Е.В. Дюкова

ПРИЛОЖЕНИЕ К УЧЕБНОМУ ПОСОБИЮ:

«Дискретные (логические) процедуры распознавания: принципы конструирования, сложность реализации и основные модели»

Москва
2003

Приложение 1.

Использование аппарата логических функций для конструирования дискретных процедур распознавания в случае целочисленной информации.

Пусть E_k^n ,k≥2, - множество наборов вида (α_1 , . . . ,α_n) ,где $\alpha_i \in \{0,1,...,k-1\}$.

Пусть переменная x принимает значения из множества E_k^n, $\sigma \in E_k^n$.

Положим $$x^\sigma = \begin{cases} 1, \text{если } x = \sigma; \\ 0, \text{если } x \neq \sigma. \end{cases}$$

Элементарной конъюнкцией (э.к.) над переменными $x_1,...,x_n$ назовём выражение вида $x_{j_1}^{\sigma_1} \cdot ... \cdot x_{j_r}^{\sigma_r}$, где
$x_{j_i} \in \{x_1,...,x_n\}$ при $i = 1,2,...,r$ и $x_{j_q} \neq x_{j_t}$ при $t,q \in \{1,2,...,r\}, t \neq q$.

Интервал истинности э.к. B будем обозначать через N_B .

Пусть $f(x_1,...,x_n)$ - функция, частично определенная на наборах из E_k^n, и принимающая значения из $\{0,1\}$, N_f и $N_{\bar{f}}$ - соответственно множество единиц и множество нулей функции f .

Определения почти допустимой, допустимой, неприводимой и максимальной конъюнкций функции f , данные в разделе 2.1 для случая k=2 , полностью переносятся на случай k>2.

Рассмотрим ситуацию, когда объекты из исследуемого множества M описаны признаками, каждый из которых принимает значения из множества $\{0,1,...,k-1\}$.
Элементарному классификатору $\sigma = (\sigma_1,...,\sigma_r)$, порожденному набором признаков $H = \{x_{j_1},...,x_{j_r}\}$, поставим в соответствие э.к. $B = x_{j_1}^{\sigma_1} \cdot ... \cdot x_{j_r}^{\sigma_r}$.
Близость объекта $S = (a_1,...,a_n)$ из M и элементарного классификатора σ будем оценивать величиной
$$B(\sigma,S,H) = \begin{cases} 1, & \textit{если} \quad a_{j_t} = \sigma_t \quad \textit{при} \quad t = 1,2,...,r, \\ 0, & \textit{в противном случае.} \end{cases}$$

Очевидно, $B(\sigma,S,H) = 1$ тогда и только тогда, когда $(a_1,...,a_n) \in N_B$.

Рассмотрим основные модели дискретных процедур распознавания и покажем, что каждый раз построение множества элементарных классификаторов для класса K сводится к построению допустимых и максимальных конъюнкций для характеристической функции класса K , т.е. такой двухзначной логической функции, которая на обучающих объектах из K и $\overline{K} = \{K_1,...,K_l\} \backslash K$ принимает разные значения.
Процедура голосования по построенной э.к. B заключается в принадлежности набора $(a_1,...,a_n)$ интервалу N_B.

1.Алгоритм голосования по представительным наборам.

В данном случае характеристическая функция класса K - частичная логическая функция $f_K(x_1,...,x_n)$, принимающая значение 1 на описаниях обучающих объектов из класса K , значение 0 на описаниях обучающих объектов из класса $\overline{K}$ и не определённая на остальных наборах из E_k^n .
Представительному набору класса K соответствует допустимая конъюнкция функции f_K , тупиковому представительному набору соответствует максимальная конъюнкция функции f_K .
Допустимая (максимальная) конъюнкция B функции f_K голосует за принадлежность объекта S классу K, если $(a_1,...,a_n) \in N_B$.

2.Алгоритм голосования по антипредставительным наборам.

Характеристическая функция класса K - частичная логическая функция $f_{\overline{K}}(x_1,...,x_n)$, принимающая значение 0 на описаниях обучающих объектов из класса K , значение 1 на описаниях обучающих объектов из класса $\overline{K}$ и не определённая на остальных наборах из E_k^n .
Антипредставительному набору класса K соответствует допустимая конъюнкция функции $f_{\overline{K}}$, тупиковому антипредставительному набору соответствует максимальная конъюнкция функции $f_{\overline{K}}$.

Допустимая (максимальная) конъюнкция B функции $f_{\overline{K}}$ голосует за принадлежность объекта S классу K, если $(a_1,...,a_n) \notin N_B$.

3.Алгоритмы голосования по покрытиям класса.

Характеристическая функция класса K - всюду определённая логическая функция $F_{\overline{K}}(x_1,...,x_n)$, принимающая значение 0 на описаниях обучающих объектов из класса K и значение 1 на остальных наборах из E_k^n.
Покрытию класса K соответствует допустимая конъюнкция функции F_K, тупиковому покрытию - максимальная конъюнкция для F_K.

Допустимая (максимальная) конъюнкция B функции $F_{\overline{K}}$ голосует за принадлежность объекта S классу K, если $(a_1,...,a_n) \notin N_B$.

Построение требуемого множества конъюнкций (ДНФ, реализующей характеристическую функцию) может быть осуществлено на основе преобразования нормальных форм.

Случай, когда k=2 и характеристическая функция класса K равна f_K, подробно рассмотрен в разделе 2.1.
Описанные в разделе 2.1. построения могут быть обобщены на рассматриваемый нами общий случай, если в качестве D_i взять дизъюнкцию вида $\overline{x_1^{\beta_{i_1}}} \vee ... \vee \overline{x_n^{\beta_{i_n}}}$ и воспользоваться равенством $\overline{x^\beta} = \underset{\alpha \neq \beta}{\vee} x^\alpha$.

Тогда преобразуемая КНФ примет вид $D_1^* \,\&\, D_2^* \,\&\, ... \,\&\, D_n^*$, где $D_i^* = \underset{\alpha \neq \beta_{i_1}}{\vee} x_1^\alpha \underset{\alpha \neq \beta_{i_2}}{\vee} x_2^\alpha ... \underset{\alpha \neq \beta_{i_n}}{\vee} x_n^\alpha$.

В утверждениях ***5*** и ***6*** следует заменить D_i на D_i^*. После перемножения логических скобок в подучившейся ДНФ следует сделать упрощения, пользуясь тем , что $x^\alpha \cdot x^\beta = 0$ при $\alpha \neq \beta$, $x \cdot x = x$, $x \vee x = x$, $x \vee x \cdot x' = x$.
Остальные рассуждения полностью совпадают с рассуждениями, которые приведены в разделе 2.1.

4.Тестовые алгоритмы распознавания.

Характеристическая функция класса K определяется так же, как и для алгоритмов голосования по представительным наборам.
Множество всех почти допустимых конъюнкций функции f_K, порождаемое набором признаков H, обозначим через $Q(H,K)$.

Очевидно, набор признаков H является тестом тогда и только тогда, когда для каждого $t \in \{1,2,...,l\}$, каждая конъюнкция из $Q(H, K_t)$ является допустимой для f_{K_t}. Очевидно также, что тест H является тупиковым тогда и только тогда, когда в $\{1,2,...,l\}$ можно указать t такое, что $Q(H, K)$ содержит максимальную конъюнкцию функции f_{K_t} .

Построение требуемого множества тестов может быть осуществлено на основе преобразования КНФ, не содержащей отрицаний переменных (реализующей монотонную булеву функцию), в ДНФ.

Действительно, рассмотрим множество P всех неупорядоченных пар наборов (α, β) таких, что $\alpha \in N_{f_{K_u}}, \beta \in N_{f_{K_v}}, u \neq v, u, v \in \{1,2,...,l\}$.

Для каждой пары (α, β) из P построим дизъюнкцию $D(\alpha, \beta) = x_{p_1} \vee ... \vee x_{p_q}$, где $p_1,..., p_q$ - номера разрядов, в которых различаются наборы α и β .

Нетрудно убедиться в том, что для построения множества тестов нужно преобразовать КНФ $K = \underset{(\alpha,\beta)\in P}{\&} D(\alpha, \beta)$ в ДНФ, состоящую из допустимых конъюнкций функции, реализуемой этой КНФ.

Для построения тупиковых тестов нужно построить сокращенную ДНФ функции, реализуемой КНФ.

Приложение 2
Тупиковые покрытия в задачах построения ДНФ двузначных логических функций

Для построения ДНФ из допустимых и максимальных конъюнкций двузначных логических функций на k- ичных n- мерных наборах, могут быть использованы методы построения покрытий булевых и целочисленных матриц.

Действительно, пусть F определена на E_k^n и принимает значения из $\{0,1\}$. Построим матрицу L, строками которой являются наборы из $N_{\overline{F}}$. Очевидным является

Утверждение 15. *Э. к. $x_{j_1}^{\sigma_1} \ldots x_{j_r}^{\sigma_r}$ является (максимальной) допустимой для F тогда и только тогда, когда набор столбцов матрицы L с номерами $j_1, \ldots, j_r$ является (тупиковым) $(\sigma_1,\ldots,\sigma_r)$- покрытием.*

Пусть f - частично определенная на E_k^n функция, принимающая значения из $\{0,1\}$. Построим матрицу L_1, строками которой являются наборы из N_f, и матрицу L_2, строками которой являются наборы из $N_{\overline{f}}$.

Утверждение 16. *Э. к. $x_{j_1}^{\sigma_1} \ldots x_{j_r}^{\sigma_r}$ является (максимальной) допустимой для f тогда и только тогда, когда набор столбцов матрицы L_2 с номерами $j_1, \ldots, j_r$ является (тупиковым) $(\sigma_1,\ldots,\sigma_r)$-покрытием и набор столбцов матрицы L_1 с номерами $j_1, \ldots, j_r$ не является $(\sigma_1,\ldots,\sigma_r)$-покрытием.*

Для построения нормальных форм из допустимых и максимальных конъюнкций функции f могут быть также использованы методы построения $(0,\ldots,0)$-покрытий и тупиковых $(0,\ldots,0)$-покрытий булевой матрицы.

Действительно, пусть $N_f = \{\alpha_1,\ldots,\alpha_v\}$, $N_{\overline{f}} = \{\beta_1,\ldots,\beta_u\}$. Поставим в соответствие набору α_i, $i \in \{1,2,\ldots,v\}$, булеву матрицу $L^{(i)}$, в которой на пересечении строки с номером p и столбца с номером q стоит 1, если наборы α_i и β_p различаются в q-й координате, и 0 - в противном случае.

Самостоятельно доказать

Утверждение 17. *Э. к. $x_{j_1}^{\sigma_1} \ldots x_{j_r}^{\sigma_r}$ является (максимальной) допустимой для f тогда и только тогда, когда можно указать i, $i \in \{1,2,\ldots,v\}$, такое, что набор столбцов матрицы $L^{(i)}$ с номерами $j_1, \ldots, j_r$ является (тупиковым) $(0,\ldots,0)$-покрытием и при $t = 1,2,\ldots,r$ координата с номером j_t набора α_i равна σ_t.*

Понятие тупикового покрытия целочисленной матрицы играет фундаментальную роль и в проблеме преобразования нормальных форм логических функций (перемножения логических скобок).

В разделе 2.2 было показано, что в случае $k = 2$ задача преобразования совершенной КНФ булевой функции F в ДНФ может быть сформулирована как задача построения тупиковых покрытий булевых матриц.

Действительно, пусть F задана КНФ вида $D_1 \& \ldots \& D_u$, где $D_i = x_1^{\sigma_{i1}} \vee \ldots \vee x_n^{\sigma_{in}}$, $i = 1,2,\ldots,u$. Рассмотрим матрицу L вида

$$\begin{pmatrix} \sigma_{11}\sigma_{12}\ldots\sigma_{1n} \\ \sigma_{21}\sigma_{22}\ldots\sigma_{2n} \\ \ldots\ldots\ldots\ldots\ldots \\ \sigma_{u1}\sigma_{u2}\ldots\sigma_{un} \end{pmatrix}.$$

Задача сводится к построению $R(\sigma)$-покрытий матрицы L, $\sigma \in E_2^r$.

Если вместо L рассмотреть матрицу $\overline{L}$ вида

$$\begin{pmatrix} \overline{\sigma}_{11}\overline{\sigma}_{12}\ldots\overline{\sigma}_{1n} \\ \overline{\sigma}_{21}\overline{\sigma}_{22}\ldots\overline{\sigma}_{2n} \\ \ldots\ldots\ldots\ldots\ldots \\ \overline{\sigma}_{u1}\overline{\sigma}_{u2}\ldots\overline{\sigma}_{un} \end{pmatrix},$$

то задача сводится к построению σ-покрытий матрицы $\overline{L}$, $\sigma \in E_2^r$.

Замечание. Если положить

$$x^{\sigma} = \begin{cases} 0, & \textit{если } x = \sigma, \\ 1, & \textit{в противном случае}, \end{cases} \qquad (1)$$

то задачи построения допустимых и максимальных конъюнкций функции F сводятся соответственно

а) к построению σ-покрытий и тупиковых σ-покрытий матрицы L;

б) к построению $R(\sigma)$-покрытий и тупиковых $R(\sigma)$-покрытий матрицы $\overline{L}$.

В разделе 2.1 было также показано, что задача построения ДНФ монотонной булевой функции, заданной КНФ, может быть сформулирована как задача построения $(0,\ldots,0)$-покрытий булевой матрицы или как задача построения $R(1,\ldots,1)$-покрытий той же матрицы.

Рассмотрим общий случай ($k \geq 2$ и исходная КНФ не обязательно является совершенной).

Пусть K - КНФ вида $D_1 \& \ldots \& D_u$, где $D_i, i = 1,2,\ldots,u$, - элементарная дизъюнкция над переменными $x_1,\ldots,x_u$.

Положим

$$x^{\sigma} = \begin{cases} 1, & \textit{если } x = \sigma, \\ 0, & \textit{в противном случае}, \end{cases}$$

$x, \sigma \in \{0,1,\ldots,k-1\}$.

КНФ K задает функцию $F_K(x_1,\ldots,x_u)$, определенную на множестве E_k^n и принимающую значение 0 или 1.

Утверждение 18. *Э. к.* B *является допустимой для* F_K *тогда и только тогда, когда каждая дизъюнкция* $D_i, i \in \{1,2,\dots,u\}$, *содержит хотя бы один множитель из* B.

Утверждение 19. *Э. к.* B *ранга* r *является неприводимой для* F_K *тогда и только тогда, когда в КНФ* K *можно указать* r *дизъюнкций* $D_{i_1},\dots,D_{i_r}$ *таких, что каждая содержит в точности один множитель из* B *и, если* $p,q \in \{i_1,\dots,i_r\}$, $p \neq q$, *дизъюнкции* D_p *и* D_q *содержат разные множители из* B.

Доказательства утверждений 18 и 19 не приводятся, так как они почти полностью совпадают с доказательствами соответственно утверждений 5 и 6.

Построим матрицу $L_K = (a_{ij}), i = 1,2,\dots,u,\ j = 1,2,\dots,n$, в которой

$$a_{ij} = \begin{cases} \sigma, & \text{если } x_j^\sigma \text{ входит в } D_i, \\ k, & \text{если } x_j^\sigma \text{ не входит в } D_i \text{ при } \sigma \in \{0,1,\dots,k-1\}. \end{cases}$$

Пусть x^σ определено по правилу (1). Тогда из утверждений 17 и 18 сразу следуют приводимые ниже утверждения 20-22.

Утверждение 20. *Э. к.* $x_{j_1}^{\sigma_1}\dots x_{j_r}^{\sigma_r}$ *является допустимой для* F_K *тогда и только тогда, когда набор столбцов матрицы* L_K *с номерами* $j_1,\dots,j_r$ *является* $R(\sigma_1,\dots,\sigma_r)$*-покрытием.*

Утверждение 21. *Э. к.* $x_{j_1}^{\sigma_1}\dots x_{j_r}^{\sigma_r}$ *является неприводимой для* F_K *тогда и только тогда, когда набор столбцов матрицы* L_K *с номерами* $j_1,\dots,j_r$ *содержит* $R(\sigma_1,\dots,\sigma_r)$*-подматрицу.*

Утверждение 22. *Э. к.* $x_{j_1}^{\sigma_1}\dots x_{j_r}^{\sigma_r}$ *является максимальной для* F_K *тогда и только тогда, когда набор столбцов матрицы* L_K *с номерами* $j_1,\dots,j_r$ *является тупиковым* $R(\sigma_1,\dots,\sigma_r)$*-покрытием.*

<u>Пример 1.</u> Пусть дана булева функция
$F_1(x_1,x_2,x_3,x_4) = (\bar{x}_1 \vee x_3 \vee x_4)(x_1 \vee \bar{x}_3 \vee x_4)(x_1 \vee x_2 \vee \bar{x}_4)(\bar{x}_1 \vee x_2 \vee x_3)$.

а) Согласно утверждению 15 задача построения сокращенной ДНФ функции F_1 может быть решена на основе построения тупиковых $R(\sigma)$-покрытий, $\sigma \in \{0,1\}$, булевой матрицы, которая имеет вид (строками матрицы являются нули функции F_1):

$$\begin{pmatrix} 0\,0\,1\,1 \\ 1\,0\,1\,1 \\ 1\,0\,0\,1 \\ 1\,1\,0\,1 \\ 1\,1\,0\,0 \\ 1\,1\,1\,0 \\ 0\,1\,1\,0 \\ 0\,1\,1\,1 \end{pmatrix}.$$

б) Согласно утверждению 22 задача построения сокращенной ДНФ функции F_1 может быть решена на основе построения тупиковых $R(\sigma)$-покрытий, $\sigma \in \{0,1\}$, матрицы с элементами из $\{0,1,2\}$, имеющей вид

$$\begin{pmatrix} 2\,0\,1\,1 \\ 1\,2\,0\,1 \\ 1\,1\,2\,0 \\ 0\,1\,1\,2 \end{pmatrix}.$$

<u>Пример 2.</u> Пусть дана булева функция

$$F_2(x_1, x_2, x_3, x_4) = (x_2 \vee x_3 \vee x_4)(x_1 \vee x_3 \vee x_4)(x_1 \vee x_2 \vee x_4)(x_1 \vee x_2 \vee x_3).$$

Согласно утверждению 22 задача построения сокращенной ДНФ функции F_2 сводится к построению тупиковых $R(1,\ldots,1)$-покрытий матрицы L' (или неприводимых покрытий матрицы L''):

$$L' = \begin{pmatrix} 2\,1\,1\,1 \\ 1\,2\,1\,1 \\ 1\,1\,2\,1 \\ 1\,1\,1\,2 \end{pmatrix} \xrightarrow{2 \to 0} L'' = \begin{pmatrix} 0\,1\,1\,1 \\ 1\,0\,1\,1 \\ 1\,1\,0\,1 \\ 1\,1\,1\,0 \end{pmatrix}.$$

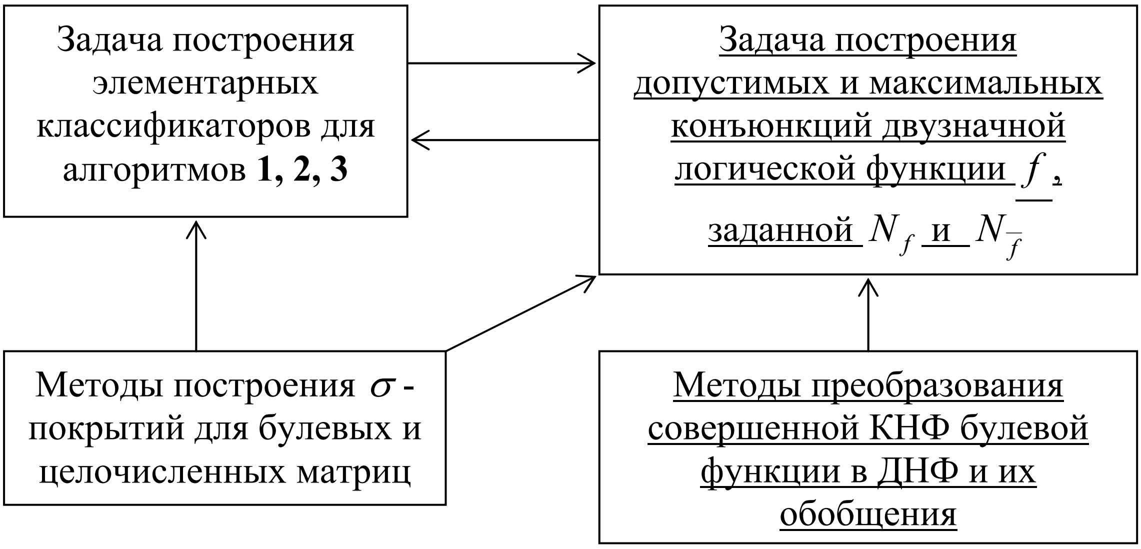

Рисунок 1.

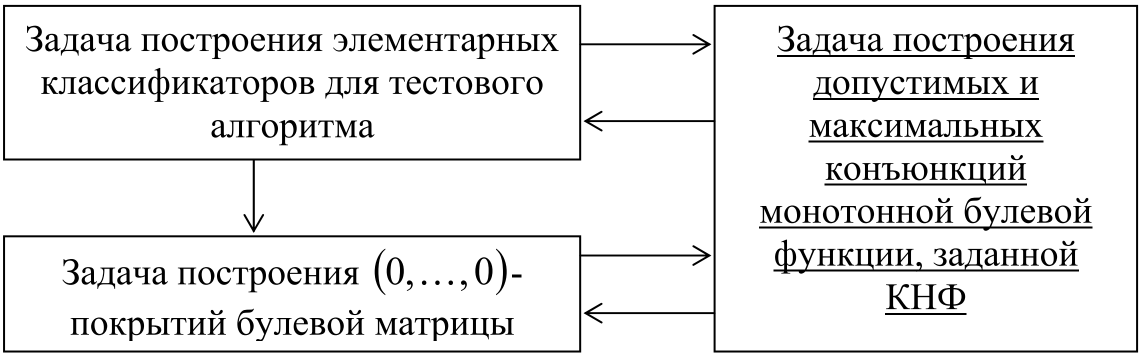

Рисунок 2.

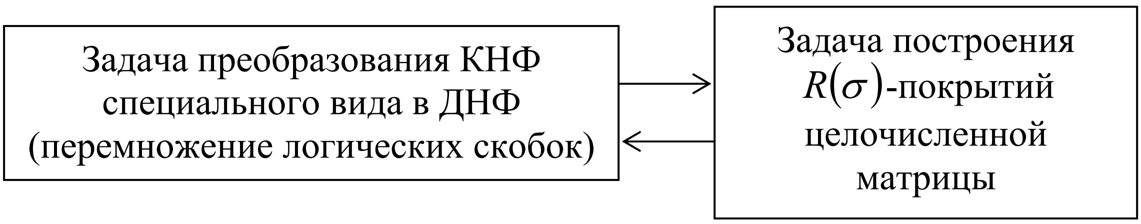

Рисунок 3.

Приложение 3.
Статистические свойства тупиковых покрытий в случае большого числа столбцов

Введем обозначения: M_{mn}^{k} - совокупность всех матриц размера $m \times n$ с элементами из $\{0,1,\ldots,k-1\}$, $k \geq 2$; E_k^r, $r \leq n$, - совокупность всех наборов вида $(\sigma_1,\ldots,\sigma_r)$, где $\sigma_i \in \{0,1,\ldots,k-1\}$, $k \geq 2$; φ_k - интервал

$$\left(\frac{1}{2}\log_k mn - \frac{1}{2}\log_k \log_k mn - \log_k \log_k \log_k n,\right.$$

$$\left.\frac{1}{2}\log_k mn - \frac{1}{2}\log_k \log_k mn + \log_k \log_k \log_k n\right).$$

Пусть $L \in M_{mn}^{k}, \sigma \in E_k^r$. Положим $B(L,\sigma)$ - множество тупиковых σ-покрытий матрицы L; $S(L,\sigma)$ - множество всех σ-подматриц матрицы L;

$$B(L) = \bigcup_{r=1}^{n} \bigcup_{\sigma \in E_k^r} B(L,\sigma);\ S(L) = \bigcup_{r=1}^{n} \bigcup_{\sigma \in E_k^r} C(L,\sigma).$$

Теорема 1. *Если* $m^{\alpha} \leq n \leq k^{m^{\beta}}$, $\alpha > 1, \beta < 1,$ *то для почти всех матриц* L *из* M_{mn}^{k} *при* $n \to \infty$ *справедливо*

$$|B(L)| \sim |S(L)| \sim \sum_{r \in \varphi_k} C_n^r C_m^r r!(k-1)^r k^{r-r^2}$$

и длины почти всех покрытий из $B(L)$ *принадлежат интервалу* φ_k.

Доказательство. Для простоты рассмотрим случай $k = 2, \sigma = (0,\ldots,0)$ (случай неприводимых покрытий). Формулировка теоремы 1 выглядит следующим образом. Пусть $B_1(L)$ - множество всех неприводимых покрытий и $S_1(L)$ - множество всех единичных подматриц в L. Требуется доказать, что

если $m^{\alpha} \leq n \leq 2^{m^{\beta}}$, $\alpha > 1, \beta < 1,$ *то для почти всех матриц* L *из* M_{mn}^{k} *при* $n \to \infty$ *справедливо*

$$|B_1(L)| \sim |S_1(L)| \sim \sum_{r \in \varphi_2} C_n^r C_m^r r! 2^{-r^2}$$

и длины почти всех неприводимых покрытий принадлежат интервалу φ_2.

Доказательство теоремы опирается на ряд приводимых ниже лемм.

Введем обозначения: $W_r^n, r \leq n$, - множество всех наборов вида $\{j_1,\ldots,j_r\}$, где $j_t \in \{1,2,\ldots,n\}$ при $t = 1,2,\ldots,r$ и $j_1 < \ldots < j_r$; $V_r^m, r \leq m$, - множество всех упорядоченных наборов вида $\{i_1,\ldots,i_r\}$, где $i_t \in \{1,2,\ldots,m\}$ при $t = 1,2,\ldots,r$ и $i_{t_1} \neq i_{t_2}$ при $t_1, t_2 = 1,2,\ldots,r$.

Пусть $v \in V_r^m, v = \{i_1,\ldots,i_r\}, w \in W_r^n, w = \{j_1,\ldots,j_r\},$ $\mathrm{M}_{(v,w)}$ -совокупность всех таких матриц $L = (a_{ij}), i = 1,2,\ldots,m,\ j = 1,2,\ldots,n$, в M_{mn}^{k}, для которых

$$a_{i_t j_q} = \begin{cases} 1, & \textit{если} \quad t = q, \\ 0, & \textit{иначе}, \end{cases}$$

$t, q = 1, 2, \ldots, r.$

Лемма 1. *Если* $v \in V_r^m$, $w \in W_r^n$, *то*

$$\left|\mathrm{M}_{(v,w)}\right| = 2^{mn - r^2}.$$

Доказательство леммы очевидно. Действительно, строки с номерами из v можно выбрать $2^{r(n-r)}$ способами, остальные строки - $2^{n(m-r)}$ способами.

Пусть $\mathrm{M}_{(v,w)}^*$ - совокупность всех таких матриц L в $\mathrm{M}_{(v,w)}$, для которых набор столбцов с номерами из w является $(0,\ldots,0)$-покрытием и $L \notin \mathrm{M}_{(v',w)}$ при $v' \neq v$.

Лемма 2. *Если* $v \in V_r^m$, $w \in W_r^n$, *то*

$$\left|\mathrm{M}_{(v,w)}^*\right| = 2^{mn - r^2}\left[1 - (r+1)/2^r\right]^{m-r}.$$

Доказательство леммы очевидно. Действительно, строки с номерами из v можно выбрать $2^{r(n-r)}$ способами, остальные строки - $\left[2^n - (r+1)2^{n-r}\right]^{m-r}$ способами. Нетрудно доказывается также

Лемма 3. *Если* $v_1 \in V_r^m$, $v_2 \in V_l^m$, $w_1 \in W_r^n$, $w_2 \in W_l^n$ *и наборы* v_1 *и* v_2 *пересекаются по* $a\,(a \geq 0)$ *элементам, а наборы* w_1 *и* w_2 *пересекаются по* $b\,(b \geq 0)$ *элементам, то*

$$\left|\mathrm{M}_{(v_1,w_1)} \cap \mathrm{M}_{(v_2,w_2)}\right| \leq 2^{mn - r^2 - l^2 + ab}.$$

Лемма 4. *Если* $m^\alpha \leq n \leq 2^{m^\beta}$, $\alpha > 1$, $\beta < 1$, *то при* $n \to \infty$ *имеет место*

$$\sum_{r=1}^{m} C_n^r C_m^r r! 2^{-r^2} \sim \sum_{r \in \varphi_2} C_n^r C_m^r r! 2^{-r^2}.$$

Положим $p = \dfrac{1}{2}\log mn - \dfrac{1}{2}\log\log mn$, $\quad q = \log\log\log n$, $\quad a_r = C_n^r C_m^r r! 2^{-r^2}$.

а) Пусть $\; r \geq p + q - 1$. Тогда имеем

$$\frac{a_{r+1}}{a_r} = \frac{(n-r)(m-r)}{r+1} 2^{-2r+1} \leq \frac{mn}{p} 2^{-2p-2q+3} \leq_n 4 \cdot 2^{-2q+3} = 32 \cdot 2^{-2q}.$$

б) Пусть $\; r \leq p - q + 1$. Тогда имеем

$$\frac{a_{r-1}}{a_r} = \frac{r 2^{2r-2}}{(n-r+1)(m-r+1)} \leq \frac{2(p-q+1)}{(n-q)(m-q)} \leq_n 16 \cdot 2^{-2q}.$$

Следовательно,

$$\sum_{r \in [p+q, m]} a_r = o\left(\sum_{r \in \varphi_2} a_r\right), \quad \sum_{r \in [1, p-q]} a_r = o\left(\sum_{r \in \varphi_2} a_r\right).$$ Ч.т.д.

Лемма 5. *Если* $r, l \leq c \log n$, $c < 1$, *то имеет место*

$$\sum_{b=0}^{\min(r,l)} 2^{lb} C_n^r C_r^b C_{n-r}^{l-b} < C_n^r C_n^l \left(1+\delta(n)\right),$$

где $\delta(n) \to 0$ *при* $n \to \infty$.

Доказательство. Обозначим $\lambda_b = 2^{lb} C_n^r C_r^b C_{n-r}^{l-b} \big/ C_n^r C_{n-r}^l$. Так как

$$\frac{C_r^b C_{n-r}^{l-b}}{C_{n-r}^l} \le \left[\frac{rl}{n-r-l}\right]^b$$

и по условию $r, l \le c \log n$, то

$$\lambda_b \le \left[\frac{\log^2 n}{n^{1-c}\left(1-2\log n/n\right)}\right]^b$$

и оцениваемая сумма не превосходит $C_n^r C_{n-r}^l [1+\delta(n)]$, где $\delta(n) \to 0$ при $n \to \infty$. Отсюда, пользуясь неравенством $C_{n-r}^l \le C_n^l$, получаем утверждение леммы.

Будем считать $M_{mn}^2 = \{L\}$ пространством элементарных событий, в котором каждое событие L происходит с вероятностью $1 \big/ \left|M_{mn}^2\right| = 1/2^{mn}$.

Через $MX(L)$ будем обозначать математическое ожидание случайной величины $X(L)$, через $DX(L)$ - дисперсию случайной величины $X(L)$.

Лемма 6. *Пусть для случайных величин* $X_1(L)$ *и* $X_2(L)$, *определенных на* M_{mn}^2, *выполнено* $X_1(L) \ge X_2(L) \ge 0$ *и при* $n \to \infty$ *верно* $MX_1(L) \sim MX_2(L)$, $DX_2(L) \big/ \left(MX_2(L)\right)^2 \to 0$. *Тогда для почти всех матриц* L *из* M_{mn}^2 *имеет место* $X_2(L) \sim X_1(L) \sim MX_2(L)$, $n \to \infty$. (Доказательство леммы не приводится.)

Пусть $v \in V_r^m$, $w \in W_r^n$. На $M_{mn}^2 = \{L\}$ рассмотрим случайные величины

$$\eta_{(v,w)}(L) = \begin{cases} 1, & \text{если } L \in \mathbf{M}_{(v,w)}, \\ 0, & \text{иначе;} \end{cases}$$

$$\xi_w(L) = \begin{cases} 1, & \text{если набор столбцов матрицы } L \\ & \text{с номерами из } w \text{ принадлежит } B_1(L), \\ 0, & \text{иначе.} \end{cases}$$

Оценим вероятность события $\eta_{(v,w)}(L) = 1$, обозначаемую далее через $P\left(\eta_{(v,w)}(L) = 1\right)$. Очевидно, в силу леммы 1,

$$P\left(\eta_{(v,w)}(L) = 1\right) = \left|\mathbf{M}_{(v,w)}\right| \Big/ \left|M_{mn}^2\right| = 2^{-r^2}. \tag{1}$$

Аналогично вероятность события $\xi_w(L) = 1$ обозначим через $P\left(\xi_w(L) = 1\right)$. Оценим $P\left(\xi_w(L) = 1\right)$, пользуясь леммой 1. Нетрудно видеть, что

$$P\left(\xi_w(L) = 1\right) \le \sum_{v \in V_r^m} \left|\mathbf{M}_{(v,w)}\right| \Big/ \left|M_{mn}^2\right| = C_m^r r! 2^{-r^2}. \tag{2}$$

С другой стороны, в силу леммы 2

$$P(\xi_w(L)=1) \geq \sum_{v \in V_r^m} \left|\mathbf{M}^*_{(v,w)}\right| \Big/ \left|M^2_{mn}\right| = C_m^r r! 2^{-r^2} \left[1-(r+1)/2^r\right]^{m-r}. \qquad (3)$$

Положим

$$\eta_1(L) = \sum_{r=1}^{n} \sum_{v \in V_r^m} \sum_{w \in W_r^n} \eta_{(v,w)}(L), \quad \eta_2(L) = \sum_{r \in \varphi_2} \sum_{v \in V_r^m} \sum_{w \in W_r^n} \eta_{(v,w)}(L).$$

Нетрудно видеть, что $\eta_1(L) = |S(L)|$, $\eta_2(L)$ - число единичных подматриц матрицы L, порядки которых принадлежат интервалу φ_2.

В силу (1)

$$M\eta_1(L) = \sum_{r=1}^{n} C_n^r C_m^r r! 2^{-r^2}, \quad M\eta_2(L) = \sum_{r \in \varphi_2} C_n^r C_m^r r! 2^{-r^2}.$$

Из полученных оценок для $M\eta_1(L)$, $M\eta_2(L)$ и леммы 4 сразу следует

Лемма 7. *Если* $m^\alpha \leq n \leq 2^{m^\beta}$, $\alpha > 1$, $\beta < 1$, *то*

$$M\eta_1(L) \sim M\eta_2(L) \sim \sum_{r \in \varphi_2} C_n^r C_m^r r! 2^{-r^2}, \; n \to \infty.$$

Пусть

$$\xi_1(L) = \sum_{r=1}^{n} \sum_{w \in W_r^n} \xi_w(L), \quad \xi_2(L) = \sum_{r \in \varphi_2} \sum_{w \in W_r^n} \xi_w(L).$$

Нетрудно видеть, что $\xi_1(L) = |B_1(L)|, \xi_2(L)$ - число неприводимых покрытий в L, длины которых принадлежат интервалу φ_2. Имеем

$$M\xi_1(L) = \sum_{r=1}^{n} \sum_{w \in W_r^n} P(\xi_w(L)=1), \quad M\xi_2(L) = \sum_{r \in \varphi_2} \sum_{w \in W_r^n} P(\xi_w(L)=1).$$

Следовательно, в силу (2)

$$M\xi_2(L) \leq M\xi_1(L) \leq \sum_{r=1}^{n} C_n^r C_m^r r! 2^{-r^2}. \qquad (4)$$

В силу (3)

$$M\xi_1(L) \geq M\xi_2(L) \geq \sum_{r \in \varphi_2} C_n^r C_m^r r! 2^{-r^2} \left[1-(r+1)/2^r\right]^{m-r} \geq F(n) \sum_{r \in \varphi_2} C_n^r C_m^r r! 2^{-r^2}, (5)$$

где $F(n) \to 1$ при $n \to \infty$. (Последнее неравенство следует из того, что $\left[1-(r+1)/2^r\right]^m = \exp\left(-m\left(1-(r+1)/2^r\right)\left(1/(1+\lambda)\right)\right)$, где $-(r+1)/2^r \leq \lambda \leq 0$ и $mr/2^r \leq \log^2 n / n^c$, $c > 0$, при $r \in \varphi_2$.)

Из (4), (5) и леммы 4 сразу следует

Лемма 8. *Если* $m^\alpha \leq n \leq 2^{m^\beta}$, $\alpha > 1$, $\beta < 1$, *то*

$$M\xi_1(L) \sim M\xi_2(L) \sim \sum_{r \in \varphi_2} C_n^r C_m^r r! 2^{-r^2}, \; n \to \infty.$$

Лемма 9. *Имеет место*

$$D\eta_2(L)\big/(M\eta_2(L))^2 \to 0$$

при $n \to \infty$.

Доказательство. Нетрудно видеть, что

$$M(\eta_2(L))^2 = \sum_{r,l\in\varphi_2} \sum_{\substack{v_1\in V_r^m, w_1\in W_r^n \\ v_2\in V_l^m, w_2\in W_l^n}} |\mathbf{M}|\big/2^{mn},$$

где $\mathbf{M} = \mathbf{M}_{(v_1,w_1)} \cap \mathbf{M}_{(v_2,w_2)}$. Отсюда, пользуясь леммами 3 и 5, получаем

$$M(\eta_2(L))^2 \le \sum_{r,l\in\varphi_2} \sum_{b=0}^{\min(r,l)} 2^{-r^2-l^2+lb} C_n^r C_r^b C_{n-r}^{l-b} C_m^r r! C_m^l l! \quad \le$$

$$\le \sum_{r,l\in\varphi_2} C_n^r C_n^l C_m^r r! C_m^l l! 2^{-r^2-l^2}(1+\delta(n)), \tag{6}$$

где $\delta(n) \to 0$ при $n \to \infty$.

С другой стороны, в силу леммы 7

$$(M\eta_2(L))^2 \sim \sum_{r\in\varphi_2} C_n^r C_n^l C_m^r r! C_m^l l! 2^{-r^2-l^2}, \quad n\to\infty. \tag{7}$$

Из (6), (7) и равенства $D\eta_2(L) = M(\eta_2(L))^2 - (M\eta_2(L))^2$ следует утверждение доказываемой леммы.

Аналогичным образом доказывается

Лемма 10. *Имеет место* $D\xi_2(L)\big/(M\xi_2(L))^2 \to 0$ *при* $n\to\infty$.

Утверждение теоремы 1 следует непосредственно из лемм 6-10.

Пусть $C_1(L)$ - совокупность всех $(0,\ldots,0)$-покрытий матрицы L из M_{mn}^k.

Теорема 2. *Если* $m^\alpha \le n \le k^{m^\beta}$, $\alpha > 1$, $\beta < 1$, *то для почти всех матриц* L *из* M_{mn}^k *при* $n\to\infty$ *справедливо*

$$|B_1(L)| \,/\, |C_1(L)| \to 0\,.$$

Доказательство. Будем считать совокупность матриц $M_{mn}^2 = \{L\}$ пространством элементарных событий, в котором каждое событие L происходит с вероятностью $1/2^{mn}$.

Пусть $w \in W_r^n$, $w = \{j_1,\ldots,j_r\}$. На множестве $M_{mn}^2 = \{L\}$ рассмотрим случайную величину

$$\zeta_w(L) = \begin{cases} 1, & \text{если набор столбцов матрицы } L \\ & \text{с номерами из } w \text{ является } (0,\ldots,0) - \text{покрытием;} \\ 0, & \text{иначе.} \end{cases}$$

Найдем $P(\zeta_w(L)=1)$ - вероятность события $\zeta_w(L)=1$. Для этого посмотрим, сколькими способами может быть построена матрица из M_{mn}^2, в которой столбцы с номерами $j_1,\ldots,j_r$ образуют $(0,\ldots,0)$-покрытие. Нетрудно видеть, что такая подматрица может быть построена $\left(2^r-1\right)^m \cdot 2^{m(n-r)}$ способами. Следовательно,

$$P(\zeta_w(L)=1)=\left(1-2^{-r}\right)^m. \tag{8}$$

Из (8) следует, что если $m2^{-r}\to 0$ при $n\to\infty$, то $P(\zeta_w(L)=1)\to 1$.

Если $m^\alpha \le n \le 2^{m^\beta}$, $\alpha>1, \beta<1$, и $r=[\log_2 n]$, то $m2^{-r}\to 0$ при $n\to\infty$. Следовательно, при указанных условиях доля тех матриц L из M_{mn}^2, в которых столбцы с номерами из w образуют $(0,\ldots,0)$-покрытие, стремится к 1 при $n\to\infty$.

Таким образом, для почти всех матриц L из M_{mn}^2 число всех $(0,\ldots,0)$-покрытий не меньше величины $2^{n-\log_2 n}+1$.

С другой стороны, в силу теоремы 1 имеем, что для почти всех матриц L из M_{mn}^2 число всех неприводимых покрытий не превосходит $(1+\delta(n))\sum\limits_{r\in\varphi_2} C_n^r < (1+\delta(n))n^{\log_2 n}\log_2 n$, где $\delta(n)\to 0$ при $n\to\infty$, и, следовательно, по порядку меньше числа всех $(0,\ldots,0)$-покрытий.

Теорема доказана.