Аппроксимируемость в итеративных системах конечных случайных величин

А. Д. Яшунский

Институт прикладной математики им. М. В. Келдыша РАН
Москва

Научный семинар
кафедры дифференциальной геометрии и приложений
под руководством академика РАН, профессора А. Т. Фоменко

13 сентября 2021 г.

Конечные случайные величины

- Случайные величины
  - Конечное множество $E_k = \{0, 1, 2, \ldots, k-1\}$
  - Случайная величина X со значениями в E_k
    $\mathsf{P}\{X = 0\} = p_0, \ldots, \mathsf{P}\{X = k-1\} = p_{k-1}$
    $$\mathbf{S}^{(k)} = \left\{ (p_0, \ldots, p_{k-1}) \colon p_0 \geqslant 0, \ldots, p_{k-1} \geqslant 0, \sum_{i=0}^{k-1} p_i = 1 \right\}$$
    Распределение $\mathsf{P}(X) = (p_0, \ldots, p_{k-1}) = \mathbf{p} \in \mathbf{S}^{(k)}$
    Носитель $\mu(\mathbf{p}) = \{i \in E_k \colon p_i > 0\}$
- Преобразования
  - $P_k(n) = \{f(x_1, \ldots, x_n) \colon E_k^n \to E_k\}$, $P_k = \bigcup_{n=0}^{\infty} P_k(n)$
  - $f \in P_k(n)$, $\quad X_1, \ldots, X_n$ – независимые в совокупности случайные величины, $Y = f(X_1, \ldots, X_n)$

Итеративные системы

- $\mathcal{X}_0$ – *начальный* набор независимых в совокупности конечных случайных величин
- $B \subseteq P_k$ – набор операций

$$\mathcal{X}_n = \left\{ \Phi(X_1, \ldots, X_n) : \begin{array}{l} \Phi \text{ -- \textit{бесповторный} терм над } B \\ X_1, \ldots, X_n \in \mathcal{X}_0 \end{array} \right\}$$

Итеративная система, порождаемая $\mathcal{X}_0$ и B: $\mathcal{X}(\mathcal{X}_0, B) = \bigcup_{n=1}^{\infty} \mathcal{X}_n$

Далее $\mathcal{X}_0 = \{X_{i,\mathbf{g}} : i \in \mathbb{N}, \mathbf{g} \in \mathbf{G}, \mathrm{P}(X_{i,\mathbf{g}}) = \mathbf{g}\}$, где $\mathbf{G} \subseteq \mathbf{S}^{(k)}$ – *начальные распределения* и $\mathcal{X} = \mathcal{X}(\mathbf{G}, B)$

Итеративные системы

- $\mathcal{X}_0$ – *начальный* набор независимых в совокупности конечных случайных величин
- $B \subseteq P_k$ – набор операций

$$\mathcal{X}_n = \left\{ \Phi(X_1, \ldots, X_n) : \begin{array}{l} \Phi \text{ – \textit{бесповторный} терм над } B \\ X_1, \ldots, X_n \in \mathcal{X}_0 \end{array} \right\}$$

Итеративная система, порождаемая $\mathcal{X}_0$ и B: $\mathcal{X}(\mathcal{X}_0, B) = \bigcup_{n=1}^{\infty} \mathcal{X}_n$

Далее $\mathcal{X}_0 = \{X_{i,\mathbf{g}} : i \in \mathbb{N}, \mathbf{g} \in \mathbf{G}, \mathrm{P}(X_{i,\mathbf{g}}) = \mathbf{g}\}$, где $\mathbf{G} \subseteq \mathbf{S}^{(k)}$ – *начальные распределения* и $\mathcal{X} = \mathcal{X}(\mathbf{G}, B)$

Пример

$\mathcal{X}(\{\mathbf{p}\}, \{+ \bmod k\}) = \{X_{i_1} + \cdots + X_{i_n} \bmod k\}_{n \in \mathbb{N}}$, где X_i – независимые, $\mathrm{P}(X_i) = \mathbf{p} \in \mathbf{S}^{(k)}$

Задачи

- Выразимость случайных величин
  Для заданных $\mathbf{G}, B$ найти $\{\mathsf{P}(Y)\colon Y \in \mathcal{X}(\mathbf{G}, B)\}$
- Аппроксимируемость случайных величин
  - $\mathbf{p}, \mathbf{q} \in \mathbf{S}^{(k)}$, метрика $\rho(\mathbf{p}, \mathbf{q}) = \sum\limits_{i \in E_k} |p_i - q_i|$
  - Для заданных $\mathbf{G}, B$ найти $\left\{\mathsf{P}(Y)\colon \begin{array}{c} \forall \varepsilon > 0 \; \exists X \in \mathcal{X}(\mathbf{G}, B)\colon \\ \rho(\mathsf{P}(X), \mathsf{P}(Y)) < \varepsilon \end{array}\right\}$

Задачи

- Выразимость случайных величин
  Для заданных $\mathbf{G}, B$ найти $\{\mathrm{P}(Y)\colon\ Y \in \mathcal{X}(\mathbf{G}, B)\}$
- Аппроксимируемость случайных величин
  - $\mathbf{p}, \mathbf{q} \in \mathbf{S}^{(k)}$, метрика $\rho(\mathbf{p}, \mathbf{q}) = \sum\limits_{i \in E_k} |p_i - q_i|$
  - Для заданных $\mathbf{G}, B$ найти $\left\{ \mathrm{P}(Y)\colon \begin{array}{c} \forall \varepsilon > 0\ \exists X \in \mathcal{X}(\mathbf{G}, B)\colon \\ \rho(\mathrm{P}(X), \mathrm{P}(Y)) < \varepsilon \end{array} \right\}$

Булевы случайные величины

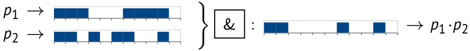
$\mathbf{G} = \{(\frac{1}{2}, \frac{1}{2})\}$, $B = \{\wedge, \vee\} \subset P_2$

- Выразимые в $\mathcal{X}(\mathbf{G}, B)$: $\mathrm{P}(Y) = (1 - \frac{m}{2^n}, \frac{m}{2^n})$
- Аппроксимируемые в $\mathcal{X}(\mathbf{G}, B)$: $\mathrm{P}(Y) \in \mathbf{S}^{(2)}$

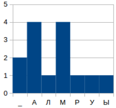
Приложения

- Вероятностные автоматы

- Вероятностные вычисления



М	А	М	А		М	Ы	Л	А		Р	А	М	У

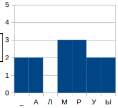


- Криптография

_	А	Л	М	Р	У	Ы
0	1	2	3	4	5	6

$$Y_1 = X_1, \quad Y_{i+1} = Y_i + X_i \pmod 7$$

М	Р		А	А	Р	М	У	Ы	Ы	М	Р		У



История вопроса

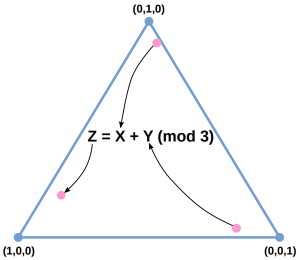
- Вероятность
  - Конечные абелевы группы: Воробьев Н.Н., 1954
  - Вероятность на алгебраических структурах (группы): Grenander U., 1963
  - Конечные группы: обзор Saloff-Coste L., 2004
- Кибернетика
  - $\{\wedge, \vee\}$-схемы: Схиртладзе Р.Л., 1960-е
  - P_k, рациональные распределения: Салимов Ф.И., 1980-е; Колпаков Р.М., 1990-е – 2000-е
  - Bruck J., Riedel M.D. et al., $\sim$2010

Индуцированные функции

$$\mathrm{P}(X) = (p_0, p_1, p_2), \mathrm{P}(Y) = (q_0, q_1, q_2)$$

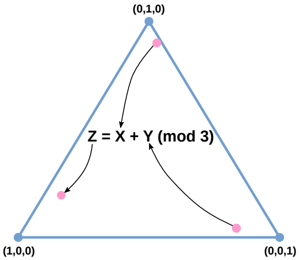
$$Z = X + Y \pmod 3$$

$$\begin{aligned}\mathrm{P}(Z) = (&p_0q_0 + p_1q_2 + p_2q_1,\\ &p_0q_1 + p_1q_0 + p_2q_2,\\ &p_0q_2 + p_1q_1 + p_2q_0)\end{aligned}$$



Индуцированные функции

$$\mathrm{P}(X) = (p_0, p_1, p_2), \mathrm{P}(Y) = (q_0, q_1, q_2)$$
$$Z = X + Y \pmod 3$$
$$\mathrm{P}(Z) = (p_0q_0 + p_1q_2 + p_2q_1,\ p_0q_1 + p_1q_0 + p_2q_2,\ p_0q_2 + p_1q_1 + p_2q_0)$$



- $f \in P_k(n)$, $\mathrm{P}(X_1) = \mathbf{p}^{(1)}, \ldots, \mathrm{P}(X_n) = \mathbf{p}^{(n)}$
- $\mathrm{P}(f(X_1, \ldots, X_n)) = \mathbf{q} = \widehat{f}(\mathbf{p}^{(1)}, \ldots, \mathbf{p}^{(n)})$: $\left(\mathbf{S}^{(k)}\right)^n \to \mathbf{S}^{(k)}$

$$q_i = \sum_{\substack{\sigma_1, \ldots, \sigma_n \in E_k \\ f(\sigma_1, \ldots, \sigma_n) = i}} p^{(1)}_{\sigma_1} \cdot p^{(2)}_{\sigma_2} \cdots p^{(n)}_{\sigma_n}.$$

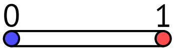
Индуцированные функции

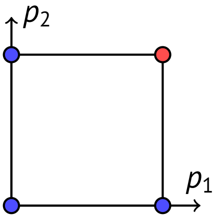
$$\mathbf{p} = (1-p, p) \in \mathbf{S}^{(2)} \leftrightarrow p \in [0;1], \quad \mathbf{G} \subseteq \mathbf{S}^{(2)} \leftrightarrow G \subseteq [0;1]$$

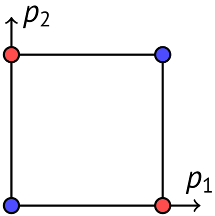
p_1	p_2	$\&$
0	0	0
0	1	0
1	0	0
1	1	1

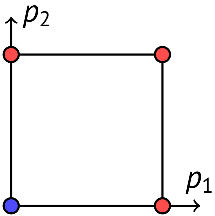
p_1	p_2	$\oplus$
0	0	0
0	1	1
1	0	1
1	1	0

p_1	p_2	$\vee$
0	0	0
0	1	1
1	0	1
1	1	1









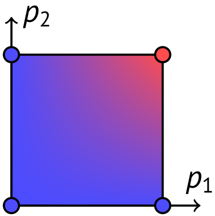
Индуцированные функции

$$\mathbf{p} = (1-p, p) \in \mathbf{S}^{(2)} \leftrightarrow p \in [0;1], \quad \mathbf{G} \subseteq \mathbf{S}^{(2)} \leftrightarrow G \subseteq [0;1]$$

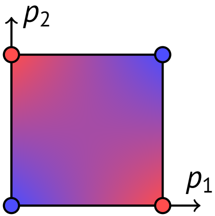
p_1	p_2	$\&$
0	0	0
0	1	0
1	0	0
1	1	1

p_1	p_2	$\oplus$
0	0	0
0	1	1
1	0	1
1	1	0

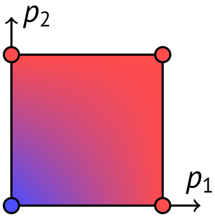
p_1	p_2	$\vee$
0	0	0
0	1	1
1	0	1
1	1	1



$p_1 p_2$



$(1-p_1)p_2 + p_1(1-p_2)$



$(1-p_1)p_2 + p_1(1-p_2) + p_1 p_2$

Решетки классов распределений

- Распределения выразимых в $\mathcal{X}(\mathbf{G}, B)$ с.в.:
  $V_B(\mathbf{G})$ – замыкание $\mathbf{G}$ относительно $\widehat{B} = \{\widehat{f} : f \in B\}$

Решетки классов распределений

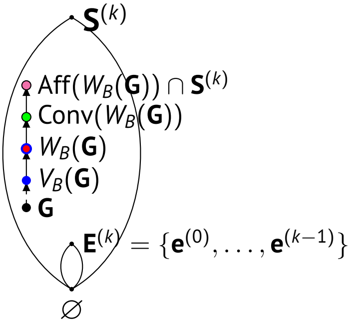
- Распределения выразимых в $\mathcal{X}(\mathbf{G}, B)$ с.в.:
  $V_B(\mathbf{G})$ – замыкание $\mathbf{G}$ относительно $\widehat{B} = \{\widehat{f} : f \in B\}$
- Распределения аппроксимируемых в $\mathcal{X}(\mathbf{G}, B)$ с.в.:

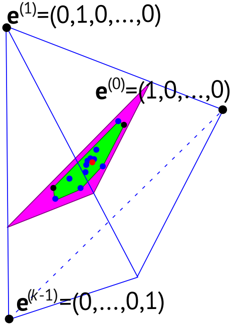
$$W_B(\mathbf{G}) = V_B(\mathbf{G}) \cup \lambda(V_B(\mathbf{G})), \quad \lambda(\mathbf{H}) \text{ – предельные точки } \mathbf{H}$$

Решетки классов распределений

- Распределения выразимых в $\mathcal{X}(\mathbf{G}, B)$ с.в.:
  $V_B(\mathbf{G})$ – замыкание $\mathbf{G}$ относительно $\widehat{B} = \{\widehat{f} : f \in B\}$
- Распределения аппроксимируемых в $\mathcal{X}(\mathbf{G}, B)$ с.в.:

$$W_B(\mathbf{G}) = V_B(\mathbf{G}) \cup \lambda(V_B(\mathbf{G})), \quad \lambda(\mathbf{H}) \text{ – предельные точки } \mathbf{H}$$



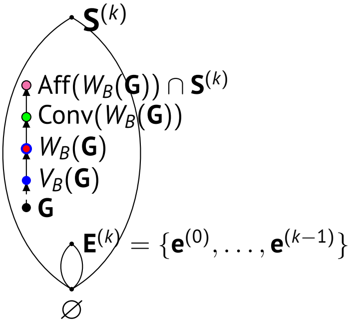


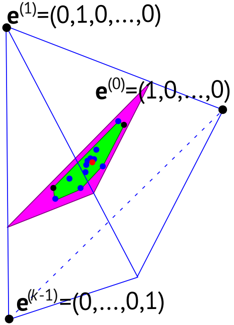
B

Решетки классов распределений

- Распределения выразимых в $\mathcal{X}(\mathbf{G}, B)$ с.в.:
  $V_B(\mathbf{G})$ – замыкание $\mathbf{G}$ относительно $\widehat{B} = \{\widehat{f} : f \in B\}$
- Распределения аппроксимируемых в $\mathcal{X}(\mathbf{G}, B)$ с.в.:

$$W_B(\mathbf{G}) = V_B(\mathbf{G}) \cup \lambda(V_B(\mathbf{G})), \quad \lambda(\mathbf{H}) \text{ – предельные точки } \mathbf{H}$$



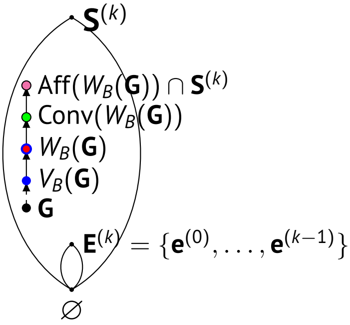


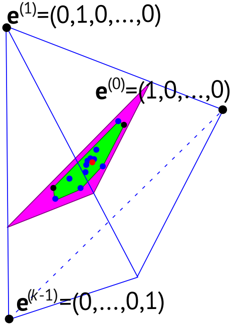
$\{x\} \subseteq \cdots \subseteq B \subseteq \cdots \subseteq P_k$

Решетки классов распределений

- Распределения выразимых в $\mathcal{X}(\mathbf{G}, B)$ с.в.:
  $V_B(\mathbf{G})$ – замыкание $\mathbf{G}$ относительно $\widehat{B} = \{\widehat{f} : f \in B\}$
- Распределения аппроксимируемых в $\mathcal{X}(\mathbf{G}, B)$ с.в.:

$$W_B(\mathbf{G}) = V_B(\mathbf{G}) \cup \lambda(V_B(\mathbf{G})), \quad \lambda(\mathbf{H}) \text{ – предельные точки } \mathbf{H}$$





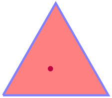
$$\{x\} \subseteq \cdots \subseteq [B]_0 \subseteq \cdots \subseteq [B] \subseteq \cdots \subseteq P_k$$

Преобразующие системы

$$W_B(\{\mathbf{p}\}) = W_B(\mathbf{p}) - ?$$

Преобразующие системы

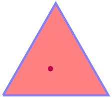
$W_B(\{\mathbf{p}\}) = W_B(\mathbf{p})$ – ?



$W_B(\mathbf{p}) = \mathbf{S}^{(k)}$: аппроксимационная полнота

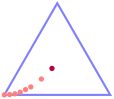
Преобразующие системы

$W_B(\{\mathbf{p}\}) = W_B(\mathbf{p})$ – ?

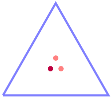


$W_B(\mathbf{p}) = \mathbf{S}^{(k)}$: аппроксимационная полнота

⋮



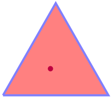
$|\lambda(W_B(\mathbf{p}))| = 1$: предельный закон



$|W_B(\mathbf{p})| < \infty$

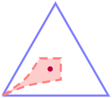
Преобразующие системы

$W_B(\{\mathbf{p}\}) = W_B(\mathbf{p})$ – ?



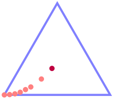
$W_B(\mathbf{p}) = \mathbf{S}^{(k)}$: аппроксимационная полнота

$\vdots$

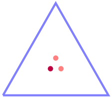


$W_B(\mathbf{p}) \subseteq W_B(\mathbf{G}) \subset \mathbf{S}^{(k)}$

$\vdots$



$|\lambda(W_B(\mathbf{p}))| = 1$: предельный закон



$|W_B(\mathbf{p})| < \infty$

Аппроксимационная полнота

Аппроксимационная полнота системы B: $W_B(\mathbf{p}) = \mathbf{S}^{(k)}$

слабая	стандартная	сильная
$\exists \mathbf{p} \in \mathbf{S}^{(k)}$	$\forall \mathbf{p} \in \mathbf{S}^{(k)}$	$\forall \mathbf{p} \in \mathbf{S}^{(k)}$
$\mu(\mathbf{p}) = E_k$	$\mu(\mathbf{p}) = E_k$	$\lvert\mu(\mathbf{p})\rvert > 1$

Аппроксимационная полнота

Аппроксимационная полнота системы B: $W_B(\mathbf{p}) = \mathbf{S}^{(k)}$

слабая	стандартная	сильная
$\exists \mathbf{p} \in \mathbf{S}^{(k)}$	$\forall \mathbf{p} \in \mathbf{S}^{(k)}$	$\forall \mathbf{p} \in \mathbf{S}^{(k)}$
$\mu(\mathbf{p}) = E_k$	$\mu(\mathbf{p}) = E_k$	$\lvert\mu(\mathbf{p})\rvert > 1$

Теорема

P_k – сильно аппроксимационно полная система.

Аппроксимационная полнота

Аппроксимационная полнота системы B: $W_B(\mathbf{p}) = \mathbf{S}^{(k)}$

слабая	стандартная	сильная
$\exists \mathbf{p} \in \mathbf{S}^{(k)}$	$\forall \mathbf{p} \in \mathbf{S}^{(k)}$	$\forall \mathbf{p} \in \mathbf{S}^{(k)}$
$\mu(\mathbf{p}) = E_k$	$\mu(\mathbf{p}) = E_k$	$\lvert\mu(\mathbf{p})\rvert > 1$

Теорема

P_k – сильно аппроксимационно полная система.

- $\mathcal{T} \subseteq E_k, \mathcal{T} \neq \varnothing,\ S_{\mathcal{T}} = \{f(x)$ – перестановка на $\mathcal{T}\}$
- $Q_{\mathcal{T}}^{\infty} = \{f : \exists i \forall \alpha_j \in E_k : f(\alpha_1, \ldots, \alpha_{i-1}, x, \alpha_i, \ldots, \alpha_{n-1}) \in S_{\mathcal{T}}\}$

Теорема

Если выполнено $B \subseteq Q_{\mathcal{T}}^{\infty}$ для некоторого $\mathcal{T} \subseteq E_k, \mathcal{T} \neq \varnothing$, то B слабо аппроксимационно не полна.

Аппроксимационная полнота

Аппроксимационная полнота системы B: $W_B(\mathbf{p}) = \mathbf{S}^{(k)}$

слабая	стандартная	сильная
$\exists \mathbf{p} \in \mathbf{S}^{(k)}$	$\forall \mathbf{p} \in \mathbf{S}^{(k)}$	$\forall \mathbf{p} \in \mathbf{S}^{(k)}$
$\mu(\mathbf{p}) = E_k$	$\mu(\mathbf{p}) = E_k$	$\lvert\mu(\mathbf{p})\rvert > 1$

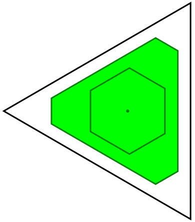
Теорема

P_k – сильно аппроксимационно полная система.

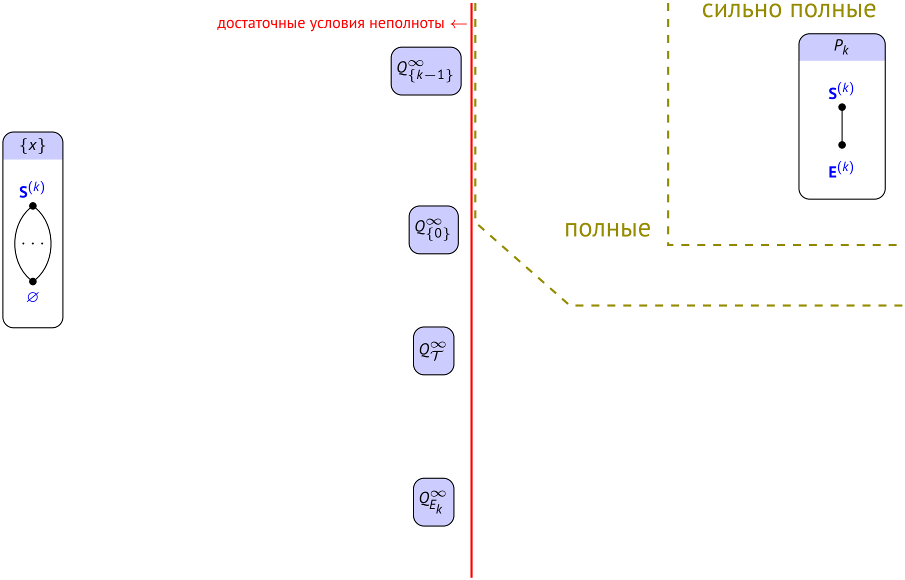
- $\mathcal{T} \subseteq E_k, \mathcal{T} \neq \varnothing$, $S_{\mathcal{T}} = \{f(x)$ – перестановка на $\mathcal{T}\}$
- $Q_{\mathcal{T}}^{\infty} = \{f : \exists i \forall \alpha_j \in E_k : f(\alpha_1, \ldots, \alpha_{i-1}, x, \alpha_i, \ldots, \alpha_{n-1}) \in S_{\mathcal{T}}\}$

Теорема

Если выполнено $B \subseteq Q_{\mathcal{T}}^{\infty}$ для некоторого $\mathcal{T} \subseteq E_k, \mathcal{T} \neq \varnothing$, то B слабо аппроксимационно не полна.



Распределения на E_k



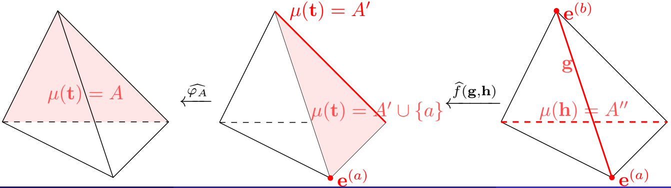
Аппроксимационная полнота

Теорема

Пусть $B \subseteq P_k$ и $\mathbf{G} \subset \mathbf{S}^{(k)}$ таковы, что $\mathbf{e}^{(0)}, \ldots, \mathbf{e}^{(k-1)} \in W_B(\mathbf{G})$ и найдутся $a, b \in E_k$, $a \neq b$, т.ч.:

- $\mathrm{Conv}(\{\mathbf{e}^{(a)}, \mathbf{e}^{(b)}\}) \subset W_B(\mathbf{G})$
- $B \ni f\colon \begin{array}{c|cccc} f & a & & \ldots & \\ \hline a & a & a & \ldots & a \\ b & a & \multicolumn{3}{c}{\text{перестановка}} \end{array}$
- Для любого $\mathcal{T} \subseteq E_k$, $|\mathcal{T}| > 1$ найдется $\varphi(x) \in B$, т.ч. $\varphi(a) \in \mathcal{T}$ и $\{\varphi(x)\colon x \in E_k\} \supseteq \mathcal{T}$

Тогда $W_B(\mathbf{G}) = \mathbf{S}^{(k)}$.



Кольца вычетов $\mathbb{Z}_k$

$+_k$, $\times_k$ – сложение и умножение $\bmod k$, c_1 – константа 1

Теорема

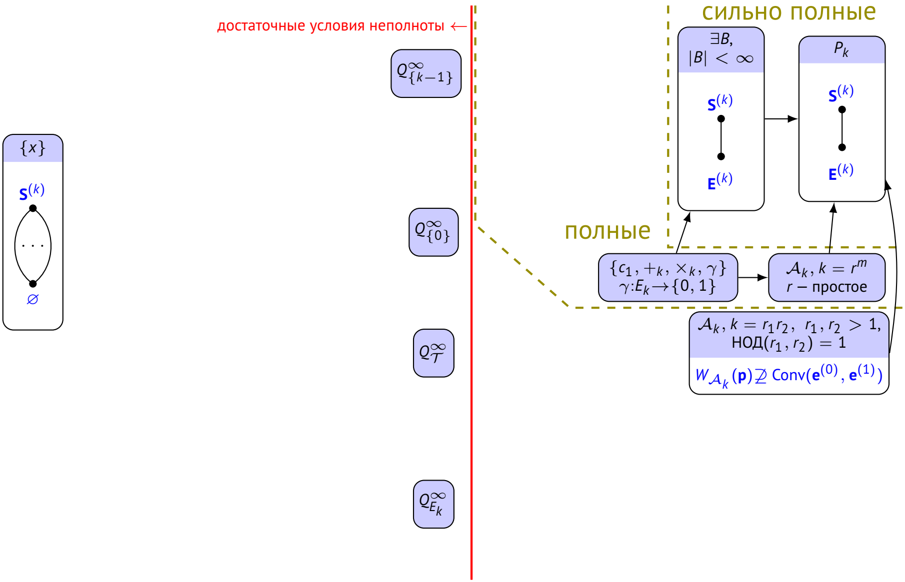
Система $\{c_1, +_k, \times_k, \gamma\}$, где $\gamma(x)$ – функция принимающая ровно два значения 0 и 1, аппроксимационно полна.

Теорема

Существуют конечные сильно аппроксимационно полные системы.

Теорема

Класс $\mathcal{A}_k$ многочленов $\bmod k$ аппроксимационно полон тогда и только тогда, когда $k = r^m$, r – простое.



достаточные условия неполноты ←
сильно полные
полные
$\{x\}$
$\mathbf{s}^{(k)}$
$\varnothing$
$Q^{\infty}_{\{k-1\}}$
$Q^{\infty}_{\{0\}}$
$Q^{\infty}_{\mathcal{T}}$
$Q^{\infty}_{E_k}$
$\exists B$, $|B| < \infty$
$\mathbf{s}^{(k)}$
$\mathbf{E}^{(k)}$
P_k
$\mathbf{s}^{(k)}$
$\mathbf{E}^{(k)}$
$\{c_1, +_k, \times_k, \gamma\}$ $\gamma{:}E_k \to \{0,1\}$
$\mathcal{A}_k, k = r^m$ r – простое
$\mathcal{A}_k, k = r_1 r_2,\ \ r_1, r_2 > 1,$ НОД$(r_1, r_2) = 1$
$W_{\mathcal{A}_k}(\mathbf{p}) \not\supseteq \mathrm{Conv}(\mathbf{e}^{(0)}, \mathbf{e}^{(1)})$

Предельные законы

- $\mathcal{T} \subseteq E_k,\ \mathcal{T} \neq \varnothing$
- $f(x_1, \ldots, x_n)$ – $\mathcal{T}$-поглощающая квазигрупповая операция, если $f(\alpha_1, \ldots, \alpha_{i-1}, x, \alpha_i, \ldots, \alpha_{n-1}) \in S_{\mathcal{T}}$ при любых $i = 1, \ldots, n$ и $\alpha_1, \ldots, \alpha_{n-1} \in E_k$
- $f(x_1, \ldots, x_n) \in Q_{\mathcal{T}}$

$\circ$	0	1	2	3	4	5
0	0	2	1	2	0	0
1	2	1	0	0	1	1
2	1	0	2	1	2	2
3	1	0	2	5	4	1
4	1	2	0	1	2	3
5	2	0	1	2	1	0

Предельные законы

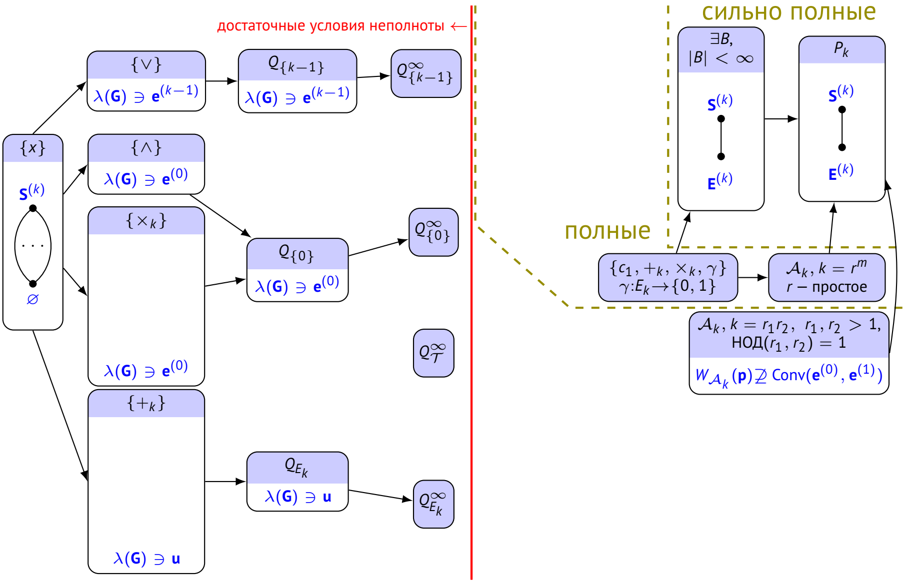
- $\mathcal{T} \subseteq E_k,\ \mathcal{T} \neq \varnothing$
- $f(x_1, \ldots, x_n)$ – $\mathcal{T}$-поглощающая квазигрупповая операция, если $f(\alpha_1, \ldots, \alpha_{i-1}, x, \alpha_i, \ldots, \alpha_{n-1}) \in S_{\mathcal{T}}$ при любых $i = 1, \ldots, n$ и $\alpha_1, \ldots, \alpha_{n-1} \in E_k$
- $f(x_1, \ldots, x_n) \in Q_{\mathcal{T}}$

$\circ$	0	1	2	3	4	5
0	0	2	1	2	0	0
1	2	1	0	0	1	1
2	1	0	2	1	2	2
3	1	0	2	5	4	1
4	1	2	0	1	2	3
5	2	0	1	2	1	0

Теорема

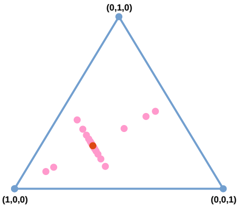
Пусть заданы $\mathcal{T} \subseteq E_k$, $\mathcal{T} \neq \varnothing$, $n > 1$, $f(x_1, \ldots, x_n) \in Q_{\mathcal{T}}$ и $\mathbf{g} \in \mathbf{S}^{(k)}$, удовлетворяющее $\mu(\mathbf{g}) \supseteq \mathcal{T}$. Тогда $\lambda(V_{\{f\}}(\mathbf{g})) \subseteq \{\mathbf{q}\}$, где $\mu(\mathbf{q}) = \mathcal{T}$ и $q_i = \frac{1}{|\mathcal{T}|}$ для $i \in \mathcal{T}$.

Распределения на E_k

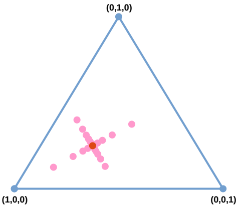


Предельные законы

G – *существенно плоское*:
$\exists |\mathbf{G}'| < \infty$, $\mathrm{Aff}(\mathbf{G} \setminus \mathbf{G}') \not\supseteq \mathbf{S}^{(k)}$

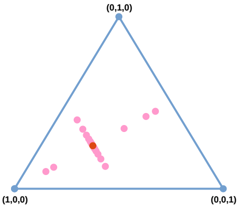


G – *X-множество*:
$\mathbf{G} = \mathbf{G}_1 \cup \mathbf{G}_2$, $\mathrm{Aff}(\mathbf{G}_i) \not\supseteq \mathbf{S}^{(k)}$

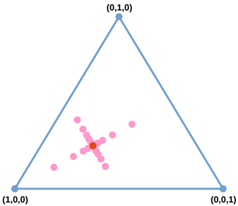


Предельные законы

G — *существенно плоское*:
$\exists |\mathbf{G}'| < \infty$, $\mathrm{Aff}(\mathbf{G} \setminus \mathbf{G}') \not\supseteq \mathbf{S}^{(k)}$



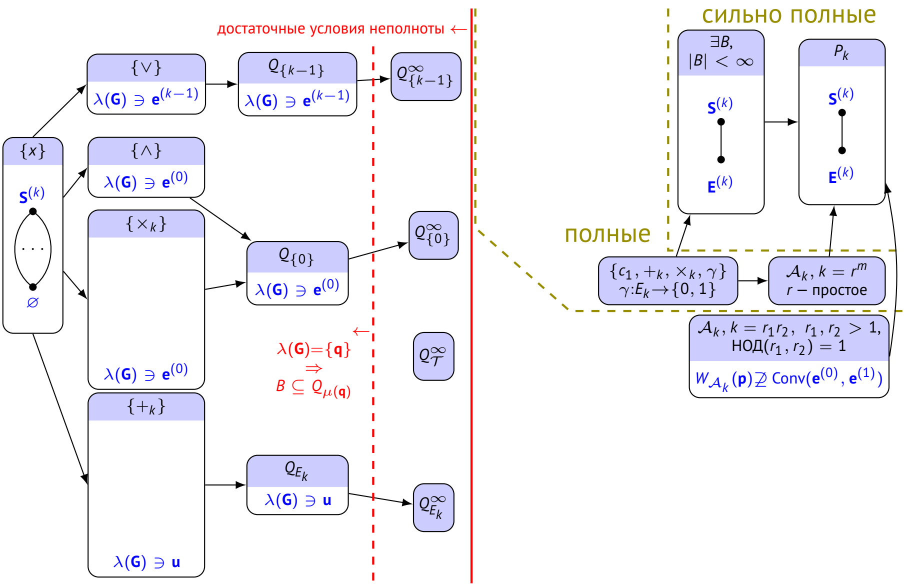
G — *X-множество*:
$\mathbf{G} = \mathbf{G}_1 \cup \mathbf{G}_2$, $\mathrm{Aff}(\mathbf{G}_i) \not\supseteq \mathbf{S}^{(k)}$



Теорема

Если для $B \subset P_k$ и $\mathbf{G} \subset \mathbf{S}^{(k)}$ выполнено $\lambda(W_B(\mathbf{G})) = \{\mathbf{q}\}$, причем $W_B(\mathbf{G})$ — не существенно плоское и не X-множество, то $B \subseteq Q_{\mu(\mathbf{q})}$.
Если при этом $B \not\subseteq P_k^1$, то $q_i = \frac{1}{|\mu(\mathbf{q})|}$ для всех $i \in \mu(\mathbf{q})$.

Распределения на E_k



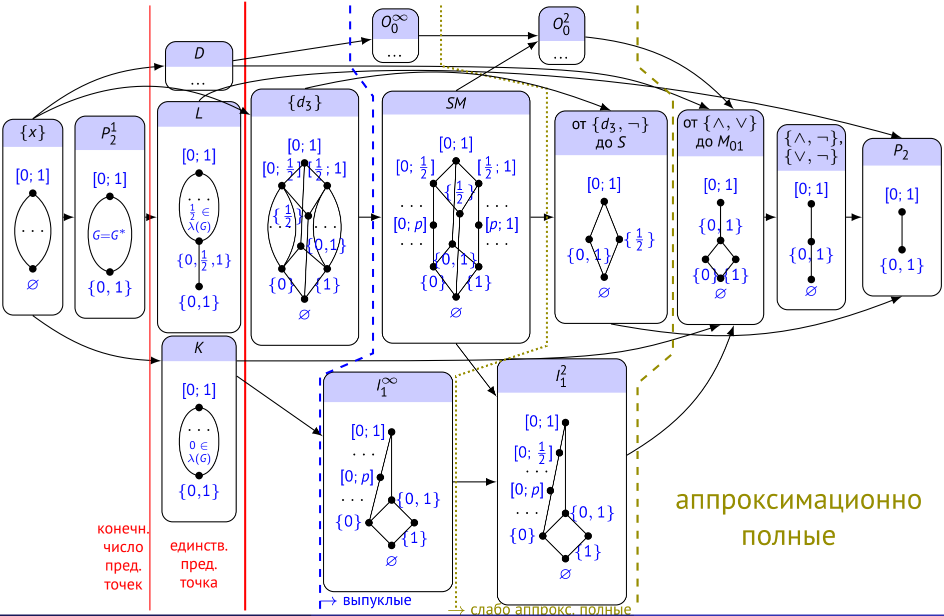
Замкнутые классы в P_2

Теорема

Пусть задан класс $A \subseteq P_2$, $[A] = A$, $A \not\subseteq K, D, L$, множество $G \subseteq [0;1]$, $G \neq \varnothing$, и выполнено $W_A(G) = G$. Тогда G имеет вид:

- $[0;1]$ или $\{0,1\}$
- $\{0\}$, если $A \subseteq T_0$; $\{1\}$, если $A \subseteq T_1$; $\{\frac{1}{2}\}$ если $A \subseteq S$
- $[0;g]$, где $g \leqslant 1 - \frac{1}{m}$, если $A \subseteq I^m$
  $[g;1]$, где $g \geqslant \frac{1}{m}$, если $A \subseteq O^m$

Бернуллиевские распределения



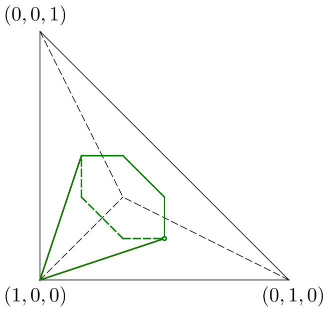
Кольца вычетов $\mathbb{Z}_k$

Для набора $\mathbf{g}^{(1)}, \ldots, \mathbf{g}^{(t)} \in \mathbf{S}^{(k)}$ и множества $M \subseteq E_k$ определим:

$$\mathbf{K}_{ij} = \{\mathbf{e}^{(j)} \mathbin{\widehat{\times}_k} (\mathbf{g}^{(i)} \mathbin{\widehat{+}_k} \mathbf{e}^{(s)}) \mid s \in E_k\} \cup \{\mathbf{e}^{(0)}\},$$

$$\mathbf{K}_i(M) = \{\mathbf{h}^{(ij_1)} \mathbin{\widehat{+}_k} \cdots \mathbin{\widehat{+}_k} \mathbf{h}^{(ij_m)} \mid \{j_1, \ldots, j_m\} = M, \mathbf{h}^{(ij_r)} \in \mathbf{K}_{ij_r}\},$$

$$\mathbf{K}(\mathbf{g}^{(1)}, \ldots, \mathbf{g}^{(t)}; M) = \{\mathbf{j}^{(1)} \mathbin{\widehat{+}_k} \cdots \mathbin{\widehat{+}_k} \mathbf{j}^{(t)} \mid \mathbf{j}^{(1)} \in \mathbf{K}_1(M), \ldots, \mathbf{j}^{(t)} \in \mathbf{K}_t(M)\}$$

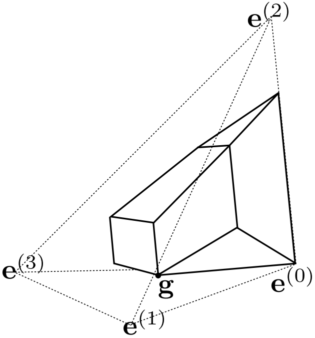


Теорема

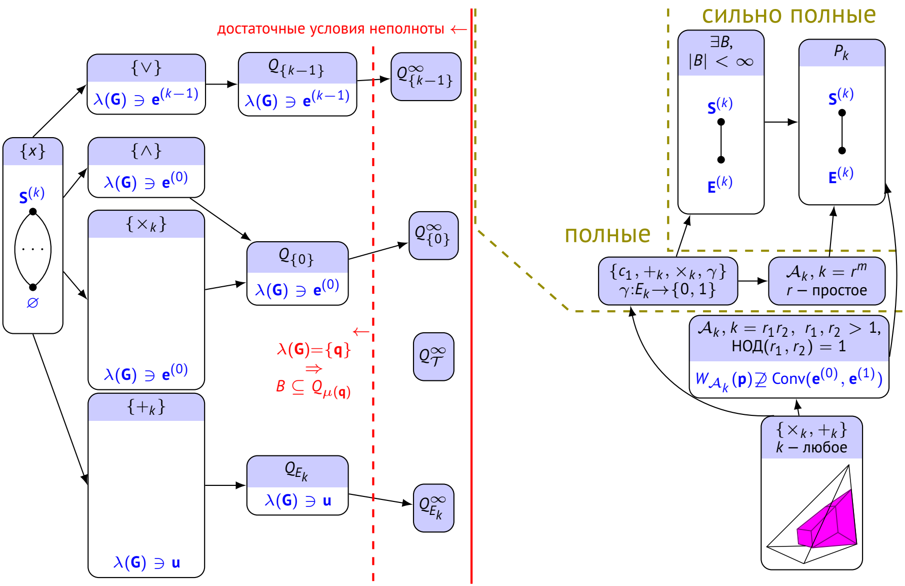
Пусть $U \subset E_k$ – группа обратимых элементов кольца $\langle E_k; \{+_k, \times_k\}\rangle$. Положим $Z = E_k \setminus (U \cup \{0\})$ и для заданных распределений $\mathbf{g}^{(1)}, \ldots, \mathbf{g}^{(t)} \in \mathbf{S}^{(k)}$ определим:

$$\mathbf{I} = \{\mathbf{e}^{(j)} \widehat{\times_k} (\mathbf{g}^{(i)} \widehat{+_k} \mathbf{e}^{(s)}) : j \in U, s \in E_k, i = 1, \ldots, t\}$$

и $\mathbf{H} = \mathrm{Conv}(\mathbf{I} \cup \mathbf{K}(\mathbf{g}^{(1)}, \ldots, \mathbf{g}^{(t)}; Z))$ Тогда $W_{\{+_k, \times_k\}}(\mathbf{H}) = \mathbf{H}$.



Распределения на E_k



Конечные цепи

$E_k\colon 0 < 1 < 2 < \cdots < k-1$; минимум — $\wedge$, максимум — $\vee$

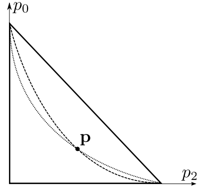
Теорема

Система $\{\wedge, \vee, \gamma\}$, где $\gamma(x)\colon E_k \to \{0, k-1\}$, аппроксимационно полна.

$$\mathbf{L}(i,\alpha) = \left\{\mathbf{p}\colon \sum_{j=0}^{i-1} p_j \leqslant \Big(\sum_{j=0}^{i} p_j\Big)^{\alpha}\right\}, \mathbf{U}(i,\alpha) = \left\{\mathbf{p}\colon \sum_{j=i+1}^{k-1} p_j \leqslant \Big(\sum_{j=i}^{k-1} p_j\Big)^{\alpha}\right\}$$

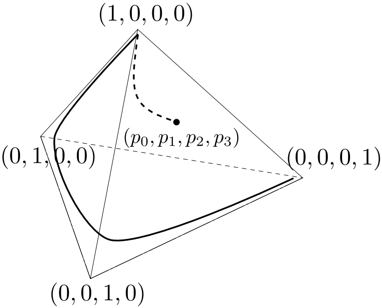
Теорема

Для любого $\alpha > 1$ и любого $i \in E_k$ выполнены соотношения $W_{\{\vee,\wedge\}}(\mathbf{L}(i,\alpha)) = \mathbf{L}(i,\alpha)$ и $W_{\{\vee,\wedge\}}(\mathbf{U}(i,\alpha)) = \mathbf{U}(i,\alpha)$.



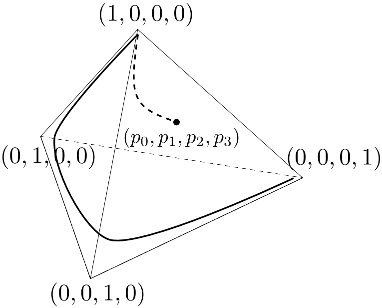
Теорема

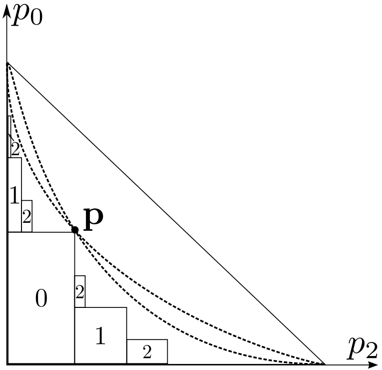
Пусть $\mathbf{p} \in \mathbf{S}^{(k)}$ удовлетворяет $\mu(\mathbf{p}) = E_k$. Тогда для всех $i \in E_k \setminus \{0\}$ выполнено $\mathrm{Conv}(\mathbf{e}^{(i-1)}, \mathbf{e}^{(i)}) \subseteq W_{\{\vee,\wedge\}}(\mathbf{p})$.



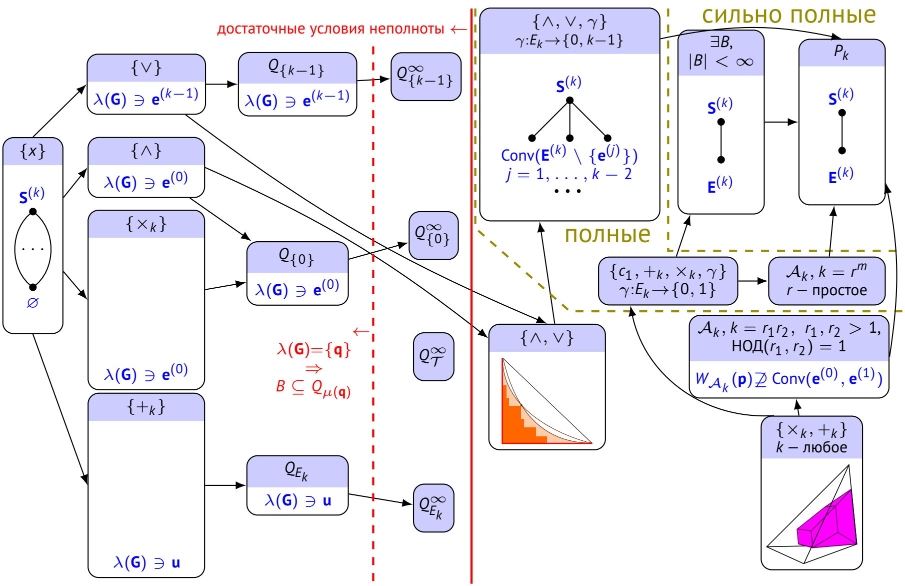
Теорема

Пусть $\mathbf{p} \in \mathbf{S}^{(k)}$ удовлетворяет $\mu(\mathbf{p}) = E_k$. Тогда для всех $i \in E_k \setminus \{0\}$ выполнено $\mathrm{Conv}(\mathbf{e}^{(i-1)}, \mathbf{e}^{(i)}) \subseteq W_{\{\vee,\wedge\}}(\mathbf{p})$.





Распределения на E_k



Для $\mathbf{p} \in \mathbf{S}^k$ положим $\varepsilon(\mathbf{p}) = 1 - p_0$, $\delta_i(\mathbf{p}) = p_i - \frac{\varepsilon(\mathbf{p})}{k-1}$, $i \in E_k \setminus \{0\}$

$$\mathbf{H}_{\alpha,b} = \{\mathbf{p} \in \mathbf{S}^{(k)} \colon \varepsilon(\mathbf{p}) \leqslant b\} \cap \left(\bigcap_{i \neq 0} \left\{ \mathbf{p} \in \mathbf{S}^{(k)} \colon |\delta_i(\mathbf{p})| \leqslant \frac{\varepsilon(\mathbf{p})^\alpha}{k-1} \right\} \right),$$

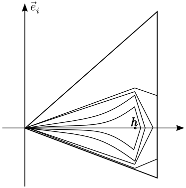
$$\mathbf{K}_{a,b,c} = \bigcap_{i \neq 0} \left\{ \mathbf{p} \in \mathbf{S}^{(k)} \colon |\delta_i(\mathbf{p})| \leqslant a - \tfrac{a}{b}(\varepsilon - h), |\delta_i(\mathbf{p})| \leqslant a + \tfrac{a}{c}(\varepsilon - h) \right\}$$

Теорема

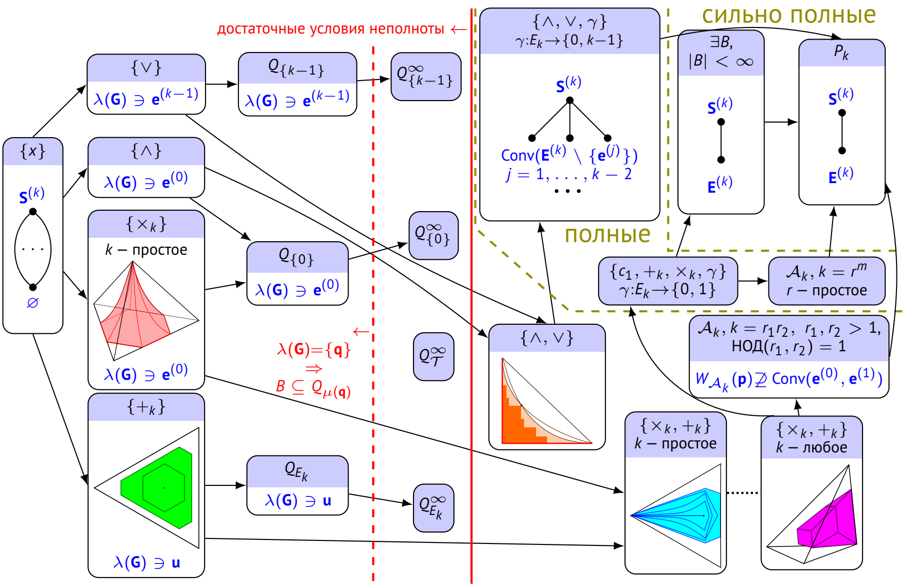
Пусть k – простое, a удовлетворяет $0 < a \leqslant \frac{1}{k}$ и $\mathbf{K} = \mathbf{K}_{a,k(k-1)a^2,h}$. Тогда $W_{\{+_k,\times_k\}}(\mathbf{K}) = \mathbf{K}$.

Теорема

Для каждого простого $k \geqslant 3$ найдется такое $\alpha_0(k)$, что при всех $\alpha \geqslant \alpha_0(k)$, $a = \frac{(k-1)^{\alpha-1}}{k^\alpha}$, множества $\mathbf{I}_\alpha = \mathbf{H}_{\alpha,h} \cup \mathbf{K}_{a,k(k-1)a^2,k(k-1)a^2}$ удовлетворяют $W_{\{+_k,\times_k\}}(\mathbf{I}_\alpha) = \mathbf{I}_\alpha$.



Распределения на E_k



Основные публикации

1. Asymptotics of the probability of values of random Boolean expressions // J. Appl. Ind. Math. 2007. **1**:4, 509–531.
2. Uniform approximation of continuous functions by probability functions of Boolean bases // Moscow Univ. Math. Bull., 2007. **62**:2, 78–84.
3. On transformations of probability distributions by read-once quasigroup formulae // Discr. Math. Appl. 2013. **23**:2, 211–223.
4. On read-once transformations of random variables over finite fields // Discr. Math. Appl. 2015.**25**:5, 311–321.
5. Convex polyhedra of distributions preserved by operations over a finite field // Moscow Univ. Math. Bull., 2017. **72**:4, 165–168.
6. Algebras of probability distributions on finite sets // Proc. Steklov Inst. Math., 2018. **301**:1, 304–318.
7. Clone-induced approximation algebras of bernoulli distributions // Algebra Universalis, 2019. **80**:1. Art. 5.
8. Выпуклые алгебры вероятностных распределений, индуцированные конечными ассоциативными кольцами // Дискр. матем., 2019. **31**:1, 133–142.
9. Finite algebras of Bernoulli distributions // Discr. Math. Appl 2019. **29**:4, 267–276.
10. Algebras of Bernoulli Distributions with a Single Limit Point Journal // Moscow Univ. Math. Bull., 2019. **74**:4, 135–140.
11. Limit Points of Bernoulli Distribution Algebras Induced by Boolean Functions // Lobachevskii J. of Math., 2019. **40**:9, 1423–1432.
12. Polynomial Transformations of Random Variables on Finite Sets // Math. Notes, 2019. **106**:6, 1024–1027.
13. О весе функций, заданных бесповторными И/ИЛИ формулами // Интеллектуальные системы. Теория и приложения, 2019. **23**:3, 41–55.
14. On Necessary Conditions of Probability Limit Theorems in Finite Algebras // Doklady Math., 2020. **102**:1, 301–303.
15. On the Approximation of Random Variables on a Finite Chain // J. Appl. Ind. Math., 2020. **14**:3, 581–591.
16. On Necessary Conditions of Finite-valued Random Variable Algebraic Approximation // Lobachevskii J. of Math., 2021. **42**:1, 217–221.