,2)}$ не является надметрикой.

Покажем, если $(i,j) = (1,2)$ и $|\Delta_1'| = 1$, то $\rho_{\Delta_1'}^{(1,2)}$ — надметрика. Очевидно, если $t \geq c$ и $A \subseteq \Delta_c$, $B \subseteq \Delta_{t-c}$, то $A + B \subseteq \bigcup_{c=0}^{t} \Delta_c$. Из утверждения 4.2 работы [5] и соотношений

$$(\Delta_1' + \Delta_1') \setminus (\Delta_0 \cup \Delta_1') = \varnothing,$$

$$(\Delta_1' + \Delta_1'') \subset \Delta_2 \cup \Delta_1 \cup \Delta_0,$$

$$(\Delta_1' + \Delta_2) \cup (\Delta_1'' + \Delta_1'') \subset \Delta_3 \cup \Delta_2 \cup \Delta_1 \cup \Delta_0,$$

$$(\Delta_1' + \Delta_{t-1}) \cup (\Delta_1'' + \Delta_{t-2}) \cup \bigcup_{c=2}^{t} (\Delta_c + \Delta_{t-c-2}) \subseteq \bigcup_{c=0}^{t} \Delta_c, \quad 4 \leq t \leq n+1,$$

следует, что $\rho_{\Delta_1'}^{(1,2)} = \chi_r^{\uparrow}$ — надметрика.

Таким образом, группа $\mathrm{Isom}\chi_r^{\uparrow}$ является подгруппой в $S_2 \uparrow S_n =$ $= \mathrm{Isom}\chi$, группа $\mathrm{Isom}\left(\chi_r^{\uparrow}\right)_{\bar{0}}$ стабилизирует вектор ε_r и $\mathrm{Isom}\chi_r^{\uparrow} = S_2 \uparrow S_{n-1}$. Утверждение доказано.

Из утверждения 5.1 следует, что число $(n+2)$-значных надметрик метрики χ равно n.

Опишем $(n+1)$-значные подметрики $(n+2)$-значной надметрики метрики Хемминга χ (обозначим их множество через $\left\{\chi^{\uparrow\downarrow}\right\}$).

Утверждение 5.2. *Пусть* $n \geq 2$, $r \in \{1,\ldots,n\}$ *и* $(n+2)$*-значная надметрика* $\chi_r^{\uparrow}$ *метрики Хемминга задана условиями*

$$\chi_r^{\uparrow}(\alpha,\alpha') = \begin{cases} 1, \text{ если } \alpha + \alpha' = \varepsilon_r, \\ 2, \text{ если } \alpha + \alpha' \in \Delta_1 \setminus \{\varepsilon_r\}, \\ t, \text{ если } \alpha + \alpha' \in \Delta_{t-1},\ t \geq 3. \end{cases}$$

Тогда $(n+1)$*-значные подметрики метрики* $\chi_r^{\uparrow}$ *для* $i \in \{1,...,n-1\}$ *исчерпываются следующим списком*:

$$\chi_{r,i}^{\uparrow\downarrow}(\alpha,\alpha') = \begin{cases} \chi(\alpha,\alpha'), & \text{если } \alpha+\alpha' \in \Delta_t,\ t > i, \\ \chi(\alpha,\alpha'), & \text{если } \alpha+\alpha' \in \Delta_1,\ i = 1, \\ i, & \text{если } \alpha+\alpha' \in \Delta_{i-1} \cup \Delta_i,\ i \geq 3, \\ 2, & \text{если } \alpha+\alpha' \in \Delta_2 \cup (\Delta_1 \setminus \{\varepsilon_r\}),\ i = 2, \\ \chi_r^{\uparrow}(\alpha,\alpha'), & \text{если } \alpha+\alpha' \in \Delta_t,\ t < i. \end{cases}$$

Доказательство аналогично доказательству утверждения 5.1.

Из утверждения 5.2 следует, что число $(n+1)$-значных подметрик $(n+2)$-значных надметрик метрики Хемминга равно $(n-1)n$, причем все они попарно изоморфны. Отметим также, что $\chi_{r,1}^{\uparrow\downarrow} = \chi_n$ для всех $r \in \{1,...,n\}$.

Утверждение 5.3. *Пусть* $t \in \{2,...,n-1\}$, $\Theta_c = \{(\alpha_1,...,\alpha_n) \in \Delta_c \mid \alpha_r = 1\}$, $c,r \in \{1,...,n\}$. *Тогда функция* $\chi_r^{t\uparrow} : V_n \times V_n \to \{1,...,n+t\}$, *заданная условиями*

$$\chi_r^{t\uparrow}(\alpha,\alpha') = \begin{cases} 1, & \text{если } \alpha+\alpha' = \varepsilon_r, \\ 2, & \text{если } \alpha+\alpha' \in \Delta_1 \setminus \{\varepsilon_r\}, \\ 2c-1, & \text{если } \alpha+\alpha' \in \Theta_c,\ 2 \leq c \leq t, \\ 2c, & \text{если } \alpha+\alpha' \in \Delta_c \setminus \Theta_c,\ 2 \leq c \leq t, \\ t+c, & \text{если } \alpha+\alpha' \in \Delta_c, c > t, \end{cases}$$

является $(n+t+1)$*-значной надметрикой метрики Хемминга и* $\mathrm{Isom}\chi_r^{t\uparrow} = S_2 \uparrow G < S_2 \uparrow S_n,\ G \cong S_{n-1}$.

Доказательство. Обозначим $\bar{\Theta}_c = \Delta_c \setminus \Theta_c = \{(\alpha_1,...,\alpha_n) \in \Delta_c \mid \alpha_r = 0\}$, $A_c = \left\{\alpha \in V_n \mid \chi_r^{t\uparrow}(\alpha,\vec{0}) = c\right\}$, $c \in \{0,...,t\}$.

Из утверждения 4.2 работы [5] следует, что $\chi_r^{t\uparrow}$ — надметрика, если для каждого $b \in \{1,...,t\}$ справедливы включения

$$\bigcup_{i=1}^{b-1} (A_i + A_{b-i}) \subseteq \bigcup_{i=0}^{b} A_i. \qquad (5.1)$$

Соотношения

$$A_{2j+1} + A_{2i+1-2j-1} = \Theta_{j+1} + \overline{\Theta}_{i-j} \subseteq \bigcup_{l=1}^{i+1} \Theta_l \subset \bigcup_{i=0}^{2i+1} A_i,$$

$$A_{2j+2} + A_{2i+1-2j-2} = \overline{\Theta}_{j+1} + \Theta_{i-j} \subseteq \bigcup_{l=1}^{i+1} \Theta_l \subset \bigcup_{i=0}^{2i+1} A_i,$$

$$A_{2j+1} + A_{2i+2-2j-1} = \Theta_{j+1} + \Theta_{i-j+1} \subseteq \bigcup_{l=1}^{i} \overline{\Theta}_l \subset \bigcup_{i=0}^{2i+2} A_i,$$

$$A_{2j+2} + A_{2i+2-2j-2} = \overline{\Theta}_{j+1} + \overline{\Theta}_{i-j} \subseteq \bigcup_{l=1}^{i+1} \overline{\Theta}_l \subset \bigcup_{i=0}^{2i+2} A_i$$

выполняются для любых $i \in \{1,...,t-1\}$, $j \in \{0,...,i-1\}$. Из них следует справедливость соотношений (5.1) для любого $b \le 2t$.

Пусть $b > 2t$. Положим $c = b - t$. Для $j \in \{0,...,\lceil (b-1)/2 \rceil\}$ выполняются включения

$$A_j + A_{t+c-j} \subseteq \begin{cases} \Delta_{\lceil j/2 \rceil} + \Delta_{c-j} \subseteq \bigcup_{i=0}^{c-j+\lceil j/2 \rceil} \Delta_i, & \text{если } j \le \min\{c-t, 2t\}, \\ \Delta_{\lceil j/2 \rceil} + \Delta_{\lceil (t+c-j)/2 \rceil} \subseteq \bigcup_{i=0}^{\lceil (t+c-j)/2 \rceil + \lceil j/2 \rceil} \Delta_i, & \text{если } c-t \le j \le 2t, \\ \Delta_{j-t} + \Delta_{c-j} \subseteq \bigcup_{i=0}^{c-t} \Delta_i, & \text{если } 2t < j < c-t. \end{cases}$$

Таким образом,

$$A_j + A_{t+b-j} \subseteq \bigcup_{i=0}^{b} \Delta_i.$$

Значит, $\chi_r^{t\uparrow}$ — надметрика метрики Хемминга. Утверждение доказано.

Следствие 5.4. *Пусть выполнены условия утверждения* 5.3 *и* μ *— такая* $(n+d+1)$*-значная надметрика метрики* $\chi_r^{t\uparrow}$, $d > t$, *что* $\chi_r^{t\uparrow}(\alpha,\alpha') = \mu(\alpha,\alpha')$, *если* $\alpha + \alpha' \in \Delta_1$. *Тогда* $\chi_r^{d\uparrow} = \mu$, *а наибольшая значность метрики* μ *достигается при* $d = n-1$ *и равна* $2n$.

Доказательство следует из утверждения 5.3.

Опишем некоторые свойства аффинных функций относительно надметрики $\chi_r^{t\uparrow}$ метрики Хемминга. В частности, покажем, что относительно $\chi_r^{t\uparrow}$ аффинные функции могут не находиться на одном расстоянии друг от друга, а бент-функции — на максимальном расстоянии от множества аффинных функций.

Пусть $\kappa: V_n \to \mathbb{Z}_{2^n}$ — (естественное) взаимно однозначное соответствие между V_n и $\mathbb{Z}_{2^n}$, а именно,

$$\kappa: (\alpha_1,...,\alpha_n) \to \sum_{i=0}^{n-1} \alpha_{n-i} 2^i.$$

Пусть $\vec{f} = (f(\vec{0}),....,f(\vec{1}))$ — вектор значений функции $f \in F_n$ и метрика μ задана на V_{2^n}. Для функций $a_1, a_2 \in F_n$ положим $\mu(a_1, a_2) = \mu(\vec{a}_1, \vec{a}_2)$.

Следствие 5.5. *Для любых аффинных функций* $a_1, a_2 \in F_n$, *чисел* $r \in \{1,...,2^n\}$, $t \in \{1,...,2^n - 1\}$ *справедливо равенство*

$$\chi_r^{t\uparrow}(a_1,a_2) = \begin{cases} 2^{n-1} + t, \text{ если } t < 2^{n-1}, \\ 2^n - 1, \text{ если } t \geq 2^{n-1} \text{ и } a_1(\kappa^{-1}(r-1)) \neq a_2(\kappa^{-1}(r-1)), \\ 2^n, \text{ если } t \geq 2^{n-1} \text{ и } a_1(\kappa^{-1}(r-1)) = a_2(\kappa^{-1}(r-1)). \end{cases}$$

Доказательство следует из утверждения 5.3.

Опишем множество $\left\{\chi^{\downarrow\uparrow}\right\}$ n-значных подметрик метрики Хемминга.

Утверждение 5.6. *Все* n*-значные подметрики* $(n+1)$*-значной метрики Хемминга исчерпываются следующим списком:*

$$\chi_t^{\downarrow}(\alpha,\alpha') = \begin{cases} i, & \text{если } \alpha + \alpha' \in \Delta_i, i < t, \\ t, & \text{если } \alpha + \alpha' \in \Delta_t \cup \Delta_{t+1}, \\ i-1, & \text{если } \alpha + \alpha' \in \Delta_i, t+1 < i, \end{cases}$$

где $\lceil n/2 \rceil \leq t \leq n-2$.

Доказательство. Рассмотрим функцию $\mu_{j,t}: V_n \times V_n \to \{0,...,n-1\}$, где

$$\mu_{j,t}(\alpha,\alpha') = \begin{cases} i, & \text{если } \alpha + \alpha' \in \Delta_i, i < j, i \neq t, \\ t, & \text{если } \alpha + \alpha' \in \Delta_t \cup \Delta_j, \\ i-1, & \text{если } \alpha + \alpha' \in \Delta_i, j+1 \leq i. \end{cases}$$

Пусть $A_c = \left\{\alpha \in V_n \mid \mu_{j,t}(\alpha,\vec{0}) = c\right\}$, где $c \in \{0,...,n-1\}$.

Если $\mu_{j,t}$ — метрика, то из утверждения 4.2 и следствия 2.3 работы [5] следует, что для каждого $c \in \{1,...,n-1\}$ должны выполняться включения

$$\bigcup_{r=1}^{c-1}(A_r + A_{c-r}) \subseteq \bigcup_{r=0}^{c} A_r. \tag{5.2}$$

Если $j > t+1$ и $\mu_{j,t}$ — метрика, то, согласно включению (5.2), имеем

$$(\Delta_t + \Delta_1) \cup (\Delta_j + \Delta_1) \subseteq \bigcup_{c=0}^{t+1} \Delta_c.$$

Однако $\Delta_j + \Delta_1 = \Delta_{j-1} + \Delta_{j+1}$, $\Delta_{j+1} \not\subset \bigcup_{c=0}^{t+1} \Delta_c$. Значит, $\mu_{j,t}$ не является метрикой.

Если $j = t+1$, $t \le (n-2)/2$, $\mu_{j,t}$ — метрика, то по включению (5.2)

$$(\Delta_t + \Delta_{t+1}) \cup (\Delta_{t+1} + \Delta_{t+1}) \cup (\Delta_t + \Delta_t) \subseteq \bigcup_{c=0}^{2t+1} \Delta_c.$$

Однако $\Delta_{2(t+1)} \subset \Delta_{t+1} + \Delta_{t+1}$ и $\Delta_{2(t+1)} \not\subset \bigcup_{c=0}^{2t+1} \Delta_c$. Значит, $\mu_{j,t}$ не является метрикой.

При $j = t+1$ и $\lceil n/2 \rceil \le t \le n-2$ из включения (5.2) легко следует, что $\mu_{t+1,t}$ — метрика для любого t, $\lceil n/2 \rceil \le t \le n-2$. Утверждение доказано.

Опишем теперь множество $\left\{\chi^{\downarrow\uparrow}\right\}$ надметрик n-значных подметрик метрики Хемминга, приведенных в утверждении 5.6.

Утверждение 5.7. *Пусть* $n \ge 2$, $\lceil n/2 \rceil \le t \le n-1$, $r \in \{1,...,n\}$ *и n-значная подметрика метрики Хемминга задана условиями*

$$\chi_t^{\downarrow}(\alpha,\alpha') = \begin{cases} i, & \text{если } \alpha + \alpha' \in \Delta_i,\ i < t, \\ t, & \text{если } \alpha + \alpha' \in \Delta_t \cup \Delta_{t+1}, \\ i-1, & \text{если } \alpha + \alpha' \in \Delta_i,\ t+1 < i. \end{cases}$$

Тогда $(n+1)$*-значные надметрики метрики* $\chi_t^{\downarrow}$ *суть*

$$\chi_{t,r}^{\downarrow\uparrow}(\alpha,\alpha')=\begin{cases}1, & \text{если } \alpha+\alpha'=\varepsilon_r,\\ 2, & \text{если } \alpha+\alpha'\in\Delta_1\setminus\{\varepsilon_r\},\\ \chi_t^{\downarrow}(\alpha,\alpha'), & \text{если } \alpha+\alpha'\in\Delta_t,\ t\geq 2.\end{cases}$$

В частности, $\left\{\chi^{\downarrow\uparrow}\right\}=\left\{\chi^{\uparrow\downarrow}\right\}$ *при* $n=2$ *и* $\left\{\chi^{\downarrow\uparrow}\right\}\subset\left\{\chi^{\uparrow\downarrow}\right\}$ *при* $n>2$.

Доказательство. Из утверждения 5.2 следует, что $\chi_{t,r}^{\downarrow\uparrow}$ — метрика. Доказательство отсутствия у метрики $\chi_t^{\downarrow}$ других надметрик проводится аналогично доказательству утверждения 5.1.

Из утверждения 5.7 следует, что число всех $(n+1)$-значных надметрик n-значных подметрик метрики Хемминга равно $\left(n-\lceil n/2\rceil\right)n$.

Утверждение 5.8. *Если* $n\geq 2$, $t\in\{3,\ldots,n-1\}$ *и* $r\in\{1,\ldots,n\}$, *то функция*

$$\chi_r^{t\uparrow t\downarrow}(\alpha,\alpha')=\begin{cases}1, & \text{если } \alpha+\alpha'=\varepsilon_r,\\ 2, & \text{если } \alpha+\alpha'\in\Delta_1\setminus\{\varepsilon_r\},\\ i+1, & \text{если } \alpha+\alpha'\in\Delta_i,\ i\in\{2,\ldots,t-2\},\\ t, & \text{если } \alpha+\alpha'\in\Delta_{t-1}\cup\Theta_t,\\ t+1, & \text{если } \alpha+\alpha'\in\Delta_{t+1}\cup\overline{\Theta}_t,\\ i, & \text{если } \alpha+\alpha'\in\Delta_i,\ i>t+1,\end{cases}$$

где $\Theta_c=\{(\alpha_1,\ldots,\alpha_n)\in\Delta_c\mid\alpha_r=1\}$, *является* $(n+1)$*-значной подметрикой* $(n+t+1)$*-значной надметрики* $\chi_r^{t\uparrow}$ *метрики Хемминга.*

Доказательство. Покажем, что функция $\chi_r^{t\uparrow t\downarrow}$ — метрика. Обозначим $\overline{\Theta}_d=\Delta_d\setminus\Theta_d$, $A_d=\left\{\alpha\in V_n\mid\chi_r^{t\uparrow t\downarrow}(\alpha,\vec{0})=d\right\}$, $d\in\{0,\ldots,n\}$.

Из следствия 2.3 работы [5] получаем, что функция $\chi_r^{t\uparrow t\downarrow}$ является метрикой, если для каждого $c\in\{1,\ldots,n\}$ выполняется включение

$$\bigcup_{i=1}^{c-1}(A_i+A_{c-i})\subseteq\bigcup_{i=0}^{c}A_i. \tag{5.3}$$

Рассмотрим произвольные числа $i, j \in \mathbb{N},\ 1 \le i \le j \le n-i$. Если $i+j \le t$, то из соотношений

$$A_i + A_j \subseteq \begin{cases} A_0, & \text{если } i=j=1, \\ \Delta_j \cup \Delta_{j-1}, & \text{если } i=1, j \ge 2, \\ \Delta_{i-1} + \Delta_{j-1}, & \text{если } 2 \le i, j < t, \end{cases}$$

вытекает включение $A_i + A_j \subseteq \bigcup\limits_{i=0}^{i+j-1} \Delta_i$. Непосредственно проверяется, что при любых $t+1 \le i+j$ справедлива формула (5.4), из которой следует включение $A_i + A_j \subseteq \bigcup\limits_{i=0}^{i+j} \Delta_i$.

$$A_i + A_j = \begin{cases} \Delta_{i-1} + \Delta_{j-1}, & \text{если } 2 < i, j < t, \\ \Delta_{i-1} + \Delta_j, & \text{если } 2 < i < t, t+1 < j, \\ \Delta_i + \Delta_j, & \text{если } t+1 < i, j, \\ \Delta_j + \varepsilon_r, & \text{если } i=1,\ t+1 < j, \\ \Delta_j + (\Delta_1 \setminus \{\varepsilon_r\}), & \text{если } i=2,\ t+1 < j, \\ (\Delta_{t-1} + \varepsilon_r) \cup (\Theta_t + \varepsilon_r), & \text{если } i=1, j=t, \\ (\Delta_{t-1} + (\Delta_1 \setminus \{\varepsilon_r\})) \cup (\Theta_t + (\Delta_1 \setminus \{\varepsilon_r\})), & \text{если } i=2, j=t, \\ (\Delta_{t+1} + \varepsilon_r) \cup (\bar{\Theta}_t + \varepsilon_r), & \text{если } i=1, j=t+1, \\ (\Delta_{t+1} + (\Delta_1 \setminus \{\varepsilon_r\})) \cup (\bar{\Theta}_t + (\Delta_1 \setminus \{\varepsilon_r\})), & \text{если } i=2, j=t+1, \\ \Theta_t + \Delta_{i-1}, & \text{если } 2 < i < t, j=t, \\ \Theta_t + \Delta_j, & \text{если } j > t+1, i=t, \\ \bar{\Theta}_t + \Delta_{i-1}, & \text{если } 2 < i < t, j=t+1, \\ (\bar{\Theta}_t + \Delta_j) \cup (\bar{\Theta}_t + \Delta_{j-1}), & \text{если } j > t+1, i=t+1, \\ (\Theta_t + \bar{\Theta}_t) \cup (\bar{\Theta}_t + \Delta_{t-1}) \cup (\Theta_t + \Delta_t) \cup (\Delta_{t+1} + \Delta_t), & \text{если } \{j,i\} = \{t, t+1\}, \\ (\Theta_t + \Theta_t) \cup (\Theta_t + \Delta_{t-1}) \cup (\Delta_{t-1} + \Delta_{t-1}), & \text{если } j=i=t, \\ (\bar{\Theta}_t + \bar{\Theta}_t) \cup (\Delta_{t+1} + \Delta_{t+1}) \cup (\bar{\Theta}_t + \Delta_{t+1}) \cup (\Delta_{t+1} + \Delta_t), & \text{если } j=i=t+1. \end{cases} \quad (5.4)$$

Значит, $\chi_r^{t\uparrow t\downarrow}$ — метрика. Очевидно, что $\chi_r^{t\uparrow t\downarrow}$ — подметрика метрики $\chi_r^{t\uparrow}$. Утверждение доказано.

Приведем пример такой n-значной подметрики надметрики метрики Хемминга, что относительно нее расстояния между некоторыми аффинными функциями не равны.

Следствие 5.9. *Если* $n = 2^m > 2$, *то для любых аффинных функций* $a_1,\ a_2 \in F_m$, *чисел* $r \in \{1,...,2^m\}$, $t \in \{3,...,2^m - 1\}$ *справедливо равенство*

$$\chi_r^{t\uparrow t\downarrow}(a_1,a_2) = \begin{cases} 2^{m-1}+1, & \text{если } t > 2^{m-1}, \\ 2^{m-1}, & \text{если } t = 2^{m-1} \text{ и } a_1(\kappa^{-1}(r-1)) \neq a_2(\kappa^{-1}(r-1)), \\ 2^{m-1}+1, & \text{если } t = 2^{m-1} \text{ и } a_1(\kappa^{-1}(r-1)) = a_2(\kappa^{-1}(r-1)), \\ 2^{m-1}, & \text{если } t < 2^{m-1}. \end{cases}$$

Доказательство следует из утверждения 5.8.

Пусть $t = 2^{m-1}$, число $r \in \{1,...,2^m\}$ фиксировано,

$$A_{0,r} = \{a \in AF_m \mid a(\kappa^{-1}(r-1))=0\},\ \ A_{1,r} = \{a \in AF_m \mid a(\kappa^{-1}(r-1))=1\}.$$

Тогда из следствия 5.9 получаем, что:

1) $\chi_r^{t\uparrow t\downarrow}(a_1,a_2) = 2^{m-1}+1$ для любых $a_1, a_2 \in A_{i,r}$, $i \in \{0,1\}$;

2) $\chi_r^{t\uparrow t\downarrow}(a_1,a_2) = 2^{m-1}$ для любых $a_1 \in A_{0,r}$, $a_2 \in A_{1,r}$.

§ 6. Натуральные метрики, инвариантные относительно группы сдвигов

Пусть $d \geq 1$, $(\bar{B}_1,...,\bar{B}_d) \in \bar{\mathbf{V}}_n^{(\mathbf{2})}$. Обозначим через M_n^+ множество всех натуральных метрик на пространстве V_n вида

$$\mu(\alpha,\alpha') = i, \text{ если } (\alpha,\alpha') \in \bar{B}_i,\ i \in \{1,...,d\},$$

группа изометрий которых содержит группу сдвига, т. е. $\mu(\alpha,\alpha+\beta) = \mu(\gamma,\gamma+\beta)$ для всех векторов $\alpha,\beta,\gamma \in V_n$. Очевидно, $\chi_n \in M_n^+$.

Отметим, что произвольная $(d+1)$-значная метрика $\mu \in M_n^+$ однозначно задается разбиением $(A_1(\mu),...,A_d(\mu))$ множества $V_n \setminus \{\vec{0}\}$, $A_j(\mu) = \{\alpha \in V_n \mid \mu(\alpha,\vec{0}) = j\}$, $j = \{0,...,d\}$, и может быть представлена в виде

$$\mu(\alpha,\alpha') = \begin{cases} 0, \text{ если } \alpha+\alpha' = \vec{0}, \\ i, \text{ если } \alpha+\alpha' \in A_i(\mu), i \in \{1,...,d\}. \end{cases}$$

Очевидно, что $d \leq 2^n - 1$, а значность метрики μ не превосходит 2^n.

Пусть $\mathrm{N}(X)$ — множество всех натуральных метрик на X и $M' \subset \mathrm{N}(X)$. Назовем μ *максимальной метрикой в* M', если в M' не существует надметрики, отличной от μ.

Опишем индуктивно максимальные метрики в M_n^+, являющиеся надметриками метрики Хемминга. Обозначим $V_{n,i} = <\varepsilon_j \mid j \in \{1,...,n\} \setminus \{i\}>$, $i \in \{1,...,n\}$.

Лемма 6.1. *Пусть* $n \geq 3$, $d \geq 2$, r *— произвольное число из* $\{1,...,n\}$ *и* μ *— произвольная* $(d+1)$*-значная метрика из* M_{n-1}^+, β *— произвольный вектор из* $V_n \setminus V_{n,r}$. *Тогда функция* $\rho_{\mu,r}^{(\beta)} : V_n \times V_n \to \mathbb{N}_0$, *заданная условиями*

$$\rho_{\mu,r}^{(\beta)}(\alpha,\alpha') = \begin{cases} \mu(\alpha,\alpha'), & \text{если } \alpha+\alpha' \in V_{n,r}, \\ d+1+\mu(\alpha,\alpha'+\beta), & \text{если } \alpha+\alpha' \in V_{n,r}+\beta, \end{cases}$$

является $2(d+1)$*-значной метрикой.*

Доказательство. Пусть $b = 2d+1$, $I(B)$ — индикатор выполнения условия B,

$$A_j = \left\{\alpha \in V_n \mid \rho_{\mu,r}^{(\beta)}(\alpha,\vec{0}) = j\right\}, \quad j \in \{0,...,b\}.$$

Согласно следствию 2.3 из [5], если $\rho_{\mu,r}^{(\beta)}$ — метрика, то

$$\bigcup_{i=1}^{c-1}(A_i + A_{c-i}) \subseteq \bigcup_{i=0}^{c} A_i \tag{6.1}$$

для каждого $c \in \{1,...,b\}$. Так как μ — метрика, то включение (6.1) справедливо для каждого $c \in \{1,...,d\}$. Так как

$$A_c = A_{c-d} + \beta,$$

$$A_{i(\mathrm{mod}\,d)} + A_{(c-i)(\mathrm{mod}\,d)} \subseteq V_{n,r}, \quad i \in \{1,...,c-1\},$$

$$A_{i(\mathrm{mod}\,d)} + A_{(c-i)(\mathrm{mod}\,d)} + \beta \subseteq \bigcup_{i=d+1}^{c} \left(A_{i(\mathrm{mod}\,d)} + \beta\right)$$

для всех $c \in \{d+1,...,b\}$, то из соотношений

$$\bigcup_{i=1}^{c-1}(A_{i(\mathrm{mod}\,d)} + A_{(c-i)(\mathrm{mod}\,d)} + (\mathrm{I}(c>d)+\mathrm{I}(c-i>d))\cdot\beta) \subseteq$$

$$\subseteq V_{n,r} \cup \bigcup_{i=d+1}^{c}\left(A_{i(\mathrm{mod}\,d)} + \beta\right),$$

$c = d+1,...,b,$ следует включение (6.1). Лемма доказана.

Лемма 6.1 позволяет описать все максимальные метрики в M_n^+ и показать их линейную эквивалентность (изоморфизм, задающийся линейным преобразованием).

Теорема 6.2. *При $n \geq 2$ каждому упорядоченному набору $\beta_1,...,\beta_n \in {V_n}^n$ линейно независимых векторов соответствует максимальная 2^n-значная метрика $\chi_{n,(\beta_1,...,\beta_n)}$ в M_n^+, заданная условиями*

$$\chi_{n,(\beta_1,...,\beta_n)} = \chi_{n,\beta_1}(\alpha,\alpha') = 1, \text{ если } \alpha+\alpha' = \beta_1,$$

$$\chi_{n,(\beta_1,...,\beta_t)}(\alpha,\alpha') = \begin{cases} \chi_{n,(\beta_1,...,\beta_{t-1})}(\alpha,\alpha'), & \text{если } \alpha+\alpha' \in \langle\beta_1,...,\beta_{t-1}\rangle, \\ \chi_{n,(\beta_1,...,\beta_{t-1})}(\alpha,\alpha'+\beta_t)+2^{t-1}, & \text{если } \alpha+\alpha'+\beta_t \in \langle\beta_1,...,\beta_{t-1}\rangle, \end{cases}$$

$t = 2,...,n$. *Все максимальные метрики в M_n^+ линейно эквивалентны, любая из них совпадает с метрикой $\chi_{n,(\beta_1,...,\beta_n)}$ для некоторого набора $(\beta_1,...,\beta_n) \in V_n^n$, а их число равно $(2^n-1)(2^n-2)...(2^n-2^{n-1})$.*

Доказательство. Пусть $A_0 = \{\vec{0}\}$, μ — произвольная максимальная $(d+1)$-значная метрика из M_n^+. Тогда она может быть представлена в виде

$$\mu(\alpha,\alpha') = i, \text{ если } \alpha+\alpha' \in A_i,\ i \in \{1,...,d\},$$

где $(A_1,...,A_d)$ — некоторое разбиение множества $V_n \setminus \{\vec{0}\}$. Очевидно, что μ является максимальной метрикой в M_n^+ тогда и только тогда, когда $d = 2^n-1$ и $|A_i| = 1$ для всех $i \in \{1,...,2^n-1\}$. Из леммы 6.1 следует, что для любых линейно независимых векторов $\beta_1,...,\beta_n \in V_n$ функция $\chi_{n,(\beta_1,...,\beta_n)}$ — метрика.

Покажем, что метриками $\chi_{n,(\beta_1,\ldots,\beta_n)}$ исчерпываются все максимальные метрики в M_n^+. Для этого рекурсивно построим метрику μ, у которой $|A_i|=1$ для всех $i=1,\ldots,d$. Согласно следствию 2.3 работы [5], для каждого $c\in\{1,\ldots,n\}$ должно выполняться включение

$$\bigcup_{i=1}^{c-1}(A_i+A_{c-i})\subseteq\bigcup_{i=0}^{c}A_i. \tag{6.2}$$

Пусть $A_1=\{\beta_1\}$. Тогда

$$A_1+A_1=<\beta_1>,\ A_1+A_1\subseteq<\beta_1>+A_2.$$

Значит, $\mu(\alpha,\alpha')=\chi_{n,\beta_1}(\alpha,\alpha')$, если $\alpha+\alpha'\in<\beta_1>$.

Предположим, что $\mu(\alpha,\alpha')=\chi_{n,(\beta_1,\ldots,\beta_{t-1})}(\alpha,\alpha')$, если $\alpha+\alpha'\in$ $\in V_n(\beta_1,\ldots,\beta_{t-1})$ и $2\le t\le n$. Тогда

$$\bigcup_{i=1}^{2^{t-1}-1}(A_i+A_{2^{t-1}-i})=\langle\beta_1,\ldots,\beta_{t-1}\rangle \text{ и } \bigcup_{i=0}^{2^{t-1}}A_i=\langle\beta_1,\ldots,\beta_{t-1}\rangle\cup A_{2^{t-1}}.$$

Значит,

$$\bigcup_{i=1}^{2^{t-1}-1}(A_i+A_{2^{t-1}-i})\subseteq\bigcup_{i=0}^{2^{t-1}}A_i$$

для произвольного одноэлементного подмножества $A_{2^{t-1}}\subseteq V_n\setminus\langle\beta_1,\ldots,\beta_{t-1}\rangle$.

Положим $A_{2^{t-1}}=\{\beta_t\}$. Тогда

$$(A_1+\beta_t)\cup\bigcup_{i=2}^{2^{t-1}-1}\left(A_i+A_{2^{t-1}+1-i}\right)\subseteq\langle\beta_1,\ldots,\beta_{t-1}\rangle>\cup A_{2^{t-1}}\cup A_{2^{t-1}+1}.$$

Теперь из соотношений

$$\bigcup_{i=2}^{2^{t-1}-1}\left(A_i+A_{2^{t-1}+1-i}\right)\subseteq\langle\beta_1,\ldots,\beta_{t-1}\rangle \text{ и } (A_1+\beta_t)\cap A_{2^{t-1}}=\varnothing$$

следует равенство $A_{2^{t-1}+1}=A_1+\beta_t$.

Пусть $A_{2^{t-1}+i} = A_i + \beta_t$ для всех $l \in \{2,...,2^{t-1}-1\}$, $i \in \{1,...,l-1\}$. Покажем, что $A_{2^{t-1}+l} = A_l + \beta_t$. Так как

$$\bigcup_{i=1}^{2^{t-1}+l} (A_i + A_{2^{t-1}+l-i}) = \bigcup_{i=1}^{l} (A_i + A_{l-i} + \beta_t) \cup \left(\bigcup_{i=l+1}^{2^{t-1}-l-1} (A_i + A_{2^{t-1}+l-i}) \right) \subseteq$$

$$\subseteq \langle \beta_1,...,\beta_{t-1} \rangle \cup \left(\bigcup_{i=1}^{l} (A_i + A_{l-i} + \beta_t) \right),$$

$$\bigcup_{i=1}^{2^{t-1}+l} (A_i + A_{2^{t-1}+l-i}) \subseteq \langle \beta_1,...,\beta_{t-1} \rangle \cup \left(\bigcup_{j=0}^{l-1} A_{2^{t-1}+j} \right) \cup A_{2^{t-1}+l},$$

то

$$(A_l + \beta_t) \cup \bigcup_{i=1}^{l-1} (A_i + A_{l-i} + \beta_t) \subseteq \left(\bigcup_{j=0}^{l-1} A_{2^{t-1}+j} \right) \cup A_{2^{t-1}+l} \cup A_0.$$

Следовательно, $A_{2^{t-1}+l} = A_l + \beta_t$ для всех $l \in \{2,...,2^{t-1}-1\}$.

Таким образом, $\mu(\alpha,\alpha') = \chi_{n,(\beta_1,...,\beta_t)}(\alpha,\alpha')$, если $\alpha + \alpha' \in \langle \beta_1,...,\beta_t \rangle$ для $t = 2,...,b$. Значит, число максимальных метрик в M_n^+ равно числу базисов пространства V_n, т. е. числу $(2^n-1)(2^n-2)...(2^n-2^{n-1})$.

Пусть $\chi_{n,(\beta_1,...,\beta_t)}$, $\chi_{n,(\beta'_1,...,\beta'_t)}$ — две произвольные максимальные метрики. Поскольку $\beta_1,...,\beta_n$ и $\beta'_1,...,\beta'_n$ — базисы V_n, то существует преобразование $g \in GL_n$, удовлетворяющее равенствам $\beta'_i = \beta_i^g$, $i = 1,...,n$. Рассмотрим такие произвольные векторы $\alpha,\alpha' \in V_n$, что $\alpha + \alpha' \in \langle \beta_1,...,\beta_t \rangle$ или $\alpha + \alpha' \in \beta_t + \langle \beta_1,...,\beta_{t-1} \rangle$. Тогда, соответственно, $\alpha^g + \alpha'^g \in \langle \beta_1^g,...,\beta_t^g \rangle$ или $\alpha^g + \alpha'^g \in \beta_t^g + \langle \beta_1^g,...,\beta_{t-1}^g \rangle$. Отсюда и из задания максимальных метрик $\chi_{n,(\beta_1,...,\beta_t)}$, $\chi_{n,(\beta'_1,...,\beta'_t)}$ получаем, что

$$\chi_{n,(\beta_1,...,\beta_t)}(\alpha,\alpha') = \chi_{n,(\beta'_1,...,\beta'_t)}(\alpha^g,\alpha'^g).$$

Значит, все максимальные метрики в M_n^+ линейно эквивалентны. Теорема доказана.

Следствие 6.3. *Пусть выполнены условия теоремы* 6.2 *и упорядоченный набор* $\beta_1,...,\beta_n$ *линейно независимых векторов из пространства* V_n *таков, что* $\beta_1 \in \Delta_1$ *и* $\beta_t \in \bigcup_{i=1}^{2^{t-1}} \Delta_i$ *для всех* $t \in \{2,...,\lfloor \log_2 n \rfloor\}$. *Тогда* $\chi_{n,(\beta_1,...,\beta_n)}$ — *максимальная* 2^n*-значная метрика в* M_n^+, *являющаяся надметрикой метрики Хемминга. Число таких максимальных* 2^n*-значных надметрик метрики Хемминга равно*

$$\prod_{t=1}^{\lfloor \log_2 n \rfloor} \left(\sum_{i=0}^{2^{t-1}} \binom{n}{i} - 2^{t-1} \right) \cdot \prod_{j=\lfloor \log_2 n \rfloor + 1}^{n-1} (2^n - 2^j).$$

Доказательство. Обозначим

$$A_j = \left\{ \alpha \in V_n \mid \chi_{n,(\beta_1,...,\beta_n)}(\alpha, \vec{0}) = j \right\} = \{\alpha^{(j)}\}, \quad j = 0,...,2^n - 1.$$

Метрика Хемминга χ является подметрикой метрики $\chi_{n,(\beta_1,...,\beta_n)}$, если для всех $(\alpha, \alpha') \in V_n \times V_n$ справедливо неравенство $\chi(\alpha, \alpha') \le \le \chi_{n,(\beta_1,...,\beta_n)}(\alpha, \alpha')$. Следовательно, $\beta_1 \in \Delta_1$, $\beta_2 \in \Delta_1 \cup \Delta_2$ и $\alpha^{(3)} = \beta_1 + \beta_2$, $\left\| \alpha^{(3)} \right\| \le 3$.

Пусть $t \in \{2,...,\lfloor \log_2 n \rfloor\}$, $\| \alpha^{(j)} \| \le j$ для всех $j \in \left\{1,...,2^{t-1} - 1\right\}$ и $\|\beta_t\| \le 2^{t-1}$. Покажем, что $\left\| \alpha^{(2^{t-1}+l)} \right\| \le 2^{t-1} + l$ для всех $l \in \left\{1,...,2^{t-1} - 1\right\}$.

Из доказательства теоремы 6.2 следует, что $A_{2^{t-1}+l} = A_l + \beta_t$. Значит, для всех $l \in \left\{1,...,2^{t-1} - 1\right\}$ имеем

$$\left\| \alpha^{(2^{t-1}+l)} \right\| = \left\| \alpha^{(l)} + \beta_t \right\| \le \left\| \alpha^{(l)} \right\| + \|\beta_t\| \le l + 2^{t-1}.$$

Найдем число максимальных 2^n-значных надметрик метрики Хемминга. Вектор $\beta_1 \in \Delta_1$ может быть выбран n способами, а вектор $\beta_2 \in (\Delta_1 \cup \Delta_2) \setminus < \beta_1 >$ может быть выбран $n + 2^{-1} n(n-1) - (2^1 - 1)$ способа-

ми. Аналогично, при $t \in \{2,...,\lfloor \log_2 n \rfloor\}$ вектор $\beta_t \in \left(\bigcup_{i=1}^{2^{t-1}} \Delta_i \right) \setminus \langle \beta_1,...,\beta_{t-1} \rangle$ может быть выбран $\left(\sum_{i=1}^{2^{t-1}} \binom{n}{i} - (2^{t-1}-1) \right)$ способами, а при $t \in$ $\in \{\lfloor \log_2 n \rfloor + 1,...,n\}$ вектор $\beta_t \in V_n \setminus \langle \beta_1,...,\beta_{t-1} \rangle$ может быть выбран $(2^n - 2^{t-1})$ способами. Следствие доказано.

Опишем классы изоморфных метрик из множества M_n^+.

Утверждение 6.4. *Пусть* $\beta_1,...,\beta_n$ *и* $\omega_1,...,\omega_n$ *— два различных базиса пространства* V_n *и* $\pi : \beta_i \to \omega_i$ *для всех* $i \in \{1,...,n\}$, $\pi \in GL_n$. *Пусть также* $2 \le d \le 2^n - 1$ *и* $\mu_{\beta_1,...,\beta_n}$ *—* $(d+1)$*-значная подметрика максимальной метрики* $\chi_{n,(\beta_1,...,\beta_n)}$ *в* M_n^+. *Тогда функция* $\mu_{\omega_1,...,\omega_n} : V_n \times V_n \to \mathbb{N}_0$, *заданная условием*

$$\mu_{\omega_1,...,\omega_n}(\alpha,\alpha') = \mu_{\beta_1,...,\beta_n}(\alpha^{\pi^{-1}}, \alpha'^{\pi^{-1}}),$$

является $(d+1)$*-значной подметрикой метрики* $\chi_{n,(\omega_1,...,\omega_n)}$. *Кроме того,*

$$A_{j_2}(\mu_{\omega_1,...,\omega_n}) = \left(A_{j_2}(\mu_{\beta_1,...,\beta_n})\right)^{\pi}, \quad A_{j_1}(\chi_{n,(\omega_1,...,\omega_n)}) = \left(A_{j_1}(\chi_{n,(\beta_1,...,\beta_n)})\right)^{\pi}$$

для всех $j_1 \in \left\{1,...,2^n - 1\right\}$, $j_2 \in \{1,...,d\}$.

Доказательство. Очевидно, что $\mu_{\omega_1,...,\omega_n}$ — $(d+1)$-значная метрика и

$$A_{j_2}(\mu_{\omega_1,...,\omega_n}) = \left(A_{j_2}(\mu_{\beta_1,...,\beta_n})\right)^{\pi}, \quad A_{j_1}(\chi_{n,(\omega_1,...,\omega_n)}) = \left(A_{j_1}(\chi_{n,(\beta_1,...,\beta_n)})\right)^{\pi}$$

для всех $j_1 \in \left\{1,...,2^n - 1\right\}$, $j_2 \in \{1,...,d\}$ в силу линейности π.

Осталось показать, что $\mu_{\omega_1,...,\omega_n}(\alpha,\alpha') \le \chi_{n,(\omega_1,...,\omega_n)}(\alpha,\alpha')$ для всех $(\alpha,\alpha') \in V_n \times V_n$. Рассмотрим произвольные различные векторы $\alpha,\alpha' \in V_n$. Пусть

$$\alpha^{\pi^{-1}} + \alpha'^{\pi^{-1}} \in A_{j_1}(\chi_{n,(\beta_1,...,\beta_n)}), \quad \alpha^{\pi^{-1}} + \alpha'^{\pi^{-1}} \in A_{j_2}(\mu_{\beta_1,...,\beta_n})$$

для некоторых $j_1 \in \left\{1,...,2^n-1\right\}$, $j_2 \in \{1,...,d\}$. Так как $\mu_{\beta_1,...,\beta_n}$ — подметрика $\chi_{n,(\beta_1,...,\beta_n)}$, то $j_2 \le j_1$. Тогда

$$\alpha+\alpha' \in \left(A_{j_1}(\chi_{n,(\beta_1,...,\beta_n)})\right)^{\pi},\ \alpha+\alpha' \in \left(A_{j_2}(\mu_{\beta_1,...,\beta_n})\right)^{\pi}$$

в силу линейности π. Следовательно,

$$\alpha+\alpha' \in A_{j_1}(\chi_{n,(\omega_1,...,\omega_n)}),\ \alpha+\alpha' \in A_{j_2}(\mu_{\omega_1,...,\omega_n}).$$

Значит, $\mu_{\omega_1,...,\omega_n}$ — подметрика метрики $\chi_{n,(\omega_1,...,\omega_n)}$. Утверждение доказано.

Таким образом, каждой подметрике метрики $\chi_{n,(\beta_1,...,\beta_n)}$ однозначно соответствует подметрика метрики $\chi_{n,(\omega_1,...,\omega_n)}$. Кроме того, все максимальные метрики в M_n^+ получаются одна из другой действием линейного преобразования из группы GL_n.

Опишем все $(n+1)$-значные подметрики максимальных метрик в M_n^+, связанные с метрикой Хемминга посредством линейной группы GL_n. Их можно рассматривать как аналоги метрики Хемминга.

Следствие 6.5. *Пусть* $\beta_1,...,\beta_n$ *— такой базис пространства* V_n, *что* $\beta_1 \in \Delta_1$ *и* $\beta_t \in \bigcup_{i=1}^{2^{t-1}} \Delta_i$ *для всех* $t \in \left\{2,...,\lfloor \log_2 n \rfloor\right\}$, $\pi : \varepsilon_i \to \beta_i$ *для всех* $i \in \{1,...,n\}$, $\pi \in GL_n$. *Тогда функция* $\mu_{\beta_1,...,\beta_n} : V_n \times V_n \to \mathbb{N}_0$, *заданная условием*

$$\mu_{\beta_1,...,\beta_n}(\alpha,\alpha') = \chi(\alpha^{\pi^{-1}},\alpha'^{\pi^{-1}}),$$

является $(n+1)$*-значной подметрикой* 2^n*-значной надметрики* $\chi_{n,(\beta_1,...,\beta_n)}$ *метрики Хемминга* χ.

Доказательство получается путем применения к подметрикам максимальной 2^n-значной метрики $\chi_{n,(\varepsilon_1,...,\varepsilon_n)} \in M_n^+$ следствия 6.3 и утверждения 6.4.

Таким образом, описание всех подметрик и надметрик на V_n сводится к описанию всех подметрик метрики $\chi_{n,(\varepsilon_1,...,\varepsilon_n)}$.

Приведем примеры двух $(n+1)$-значных метрик, линейно эквивалентных метрике Хемминга χ_n и «разбивающих» множества аффинных и бент-функций, соответственно. Отметим, что эти метрики являются подметриками максимальных метрик в M_n^+.

Для произвольных функций $f_2, f_1 \in F_m$ обозначим через $f_2 + f_1$ функцию из F_m, заданную условием $(f_2 + f_1)(\alpha) = f_2(\alpha) + f_1(\alpha)$ для всех $\alpha \in V_m$.

Пусть BF_m — множество всех бент-функций из множества F_m, AF_m — множество всех аффинных функций из множества F_m и

$$d_f^{AF}(\mu) = \min\{\mu(a, f) \mid a \in AF_m\}, \quad f \in F_m.$$

Обозначим через $\vec{f} = (f(\vec{0}), ..., f(\vec{1}))$ вектор значений функции $f \in F_m$. Пусть $H(f) = \{\overrightarrow{(a+f)} \mid a \in AF_m\}$ для $f \in F_m$; $B_\gamma = \{f \in BF_m \mid \gamma \in H(f)\}$, $\overline{B}_\gamma = \{f \in BF_m \mid \gamma \notin H(f)\}$, $\gamma \in V_{2^m}$. Заметим, что $\overline{B}_\gamma \neq \varnothing$, если $B_\gamma \neq \varnothing$, и $\|\gamma\| = 2^{m-1} - 2^{m/2-1}$, если $B_\gamma \neq \varnothing$. Положим $B^{(m)} = \{\gamma \in V_{2^m} \mid B_\gamma \neq \varnothing\}$.

Утверждение 6.6. *Пусть m четно, $n = 2^m$, γ — произвольный вектор из множества $B^{(m)}$ и $\varepsilon_{i_1}, ..., \varepsilon_{i_t}, \gamma, \varepsilon_{i_{t+1}}, ..., \varepsilon_{i_{n-1}}$ — произвольный базис пространства V_n, $t \geq m$. Пусть линейное преобразование $\pi \in GL_n$ задано как $\pi : \varepsilon_{i_l} \to \varepsilon_{i_l}$ для всех $l \in \{1, ..., n-1\}$, $\pi : \varepsilon_{i_n} \to \gamma$, где $\{i_j \mid j \in \{1, ..., n\}\} = \{1, ..., n\}$, и*

$$\mu(\alpha, \alpha') = \chi_n(\alpha^{\pi^{-1}}, \alpha'^{\pi^{-1}})$$

для всех $(\alpha, \alpha') \in V_n \times V_n$. Тогда $d_{f_1}^{AF}(\mu) = 1$ и $d_{f_1}^{AF}(\mu) < d_{f_2}^{AF}(\mu)$ для любых функций $f_1 \in B_\gamma$, $f_2 \in \overline{B}_\gamma$.

Доказательство непосредственно вытекает из следствий 6.3, 6.5 и равенств $A_1(\mu) = \{\varepsilon_{i_1}, ..., \varepsilon_{i_t}, \gamma, \varepsilon_{i_{t+1}}, ..., \varepsilon_{i_{n-1}}\}$, $\|\theta\| = 2^{m-1} - 2^{m/2-1}$ для $\theta \in H(f_2)$.

Утверждение 6.7. *Пусть выполняются следующие условия:*

1) *m четно, $n = 2^m$, $r = 2^{m-1} - 2^{m/2-1}$;*
2) *γ — произвольный вектор из множества $B^{(m)}$, $\gamma = \theta_1 + \theta_2, \theta_1, \theta_2 \in V_n$;*

3) $\|\theta_1\|,\|\theta_2\| \notin \left\{1, r, r-1, r+1, 2^{m-1}+2^{m/2-1}, 2^{m-1}+2^{m/2-1}+1, 2^{m-1}+2^{m/2-1}-1\right\}$;

4) $\varepsilon_{i_1},...,\varepsilon_{i_t},\theta_1,\varepsilon_{i_{t+1}},...,\varepsilon_{i_c},\theta_2,\varepsilon_{i_{c+1}}...,\varepsilon_{i_{n-2}}$ — *произвольный базис пространства* V_n, $t \geq m$;

5) *линейное преобразование* $\pi \in GL_n$ *задано условиями:* $\pi : \varepsilon_{i_l} \to \varepsilon_{i_l}$ *для всех* $l \in \{1,...,n-2\}$, $\pi : \varepsilon_{i_{n-1}} \to \theta_1$, $\pi : \varepsilon_{i_n} \to \theta_2$, *где* $\left\{i_j \mid j \in \{1,...,n\}\right\} = \{1,...,n\}$, *и* $\mu(\alpha,\alpha') = \chi(\alpha^{\pi^{-1}}, \alpha'^{\pi^{-1}})$ *для всех* $(\alpha,\alpha') \in V_n \times V_n$.

Тогда $d_{f_1}^{AF}(\mu) = 2$ *и* $d_{f_1}^{AF}(\mu) < d_{f_2}^{AF}(\mu)$ *для любых функций* $f_1 \in B_\gamma$, $f_2 \in \overline{B}_\gamma$.

Доказательство следует из следствий 6.3, 6.5 и того, что

$$A_1(\mu) = \left\{\varepsilon_{i_1},...,\varepsilon_{i_t},\theta_1,\varepsilon_{i_{t+1}},...,\varepsilon_{i_c},\theta_2,\varepsilon_{i_{c+1}}...,\varepsilon_{i_{n-2}}\right\},$$

$$A_2(\mu) = \left\{\varepsilon_{i_{j_1}} + \varepsilon_{i_{j_2}} \mid j_1, j_2 \in \{1,...,n-2\}\right\} \cup \left\{\varepsilon_{i_j} + \theta_t \mid t \in \{1,2\}, j \in \{1,...,n-2\}\right\} \cup \{\gamma\}.$$

§ 7. Групповые свойства натуральных d-значных метрик

В работах [1], [2], [3] по группе подстановок (прежде всего содержащей группу Джевонса) строились метрики с данной группой изометрий. В общем случае сложно описать группу изометрий произвольной натуральной метрики. Следующая лемма сводит данную задачу к нахождению группы автоморфизмов графов соответствующих метрических орбиталов.

Лемма 7.1. *Пусть* $d \geq 2$ *и* $(d+1)$*-значная метрика* $\mu : X \times X \to \mathbb{N}_0$ *задана условиями*

$$\mu(\alpha,\alpha') = i, \text{ если } (\alpha,\alpha') \in A_i, i \in \{1,...,d\}.$$

Пусть также $\overline{\Gamma}^{(i)} = (X, A_i)$ — *граф с множеством вершин* X *и множеством ребер* A_i, $i \in \{1,...,d\}$. *Тогда* $\mathrm{Isom}\mu = \bigcap_{i=1}^{d} \mathrm{Aut}\overline{\Gamma}^{(i)}$.

Доказательство очевидно.

Замечание. В случае $d = 2$ легко видеть, что $\mathrm{Isom}\mu = \mathrm{Aut}\overline{\Gamma}^{(i)}$, $i = 1, 2$.

Кроме того, если граф $\Gamma = (X, \Theta)$ связен, то метрика $\tilde{\mu}_\Theta$, определяемая длиной пути между вершинами в графе, является надметрикой метрики μ_Θ.

В работе [3] приведены группы изометрий 3-значных групповых подметрик метрики Хемминга, определяемые графами орбиталов подсхем схемы Хемминга. Используя лемму 7.1, можно найти группы изометрий 3-значных подметрик метрики Хемминга. Для удобства чтения напомним ряд фактов, использующихся в работе [2].

Каждой транзитивной группе подстановок $H \le S(\Omega)$ с орбиталами (орбитами при действии на множестве $\Omega\times\Omega$, т. е. $(\alpha,\beta)^g = (\alpha^g, \beta^g)$) $\Psi_0,...,\Psi_d$ можно поставить в соответствие схему отношений $\mathbb{S} = (\Omega;\Psi_0,...,\Psi_d)$. Схема отношений $\mathbb{S}' = (\Omega;\Psi'_0,...,\Psi'_m)$ называется подсхемой схемы $\mathbb{S} = (\Omega;\Psi_0,...,\Psi_d)$, если для каждого $i \in \{0,...,m\}$ найдется такое $j \in \{0,...,d\}$, что $\Psi'_i \subseteq \Psi_j$.

Пусть $\Phi_{i,n} = \left\{J^{(i)}_{1,n},...,J^{(i)}_{r_i,n}\right\}$, $i \in \mathbb{N}$, и $\left(J^{(i)}_{1,n},...,J^{(i)}_{r_i,n}\right)$ — такое разбиение множества $\{1,...,n\}$, что $J \in \Phi_{i,n}$ для каждого подорбитала $\bigcup_{j\in J}\Delta_j$ i-й подсхемы схемы Хемминга в классификации Музычука [4]. Через $G_{i,n}$ обозначим наибольшую группу, задающую i-ю подсхему схемы Хемминга и описанную в [2]. Положим $\Phi_{0,n} = \{1,...,n\}$, $G_{0,n} = S_2 \uparrow S_n$.

Перечислим все 3-значные подметрики метрики Хемминга и их группы изометрий.

Утверждение 7.1. *Для любого* $n \ge 6$ *все* 3*-значные подметрики метрики Хемминга задаются равенствами*

$$\mu_\Theta(\alpha,\alpha') = \begin{cases} 1, \text{ если } \alpha+\alpha' \in \Delta_1 \cup \bigcup\limits_{i\in\Theta}\Delta_i, \\ 2, \text{ если } \alpha+\alpha' \in \bigcup\limits_{i\in\bar\Theta}\Delta_i, \end{cases}$$

где $\Theta \subset \{2,...,n\}$, $\bar\Theta = \{2,...,n\} \setminus \Theta$. *Группа изометрий* $\mathrm{Isom}\mu_\Theta$ *метрики* μ_Θ *совпадает с наибольшей группой из множества* $\left\{G_{i,n} \mid i \in \mathrm{T}_\Theta\right\}$, *где*

$$\mathrm{T}_\Theta = \left\{ i \in \mathbb{N}_0 \mid \Theta \cup \{1\} = \bigcup_{c\in X} J^{(i)}_{c,n}, \bar\Theta = \bigcup_{c\in\bar X} J^{(i)}_{c,n}, \bar X \cup X = \{1,...,r_i\} \right\}.$$

Доказательство следует из утверждения 3.2 работы [5].

§ 8. Коды с нехемминговыми метриками

С помощью $(n+1)$-значных подметрик 2^n-значных надметрик метрики Хемминга можно строить класс кодов следующим образом.

Пусть (H,χ) — произвольный код $H\subset V_n$ с кодовым расстоянием d относительно метрики Хемминга χ и $\beta_1,...,\beta_n$ — такой базис пространства V_n, что $\beta_1\in\Delta_1$ и $\beta_t\in\bigcup_{i=1}^{2^{t-1}}\Delta_i$ для всех $t\in\{2,...,\lfloor\log_2 n\rfloor\}$. Пусть линейное преобразование $\pi\in GL_n$ задано условиями $\pi:\varepsilon_i\to\beta_i$, $i=1,...,n$, и пусть

$$\mu_{\beta_1,...,\beta_n}(\alpha,\alpha')=\chi(\alpha^{\pi^{-1}},\alpha'^{\pi^{-1}})$$

для всех $(\alpha,\alpha')\in V_n\times V_n$. В силу следствия 6.5 $(H^\pi,\mu_{\beta_1,...,\beta_n})$ — код относительно метрики $\mu_{\beta_1,...,\beta_n}$ с кодовым расстоянием d, линейно изоморфный исходному коду с метрикой Хемминга.

Опишем коды с кодовым расстоянием d относительно $(d+1)$-значной метрики из M_n^+.

Утверждение 8.1. *Пусть $d\ge 2$, μ — произвольная $(d+1)$-значная метрика из M_n^+, $H\subset V_n$, и (H,μ) — код с кодовым расстоянием d относительно метрики μ, $\mu(\alpha,\beta)\ne d$ для всех векторов $\alpha\in H$, $\beta\notin H$. Тогда коду (H,μ) соответствуют такие линейное пространство $W_H\subseteq A_d(\mu)$ и вектор $\alpha_H\in V_n$, что $H=\alpha_H+W_H$.*

Доказательство. Пусть $\alpha\in H$ — произвольное кодовое слово. Тогда существует такое наибольшее число $t\ge 1$ линейно независимых векторов $\beta_1,...,\beta_t\in A_d(\mu)$, что $\alpha+\beta_j\in H$ для всех $j\in\{1,...,t\}$. Предположим, что при $r\in\{2,...,t\}$ для всех подмножеств $\{j_1,...,j_{r-1}\}\subseteq\{1,...,t\}$ справедливы включения

$$\alpha+\sum_{c=1}^{r-1}\beta_{j_c}\in H,\ \sum_{c=1}^{r-1}\beta_{j_c}\in A_d(\mu).$$

Так как

$$\mu\left(\alpha+\beta_{j_r},\alpha+\sum_{c=1}^{r-1}\beta_{j_c}\right)=\mu\left(\alpha,\alpha+\sum_{c=1}^{r-1}\beta_{j_c}+\beta_{j_r}\right)=2,$$

то $\sum_{c=1}^{r-1}\beta_{j_c}\in A_d(\mu)$ для всех различных $\{j_1,...,j_r\}\subseteq\{1,...,t\}$. Следовательно, $\alpha+\langle\beta_1,...,\beta_t\rangle\subseteq H$ и $\langle\beta_1,...,\beta_t\rangle\subseteq A_d(\mu)$.

Покажем, что $\alpha+\langle\beta_1,...,\beta_t\rangle=H$. Пусть существует кодовое слово $\theta\notin H\setminus\left(\alpha+\langle\beta_1,...,\beta_t\rangle\right)$. Тогда $\theta=\alpha+\beta_{t+1}$ для некоторого вектора $\beta_{t+1}\in A_d(\mu)\setminus\langle\beta_1,...,\beta_t\rangle$ и векторы $\beta_1,...,\beta_t,\beta_{t+1}$ линейно независимы. По построению t — наибольшее число линейно независимых векторов со свойством $\alpha+\beta_j\in H$. Значит, $\alpha+\langle\beta_1,...,\beta_t\rangle=H$. Утверждение доказано.

Следствие 8.2. *Пусть выполнены условия утверждения* 8.1. *Тогда:*

1) *каждому линейному коду* (H,χ) *однозначно соответствует* 3*-значная метрика* $\mu_{H,3}\in M_n^+$, *заданная условием*

$$a.\qquad \mu_{H,3}(\alpha,\alpha')=\begin{cases}1, & \text{если } \alpha+\alpha'\notin H,\\ 2, & \text{если } \alpha+\alpha'\in H;\end{cases}$$

2) *каждому линейному коду* (H,χ) *с кодовым расстоянием* $d\geq 3$ *и числу* $r\in\left\{2,...,2^{d-1}\right\}$ *соответствует* $(r+2)$*-значная метрика* $\mu_{H,d}\in M_n^+$, *заданная условием*

$$a.\quad \mu_{H,d}(\alpha,\alpha')=\begin{cases}\mu'_{V_{d-1}}(\alpha,\alpha'), & \text{если } \alpha+\alpha'\in<\varepsilon_1,...,\varepsilon_{d-1}>,\\ r+1, & \text{если } \alpha+\alpha'\in V_n\setminus<\varepsilon_1,...,\varepsilon_{d-1}>,\end{cases}$$

где $\mu'_{V_{d-1}}-(r+1)$*-значная метрика на* $<\varepsilon_1,...,\varepsilon_{d-1}>$ *из* M_{d-1}^+.

Следствие 8.3. *Пусть* $d\geq 2$, μ *— произвольная* $(d+1)$*-значная метрика из* M_n^+, $H\subset V_n$, *и* (H,μ) *— нелинейный код с кодовым расстоянием* d *относительно метрики* μ, $\alpha\in H$. *Тогда*

$$H\subseteq\left(\alpha+\left(\langle\beta_1,...,\beta_t\rangle\cap A_d(\mu)\right)\right)\cup\{\alpha\},$$

где $\beta_1,...,\beta_t$ *— такой наибольший набор линейно независимых векторов из* $A_d(\mu)$, *что* $\alpha+\beta_i\in H$ *для всех* $i\in\{2,...,t\}$.

Следствие 8.4. *Пусть* $d \geq 2$, μ *— произвольная* $(d+1)$*-значная метрика из* M_n^+, H *— подпространство* V_n *и* (H, μ) *— код с кодовым расстоянием* $r \in \{2,...,d\}$ *относительно метрики* μ. *Тогда* $H \subseteq \bigcup_{i=r}^{d} A_i(\mu) \cup \{\vec{0}\}$.

Доказательства этих следствий очевидны. В последнем случае надо учесть, что $\vec{0} \in H$, а потому $\mu(\vec{0}, \beta) \geq d$ для любого $\beta \in H \setminus \vec{0}$.

Список литературы

1. *Погорелов Б. А.* Подметрики метрики Хемминга и теорема А. А. Маркова // В сб.: Труды по дискретной математике, т. 9. — М.: ФИЗМАТЛИТ, 2006. — С. 190–219.
2. *Погорелов Б. А., Пудовкина М. А.* Подметрики метрики Хемминга и преобразования, распространяющие искажения в заданное число раз // В сб.: Труды по дискретной математике, т. 10. — М.: ФИЗМАТЛИТ, 2007. — С. 202–238.
3. *Погорелов Б. А., Пудовкина М. А.* Подметрики Хемминга и их группы изометрий // В сб.: Труды по дискретной математике, т. 11. — М.: ФИЗМАТЛИТ, 2008. — С. 147–191.
4. *Музычук М. Е.* Подсхемы схемы Хэмминга // В сб.: Исследования по алгебраической теории комбинаторных объектов, ВНИИСИ, тр. семинара. — М., 1985. — С. 49–76.
5. *Погорелов Б. А., Пудовкина М. А.* Натуральные метрики и их свойства. Ч. 1. Подметрики и надметрики // Математические вопросы криптографии. — 2011. — Т. 2. Вып. 4. — С. 49–74.