Math-Net.Ru

Общероссийский математический портал

Ю. Н. Горчинский, О π -гомоморфизмах конечных много-
основных универсальных алгебр, *Дискрет. матем.*, 1999,
том 11, выпуск 2, 3–19

DOI: <https://doi.org/10.4213/dm372>

Использование Общероссийского математического портала Math-Net.Ru под-
разумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.84.234.179

26 апреля 2023 г., 12:57:40

УДК 519.7

О $\bar{\pi}$ -гомоморфизмах конечных многоосновных универсальных алгебр

© 1999 г.

Ю. Н. Горчинский

Вводятся и изучаются обобщения эндоморфизмов конечных многоосновных универсальных алгебр, определяемые путем замены тождественных соотношений на вероятностные. Доказывается аналог классификационной теоремы о гомоморфизмах.

1. Основные понятия

С формальной точки зрения понятие $\bar{\pi}$ -гомоморфизма многоосновной универсальной алгебры синтезирует в себе два фундаментальных математических объекта, алгебраическую операцию и вероятностную меру. По существу же, оно основывается на идее приближения, не чуждой и дискретной математике. Для того чтобы дать точное определение, мы здесь будем придерживаться терминологии теории многоосновных универсальных алгебр, использованной в [1]. Пусть $\mathcal{A} = (\mathcal{M}, \Sigma)$ — конечная многоосновная универсальная алгебра, $\mathcal{M}$ — семейство ее основных множеств, Σ — семейство ее операций (сигнатура), $\bar{\mathcal{A}} = (\bar{\mathcal{M}}, \bar{\Sigma})$ — равнотипная $\mathcal{A}$ многоосновная универсальная алгебра. Будем предполагать, что на множестве всех подмножеств множества

$$X_1 \times \dots \times X_n,$$

где

$$X_1 \times \dots \times X_n \xrightarrow{\omega} X_0, \quad X_i \in \mathcal{M}, \quad i = 0, 1, \dots, n, \quad \omega \in \Sigma,$$

задана вероятностная мера $\mathbf{P}^{(\omega)}$. Вероятностной мере $\mathbf{P}^{(\omega)}$ отвечают случайные переменные $\xi_i^{(\omega)}$, заданные на X_i , $i = 1, \dots, n$. Положим $\bar{\pi} = (\pi^{(\omega)})$, где $\pi^{(\omega)}$ — вещественные числа, $0 < \pi^{(\omega)} \leq 1$, $\omega \in \Sigma$.

Определение 1. Набор $\varphi_{\mathcal{A}} = (\varphi_X)_{X \in \mathcal{M}}$, где φ_X — отображение множества X в соответствующее основное множество алгебры $\bar{\mathcal{A}}$ называется $\bar{\pi}$ -гомоморфизмом $\mathcal{A}$ в $\bar{\mathcal{A}}$, если для любой операции $\omega \in \Sigma$, $X_1 \times \dots \times X_n \xrightarrow{\omega} X_0$, и случайных переменных $\xi_i^{(\omega)}$ основных множеств X_i , $i = 1, \dots, n$,

$$\mathbf{P}^{(\omega)}(\omega'((\xi_1^{(\omega)})^{\varphi_{X_1}}, \dots, (\xi_n^{(\omega)})^{\varphi_{X_n}}) = (\omega(\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)})^{\varphi_{X_0}}) \geq \pi^{(\omega)},$$

где $\omega' \in \bar{\Sigma}$ соответствует ω .

Напомним, что основные множества (операции) алгебры $\overline{\mathcal{A}}$, соответствующие основным множествам (операциям) алгебры $\mathcal{A}$, связаны с определением равнотипности этих алгебр. Очевидно, что $\bar{\pi}$ -гомоморфизм $\mathcal{A}$ в $\overline{\mathcal{A}}$ при $\pi^{(\omega)} = 1$ будет гомоморфизмом $\mathcal{A}$ в $\overline{\mathcal{A}}$.

Следует заметить, что в отличие от гомоморфизма, алгебра $\overline{\mathcal{A}}$, вообще говоря, не определяется однозначно алгеброй $\mathcal{A}$ и набором отображений $\varphi_{\mathcal{A}}$, входящем в определение 1.

Определение 2. Если $\pi^{(\omega)} = \pi$, $\omega \in \Sigma$, то $\bar{\pi}$ -гомоморфизм $\mathcal{A}$ в $\overline{\mathcal{A}}$ называется π -гомоморфизмом $\mathcal{A}$ в $\overline{\mathcal{A}}$.

Очевидно, что всякий $\bar{\pi}$ -гомоморфизм $\mathcal{A}$ в $\overline{\mathcal{A}}$ является π -гомоморфизмом $\mathcal{A}$ в $\overline{\mathcal{A}}$ при $\pi = \min_{\omega \in \Sigma} \pi^{(\omega)}$.

В литературе по теории групп встречались различные обобщения гомоморфизмов групп, аналогичные π -гомоморфизмам. Именно, рассматривались отображения φ группы G , для некоторых пар x, y элементов которой выполнено условие $(xy)^{\varphi} = x^{\varphi}y^{\varphi}$. Так, в [2–7] изучался случай, когда это соотношение имеет место для всех $x, y \in H$, а $x^{\varphi}, y^{\varphi} \in F$, где H и F — фиксированные подгруппы группы G . В [8] доказано, что если $(xy)^{\varphi} = x^{\varphi}y^{\varphi}$ для некоторых пар $x, y \in G$, а для остальных пар $(xy)^{\varphi} = y^{\varphi}x^{\varphi}$, то либо φ — гомоморфизм, либо φ — антигомоморфизм:

$$(xy)^{\varphi} = y^{\varphi}x^{\varphi}, \quad x, y \in G.$$

Статьи [9, 10] посвящены полугомоморфизмам, т. е. отображениям φ , удовлетворяющим тождеству

$$(xux)^{\varphi} = x^{\varphi}y^{\varphi}x^{\varphi}, \quad x, y \in G.$$

Нетрудно видеть, что полугомоморфизм группы G является аналогичным π -гомоморфизму обобщением гомоморфизма 3-группы, определенной группой G (см. [11]).

Понятие $\bar{\pi}$ -гомоморфизма представляет интерес для криптографии, об этом свидетельствует, например, работа [12], в которой вычислена вероятность p выполнения равенства дистрибутивности

$$(x + y) \cdot z = x \cdot z + y \cdot z$$

при равновероятном выборе тройки x, y, z элементов некоторой универсальной алгебры $\mathcal{A}$ с групповыми операциями $+$ и $\cdot$, рассматриваемой в качестве модели блочного шифра. Легко видеть, что p здесь является средним значением тех π_z , $z \in A$, для которых отображения

$$x \xrightarrow{\varphi_z} x \cdot z, \quad x \in \mathcal{A},$$

суть π_z -гомоморфизмы группы с операцией $+$ в себя. Заметим, что аналогичный результат получен в [12] и для левого равенства дистрибутивности

$$z \cdot (x + y) = z \cdot x + z \cdot y.$$

Определение 3. $\bar{\pi}$ -гомоморфизм (π -гомоморфизм) $\varphi_{\mathcal{A}} = (\varphi_X)_{X \in \mathcal{M}}$ алгебры $\mathcal{A}$ в алгебру $\overline{\mathcal{A}}$, где φ_X , $X \in \mathcal{M}$, — инъективные отображения, называется $\bar{\pi}$ -изоморфизмом (π -изоморфизмом) $\mathcal{A}$ в $\overline{\mathcal{A}}$.

Определение 4. $\bar{\pi}$ -гомоморфизм (π -гомоморфизм) алгебры $\mathcal{A}$ в алгебру $\mathcal{A}$ называется $\bar{\pi}$ -эндоморфизмом (π -эндоморфизмом) алгебры $\mathcal{A}$.

Определение 5. $\bar{\pi}$ -гомоморфизм (π -гомоморфизм) $\varphi_{\mathcal{A}} = (\varphi_X)_{X \in \mathcal{M}}$ алгебры $\mathcal{A}$ алгебру $\bar{\mathcal{A}}$, называется сюръективным, если отображения φ_X , $X \in \mathcal{M}$, являются сюръективными. Если $\varphi_{\mathcal{A}}$ — сюръективный $\bar{\pi}$ -гомоморфизм $\mathcal{A}$ в $\bar{\mathcal{A}}$, то алгебра $\mathcal{A}$ называется $\bar{\pi}$ -гомоморфным образом алгебры $\mathcal{A}$.

Определение 6. $\bar{\pi}$ -эндоморфизм (π -эндоморфизм) алгебры $\mathcal{A}$ в алгебру $\mathcal{A}$, являющийся сюръективным $\bar{\pi}$ -изоморфизмом (π -изоморфизмом) алгебры $\mathcal{A}$ называется $\bar{\pi}$ -автоморфизмом (π -автоморфизмом) алгебры $\mathcal{A}$.

2. Конструкция $\bar{\pi}$ -фактор-алгебр

Рассмотрим набор $\varepsilon_{\mathcal{A}} = (\varepsilon_X)_{X \in \mathcal{M}}$, где ε_X — произвольная эквивалентность на основном множестве X многоосновной универсальной алгебры $\mathcal{A}$. Исходя из $\varepsilon_{\mathcal{A}}$, определим для любой операции

$$\omega \in \Sigma, \quad X_1 \times \dots \times X_n \xrightarrow{\omega} X_0,$$

эквивалентность $\varepsilon_{\mathcal{A}}^{[\omega]}$ на множестве $X_1 \times \dots \times X_n = [\omega]$:

$$(x_1, \dots, x_n) \equiv (x'_1, \dots, x'_n) \pmod{\varepsilon_{\mathcal{A}}^{[\omega]}}, \quad x_i, x'_i \in X_i, \quad i = 1, \dots, n,$$

тогда и только тогда, когда

$$x_i \equiv x'_i \pmod{\varepsilon_{X_i}}, \quad i = 1, \dots, n.$$

Легко видеть, что определение эквивалентности $\varepsilon_{\mathcal{A}}^{[\omega]}$ корректно, так как соответствующее бинарное отношение является рефлексивным, симметричным и транзитивным.

Обозначим $K_1^{[\omega]}, \dots, K_{r^{[\omega]}}^{[\omega]}$ классы эквивалентности относительно $\varepsilon_{\mathcal{A}}^{[\omega]}$. На множестве $K_i^{[\omega]}$ определим следующим образом эквивалентность $\varepsilon_i^{[\omega]}$:

$$(x_1, \dots, x_n) \equiv (x'_1, \dots, x'_n) \pmod{\varepsilon_i^{[\omega]}}, \quad (x_1, \dots, x_n), (x'_1, \dots, x'_n) \in K_i^{[\omega]},$$

тогда и только тогда, когда

$$\omega(x_1, \dots, x_n) \equiv \omega(x'_1, \dots, x'_n) \pmod{\varepsilon_{X_0}}.$$

Очевидно, что бинарное отношение $\varepsilon_i^{[\omega]}$ действительно обладает рефлексивностью, симметричностью и транзитивностью.

Обозначим $K_{i1}^{(\omega)}, \dots, K_{it_i^{(\omega)}}^{(\omega)}$ классы эквивалентности $\varepsilon_i^{(\omega)}$.

Определение 7. Набор $\varepsilon_{\mathcal{A}}$ будем называть $\bar{\pi}$ -конгруэнцией на $\mathcal{A}$, если для любой операции $\omega \in \Sigma$ и любого i , $1 \leq i \leq r^{[\omega]}$, найдется такое $s_i^{(\omega)}$, $1 \leq s_i^{(\omega)} \leq t_i^{(\omega)}$, что

$$\sum_{i=1}^{r^{[\omega]}} \mathbf{P}^{(\omega)}(K_{is_i^{(\omega)}}^{(\omega)}) \geq \pi^{(\omega)}, \quad \omega \in \Sigma. \quad (1)$$

Пусть задана $\bar{\pi}$ -конгруэнция $\varepsilon_{\mathcal{A}} = (\varepsilon_X)_{X \in \mathcal{M}}$ на многоосновной универсальной алгебре $\mathcal{A} = (\mathcal{M}, \Sigma)$. Построим многоосновную универсальную алгебру $(\overline{\mathcal{M}}, \overline{\Sigma})$, называемую $\bar{\pi}$ -фактор-алгеброй алгебры $\mathcal{A}$ по $\bar{\pi}$ -конгруэнции $\varepsilon_{\mathcal{A}}$. Для этого положим

$$\overline{\mathcal{M}} = (X/\varepsilon_X)_{X \in \mathcal{M}}, \quad (2)$$

где X/ε_X — фактор-множество множества X по эквивалентности ε_X . Выберем произвольно и зафиксируем числа

$$s_i^{(\omega)}, \quad i = 1, \dots, t_i^{(\omega)}, \quad \omega \in \Sigma,$$

удовлетворяющие (1). Операции $\omega \in \Sigma$ поставим в соответствие операцию $\bar{\omega} \in \overline{\Sigma}$, определяемую так: если

$$X_1 \times \dots \times X_n \xrightarrow{\omega} X_0,$$

то

$$X_1/\varepsilon_{X_1} \times \dots \times X_n/\varepsilon_{X_n} \xrightarrow{\bar{\omega}} X_0/\varepsilon_{X_0},$$

и для произвольных $x_i \in X_i$, $i = 1, \dots, n$,

$$\bar{\omega}(x_1^{\varepsilon_{x_1}}, \dots, x_n^{\varepsilon_{x_n}}) = (\omega(\bar{x}_1, \dots, \bar{x}_n))^{\varepsilon_{x_0}}, \quad (3)$$

где, если $(x_1, \dots, x_n) \in K_j^{[\omega]}$, то $(\bar{x}_1, \dots, \bar{x}_n) \in K_{js_j^{(\omega)}}^{(\omega)}$.

Покажем, что это определение корректно, т.е. правая часть (3) зависит только от классов $x_1^{\varepsilon_{x_1}}, \dots, x_n^{\varepsilon_{x_n}}$. С этой целью предположим, что

$$x_i^{\varepsilon_{x_i}} = (x'_i)^{\varepsilon_{x_i}}, \quad i = 1, \dots, n.$$

Тогда

$$x_i \equiv x'_i \pmod{\varepsilon_{X_i}}, \quad i = 1, \dots, n. \quad (4)$$

Из (4) следует, что

$$(x_1, \dots, x_n) \equiv (x'_1, \dots, x'_n) \pmod{\varepsilon_{\mathcal{A}}^{[\omega]}}.$$

Поэтому

$$\omega(\bar{x}_1, \dots, \bar{x}_n) \equiv \omega(\bar{x}'_1, \dots, \bar{x}'_n) \pmod{\varepsilon_{X_0}},$$

откуда

$$(\omega(\bar{x}_1, \dots, \bar{x}_n))^{\varepsilon_{x_0}} = (\omega(\bar{x}'_1, \dots, \bar{x}'_n))^{\varepsilon_{x_0}}.$$

Этим корректность определения (3) доказана.

Теперь полагаем

$$\overline{\Sigma} = (\bar{\omega})_{\omega \in \Sigma}. \quad (5)$$

Равенствами (2) и (5) определена $\bar{\pi}$ -фактор-алгебра $(\mathcal{A}/\varepsilon_{\mathcal{A}})_{\bar{\Sigma}}$, где

$$\bar{s} = (s_i^{(\omega)})_{i=1}^{t_i^{(\omega)}}, \quad \omega \in \Sigma.$$

Следует подчеркнуть, что она зависит не только от $\bar{\pi}$ -конгруэнции $\varepsilon_{\mathcal{A}}$, но и от выбора чисел $s_i^{(\omega)}$, $i = 1, \dots, t_i^{(\omega)}$, $\omega \in \Sigma$, удовлетворяющих (1).

3. Описание $\bar{\pi}$ -гомоморфизмов

Пусть $\varepsilon_{\mathcal{A}} = (\varepsilon_X)_{X \in \mathcal{M}}$ — $\bar{\pi}$ -конгруэнция на многоосновной универсальной алгебре

$$\mathcal{A} = (\mathcal{M}, \Sigma), \quad \psi_{\mathcal{A}} = (\psi_X)_{X \in \mathcal{M}},$$

где ψ_X — отображение множества X на его фактор-множество X/ε_X , т. е.

$$x^{\psi_X} = x^{\varepsilon_X}, \quad X \in \mathcal{M}. \quad (6)$$

Тогда $\psi_{\mathcal{A}}$ представляет собой набор отображений основных множеств алгебры $\mathcal{A}$ на соответствующие основные множества произвольной $\bar{\pi}$ -фактор-алгебры $(\mathcal{A}/\varepsilon_{\mathcal{A}})_{\bar{s}}$.

Лемма 1. *Отображение $\psi_{\mathcal{A}}$ является сюръективным $\bar{\pi}$ -гомоморфизмом алгебры $\mathcal{A}$ в ее произвольную $\bar{\pi}$ -фактор-алгебру по $\bar{\pi}$ -конгруэнции $\varepsilon_{\mathcal{A}}$.*

Доказательство. Пусть

$$\omega \in \Sigma, \quad X_1 \times \dots \times X_n \xrightarrow{\omega} X_0, \quad x_i \in X_i, \quad i = 1, \dots, n.$$

Тогда в соответствии с (6)

$$\bar{\omega}(x_1^{\psi_{X_1}}, \dots, x_n^{\psi_{X_n}}) = \bar{\omega}(x_1^{\varepsilon_{X_1}}, \dots, x_n^{\varepsilon_{X_n}}). \quad (7)$$

Но согласно (3)

$$\bar{\omega}(\bar{x}_1^{\varepsilon_{X_1}}, \dots, \bar{x}_n^{\varepsilon_{X_n}}) = (\omega(\bar{x}_1, \dots, \bar{x}_n))^{\varepsilon_{X_0}}, \quad (8)$$

а согласно (6)

$$(\omega(\bar{x}_1, \dots, \bar{x}_n))^{\varepsilon_{X_0}} = (\omega(\bar{x}_1, \dots, \bar{x}_n))^{\psi_{X_0}}. \quad (9)$$

Из (7)–(9) следует, что

$$\bar{\omega}(\bar{x}_1^{\psi_{X_1}}, \dots, \bar{x}_n^{\psi_{X_n}}) = (\omega(\bar{x}_1, \dots, \bar{x}_n))^{\psi_{X_0}}. \quad (10)$$

В силу (10)

$$\begin{aligned} \mathbf{P}^{(\omega)}(\bar{\omega}((\xi_1^{(\omega)})^{\psi_{X_1}}, \dots, (\xi_n^{(\omega)})^{\psi_{X_n}})) &= (\omega(\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}))^{\psi_{X_0}} \\ &\geq \sum_{i=1}^{r^{[\omega]}} \mathbf{P}^{(\omega)}(K_{is_i^{(\omega)}}^{(\omega)}), \end{aligned} \quad (11)$$

где числа $s_i^{(\omega)}$, $i = 1, \dots, t_i^{(\omega)}$, $\omega \in \Sigma$, отвечают рассматриваемой $\bar{\pi}$ -фактор-алгебре $\mathcal{A}/\varepsilon_{\mathcal{A}}$. Пользуясь теперь (1), заключаем на основании (11), что

$$\mathbf{P}^{(\omega)}(\bar{\omega}((\xi_1^{(\omega)})^{\psi_{X_1}}, \dots, (\xi_n^{(\omega)})^{\psi_{X_n}})) = (\omega(\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}))^{\psi_{X_0}} \geq \pi^{(\omega)}.$$

Согласно определению 1 этим доказано, что $\psi_{\mathcal{A}}$ — $\bar{\pi}$ -гомоморфизм $\mathcal{A}$ в $(\mathcal{A}/\varepsilon_{\mathcal{A}})_{\bar{s}}$. Сюръективность этого гомоморфизма вытекает из того, что в силу (6) отображения ψ_X , $X \in \mathcal{M}$, сюръективны. Таким образом, лемма полностью доказана.

Мы будем называть $\bar{\pi}$ -гомоморфизм $\psi_{\mathcal{A}}$ алгебры $\mathcal{A}$ в произвольную $\bar{\pi}$ -фактор-алгебру $(\mathcal{A}/\varepsilon_{\mathcal{A}})_{\bar{s}}$ естественным. Таким образом, для каждой $\bar{\pi}$ -конгруэнции $\varepsilon_{\mathcal{A}}$ на алгебре $\mathcal{A}$ определены естественные $\bar{\pi}$ -гомоморфизмы алгебры $\mathcal{A}$ в фактор-алгебры $(\mathcal{A}/\varepsilon_{\mathcal{A}})_{\bar{s}}$.

Лемма 2. Пусть $\varphi_{\mathcal{A}} = (\varphi_X)_{X \in \mathcal{M}}$ — $\bar{\pi}$ -гомоморфизм алгебры $\mathcal{A}$ в алгебру $\overline{\mathcal{A}} = (\overline{\mathcal{M}}, \overline{\Sigma})$, $\varphi_{\overline{\mathcal{A}}} = (\varphi_{X'})_{X' \in \overline{\mathcal{M}}}$ — гомоморфизм алгебры $\overline{\mathcal{A}}$ в алгебру $\overline{\overline{\mathcal{A}}}$. Тогда

$$\varphi_{\mathcal{A}} \varphi_{\overline{\mathcal{A}}} = (\varphi_X \cdot \varphi_{X'})_{X \in \mathcal{M}}$$

— $\bar{\pi}$ -гомоморфизм алгебры $\mathcal{A}$ в алгебру $\overline{\overline{\mathcal{A}}}$.

Доказательство. Пусть $\omega \in \Sigma$,

$$X_1 \times X_2 \times \dots \times X_n \xrightarrow{\omega} X_0, \quad \omega \in \Sigma,$$

$$X'_1 \times X'_2 \times \dots \times X'_n \xrightarrow{\omega'} X'_0, \quad \omega' \in \overline{\Sigma},$$

причем ω' соответствует ω , а ω'' соответствует ω' . Тогда, так как $\varphi_{\overline{\mathcal{A}}}$ — гомоморфизм $\overline{\mathcal{A}}$ в $\overline{\overline{\mathcal{A}}}$, для любых $x_i \in X_i$, $i = 1, \dots, n$,

$$\begin{aligned} \omega''(x_1^{\varphi_{X_1} \varphi_{X'_1}}, \dots, x_n^{\varphi_{X_n} \varphi_{X'_n}}) &= \omega''((x_1^{\varphi_{X_1}})^{\varphi_{X'_1}}, \dots, (x_n^{\varphi_{X_n}})^{\varphi_{X'_n}}) \\ &= (\omega'(x_1^{\varphi_{X_1}}, \dots, x_n^{\varphi_{X_n}}))^{\varphi_{X'_0}}. \end{aligned} \quad (12)$$

В силу (12)

$$\begin{aligned} \{\omega'((\xi_1^{(\omega)})^{\psi_{X_1}}, \dots, (\xi_n^{(\omega)})^{\psi_{X_n}}) &= (\omega(\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}))^{\psi_{X_0}}\} \\ \subset \{\omega''((\xi_1^{(\omega)})^{\psi_{X_1} \psi_{X'_1}}, \dots, (\xi_n^{(\omega)})^{\psi_{X_n} \psi_{X'_n}}) &= (\omega(\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}))^{\psi_{X_0} \psi_{X'_0}}\}, \end{aligned}$$

откуда получаем неравенство

$$\begin{aligned} \mathbf{P}^{(\omega)}(\omega''((\xi_1^{(\omega)})^{\psi_{X_1} \psi_{X'_1}}, \dots, (\xi_n^{(\omega)})^{\psi_{X_n} \psi_{X'_n}}) &= (\omega(\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}))^{\psi_{X_0} \psi_{X'_0}}) \\ &\geq \mathbf{P}^{(\omega)}(\omega'((\xi_1^{(\omega)})^{\psi_{X_1}}, \dots, (\xi_n^{(\omega)})^{\psi_{X_n}}) = (\omega(\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}))^{\psi_{X_0}}). \end{aligned} \quad (13)$$

Но так как $\psi_{\mathcal{A}}$ — $\bar{\pi}$ -гомоморфизм $\mathcal{A}$ в $\overline{\mathcal{A}}$, то

$$\mathbf{P}^{(\omega)}(\omega'((\xi_1^{(\omega)})^{\psi_{X_1}}, \dots, (\xi_n^{(\omega)})^{\psi_{X_n}}) = (\omega(\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}))^{\psi_{X_0}}) \geq \pi^{(\omega)}. \quad (14)$$

Из (13) и (14) следует, что при $\omega \in \Sigma$

$$\mathbf{P}^{(\omega)}(\omega''((\xi_1^{(\omega)})^{\psi_{X_1} \psi_{X'_1}}, \dots, (\xi_n^{(\omega)})^{\psi_{X_n} \psi_{X'_n}}) = (\omega(\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}))^{\psi_{X_0} \psi_{X'_0}}) \geq \pi^{(\omega)}. \quad (15)$$

Неравенство (15) показывает в соответствии с определением 1, что $\varphi_{\mathcal{A}} \varphi_{\overline{\mathcal{A}}}$ есть $\bar{\pi}$ -гомоморфизм $\mathcal{A}$ в $\overline{\overline{\mathcal{A}}}$. Этим лемма 2 доказана.

Теорема 1 (о $\bar{\pi}$ -гомоморфизмах). Набор $\varphi_{\mathcal{A}} = (\varphi_X)_{X \in \mathcal{M}}$ будет $\bar{\pi}$ -гомоморфизмом многоосновной универсальной алгебры $\mathcal{A}$ в равнотипную алгебру $\overline{\mathcal{A}}$, удовлетворяющую условию

$$\begin{aligned} \mathbf{P}^{(\omega)}(x_1^{\varphi_{X_1} \varphi_{X'_1}^{-1}} \times \dots \times x_n^{\varphi_{X_n} \varphi_{X'_n}^{-1}}) &> 1 - \pi^{(\omega)}, \\ x_i \in X_i, \quad i = 1, \dots, n, \quad \omega \in \Sigma, \quad X_1 \times \dots \times X_n &\xrightarrow{\omega} X_0, \end{aligned} \quad (16)$$

тогда и только тогда, когда

$$\varphi_{\mathcal{A}} = \psi_{\mathcal{A}} \cdot \mu_{\mathcal{A}} / \varepsilon_{\mathcal{A}},$$

где $\psi_{\mathcal{A}}$ — единственный $\bar{\pi}$ -гомоморфизм $\mathcal{A}$ в некоторую фактор-алгебру $(\mathcal{A} / \varepsilon_{\mathcal{A}})_{\bar{\pi}}$ по $\bar{\pi}$ -конгруэнции $\varepsilon_{\mathcal{A}}$, удовлетворяющей условию

$$\begin{aligned} \mathbf{P}^{(\omega)}(x_1^{\varepsilon_{\mathcal{A}}} \times \dots \times x_n^{\varepsilon_{\mathcal{A}}}) &> 1 - \pi^{(\omega)}, \\ x_i &\in X_i, \quad i = 1, \dots, n, \quad \omega \in \Sigma, \quad X_1 \times \dots \times X_n \xrightarrow{\omega} X_0, \end{aligned} \quad (17)$$

$\mu_{\mathcal{A}} / \varepsilon_{\mathcal{A}}$ — изоморфизм $\mathcal{A} / \varepsilon_{\mathcal{A}}$ в $\overline{\mathcal{A}}$.

Доказательство. Пусть $\varphi_{\mathcal{A}}$ — $\bar{\pi}$ -гомоморфизм $\mathcal{A}$ в $\overline{\mathcal{A}}$, удовлетворяющий условию (16). Положим

$$\varepsilon_X = \text{Ker}_{\varphi_X}, \quad X \in \mathcal{M}.$$

Покажем, что

$$\varepsilon_{\mathcal{A}} = (\varepsilon_X)_{X \in \mathcal{M}}$$

— $\bar{\pi}$ -конгруэнция на $\mathcal{A}$, удовлетворяющая условию (17). Для этого обозначим через $H^{(\omega)}$ множество всех $(x_1, \dots, x_n)$, $x_i \in X_i$, $i = 1, \dots, n$, где $\omega \in \Sigma$, $X_1 \times \dots \times X_n \xrightarrow{\omega} X_0$, для которых

$$\omega'(x_1^{\varphi_{X_1}}, \dots, x_n^{\varphi_{X_n}}) = (\omega(x_1, \dots, x_n))^{\varphi_{X_0}},$$

где ω' — операция алгебры $\overline{\mathcal{A}}$, соответствующая ω .

Допустим, что для некоторого j , $1 \leq j \leq r^{[\omega]}$, выполняется равенство

$$K_j^{[\omega]} \cap H^{(\omega)} = \emptyset. \quad (18)$$

Так как по определению ε_{X_i} выполнено равенство

$$x_i^{\varepsilon_{X_i}} = x_i^{\varphi_{X_i} \varphi_{X_i}^{-1}},$$

условие (16) влечет за собой условие (17). Поэтому, учитывая, что

$$K_j^{[\omega]} = x_1^{\varepsilon_{X_1}} \times \dots \times x_n^{\varepsilon_{X_n}}$$

для некоторых $x_i \in X_i$, $i = 1, \dots, n$, получим неравенство

$$\mathbf{P}^{(\omega)}(K_j^{[\omega]}) = \mathbf{P}^{(\omega)}(x_1^{\varepsilon_{X_1}} \times \dots \times x_n^{\varepsilon_{X_n}}) > 1 - \pi^{(\omega)}. \quad (19)$$

По формуле полной вероятности

$$\mathbf{P}^{(\omega)}(H^{(\omega)}) = \mathbf{P}^{(\omega)}(K_j^{[\omega]} \cap H^{(\omega)}) + \mathbf{P}^{(\omega)}(\overline{K_j^{[\omega]}} \cap H^{(\omega)}), \quad (20)$$

где $\overline{K_j^{[\omega]}}$ — дополнение подмножества $K_j^{[\omega]}$ в множестве $X_1 \times \dots \times X_n$. Но, ввиду (18),

$$\mathbf{P}^{(\omega)}(K_j^{[\omega]} \cap H^{(\omega)}) = 0. \quad (21)$$

Из (20) и (21) получаем, что

$$\mathbf{P}^{(\omega)}(H^{(\omega)}) = \mathbf{P}^{(\omega)}(\overline{K}_j^{[\omega]} \cap H^{(\omega)}) \leq \mathbf{P}^{(\omega)}(\overline{K}_j^{[\omega]}). \quad (22)$$

С другой стороны, согласно (19)

$$\mathbf{P}^{(\omega)}(\overline{K}_j^{[\omega]}) = 1 - \mathbf{P}^{(\omega)}(K_j^{[\omega]}) < \pi^{(\omega)}. \quad (23)$$

Учитывая (23), на основании (22) приходим к неравенству

$$\mathbf{P}^{(\omega)}(H^{(\omega)}) < \pi^{(\omega)},$$

которое в соответствии с определением $H^{(\omega)}$ противоречит тому, что $\varphi_{\mathcal{A}}$ — $\bar{\pi}$ -гомоморфизм $\mathcal{A}$ в $\overline{\mathcal{A}}$. Следовательно, допущение (18) неверно и, значит,

$$K_i^{[\omega]} \cap H^{(\omega)} \neq \emptyset, \quad \omega \in \Sigma, \quad i = 1, \dots, r^{[\omega]}. \quad (24)$$

Пусть теперь

$$\begin{aligned} (x_1, \dots, x_n) &\in K_i^{[\omega]} \cap H^{(\omega)}, \\ (x'_1, \dots, x'_n) &\in K_i^{[\omega]} \cap H^{(\omega)}. \end{aligned} \quad (25)$$

Тогда по определению $\varepsilon_{\mathcal{A}}^{[\omega]}$

$$x_i \equiv x'_i \pmod{\varepsilon_{X_i}},$$

откуда, учитывая, что

$$\varepsilon_{X_i} = \text{Ker } \varphi_{X_i}, \quad i = 1, \dots, n,$$

получаем, что

$$x_i^{\varphi_{X_i}} = (x'_i)^{\varphi_{X_i}}, \quad i = 1, \dots, n. \quad (26)$$

Ввиду (26)

$$\omega'(x_1^{\varphi_{X_1}}, \dots, x_n^{\varphi_{X_n}}) = \omega'((x'_1)^{\varphi_{X_1}}, \dots, (x'_n)^{\varphi_{X_n}}). \quad (27)$$

Но из (25) следует, что

$$\omega'(x_1^{\varphi_{X_1}}, \dots, x_n^{\varphi_{X_n}}) = (\omega(x_1, \dots, x_n))^{\varphi_{X_0}}, \quad (28)$$

$$\omega'((x'_1)^{\varphi_{X_1}}, \dots, (x'_n)^{\varphi_{X_n}}) = (\omega(x'_1, \dots, x'_n))^{\varphi_{X_0}}. \quad (29)$$

Согласно (27) левые части (28) и (29) совпадают, поэтому совпадают и их правые части, так что

$$(\omega(x_1, \dots, x_n))^{\varphi_{X_0}} = (\omega(x'_1, \dots, x'_n))^{\varphi_{X_0}},$$

откуда, учитывая, что $\varepsilon_{X_0} = \text{Ker } \varphi_{X_0}$, получаем, что

$$\omega(x_1, \dots, x_n) \equiv \omega(x'_1, \dots, x'_n) \pmod{\varepsilon_{X_0}}. \quad (30)$$

Сравнение (30) показывает, ввиду (25), что

$$(x_1, \dots, x_n) \equiv (x'_1, \dots, x'_n) \pmod{\varepsilon_i^{[\omega]}}. \quad (31)$$

В силу (31) найдется такое $1 \leq s_i^{(\omega)} \leq t_i^{(\omega)}$, что

$$(x_1, \dots, x_n) \in K_{is_i^{(\omega)}}^{(\omega)}, \quad (x'_1, \dots, x'_n) \in K_{is_i^{(\omega)}}^{(\omega)}. \quad (32)$$

Отсюда, ввиду произвольности выбора $(x_1, \dots, x_n)$ и $(x'_1, \dots, x'_n)$ из $K_i^{(\omega)} \cap H^{(\omega)}$ следует, что

$$K_i^{[\omega]} \cap H^{(\omega)} \subset K_{is_i^{(\omega)}}^{(\omega)}, \quad \omega \in \Sigma, \quad i = 1, \dots, r^{[\omega]}. \quad (33)$$

Пользуясь включениями (33), получаем, что

$$\mathbf{P}^{(\omega)}(K_{is_i^{(\omega)}}^{(\omega)}) \geq \mathbf{P}^{(\omega)}(K_i^{[\omega]} \cap H^{(\omega)}), \quad \omega \in \Sigma, \quad i = 1, \dots, r^{[\omega]}. \quad (34)$$

Просуммировав теперь неравенства (34), приходим к неравенству

$$\sum_{i=1}^{r^{[\omega]}} \mathbf{P}^{(\omega)}(K_{is_i^{(\omega)}}^{(\omega)}) \geq \sum_{i=1}^{r^{[\omega]}} \mathbf{P}^{(\omega)}(K_i^{[\omega]} \cap H^{(\omega)}), \quad \omega \in \Sigma. \quad (35)$$

Но

$$\sum_{i=1}^{r^{[\omega]}} \mathbf{P}^{(\omega)}(K_i^{[\omega]} \cap H^{(\omega)}) = \mathbf{P}^{(\omega)}(H^{(\omega)}), \quad \omega \in \Sigma, \quad (36)$$

а так как $\varphi_{\mathcal{A}} - \bar{\pi}$ -гомоморфизм $\mathcal{A}$ в $\overline{\mathcal{A}}$, то

$$\mathbf{P}^{(\omega)}(H^{(\omega)}) \geq \pi^{(\omega)}, \quad \omega \in \Sigma. \quad (37)$$

Принимая во внимание (36) и (37), на основании (35) заключаем, что

$$\sum_{i=1}^{r^{[\omega]}} \mathbf{P}^{(\omega)}(K_{is_i^{(\omega)}}^{(\omega)}) \geq \pi^{(\omega)}, \quad \omega \in \Sigma.$$

Следовательно, $\varepsilon_{\mathcal{A}} - \bar{\pi}$ -конгруэнция на $\mathcal{A}$. При этом условие (17) непосредственно вытекает из (16).

Рассмотрим $\bar{\pi}$ -фактор-алгебру $(\mathcal{A}/\varepsilon_{\mathcal{A}})_{\bar{s}}$, соответствующую выбору чисел $s_i^{(\omega)}$, $i = 1, \dots, r^{[\omega]}$, в (32). В этом случае в силу (24) и (33) мы можем взять в (3) для $(x_1, \dots, x_n) \in K_j^{[\omega]}$

$$(\bar{x}_1, \dots, \bar{x}_n) \in K_j^{[\omega]} \cap H^{(\omega)}, \quad \omega \in \Sigma. \quad (38)$$

Положим теперь

$$(x^{\varepsilon_x})^{\mu_X/\varepsilon_X} = x^{\varphi_X}, \quad X \in \mathcal{M}. \quad (39)$$

Так как

$$\varepsilon_X = \text{Ker } \varphi_X, \quad X \in \mathcal{M},$$

равенства (39) определяют инъективные отображения

$$X/\varepsilon_X \xrightarrow{\mu_X/\varepsilon_X} X',$$

где X' — основное множество алгебры $\overline{\mathcal{A}}$, соответствующее X . Используя (39), (28), (3), получаем, что

$$\begin{aligned} \omega'((x_1^{\varepsilon_{X_1}})^{\mu_{X_1}/\varepsilon_{X_1}}, \dots, (x_n^{\varepsilon_{X_n}})^{\mu_{X_n}/\varepsilon_{X_n}}) &= \omega'((\bar{x}_1^{\varepsilon_{X_1}})^{\mu_{X_1}/\varepsilon_{X_1}}, \dots, (\bar{x}_n^{\varepsilon_{X_n}})^{\mu_{X_n}/\varepsilon_{X_n}}) \\ &= \omega'(\bar{x}_1^{\varphi_{X_1}}, \dots, \bar{x}_n^{\varphi_{X_n}}) = (\omega(\bar{x}_1, \dots, \bar{x}_n))^{\varphi_{X_0}} \\ &= ((\omega(\bar{x}_1, \dots, \bar{x}_n))^{\varepsilon_{X_0}})^{\mu_{X_0}/\varepsilon_{X_0}} \\ &= (\bar{\omega}(x_1^{\varepsilon_{X_1}}, \dots, x_n^{\varepsilon_{X_n}}))^{\mu_{X_0}/\varepsilon_{X_0}}. \end{aligned}$$

Следовательно,

$$\mu_{\mathcal{A}/\varepsilon_{\mathcal{A}}} = (\mu_X/\varepsilon_X)_{X \in \mathcal{M}}$$

— изоморфизм $(\mathcal{A}/\varepsilon_{\mathcal{A}})_{\bar{s}}$ в $\overline{\mathcal{A}}$. Наконец, из (39) и (6) следует, что

$$\psi_{\mathcal{A}} \cdot \mu_{\mathcal{A}}/\varepsilon_{\mathcal{A}} = \varphi_{\mathcal{A}},$$

где $\psi_{\mathcal{A}}$ — естественный гомоморфизм $\mathcal{A}$ в $(\mathcal{A}/\varepsilon_{\mathcal{A}})_{\bar{s}}$. Этим необходимость условия $\varphi_{\mathcal{A}} = \psi_{\mathcal{A}} \cdot \mu_{\mathcal{A}}/\varepsilon_{\mathcal{A}}$ теоремы доказана.

Достаточность этого условия следует из лемм 1 и 2, так как условие (16) вытекает непосредственно из (17). Таким образом, теорема доказана.

Частным случаем доказанной теоремы о $\bar{\pi}$ -гомоморфизмах является теорема о гомоморфизмах многоосновных универсальных алгебр (см. [13]).

Следует отметить, что в доказательстве теоремы 1 определены $\bar{\pi}$ -конгруэнции, о которых говорится в формулировке теоремы. Именно, $\bar{\pi}$ -гомоморфизму

$$\varphi_{\mathcal{A}} = (\varphi_X)_{X \in \mathcal{M}},$$

удовлетворяющему (16), отвечает $\bar{\pi}$ -конгруэнция

$$\varepsilon_{\mathcal{A}} = (\varepsilon_X)_{X \in \mathcal{M}},$$

удовлетворяющая (17). Здесь

$$\varepsilon_X = \text{Ker } \varphi_X, \quad X \in \mathcal{M}.$$

Эту $\bar{\pi}$ -конгруэнцию будем называть ядром $\bar{\pi}$ -гомоморфизма $\varphi_{\mathcal{A}}$ и обозначать $\text{Ker } \varphi_{\mathcal{A}}$. Таким образом, устанавливается соответствие между $\bar{\pi}$ -гомоморфизмами, удовлетворяющими условию (16), и их ядрами — $\bar{\pi}$ -конгруэнциями, удовлетворяющими условию (17).

Так как изоморфизм $\mu_{\mathcal{A}}/\varepsilon_{\mathcal{A}}$ алгебры $(\mathcal{A}/\varepsilon_{\mathcal{A}})_{\bar{s}}$ в алгебру $\overline{\mathcal{A}}$ является сюръективным изоморфизмом алгебры в подалгебру, а естественный изоморфизм также сюръективен в смысле определения 5, из теоремы о $\bar{\pi}$ -гомоморфизмах вытекает следующее утверждение.

Следствие 1. *Всякий $\bar{\pi}$ -гомоморфизм многоосновной универсальной алгебры $\mathcal{A}$ в равнотипную алгебру $\overline{\mathcal{A}}$, удовлетворяющий условию (16), является сюръективным $\bar{\pi}$ -гомоморфизмом алгебры $\mathcal{A}$ в подалгебру алгебры $\overline{\mathcal{A}}$.*

Этим утверждением $\bar{\pi}$ -гомоморфизмы, удовлетворяющие условию (16), сводятся к сюръективным $\bar{\pi}$ -гомоморфизмам.

Следствие 2. *Всякий $\bar{\pi}$ -гомоморфный образ многоосновной универсальной алгебры $\mathcal{A}$, удовлетворяющий условию (16), изоморфен $\bar{\pi}$ -фактор-алгебре алгебры $\mathcal{A}$.*

Действительно, если $\varphi_{\mathcal{A}}$ — сюръективный $\bar{\pi}$ -гомоморфизм, то и изоморфизм $\mu_{\mathcal{A}}/\varepsilon_{\mathcal{A}}$ также сюръективен.

В общем случае произвольного $\bar{\pi}$ -гомоморфизма алгебры $\mathcal{A}$ в $\overline{\mathcal{A}}$

$$\varphi_{\mathcal{A}} = (\varphi_X)_{X \in \mathcal{M}}$$

мы будем называть его ядром

$$\text{Ker } \varphi_{\mathcal{A}} = (\text{Ker } \varphi_X)_{X \in \mathcal{M}}.$$

Следствие 3. *Для того чтобы*

$$\varepsilon_{\mathcal{A}} = (\varepsilon_X)_{X \in \mathcal{M}},$$

где ε_X — эквивалентность на X , было ядром некоторого $\bar{\pi}$ -гомоморфизма алгебры $\mathcal{A}$ в равнотипную алгебру, необходимо и достаточно, чтобы $\varepsilon_{\mathcal{A}}$ было $\bar{\pi}$ -конгруэнцией на $\mathcal{A}$.

Доказательство. Заметим, что при выводе формул (35)–(37) не использовалось условие (16). Поэтому ядро $\bar{\pi}$ -гомоморфизма алгебры $\mathcal{A}$ в равнотипную алгебру является $\bar{\pi}$ -конгруэнцией на $\mathcal{A}$. С другой стороны, всякая $\bar{\pi}$ -конгруэнция на $\mathcal{A}$ является, согласно лемме 1, ядром естественного $\bar{\pi}$ -гомоморфизма алгебры $\mathcal{A}$ в ее произвольную фактор-алгебру по этой $\bar{\pi}$ -конгруэнции. Этим следствие 3 доказано.

Доказанным утверждением описаны ядра всех $\bar{\pi}$ -гомоморфизмов алгебры $\mathcal{A}$ в равнотипные алгебры: это $\bar{\pi}$ -конгруэнции на $\mathcal{A}$ и только они. Однако данное описание, конечно, не дает описания $\bar{\pi}$ -гомоморфизмов алгебры $\mathcal{A}$ в равнотипные алгебры, содержащегося в теореме о $\bar{\pi}$ -гомоморфизмах. Следует подчеркнуть, что в этой теореме описываются не все $\bar{\pi}$ -гомоморфизмы, а только удовлетворяющие условию (16), которое при доказательстве (24) и тем самым (38) существенно используется.

4. Связь $\bar{\pi}$ -гомоморфизмов со случайными отображениями и стохастическими алгебрами

Пусть $\varepsilon_{\mathcal{A}} = (\varepsilon_X)_{X \in \mathcal{M}}$, ε_X — произвольная эквивалентность на множестве X . Поставим в соответствие операции $\omega \in \Sigma$, $X_1 \times \dots \times X_n \xrightarrow{\omega} X_0$, случайное отображение

$$X_1/\varepsilon_{X_1} \times \dots \times X_n/\varepsilon_{X_n} \xrightarrow{\tilde{\omega}} X_0/\varepsilon_{X_0},$$

для которого

$$\begin{aligned} \mathbf{P}(\tilde{\omega}(e_1, \dots, e_n) = e_0) &= \mathbf{P}^{(\omega)}(\omega(\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}) \in e_0 \mid \xi_1^{(\omega)} \in e_1, \dots, \xi_n^{(\omega)} \in e_n), \\ &e_i \in X_i/\varepsilon_{X_i}, \quad i = 1, \dots, n. \end{aligned} \quad (40)$$

При этом мы предполагаем, что

$$\mathbf{P}^{(\omega)}(\xi_1^{(\omega)} \in e_1, \dots, \xi_n^{(\omega)} \in e_n) > 0, \quad e_i \in X_i/\varepsilon_{X_i}, \quad i = 1, \dots, n.$$

Следующая теорема дает в терминах случайного отображения $\tilde{\omega}$ необходимые и достаточные условия для того, чтобы $\varepsilon_{\mathcal{A}}$ было $\bar{\pi}$ -конгруэнцией на $\mathcal{A}$.

Теорема 2. *Эквивалентность $\varepsilon_{\mathcal{A}}$ есть $\bar{\pi}$ -конгруэнция на $\mathcal{A}$ тогда и только тогда, когда выполнены неравенства*

$$\begin{aligned} & \sum_{e_i \in X_1/\varepsilon_{X_1}} \dots \sum_{e_n \in X_n/\varepsilon_{X_n}} \mathbf{P}^{(\omega)}(\xi_1^{(\omega)} \in e_1, \dots, \xi_n^{(\omega)} \in e_n) \\ & \times \max_{e_0 \in X_0/\varepsilon_{X_0}} \mathbf{P}(\tilde{\omega}(e_1, \dots, e_n) = e_0) \geq \pi^{(\omega)}, \quad \omega \in \Sigma, \quad X_1 \times \dots \times X_n \xrightarrow{\omega} X_0. \end{aligned}$$

Доказательство. Рассмотрим класс $K_i^{[\omega]}$ эквивалентности $\varepsilon_{\mathcal{A}}^{[\omega]}$, определенный во втором параграфе, $1 \leq i \leq r^{[\omega]}$, $\omega \in \Sigma$. Ему отвечает некоторое $e_i \in X_i/\varepsilon_{X_i}$, $i = 1, \dots, n$, такое, что

$$K_i^{[\omega]} = e_1 \times \dots \times e_n. \quad (41)$$

Наоборот, если e_j в (41) пробегает X_j/ε_{X_j} , $j = 1, \dots, n$, то i в левой части (41) пробегает все числа от 1 до $r^{[\omega]}$.

Далее, имеется взаимно однозначное соответствие между X_0/ε_{X_0} и $K_i^{[\omega]}/\varepsilon_i^{[\omega]}$, где эквивалентность $e_i^{[\omega]}$ определена во втором параграфе, так что, если классу $K_{ij}^{(\omega)}$ отвечает $e_0 \in X_0/\varepsilon_{X_0}$, то тогда и только тогда

$$(x_1, \dots, x_n) \in K_{ij}^{(\omega)}, \quad x_1 \in X_1, \dots, x_n \in X_n,$$

когда

$$x_1 \in e_1, \dots, x_n \in e_n, \quad \omega(x_1, \dots, x_n) \in e_0^{(j)}, \quad j = 1, \dots, t_i^{(\omega)}.$$

Следовательно,

$$\mathbf{P}^{(\omega)}(K_{ij}^{(\omega)}) = \mathbf{P}^{(\omega)}(\xi_1^{(\omega)} \in e_1, \dots, \xi_n^{(\omega)} \in e_n, \omega(\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}) \in e_0). \quad (42)$$

Согласно (40) и (42)

$$\mathbf{P}^{(\omega)}(K_{ij}^{(\omega)}) = \mathbf{P}^{(\omega)}(\xi_1^{(\omega)} \in e_1, \dots, \xi_n^{(\omega)} \in e_n) \mathbf{P}(\tilde{\omega}(e_1, \dots, e_n) = e_0). \quad (43)$$

Пусть теперь $\varepsilon_{\mathcal{A}}$ — $\bar{\pi}$ -конгруэнция на $\mathcal{A}$. Тогда, согласно определению 7, выполнены неравенства (1), откуда, ввиду (43), для любых

$$e_1 \in X_1/\varepsilon_{X_1}, \dots, e_n \in X_n/\varepsilon_{X_n}$$

найдется такой класс $e_0^{(e_1, \dots, e_n)} \in X_0/\varepsilon_{X_0}$, что

$$\begin{aligned} & \sum_{e_1 \in X_1/\varepsilon_{X_1}} \dots \sum_{e_n \in X_n/\varepsilon_{X_n}} \mathbf{P}^{(\omega)}(\xi_1^{(\omega)} \in e_1, \dots, \xi_n^{(\omega)} \in e_n) \\ & \times \mathbf{P}(\tilde{\omega}(e_1, \dots, e_n) = e_0^{(e_1, \dots, e_n)}) \geq \pi^{(\omega)}, \quad \omega \in \Sigma. \end{aligned} \quad (44)$$

С другой стороны,

$$\begin{aligned} \sum_{e_1 \in X_1/\varepsilon_{X_1}} \dots \sum_{e_n \in X_n/\varepsilon_{X_n}} \mathbf{P}^{(\omega)}(\xi_1^{(\omega)} \in e_1, \dots, \xi_n^{(\omega)} \in e_n) \max_{e_0 \in X_0/\varepsilon_{X_0}} \mathbf{P}(\tilde{\omega}(e_1, \dots, e_n) = e_0) \\ \geq \sum_{e_1 \in X_1/\varepsilon_{X_1}} \dots \sum_{e_n \in X_n/\varepsilon_{X_n}} \mathbf{P}^{(\omega)}(\xi_1^{(\omega)} \in e_1, \dots, \xi_n^{(\omega)} \in e_n) \\ \times \mathbf{P}(\tilde{\omega}(e_1, \dots, e_n) = e_0^{(e_1, \dots, e_n)}). \end{aligned} \quad (45)$$

Необходимость условий теоремы 2 теперь следует из (44) и (45).

Пусть, наоборот, условия теоремы 2 выполнены. Тогда, полагая

$$\max_{e_0 \in X_0/\varepsilon_{X_0}} \mathbf{P}(\tilde{\omega}(e_1, \dots, e_n) = e_0) = \mathbf{P}(\tilde{\omega}(e_1, \dots, e_n) = e_0^{(e_1, \dots, e_n)}),$$

$e_i \in X_i/\varepsilon_{X_i}$, $i = 1, \dots, n$, мы получим неравенства (44), откуда, ввиду (43), следуют неравенства (1).

Согласно определению (7), это означает, что $\varepsilon_{\mathcal{A}}$ — $\bar{\pi}$ -конгруэнция на $\mathcal{A}$. Этим теорема полностью доказана.

Введем теперь стохастическую алгебру (см. [14])

$$S(\mathcal{A}, \varepsilon_{\mathcal{A}}, (\mathbf{P}^{(\omega)})_{\omega \in \Sigma})$$

со стохастическим базисом

$$\mathcal{E} = (X/\varepsilon_X)_{X \in \mathcal{M}}$$

и структурными константами

$$P_{e_1, \dots, e_n}^{(\omega^*)}(e_0) = \mathbf{P}(\tilde{\omega}(e_1, \dots, e_n) = e_0), \quad e_i \in X_i/\varepsilon_{X_i}, \quad i = 1, \dots, n, \quad \omega \in \Sigma, \quad (46)$$

где ω^* — операция векторного умножения, отвечающая $\omega \in \Sigma$.

Рассмотрим векторы

$$x_i^{(\omega)}, \quad i = 1, \dots, n, \quad \omega \in \Sigma, \quad X_1 \times \dots \times X_n \xrightarrow{\omega} X_0,$$

заданные следующими разложениями по базисам, соответственно, X_i/ε_{X_i} , $i = 1, \dots, n$:

$$x_i^{(\omega)} = \sum_{e_i \in X_i/\varepsilon_{X_i}} \mathbf{P}^{(\omega)}(\xi_i^{(\omega)} \in e_i) e_i, \quad (47)$$

($\mathbf{P}^{(\omega)}(\xi_i^{(\omega)} \in e_i)$ — координата разложения при базисном векторе e_i).

Вектор $\omega^*(x_1^{(\omega)}, \dots, x_n^{(\omega)})$ также разложим по базису X_0/ε_{X_0} :

$$\omega^*(x_1^{(\omega)}, \dots, x_n^{(\omega)}) = \sum_{e_0 \in X_0/\varepsilon_{X_0}} \nu^{(\omega)}(e_0) e_0, \quad (48)$$

($\nu^{(\omega)}(e_0)$ — координата разложения при базисном векторе e_0).

Теперь мы можем вывести следствие из теоремы 2, выражающее в терминах стохастической алгебры $S(\mathcal{A}, \varepsilon_{\mathcal{A}}, (\mathbf{P}^{(\omega)})_{\omega \in \Sigma})$ условия того, что $\varepsilon_{\mathcal{A}}$ является конгруэнцией на $\mathcal{A}$, если $\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}$ независимы.

Следствие 4. Пусть $\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}$ — независимы в совокупности и для некоторого $e_0 \in X_0/\varepsilon_{X_0}$ выполнено неравенство

$$\nu^{(\omega)}(e_0) \geq \pi^{(\omega)}$$

при любом $\omega \in \Sigma$, $X_1 \times \dots \times X_n \xrightarrow{\omega} X_0$. Тогда $\varepsilon_{\mathcal{A}}$ — $\bar{\pi}$ -конгруэнция на $\mathcal{A}$.

Доказательство. Предположим, что условия следствия 4 выполнены. Тогда, ввиду независимости $\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}$ выполнено равенство

$$\mathbf{P}^{(\omega)}(\xi_1^{(\omega)} \in e_1, \dots, \xi_n^{(\omega)} \in e_n) = \prod_{i=1}^n \mathbf{P}^{(\omega)}(\xi_i^{(\omega)} \in e_i), \quad (49)$$

$e_i \in X_i/\varepsilon_{X_i}$, $i = 1, \dots, n$. Согласно формуле, приведенной в [6], для векторов (47)

$$\begin{aligned} & \omega^*(x_1^{(\omega)}, \dots, x_n^{(\omega)}) \\ &= \sum_{\tilde{e}_0 \in X_0/\varepsilon_{X_0}} \left(\sum_{e_1 \in X_1/\varepsilon_{X_1}} \dots \sum_{e_n \in X_n/\varepsilon_{X_n}} \prod_{i=1}^n \mathbf{P}^{(\omega)}(\xi_i^{(\omega)} \in e_i) P_{e_1, \dots, e_n}^{(\omega^*)}(\tilde{e}_0) \right) \tilde{e}_0. \end{aligned} \quad (50)$$

Сравнивая (50) с (48), заключаем, что, в силу однозначности разложения по базису,

$$\nu^{(\omega)}(\tilde{e}_0) = \sum_{e_1 \in X_1/\varepsilon_{X_1}} \dots \sum_{e_n \in X_n/\varepsilon_{X_n}} \prod_{i=1}^n \mathbf{P}^{(\omega)}(\xi_i^{(\omega)} \in e_i) P_{e_1, \dots, e_n}^{(\omega^*)}(\tilde{e}_0). \quad (51)$$

Подставляя в правую часть (51) правые части (46), получаем, что

$$\nu^{(\omega)}(\tilde{e}_0) = \sum_{e_1 \in X_1/\varepsilon_{X_1}} \dots \sum_{e_n \in X_n/\varepsilon_{X_n}} \prod_{i=1}^n \mathbf{P}^{(\omega)}(\xi_i^{(\omega)} \in e_i) \mathbf{P}(\tilde{\omega}(e_1, \dots, e_n) = \tilde{e}_0), \quad (52)$$

$\tilde{e}_0 \in X_0/\varepsilon_{X_0}$. Из (52) и (49) следует, что

$$\begin{aligned} & \sum_{e_1 \in X_1/\varepsilon_{X_1}} \dots \sum_{e_n \in X_n/\varepsilon_{X_n}} \mathbf{P}^{(\omega)}(\xi_1^{(\omega)} \in e_1, \dots, \xi_n^{(\omega)} \in e_n) \\ & \times \max_{e_0 \in X_0/\varepsilon_{X_0}} \mathbf{P}(\tilde{\omega}(e_1, \dots, e_n) = e_0) \geq \nu^{(\omega)}(\tilde{e}_0), \quad \tilde{e}_0 \in X_0/\varepsilon_{X_0}. \end{aligned} \quad (53)$$

В силу (53) и условий следствия 4, выполнены условия теоремы 2. По теореме 2 $\varepsilon_{\mathcal{A}}$ есть $\bar{\pi}$ -конгруэнция на $\mathcal{A}$.

Следствие 5. Если $\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}$ независимы в совокупности и имеют место равенства

$$\mathbf{P}(\omega(\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}) \in e_0 \mid \xi_1^{(\omega)} \in e_1, \dots, \xi_n^{(\omega)} \in e_n) = \frac{1}{|X_0/\varepsilon_{X_0}|}, \quad (54)$$

$\omega \in \Sigma$, $X_1 \times \dots \times X_n \xrightarrow{\omega} X_0$, то для того чтобы $\varepsilon_{\mathcal{A}}$ была $\bar{\pi}$ -конгруэнцией на $\mathcal{A}$ необходимо и достаточно, чтобы для некоторого $e_0 \in X_0/\varepsilon_{X_0}$ было выполнено неравенство

$$\nu^{(\omega)}(e_0) \geq \pi^{(\omega)}, \quad \omega \in \Sigma, \quad X_1 \times \dots \times X_n \xrightarrow{\omega} X_0.$$

Доказательство. Пусть $\xi_1^{(\omega)}, \dots, \xi_n^{(\omega)}$ независимы в совокупности и выполнены равенства (54). Тогда справедливы (49) и (52). Кроме того, из (40) и (54) следует, что

$$\mathbf{P}(\tilde{\omega}(e_1, \dots, e_n) = \tilde{e}_0) = \frac{1}{|X_0/\varepsilon_{X_0}|}, \quad \tilde{e}_0 \in X_0/\varepsilon_{X_0}. \quad (55)$$

В силу (52) и (55)

$$\begin{aligned} \nu^{(\omega)}(\tilde{e}_0) &= \sum_{e_1 \in X_1/\varepsilon_{X_1}} \dots \sum_{e_n \in X_n/\varepsilon_{X_n}} \mathbf{P}^{(\omega)}(\xi_1^{(\omega)} \in e_1, \dots, \xi_n^{(\omega)} \in e_n) \\ &\quad \times \max_{e_0 \in X_0/\varepsilon_{X_0}} \mathbf{P}(\tilde{\omega}(e_1, \dots, e_n) = e_0), \quad \tilde{e}_0 \in X_0/\varepsilon_{X_0}. \end{aligned} \quad (56)$$

Теперь, ввиду (56), утверждение следствия 5 вытекает из теоремы 2.

Заметим, что хотя в условиях следствия 5 говорится о некотором $e_0 \in X_0/\varepsilon_{X_0}$, в его условиях $\nu^{(\omega)}(e_0)$ не зависит от e_0 . Естественно, возникает вопрос, как описать стохастические алгебры $S(\mathcal{A}, \varepsilon_{\mathcal{A}}, (P^{(\omega)})_{\omega \in \Sigma})$ при всевозможном выборе $\mathcal{A}$, $\varepsilon_{\mathcal{A}}$, $(P^{(\omega)})_{\omega \in \Sigma}$. Ответом на него служит следующая теорема.

Теорема 3. Для любой стохастической алгебры $\mathcal{A}^*$ найдутся такие $\mathcal{A}$, $\varepsilon_{\mathcal{A}}$ и $(P^{(\omega)})_{\omega \in \Sigma}$, что

$$S(\mathcal{A}, \varepsilon_{\mathcal{A}}, (P^{(\omega)})_{\omega \in \Sigma}) \simeq \mathcal{A}^*.$$

Доказательство. Пусть задана стохастическая алгебра

$$\mathcal{A}^* = (\mathcal{M}^*, \Sigma^*)$$

со стохастическим базисом

$$\mathcal{E}^* = (\mathcal{E}^{\mathcal{X}^*})_{\mathcal{X}^* \in \mathcal{M}^*}$$

и структурными компонентами

$$P_{e_1, \dots, e_n}^{(\omega^*)}(e_0), \quad X_1^* \times \dots \times X_n^* \xrightarrow{\omega^*} X_0^*.$$

Рассмотрим семейство $\mathcal{M}$ конечных множеств и набор

$$\varepsilon = (\varepsilon_X)_{X \in \mathcal{M}},$$

где ε_X — эквивалентность на X , удовлетворяющие условиям

$$|\mathcal{M}| = |\mathcal{E}|, \quad (57)$$

$$\min_{X \in \mathcal{M}} \min_{x \in X} |x^{\varepsilon_X}| \geq \max_{X^* \in \mathcal{M}^*} |E_{X^*}|, \quad (58)$$

$$|X/\varepsilon_X| = |E_{X^*}|, \quad X \in \mathcal{M}, \quad (59)$$

где на основании (57) поставим в соответствие взаимно-однозначным образом каждому $X \in \mathcal{M}$ множество $X^* \in \mathcal{M}^*$. В силу (58) и (59)

$$|\bar{e}_1| \dots |\bar{e}_n| \geq |E_{X^*}|, \quad \bar{e}_i \in X_i/\varepsilon_{X_i}, \quad i = 1, \dots, n, \quad X_1^* \times \dots \times X_n^* \xrightarrow{\omega^*} X_0^*, \quad (60)$$

где ω^* — произвольная операция векторного умножения из Σ^* , $e \rightarrow \bar{e}$, $e \in E_{X^*}$ — биекция E_{X^*} на X^*/ε_{X^*} . Далее рассмотрим классы $K_i^{(\omega^*)}$, $i = 1, \dots, r^{(\omega^*)}$, представляющие собой $\bar{e}_1 \times \dots \times \bar{e}_n$, $\bar{e}_i \in X_i/\varepsilon_{X_i}$, $i = 1, \dots, n$, для операции ω^* , указанной в (60). Разобьем произвольным образом класс $K_i^{[\omega^*]}$ на подклассы $K_i^{(\omega^*)}(j)$, $j = 1, \dots, |E_{X_0^*}|$.

Пусть $E_{X_0^*} = (e_0^{(1)}, \dots, e_0^{[E_{X_0^*}]})$. Поставим в соответствие операции ω^* операцию ω алгебры $\mathcal{A} = (\mathcal{M}, \Sigma)$, $\omega \in \Sigma$, определяемую следующим образом:

$$\begin{aligned} \omega(x_1, \dots, x_n) &\in \bar{e}_0^{(j)}, & (x_1, \dots, x_n) &\in K_i^{(\omega^*)}, \\ x_i &\in X_i, & i = 1, \dots, n, & \quad X_1 \times \dots \times X_n \xrightarrow{\omega} X_0. \end{aligned} \quad (61)$$

Тогда $K_i^{[\omega]} = K_i^{(\omega^*)}$, $i = 1, \dots, r^{[\omega]}$, $r^{[\omega]} = r^{(\omega^*)}$, — классы эквивалентности $\varepsilon_{\mathcal{A}}^{[\omega]}$, а $K_{ij}^{(\omega)} = K_i^{(\omega^*)}(j)$, $j = 1, \dots, t_i^{(\omega)}$, $t_i^{(\omega)} = |E_{X_0^*}|$, — классы эквивалентности $\varepsilon_i^{(\omega)}$.

Выберем такие вещественные числа

$$P^{(\omega)}(x_1, \dots, x_n) \geq 0, \quad x_i \in X_i, \quad i = 1, \dots, n,$$

что для $j = 1, \dots, t_i^{(\omega)}$, $i = 1, \dots, r^{[\omega]}$, $\omega \in \Sigma$

$$\sum_{(x_1, \dots, x_n) \in K_{ij}^{(\omega)}} P^{(\omega)}(x_1, \dots, x_n) = p_i^{(\omega)} P_{e_1, \dots, e_n}^{(\omega^*)}(e_0^{(j)}), \quad (62)$$

где

$$p_i^{(\omega)} \geq 0, \quad \sum_{i=1}^{r^{(\omega)}} p_i^{(\omega)} = 1, \quad \omega \in \Sigma.$$

Из (61) и (62) согласно (40) следует, что

$$P(\tilde{\omega}(e_1, \dots, e_n) = e_0^{(j)}) = \frac{\sum_{(x_1, \dots, x_n) \in K_{ij}^{[\omega]}} P^{(\omega)}(x_1, \dots, x_n)}{\sum_{(x_1, \dots, x_n) \in K_i^{[\omega]}} P^{(\omega)}(x_1, \dots, x_n)} = P_{e_1, \dots, e_n}^{(\omega^*)}(e_0^{(j)}), \quad (63)$$

где $j = 1, \dots, t_i^{(\omega)}$, $i = 1, \dots, r^{[\omega]}$, $K_i^{[\omega]} = \bar{e}_1 \times \dots \times \bar{e}_n$. Из (63) следует, в силу (46), что структурные константы стохастической алгебры $S(\mathcal{A}, \varepsilon_{\mathcal{A}}, (\mathbf{P}^{(\omega)})_{\omega \in \Sigma})$ относительно базиса $\mathcal{E} = (\mathcal{X}/\varepsilon_{\mathcal{X}})_{\mathcal{X} \in \mathcal{M}}$ совпадают со структурными константами стохастической алгебры $\mathcal{A}^*$ относительно базиса $\mathcal{E}^* = (\mathcal{E}_{\mathcal{X}^*})_{\mathcal{X}^* \in \mathcal{M}^*}$. Это означает, что

$$S(\mathcal{A}, \varepsilon_{\mathcal{A}}, (\mathbf{P}^{(\omega)})_{\omega \in \Sigma}) \simeq \mathcal{A}^*.$$

Таким образом, теорема 3 доказана.

Список литературы

1. Горчинский Ю. Н. О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями. *Труды по дискретной математике*, т. 1. Научное изд. ТВП, Москва, 1997, с 67–84.

2. Neumann B., Neumann H. Extending partial endomorphisms of groups. *Proc. London Math. Soc.* (1952) **2**, 337–348.
3. Neumann B., Neumann H. Partial endomorphisms of groups of finite groups. *J. London Math. Soc.* (1954) **29**, 434–440.
4. Chehata C. Commutative extension of partial automorphisms of groups. *Proc. Glasgow Math. Assoc.* (1955) **1**.
5. Chehata C. Embedding theorems for groups. *Proc. Edinburg Math. Soc.* (1962) **13**, 153–157.
6. Chehata C. Embedding theorems for abelian groups. *Canadian J. Math.* (1963) **15**, 766–770.
7. Chehata C. Existence theorem for groups. *Proc. Edinburg Math. Soc.* (1963) **14**, 291–294.
8. Scott W. Half-homomorphisms of groups. *Proc. Amer. Math. Soc.* (1957) **8**, 1141–1143.
9. Herstein J. Semi-homomorphisms of groups. *Canadian J. Math.* (1968) **20**, 384–388.
10. Morgado J. Extension of some results of Herstein on semi-homomorphisms groups. *Notas e Commun. Mat.* (1969) №23.
11. Курош А. Г. *Общая алгебра*. Наука, Москва, 1974.
12. Meier W. On the security of the IDEA block cipher. *Eurocrypt-93*, 371–385.
13. Higgins P. Algebras with a scheme of operators. *Math. Nachr.* (1963) **27**, №1–2, 115–132.
14. Горчинский Ю. Н. Стохастические алгебры. *Труды по дискретной математике, т. 2*. Научное изд. ТВП, Москва, 1998, с. 55–87.

Статья поступила 29.09.1998.