УДК 519.217

Е.В. ХРАМОВА

ОБ УСЛОВИЯХ МАРКОВОСТИ РЕЗУЛЬТАТА ПРЕОБРАЗОВАНИЯ ОДНОРОДНЫХ ЦЕПЕЙ МАРКОВА С ПОМОЩЬЮ БУЛЕВЫХ ФУНКЦИЙ

We investigate the Markov property of a Boolean function of a finite number of homogeneous Markov chains. In particular, we proved that among all Boolean functions of $n \ge 2$ variables only Boolean function $f(x_1,\dots,x_n) = x_1 \oplus \dots \oplus x_n$ still enjoys the Markov-type property if transition probability matrices are symmetric.

Задача об общих условиях сохранения марковости рассматривалась во многих работах, изучающих укрупненные процессы (lumping) [1–4]. В теории конечных цепей Маркова известен следующий общий результат, вытекающий из теоремы [1] об укрупнении состояний, а именно общее условие сохранения марковости преобразования $n \ge 2$ независимых последовательностей бинарных случайных величин $\{x_t^{(i)}, t = 0, 1, 2, \dots\}$ $(i = 1, 2, \dots, n)$, являющихся однородными односвязными цепями Маркова (ОЦМ) с векторами начальных распределений вероятностей и матрицами вероятностей одношаговых переходов:

$$\pi^{(i)} = \left(\pi_j^{(i)}\right): \quad \pi_j^{(i)} = \mathrm{P}\left\{x_0^{(i)} = j\right\} > 0, \quad j = 0, 1, \tag{1}$$

$$P^{(i)} = \left(p_{j_1,j_2}^{(i)}\right): \quad p_{j_1,j_2}^{(i)} = \mathrm{P}\left\{x_{t+1}^{(i)} = j_2 \mid x_t^{(i)} = j_1\right\} > 0, \quad j_1, j_2 = 0, 1, \tag{2}$$

соответственно с помощью произвольной булевой функции $f(x_1,\dots,x_n)$ от n существенных переменных.

Теорема 1 [1]. *Пусть* $\{x_t^{(i)}, t = 0, 1, 2, \dots\}$ $(i = \overline{1,n})$ *– независимые последовательности бинарных случайных величин, образующие ОЦМ с параметрами* (1), (2). *Последовательность* $y_t = f(x_t^{(1)},\dots,x_t^{(n)})$ *является ОЦМ тогда и только тогда, когда для любых фиксированных* $u, v \in \{0,1\}$ *выполняется следующее условие* **У**: *значения функции* $g_f(v,u_1,\dots,u_n) = \sum\limits_{\substack{v_1,\dots,v_n \in \{0,1\},\\ f(v_1,\dots,v_n)=v}} \prod\limits_{j=1}^{n} p_{u_j,v_j}^{(j)}$ *не зависят от значений* $u_1,\dots,u_n \in \{0,1\}$ *таких, что* $f(u_1,\dots,u_n) = u$.

Отметим, что проверка выполнения **У** для конкретной булевой функции – сложная задача. Для функции суммы по модулю 2 конечного числа независимых ОЦМ на конечной группе условия марковости в алгебраических терминах были найдены в работе [5], из которой следует, что данная функция сохраняет марковское свойство в случае, если матрицы вероятностей одношаговых переходов являются симметрическими, причем матрица вероятностей одношаговых переходов для результата преобразования также симметрическая.

В настоящей работе рассматривается задача определения множества всех булевых функций от $n \ge 2$ переменных, сохраняющих марковское свойство.

Замечание. Пусть $\{x_t^{(i)}, t = 0, 1, 2, \dots\}$ $(i = 1, 2, \dots, n)$ являются вырожденным случаем ОЦМ, а именно схемами независимых испытаний (СНИ), т. е. для матриц вероятностей одношаговых переходов (2) справедливы следующие соотношения: $p_{j_1,j_2}^{(i)} = p_{j_1 \oplus 1,j_2}^{(i)}$, $j_1, j_2 = 0, 1$. Тогда для любой булевой функции от n переменных последовательность $y_t = f(x_t^{(1)},\dots,x_t^{(n)})$ также будет являться СНИ. Поэтому в дальнейшем будем рассматривать только ОЦМ, для которых выполняются следующие ограничения на вид матриц вероятностей одношаговых переходов:

$$p_{j_1,j_2}^{(i)} \ne p_{j_1 \oplus 1,j_2}^{(i)}, \quad j_1, j_2 = 0, 1, \quad i = 1, 2, \dots, n. \tag{3}$$

1. Множество булевых функций от двух переменных, сохраняющих марковское свойство. Рассмотрим вначале множество всех булевых функций от $n = 2$ переменных и выделим из них те, которые сохраняют марковское свойство. Покажем, что для проверки выполнения свойства марковости для произвольной булевой функции от двух переменных необходимо проверить выполнение данного свойства только для двух булевых функций: $f(x_1,x_2) = x_1 \oplus x_2$, $f(x_1,x_2) = x_1 \wedge x_2$. Известно, что существует 16 булевых функций от $n = 2$ переменных [6]:

$$f_j(x_1,x_2) = p_0 \oplus (x_2 \wedge p_1) \oplus (x_1 \wedge p_2) \oplus (x_1 \wedge x_2 \wedge p_3), \quad j = \sum_{i=0}^{3} 2^i p_i,\ p_i \in \{0,1\},\ j = \overline{0,15}.$$

Так как в данной работе рассматриваются только булевы функции от существенных переменных и добавление константы 1 к булевой функции не влияет на выполнение свойства марковости, то необходимо проверить выполнение свойства марковости для функций $f_{2j}(x_1, x_2),\ j=\overline{3,7}$. Так как последовательности $f_{10}(x_1,x_2)=x_2\wedge(x_1\oplus 1)=x_2\wedge\bar{x}_1$, $f_{12}(x_1,x_2)=x_1\wedge\bar{x}_2$, $f_{14}(x_1,x_2)=\bar{x}_1\wedge\bar{x}_2\oplus 1$ являются ОЦМ, если $f_8(x_1,x_2)$ также ОЦМ, то достаточно проверить выполнение свойства марковости для функций $f_6(x_1,x_2)=x_1\oplus x_2$ и $f_8(x_1,x_2)=x_1\wedge x_2$. Как уже отмечалось, задача нахождения условий марковости суммы по модулю два двух ОЦМ была рассмотрена в общем случае в работе [5]. Таким образом, для нахождения всех булевых функций от двух переменных, сохраняющих марковское свойство, необходимо рассмотреть задачу нахождения условий марковости конъюнкции двух ОЦМ.

Лемма 1. *В условиях теоремы* 1 *при выполнении ограничений* (3) *не существует таких ОЦМ* $x_t^{(1)}$, $x_t^{(2)}$, *что последовательность* $y_t=x_t^{(1)}\wedge x_t^{(2)}$ *является ОЦМ.*

Доказательство. Из теоремы 1 следует, что $y_t=x_t^{(1)}\wedge x_t^{(2)}$ является ОЦМ тогда и только тогда, когда выполняется **У**. Рассмотрим выполнение **У** для фиксированных значений $u=v=0$. Значения функции

$$g_{\wedge}(0,u_1,u_2)=\sum_{v_1\wedge v_2=0} p^{(1)}_{u_1,v_1}p^{(2)}_{u_2,v_2}=p^{(1)}_{u_1,0}p^{(2)}_{u_2,0}+p^{(1)}_{u_1,0}p^{(2)}_{u_2,1}+p^{(1)}_{u_1,1}p^{(2)}_{u_2,0}\equiv p^{(1)}_{u_1,0}+p^{(1)}_{u_1,1}p^{(2)}_{u_2,0}$$

не зависят от значений $u_1,u_2\in\{0,1\}$ таких, что $u_1\wedge u_2=0$, т. е. не зависят от $u_1,u_2\in\{(0,0),(0,1),(1,0)\}$. Тогда **У** можно представить в следующем виде:

$$p^{(1)}_{0,0}+p^{(1)}_{0,1}p^{(2)}_{0,0}=p^{(1)}_{0,0}+p^{(1)}_{0,1}p^{(2)}_{1,0}=p^{(1)}_{1,0}+p^{(1)}_{1,1}p^{(2)}_{0,0}. \tag{4}$$

Из равенств (4) получаем: $p^{(1)}_{0,0}=p^{(1)}_{1,0}$, $p^{(1)}_{0,1}=p^{(1)}_{1,1}$ и $p^{(2)}_{0,0}=p^{(2)}_{1,0}$, $p^{(2)}_{0,1}=p^{(2)}_{1,1}$, что противоречит ограничениям (3), откуда вытекает справедливость леммы 1. ■

Таким образом, при выполнении ограничений (3) среди всех булевых функций от двух переменных только функция $f(x_1,x_2)=x_1\oplus x_2$ сохраняет марковское свойство в случае симметричности матриц вероятностей одношаговых переходов.

2. Множество булевых функций от $n\geq 2$ переменных, сохраняющих марковское свойство. Покажем, что среди всех булевых функций от $n\geq 2$ переменных только функция $f(x_1,\ldots,x_n)=x_1\oplus\ldots\oplus x_n$ сохраняет марковское свойство. Сформулируем данный результат в виде следующей теоремы.

Теорема 2. *В условиях теоремы* 1 *при выполнении ограничений* (3) *последовательность* $y_t=f(x_t^{(1)},\ldots,x_t^{(n)})$ *является ОЦМ тогда и только тогда, когда функция* $f:\{0,1\}^n\to\{0,1\}$ *может быть представлена в виде*

$$f(x_t^{(1)},\ldots,x_t^{(n)})=x_t^{(1)}\oplus\ldots\oplus x_t^{(n)}\oplus c,\quad c\in\{0,1\},\quad i=\overline{1,n}, \tag{5}$$

и матрицы $P^{(i)}$, $i=\overline{1,n}$, *имеют следующий вид:*

$$P^{(i)}=\begin{pmatrix}1-p_i & p_i\\ p_i & 1-p_i\end{pmatrix},\quad 0<p_i<1,\quad i=\overline{1,n}. \tag{6}$$

Доказательство. Справедливость теоремы при $n=2$ была показана в п. 1. Справедливость теоремы при $n>2$ докажем по индукции. Пусть для случая $n=k-1$ теорема 2 справедлива, т. е. среди всех булевых функций от $k-1$ переменной только булева функция $f(x_t^{(1)},\ldots,x_t^{(k-1)})=x_t^{(1)}\oplus\ldots\oplus x_t^{(k-1)}$ является ОЦМ в случае, если матрицы $P^{(i)}$, $i=\overline{1,k-1}$, являются симметрическими [5]. Покажем, что теорема 2 справедлива при $n=k$. Для этого, как следует из результата теоремы 1, необходимо показать, что **У** выполняется, только если справедливы (5), (6). Любую булеву функцию $f(x_1,\ldots,x_k)$ можно представить в виде [6]

$$f(x_1,\ldots,x_k)=h_1(x_1,\ldots,x_{k-1})\oplus(x_k\wedge h_2(x_1,\ldots,x_{k-1})), \tag{7}$$

где $h_1,h_2:\{0,1\}^{k-1}\to\{0,1\}$ – некоторые фиксированные булевы функции.

Тогда функцию $g_f(v,u_1,\ldots,u_k)$ можно записать в виде

$$g_f(v,u_1,\ldots,u_k)=\sum_{h_1(v_1,\ldots,v_{k-1})\oplus(v_k\wedge h_2(v_1,\ldots,v_{k-1}))=v}\prod_{j=1}^{k}p^{(j)}_{u_j,v_j}=p^{(k)}_{u_k,0}\sum_{h_1(v_1,\ldots,v_{k-1})=v}\prod_{j=1}^{k-1}p^{(j)}_{u_j,v_j}+$$

$$+p^{(k)}_{u_k,1}\sum_{h_1(v_1,\ldots,v_{k-1})\oplus h_2(v_1,\ldots,v_{k-1})=v}\prod_{j=1}^{k-1}p^{(j)}_{u_j,v_j}=p^{(k)}_{u_k,0}g_{h_1}(v,u_1,\ldots,u_{k-1})+p^{(k)}_{u_k,1}g_{h_1\oplus h_2}(v,u_1,\ldots,u_{k-1}).$$

Тогда **У** можно записать в виде следующих трех условий.

$У_1$: для любых фиксированных $u,v\in\{0,1\}$ значения функции

$$g_f(v,u_1,\ldots,u_{k-1},0)=p^{(k)}_{0,0}g_{h_1}(v,u_1,\ldots,u_{k-1})+p^{(k)}_{0,1}g_{h_1\oplus h_2}(v,u_1,\ldots,u_{k-1})$$

не зависят от $u_1,\ldots,u_{k-1}\in\{0,1\}$ таких, что $h_1(u_1,\ldots,u_{k-1})=u$;

$У_2$: для любых фиксированных $u,v\in\{0,1\}$ значения функции

$$g_f(v,u_1,\ldots,u_{k-1},1)=p^{(k)}_{1,0}g_{h_1}(v,u_1,\ldots,u_{k-1})+p^{(k)}_{1,1}g_{h_1\oplus h_2}(v,u_1,\ldots,u_{k-1})$$

не зависят от $u_1,\ldots,u_{k-1}\in\{0,1\}$ таких, что $h_1(u_1,\ldots,u_{k-1})\oplus h_2(u_1,\ldots,u_{k-1})=u$;

$У_3$: $g_f(v,u^{(1)}_1,\ldots,u^{(1)}_{k-1},0)=g_f(v,u^{(2)}_1,\ldots,u^{(2)}_{k-1},1)$ для $u^{(i)}_1,\ldots,u^{(i)}_{k-1}\in\{0,1\}$, $i=1,2$, таких, что $h_1(u^{(2)}_1,\ldots,u^{(2)}_{k-1})\oplus h_2(u^{(2)}_1,\ldots,u^{(2)}_{k-1})=u$, $h_1(u^{(1)}_1,\ldots,u^{(1)}_{k-1})=u$.

Отметим, что для выполнения **$У_1$** и **$У_2$** необходимо, чтобы функции h_1 и $h_1\oplus h_2$ от $k-1$ переменной являлись ОЦМ, т. е. по предположению теоремы функции h_1 и h_2 имеют следующий вид:

$$\begin{aligned}&h_1(x_1,\ldots,x_{k-1})=\alpha_0\oplus\alpha_1x_1\oplus\ldots\oplus\alpha_{k-1}x_{k-1},\quad \alpha_j\in\{0,1\},\ j=\overline{1,k-1},\\&h_2(x_1,\ldots,x_{k-1})=\beta_0\oplus\beta_1x_1\oplus\ldots\oplus\beta_{k-1}x_{k-1},\quad \beta_j\in\{0,1\},\ j=\overline{1,k-1}.\end{aligned}\tag{8}$$

Подставляя (8) в (7), получим, что функция f будет иметь следующий вид:

$$f(x_1,\ldots,x_k)=\alpha_0\oplus\alpha_1x_1\oplus\ldots\oplus\alpha_{k-1}x_{k-1}\oplus x_k\wedge(\beta_0\oplus\beta_1x_1\oplus\ldots\oplus\beta_{k-1}x_{k-1}).$$

Определим множества: $K=\{1,\ldots,k-1\}$, $\mathrm{A}=\{i:\ \alpha_i=1,i\in K\}$, $\mathrm{B}=\{i:\ \beta_i=1,i\in K\}$, $\mathrm{A}\cup\mathrm{B}=K$.

1) Пусть $\mathrm{A}=K$, $\mathrm{B}=\varnothing$, тогда функция f представима в виде: $f(x_1,\ldots,x_k)=$ $=\alpha_0\oplus x_1\oplus\ldots\oplus x_{k-1}\oplus x_k=z\oplus x_k$. Так как по предположению теоремы z является ОЦМ с симметрической матрицей вероятностей одношаговых переходов, то из работы [5] следует, что только в случае, если $\beta_0=1$ и матрица $P^{(k)}$ является симметрической, для функции $f(x_1,\ldots,x_k)=\alpha_0\oplus x_1\oplus\ldots\oplus x_k$ выполняется свойство марковости.

2) Для случаев: а) $\mathrm{B}=K$, $\mathrm{A}=\varnothing$: $f(x_1,\ldots,x_k)=\alpha_0\oplus x_k\wedge(\beta_0\oplus\bigoplus_{l\in K}x_l)=\alpha_0\oplus x_k\wedge z$, где по предположению теоремы $z-$ОЦМ с симметрической матрицей вероятностей одношаговых переходов; б) $A\subset K$, $B=K\setminus A$, $A,B\neq\varnothing$: $f(x_1,\ldots,x_k)=\alpha_0\oplus\bigoplus_{l\in A}x_l\oplus x_k\wedge(\beta_0\oplus\bigoplus_{l\in K\setminus A}x_l)=z_1\oplus x_k\wedge z_2$, где по предположению теоремы z_1, z_2 – независимые ОЦМ с симметрическими матрицами вероятностей одношаговых переходов; из леммы 1 следует, что функция f не является ОЦМ, так как операция конъюнкции не сохраняет марковское свойство.

3) Пусть $A=A_1\cup C$, $B=K\setminus A_1$, $A,B,C\neq\varnothing$, тогда функция f представима в виде: $f(x_1,\ldots,x_k)=\alpha_0\oplus\bigoplus_{l\in A_1}x_l\oplus\bigoplus_{l\in C}x_l\oplus x_k\wedge(\bigoplus_{l\in K\setminus A}x_l\oplus\bigoplus_{l\in C}x_l)$. Отметим, что в данном случае f будет являться ОЦМ, если результат преобразования с помощью функции $h(x_1,x_2,x_3)=x_1\oplus x_3\wedge(x_1\oplus x_2)$, где x_1, x_2, x_3 – независимые ОЦМ, причем только для x_1, x_2 матрицы вероятностей одношаговых переходов должны быть симметрическими. Проверим выполнение свойства марковости **У** для функции h. Пусть зафиксированы значения $u=v=0$. Тогда множество таких $(u_1,u_2,u_3)\in\{0,1\}$, что $u_1\oplus u_3\wedge(u_1\oplus u_2)=0$, имеет следующий вид $\{(0,0,0),(0,0,1),(0,1,0),(1,0,1)\}$. Тогда для выполнения **У** необходимо выполнение следующего равенства: $g_h(0,0,0,1)=g_h(0,0,1,0)$, т. е.

$$p^{(1)}_{0,0}p^{(2)}_{0,0}+p^{(1)}_{0,0}p^{(2)}_{0,1}p^{(3)}_{1,0}+p^{(1)}_{0,1}p^{(2)}_{0,0}p^{(3)}_{1,1}=p^{(1)}_{0,0}p^{(2)}_{1,0}+p^{(1)}_{0,0}p^{(2)}_{1,1}p^{(3)}_{0,0}+p^{(1)}_{0,1}p^{(2)}_{1,0}p^{(3)}_{0,1}.$$

Откуда, используя свойство матриц вероятностей одношаговых переходов: $p^{(j)}_{j_1,j_2} = 1 - p^{(j)}_{j_1,j_2 \oplus 1}$, $j_1, j_2 = 0, 1,$ получаем следующее равенство:

$$p^{(1)}_{0,0}(p^{(3)}_{0,0} + p^{(3)}_{1,1} - 1) + (1 - p^{(2)}_{1,1})(1 - p^{(3)}_{0,0}) - p^{(2)}_{0,0} p^{(3)}_{1,1} = 0,$$

которое выполняется, если $p^{(3)}_{0,0} + p^{(3)}_{1,1} = 1$ и $(1 - p^{(2)}_{1,1})(1 - p^{(3)}_{0,0}) = p^{(2)}_{0,0} p^{(3)}_{1,1}$, т. е. если $p^{(2)}_{0,0} = p^{(2)}_{1,0}$, $p^{(2)}_{0,1} = p^{(2)}_{1,1}$ и $p^{(3)}_{0,0} = p^{(3)}_{1,0}$, $p^{(3)}_{0,1} = p^{(3)}_{1,1}$, что противоречит ограничениям (3). Таким образом, условие марковости выполняется только в случае, если булева функция от k переменных имеет вид $f(x_1, \ldots, x_k) = x_1 \oplus \ldots \oplus x_k \oplus c$, $c \in \{0, 1\}$, и $p^{(k)}_{0,0} = p^{(k)}_{1,1}$, $p^{(k)}_{0,1} = p^{(k)}_{1,0}$, т. е. справедливы (5), (6). Откуда получаем справедливость теоремы 2.■

Таким образом, при выполнении ограничений (3) среди всех булевых функций от $n \geq 2$ существенных переменных только функция $f(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n$ сохраняет марковское свойство в случае, если матрицы вероятностей одношаговых переходов являются симметрическими. Отметим, что для вырожденного случая ОЦМ, а именно схем независимых испытаний, марковское свойство выполняется для всех булевых функций.

1. Кемени Дж., Снелл Дж. Конечные цепи Маркова. М., 1970. С. 159.
2. Rogers L.C.G., Pitman J.W. // Ann. Probab. 1981. Vol. 9. P. 573.
3. Gurvits L., Ledoux J. // Algebra and its Applications. 2005. Vol. 404. P. 85.
4. Nilsson Jacobi M., Goernerup O. // ArXiv e-prints. 2007. Vol. 710. P. 6.
5. Рожков М.И. О суммировании цепей Маркова на конечной группе // Труды по дискретной математике. 2000. Т. 3. С. 195.
6. Wegener I. The complexity of Boolean functions. Stuttgart, 1987. С. 6.

Поступила в редакцию 16.10.08.

Елизавета Владимировна Храмова – научный сотрудник НИЛ математических методов защиты информации НИИППМИ.