Экстракция доказуемо *случайной* битовой последовательности из траекторий цепи Маркова

1 Общая схема ФГСЧ

ИСТОЧНИК ШУМА

↓

исходная **0,1-последовательность** $\boldsymbol{X}$

↓

преобразование (экстракция) $\boldsymbol{\Psi}$

↓

выходная **0,1-последовательность** $\boldsymbol{Y}$

2 Основной результат

$\boldsymbol{X}$- цепь Маркова произвольного порядка $\boldsymbol{r} \geq 1$

$\boldsymbol{\Psi}$- алгоритм арифметического кодирования В.Ф. Бабкина

$\boldsymbol{Y}$- равновероятная последовательность, $\boldsymbol{P}(\boldsymbol{Y}) = \boldsymbol{2}^{-\ell}$

3 Арифметическое кодирование В.Ф. Бабкина

3.1 Нумерация, *бинарный* алфавит

Блок

$$\boldsymbol{X = x_1, ..., x_n},$$

$$\boldsymbol{x_i \in \{s_1, s_2\}},$$

$\boldsymbol{k}$ символов $\boldsymbol{s_1}$ на местах

$$\boldsymbol{(i_1, i_2, ..., i_k), 1 \leq i_1 < i_2 < ..... < i_k \leq n},$$

$\boldsymbol{\mathcal{R}_n(k) = C_n^k}$ – число таких блоков. Блоку присваивается номер

$$\boldsymbol{Num(i_1, i_2, ..., i_k) = C^1_{i_1-1} + C^2_{i_2-1} + ... C^{k-1}_{i_{k-1}-1} + C^k_{i_k-1}, C^i_j = 0}, \text{если} \boldsymbol{j < i}.$$

Нумерация – скоростная, *по ходу* появления $\boldsymbol{i_1, i_2, ..., i_k}$.
Имеет место взаимно-однозначное соответствие

$$\boldsymbol{x_1, ..., x_n \Longleftrightarrow (i_1, i_2, ..., i_k) \Longleftrightarrow Num(i_1, i_2, ..., i_k)}$$

3.2 Экстракция битов из номера

Число блоков

$$\boldsymbol{\mathcal{R}_n(k) = C_n^k = 2^{r_m} + \ldots + 2^{r_1} + 2^{r_0}}$$

Двоичное *разложение* номера блока

$$\boldsymbol{Num(i_1, i_2, \ldots i_k) =}$$

$$\boldsymbol{= \varepsilon_{r_m+1} 2^{r_m+1} + \varepsilon_{r_m} 2^{r_m} + \varepsilon_{r_m-1} 2^{r_m-1} + \ldots + \varepsilon_1 2^1 + \varepsilon_0 2^0, \quad \varepsilon_r \in \{0, 1\},}$$

Номера $\boldsymbol{Num(i_1, i_2, \ldots i_k)}$ упорядочиваются по возрастанию

номер	блок $\{\varepsilon\}$ случайных 0 и 1
$\boldsymbol{0 \le Num(i_1, i_2, \ldots i_k) \le 2^{r_0} - 1}$	$\boldsymbol{\varepsilon_{r_0-1}, \ldots, \varepsilon_0}$
$\boldsymbol{2^{r_0} \le Num(i_1, i_2, \ldots i_k) \le 2^{r_0} + 2^{r_1} - 1}$	$\boldsymbol{\varepsilon_{r_1-1}, \ldots, \varepsilon_0}$
$\boldsymbol{2^{r_0} + 2^{r_1} \le Num(i_1, i_2, \ldots i_k) \le 2^{r_0} + 2^{r_1} + 2^{r_2} - 1}$	$\boldsymbol{\varepsilon_{r_2-1}, \ldots, \varepsilon_0}$
$\boldsymbol{\ldots}$	$\boldsymbol{\ldots}$
$\boldsymbol{2^{r_0} + \ldots + 2^{r_m} \le Num(i_1, i_2, \ldots i_k) \le 2^{r_0} + \ldots + 2^{r_m} - 1}$	$\boldsymbol{\varepsilon_{r_m-1}, \ldots, \varepsilon_0}$

Пример $\boldsymbol{n = 8, k = 2,}$

$$\boldsymbol{\mathcal{R}_n(k) = \frac{8!}{2!4!} = 28 = 2^4 + 2^3 + 2^2, \quad m = 2, \quad r_2 = 4, \quad r_1 = 3, \quad r_0 = 2.}$$

Двоичный *выход* содержит двоичные вектора *фиксированной* длины ***ровно по одному разу***.

(i_1, i_2) позиции s_1,s_2	$N(i_1, i_2)$ номер	двоичное представление	$\{\varepsilon\} = \varepsilon_{r_j-1}, \ldots, \varepsilon_0$ случайный блок
$\overbrace{s_1 s_1}\, s_2 s_2 s_2 s_2 s_2 s_2$	**0**	**00000**	**00**
...	**1**	**00001**	**01**
$j = 0$	**2**	**00010**	**10**
	$3 = 2^{r_0} - 1$	**00011**	**11**
	4	**00100**	**100**
	5	**00101**	**101**
	6	**00110**	**110**
$j = 1$	**7**	**00111**	**111**
	8	**01000**	**000**
	9	**01001**	**001**
	10	**01010**	**010**
	$11 = 2^{r_1} + 2^{r_0} - 1$	**01011**	**011**
	12	**01100**	**1100**
	13	**01101**	**1101**
	14	**01110**	**1110**
	15	**01111**	**1111**
	16	**10000**	**0000**
	17	**10001**	**0001**
$j = 2$	**18**	**10010**	**0010**
	19	**10011**	**0011**
	20	**10100**	**0100**
	21	**10101**	**0101**
	22	**10110**	**0110**
	23	**10111**	**0111**
	24	**11000**	**1000**
	25	**11001**	**1001**
	26	**11010**	**1010**
$s_2 s_2 s_2 s_2 s_2 s_2 \overbrace{s_1 s_1}$	$27 = 2^{r_2} + 2^{r_1} + 2^{r_0} - 1$	**11011**	**1011**

Таблица 1: Алгоритм В.Ф. Бабкина $\boldsymbol{\Psi}$, двоичный выход, $\boldsymbol{n = 8, k = 2}$

3.3 Нумерация, m-арный алфавит

Блок

$$\boldsymbol{x_1, ..., x_n},,$$

$$\boldsymbol{x_i \in \{s_1, ..., s_m\}},$$

содержит $\boldsymbol{k_1, ..., k_m}$ символов $\boldsymbol{s_1, ..., s_m}$, $\boldsymbol{k_1 + ... + k_m = n}$,

$$\boldsymbol{\mathcal{R}_n(k_1, ..., k_m) = \frac{n!}{k_1!k_2!..., k_m!}}.$$

Существует алгоритм (сложно реализуемый) *однозначной* нумерации

$$\boldsymbol{X = x_1, ..., x_n \Longleftrightarrow Num(X),}$$

$$\boldsymbol{0 \leq Num(X) \leq \mathcal{R}_n(k_1, ..., k_m) - 1}$$

Экстракция двоичных битов

$$\boldsymbol{Num(X) \Longrightarrow \{\varepsilon\} = \varepsilon_{r_j - 1}, \ldots, \varepsilon_0}$$

происходит аналогично случаю ***бинарного*** алфавита.

4 Доказательство случайности, независимый вход, бинарный алфавит

$$\boldsymbol{X} = (\boldsymbol{X_1}, ..., \boldsymbol{X_M})\,.$$

$\boldsymbol{Y_i} = \boldsymbol{\Psi}\,(\boldsymbol{X_i})$ – *отдельный* двоичный выход алгоритма Бабкина на блоке $\boldsymbol{X_i}$,

$$\boldsymbol{Y} = \boldsymbol{\Psi}\,(\boldsymbol{X}) = \underbrace{\boldsymbol{\Psi}(\boldsymbol{X_1}) \parallel ... \parallel \boldsymbol{\Psi}\,(\boldsymbol{X_M})} = \boldsymbol{Y_1} \parallel ... \parallel \boldsymbol{Y_M}$$

– *полный* двоичный выход алгоритма В.Ф. Бабкина, *конкатенация.*

4.1 Центральное место доказательства (H. Zhou)

Разбиение всех последовательностей $\{\boldsymbol{X} = (\boldsymbol{X_1}, ..., \boldsymbol{X_M})\}$ ***на классы одинаково-вероятных последовательностей*** $\boldsymbol{S}$**.**

Пусть *инициирующая* последовательность

$$\boldsymbol{X} = (\boldsymbol{X_1}, ..., \boldsymbol{X_M})$$

задает **класс** $\boldsymbol{S}$**.** Тогда включаем

$$\boldsymbol{X'} = (\boldsymbol{X'_1}, ..., \boldsymbol{X'_M}) \in \boldsymbol{S},$$

если $\boldsymbol{X'_i} \equiv \boldsymbol{X_i}$ – ***перестановка***.

Вероятность $\boldsymbol{P}\,(\boldsymbol{X'}) = \boldsymbol{P}\,(\boldsymbol{X})$.

Фиксируем $\boldsymbol{Y}$,

$$\boldsymbol{B_Y = \{X : \Psi(X) = Y\} = \bigcup_S \left\{ S \bigcap B_Y \right\}}$$

– множество последовательностей $\boldsymbol{X}$ таких, что $\boldsymbol{\Psi(X) = Y}$ (множество прообразов $\boldsymbol{Y}$).

Используем *конструктивное* свойство двоичного выхода алгоритма В.Ф. Бабкина:

на *перестановках* отдельных блоков двоичный *выход* содержит ***все*** двоичные вектора ***фиксированной*** длины ***ровно по одному разу***.

Следствие:

в каждом классе $\boldsymbol{S}$ *одинаково-вероятных последовательностей число* прообразов $\boldsymbol{X}$ для двоичного выхода $\boldsymbol{Y}$ и $\boldsymbol{Y'}$ одинаково:

$$\boldsymbol{|S \bigcap B_{Y'}| = |S \bigcap B_Y|.}$$

4.2 Пример. 3 блока

Пусть $\boldsymbol{X = (X_1, X_2, X_3)}$, $\boldsymbol{n_1 = n_2 = n_3 = 8}$, $\boldsymbol{k_1^{(1)} = k_1^{(2)} = k_1^{(3)} = 2}$.

«Битовые» длины $\boldsymbol{2, 3, 4}$, суммарная длина $\boldsymbol{\ell = 6, 7, ..., 12}$. Как может получиться, например, $\boldsymbol{Y = (01101001110)}$ длиной $\boldsymbol{\ell = 11}$? Ответ – в 3-х вариантах *конкатенации*:

$$\boldsymbol{011 \parallel 0100 \parallel 1110}$$
$$\boldsymbol{0110 \parallel 100 \parallel 1110}$$
$$\boldsymbol{0110 \parallel 1001 \parallel 110}$$

Этим 3-м вариантам соответствуют 3 прообраза $\boldsymbol{X}$ из класса $\boldsymbol{S}$ *одинаково-вероятных последовательностей, порождаемого* $\boldsymbol{X = (X_1, X_2, X_3)}$.

Аналогично для $\boldsymbol{Y' = (10010001001)}$ длиной $\boldsymbol{\ell = 11}$ имеем 3 варианта *конкатенации*:

$$\begin{array}{l} \mathbf{100} \parallel \mathbf{1000} \parallel \mathbf{1001} \\ \mathbf{1001} \parallel \mathbf{000} \parallel \mathbf{1001} \\ \mathbf{1001} \parallel \mathbf{0001} \parallel \mathbf{001} \end{array},$$

которым соответствуют *свои* 3 прообраза $\boldsymbol{X = (X_1, X_2, X_3)}$.

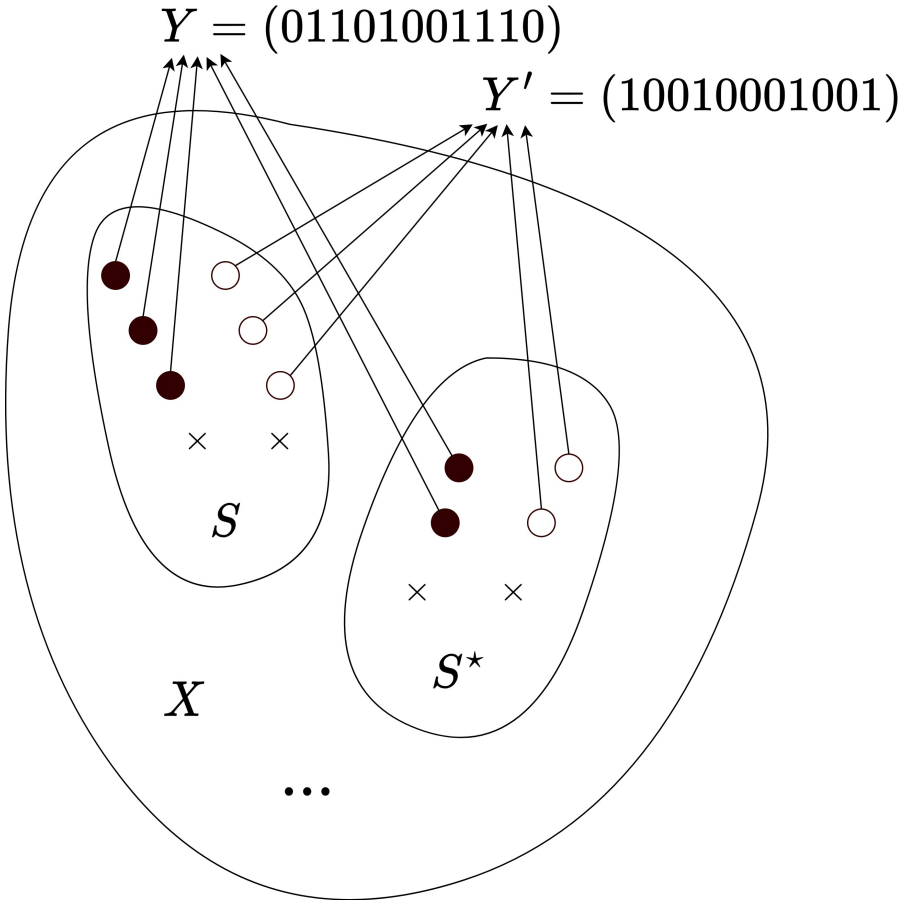

Рис. 1: К доказательству случайности

По формуле полной вероятности имеем

$$\boldsymbol{P}(\boldsymbol{Y}) = \boldsymbol{P}(\boldsymbol{X} \in \boldsymbol{B_Y}) =$$
$$= \sum_{\boldsymbol{S} \in \boldsymbol{G}} \boldsymbol{P}(\boldsymbol{X} \in \boldsymbol{S})\, \boldsymbol{P}(\boldsymbol{X} \in \boldsymbol{B_Y} \mid \boldsymbol{X} \in \boldsymbol{S}) =$$
$$= \sum_{\boldsymbol{S} \in \boldsymbol{G}} \boldsymbol{P}(\boldsymbol{X} \in \boldsymbol{S})\, \frac{\boldsymbol{P}(\boldsymbol{X} \in \boldsymbol{S} \bigcap \boldsymbol{B_Y})}{\boldsymbol{P}(\boldsymbol{X} \in \boldsymbol{S})} =$$
$$= \sum_{\boldsymbol{S} \in \boldsymbol{G}} \boldsymbol{P}(\boldsymbol{X} \in \boldsymbol{S})\, \frac{\boldsymbol{P_S}(\boldsymbol{X}) \cdot |\boldsymbol{S} \bigcap \boldsymbol{B_Y}|}{\boldsymbol{P_S}(\boldsymbol{X}) \cdot |\boldsymbol{S}|} =$$
$$= \sum_{\boldsymbol{S} \in \boldsymbol{G}} \boldsymbol{P}(\boldsymbol{X} \in \boldsymbol{S})\, \frac{|\boldsymbol{S} \bigcap \boldsymbol{B_Y}|}{|\boldsymbol{S}|}.$$

Рассмотрим теперь любой другой выход $\boldsymbol{Y'} \in \{\boldsymbol{0,1}\}^{\boldsymbol{\ell}}$. Имеем

$$|\boldsymbol{S} \bigcap \boldsymbol{B_{Y'}}| = |\boldsymbol{S} \bigcap \boldsymbol{B_Y}|.$$

Отсюда немедленно заключаем, что

$$\boldsymbol{P}(\boldsymbol{Y}) = \boldsymbol{P}(\boldsymbol{Y'}).$$

Поскольку это равенство выполняется для любых $\boldsymbol{Y, Y'} \in \{\boldsymbol{0,1}\}^{\boldsymbol{\ell}}$, то отсюда следует, что

$$\boldsymbol{P}(\boldsymbol{Y}) = \boldsymbol{2^{-\ell}}.$$

5 Цепь Маркова с m состояниями порядка $r = 1$

Траектория цепи Маркова

$$\boldsymbol{X = x_1 x_2 ... x_N},$$

$$\boldsymbol{x_i \in \{s_1, ..., s_m\}}.$$

$$\boldsymbol{P(X) = P(x_1 x_2 ... x_N) = P(x_1) \prod_{i=1}^{N-1} P(x_{i+1}|x_i)}.$$

5.1 π-последовательности, классы одинаково-вероятных траекторий

Для траектории цепи Маркова $\boldsymbol{X = x_1 x_2 ... x_N}$ *вводится* совокупность $\boldsymbol{\pi}$-последовательностей

$$\boldsymbol{\pi(X) = [\pi_1(X), \pi_2(X), ..., \pi_m(X)]},$$

где $\boldsymbol{\pi_i(X)}$ – подпоследовательность состояний из $\boldsymbol{X = x_1 x_2 ... x_N}$, следующих за состоянием $\boldsymbol{s_i}$:

$$\boldsymbol{\pi_i(X) = \{x_{j+1} : x_j = s_i, 1 \le j \le N\}}.$$

Например, для $\boldsymbol{m = 4}$

$$\boldsymbol{X = \overset{\bullet}{\overbrace{s_1}} s_4 s_2 \overset{\bullet}{\overbrace{s_1}} s_3 s_2 s_3 \overset{\bullet}{\overbrace{s_1}} \overset{\bullet}{\overbrace{s_1}} s_2 s_3 s_4 s_1}$$

$$\boldsymbol{\pi(X) = [\pi_1(X) = (s_4 s_3 s_1 s_2), \pi_2(X) = (s_1 s_3 s_3), \pi_3(X) = (s_2 s_1 s_4), \pi_4(X) = (s_2 s_1)]}$$

Пусть *инициирующая* траектория цепи Маркова

$$\boldsymbol{X = x_1 x_2 ... x_N}$$

задает класс S. Тогда включаем

$$\boldsymbol{X' = x'_1 x'_2 ... x'_N \in S},$$

если:

1) $\boldsymbol{x'_1 = x_1}$ и $\boldsymbol{x'_N = x_N = s_\chi}$ – *начало и конец* траекторий X и X' одинаковы,

2) $\boldsymbol{\pi_\chi (X') \equiv \pi_\chi (X)}$ – любая перестановка,

3) $\boldsymbol{\pi_i (X') \overset{\bullet}{\equiv} \pi_i (X)\,,\ i \neq \chi}$ – перестановка *с фиксированным хвостом.*

Именно для таких $\boldsymbol{\pi}$ – последовательностей будет ***существовать*** траектория $\boldsymbol{X'}$ (сложно доказывается).

Легко получаем *одинаково-вероятность* траекторий:

$$\boldsymbol{P(X) = P(x_1) \prod_{i=1}^{N-1} P(x_{i+1}|x_i) = P(x'_1) \prod_{i=1}^{N-1} P(x'_{i+1}|x'_i) = P(X')}$$

5.2 Экстракция случайных битов. Алгоритм А

Траектории цепи Маркова ставятся в *однозначное* соответствие $\boldsymbol{\pi}$-последовательности:

$$\boldsymbol{X = x_1 x_2 ... x_N, \Leftrightarrow \pi(X) = \{\pi_1(X), \ldots, \pi_\chi(X), \ldots, \pi_m(X)\}},$$

где $\boldsymbol{s_\chi = x_N}$ – *глобально* последний элемент цепи. Вероятность

$$\boldsymbol{P\left(X\right) = P\left(\pi_1(X), \ldots, \pi_\chi(X), \ldots, \pi_m(X)\right)}$$

Двоичный выход после применения m-арного алгоритма В.Ф. Бабкина записывается как

$$\boldsymbol{Y_\chi = \Psi\left(\pi_\chi(X)\right), Y_i = \Psi\left(\pi_i(X)^{|\pi_i(X)|-1}\right), i \neq \chi,}$$

где выражение $\boldsymbol{\pi_i(X)^{|\pi_i(X)|-1}}$ означает, что *последний* элемент в блоках $\boldsymbol{\pi_i(X), i \neq \chi}$, ***игнорируется***.

Конкатенируем

$$\boldsymbol{Y = \Psi\left(X\right) =}$$

$$\boldsymbol{= \Psi\left(\pi_1(X)^{|\pi_1(X)|-1}\right) \| \Psi\left(\pi_2(X)^{|\pi_2(X)|-1}\right) \| ... \| \Psi\left(\pi_\chi(X)\right) \| ... \| \Psi\left(\pi_m(X)^{|\pi_m(X)|-1}\right).}$$

Доказательство $\boldsymbol{P\left(Y\right) = 2^{-\ell}}$ проводится аналогично доказательству для *бернуллиевского* случая.

А именно, в классе эквивалентности $\boldsymbol{S}$ траекториям $\boldsymbol{X}$ и $\boldsymbol{X'}$ ставим ***однозначно*** в соответствие $\boldsymbol{\pi}$-последовательности

$$\boldsymbol{\pi_1(X) \ldots \pi_\chi(X) \ldots \pi_m(X)} \text{ и } \boldsymbol{\pi_1(X') \ldots \pi_\chi(X') \ldots \pi_m(X').}$$

Тогда

$$\boldsymbol{P}\left(\boldsymbol{\pi_1(X)\ldots\pi_\chi(X)\ldots\pi_m(X)}\right)=\boldsymbol{P}\left(\boldsymbol{\pi_1(X')\ldots\pi_\chi(X')\ldots\pi_m(X')}\right)$$

Получаем класс $\boldsymbol{S}$ *одинаково-вероятных* $\boldsymbol{\pi}$*-последовательностей*

$$\boldsymbol{\left(\pi_1(X)\ldots\pi_\chi(X)\ldots\pi_m(X)\right),}$$

$$\boldsymbol{X\rightarrow\left(\pi_1(X)\ldots\pi_\chi(X)\ldots\pi_m(X)\right)\rightarrow}$$

$$\boldsymbol{\Psi(X)=\Psi\left(\pi_1(X)^{|\pi_1(X)|-1}\right)\parallel\ldots\parallel\Psi\left(\pi_m(X)^{|\pi_m(X)|-1}\right)=Y}$$

Определяем

$$\boldsymbol{B_Y=\{X:\Psi(X)=Y\}}$$

В каждом классе $\boldsymbol{S}$ *одинаково-вероятных последовательностей* $\boldsymbol{X}$ существует *одинаковое число* прообразов:

$$\boldsymbol{|S\bigcap B_{Y'}|=|S\bigcap B_Y|.}$$

Отсюда, *аналогично* предыдущему, получаем

$$\boldsymbol{P\left(Y\right)=P\left(X:\Psi\left(X\right)=Y\right)=2^{-\ell}.}$$

Здесь появляется разветвление (распараллеливание) движения по траектории цепи Маркова на каналы:

$$\boldsymbol{\{\pi_1(X),\ldots,\pi_\chi(X),\ldots,\pi_m(X)\}}$$

5.3 Экстракция случайных битов, *текущий* Алгоритм B

В **Алгоритме A** надо ждать, пока наполнятся все $\boldsymbol{\pi}$-последовательности.

В **Алгоритме B** экстракция происходит по блокам размера $\boldsymbol{\varpi}$.

$$\boldsymbol{X = x_1 x_2 ... x_N \Leftrightarrow \pi(X) = \{\pi_1(X), \ldots, \pi_m(X)\}}$$

Для всех $\mathbf{1 \le i \le m}$ мы можем написать

$$\boldsymbol{\pi_i(X) = F_{i1} F_{i2} ... F_{i\alpha_i} E_i,}$$

где $\boldsymbol{|F_{ij}| = \varpi}$, $\mathbf{1 \le j \le \alpha_i}$ — это блоки размера $\boldsymbol{\varpi}$ (окно), *потенциально* используемые для экстракции *двоичных* данных. Блоки наполняются в $\boldsymbol{\pi_1(X), \ldots, \pi_m(X)}$ ***параллельно*** по времени.

Пусть *инициирующая* траектория цепи Маркова

$$\boldsymbol{X = x_1 x_2 ... x_N}$$

задает класс $\boldsymbol{S}$. Тогда включаем

$$\boldsymbol{X' = x'_1 x'_2 ... x'_N \in S,}$$

если:

1) $\boldsymbol{x_1 = x'_1}$ и $\boldsymbol{x_N = x'_N}$ – *начало и конец совпадают,*

2) для всех $\mathbf{1 \le i \le m}$

$$\boldsymbol{\pi_i(X') = F'_{i1} F'_{i2} ... F'_{i\alpha_i} E_i,}$$

3) $\boldsymbol{F_{ij} \equiv F'_{ij}}$ – *перестановка,*

4) хвосты $\boldsymbol{E_i}$ не переставляются.

Особенность! А как считывать блоки?

Главное! Для того, чтобы *в каждом классе одинаково-вероятных траекторий* для *любого* двоичного выхода $\boldsymbol{Y}$ существовало *одинаковое число* прообразов $\boldsymbol{X}$, считывание блоков должно быть ***особенным***, не совпадающим с ***естественно-временным*** считыванием, т.е ***не по мере наполнения блоков*** (сложно доказывается).

Алгоритм В

1) Блок $\boldsymbol{F_{ik} = s_{i_1}, ..., s_{\varpi}}$ ***сразу отправляется на обработку по алгоритму Бабкина и конкатенацию***, если последний элемент в блоке $\boldsymbol{s_{\varpi} = s_i}$.

2) Если в блоке $\boldsymbol{F_{ik}}$ последний элемент $\boldsymbol{s_{\varpi} \neq s_i}$, то блок $\boldsymbol{F_{ik}}$ ***ждет***, пока в траектории цепи Маркова ***не появится*** s_i.

Пример, $\boldsymbol{m = 2, \varpi = 3}$

$$\boldsymbol{X = s_1.s_2.s_2.s_1.s_1.s_2.s_2.s_1.s_1.s_2.s_2.s_1.s_1.s_2.s_2.s_1.s_1.s_2.s_2.s_1.s_1.s_2.s_2.s_1.s_1.s_2.s_2.s_1.s_1.s_2.s_2.s_1}$$

$$\boldsymbol{\pi_1(X) = \overbrace{s_2 - -s_1 s_2}^{F_{11}} - -\overbrace{s_1 s_2 - -s_1}^{F_{12}}\overbrace{s_2 - -s_1 s_2}^{F_{13}} - -\overbrace{s_1 s_2 - -s_1}^{F_{14}}\overbrace{s_2 - -s_1}^{E_1}}$$

$$\boldsymbol{\pi_2(X) = -\overbrace{s_2 s_1 - -s_2}^{F_{21}}\overbrace{s_1 - -s_2 s_1}^{F_{22}} - -\overbrace{s_2 s_1 - -s_2}^{F_{23}}\overbrace{s_1 - -s_2 s_1}^{F_{24}} - -\overbrace{s_2 s_1}^{E_2} -}$$

Естественно-временной порядок считывания блоков:

$$\boldsymbol{F_{11}.....F_{21}.....F_{22}.....F_{12}.....F_{13}.....F_{23}.....F_{24}.....F_{14}}$$

Порядок считывания блоков ***Алгоритмом B***:

$$\boldsymbol{F_{21}.....F_{11}.....F_{12}.....F_{22}.....F_{23}.....F_{13}.....F_{14}.....F_{24}}$$

Таким образом, появляется некоторый порядок считывания блоков **Алгоритмом** B:

$$\boldsymbol{F_{i_1j_1}, F_{i_2j_2}, ..., F_{i_Lj_L}.}$$

Определяем

$$\boldsymbol{Y = \Psi\left(X\right) = \Psi\left(F_{i_1j_1}\right) \parallel \Psi\left(F_{i_2j_2}\right) \parallel ..... \parallel \Psi\left(F_{i_Lj_L}\right) \in \left\{0,1\right\}^{\ell}.}$$

Тогда вероятность

$$\boldsymbol{P\left(Y\right) = 2^{-\ell}.}$$

6 Цепь Маркова с 2-мя состояниями порядка $r \geq 1$

Траектория

$$\boldsymbol{E = \varepsilon_1\varepsilon_2.....\varepsilon_L, \varepsilon_i \in \{0,1\}},$$

$$P(\boldsymbol{E}) = \boldsymbol{P}(\varepsilon_1, ..., \varepsilon_r) \prod_{i=1}^{L-r} \boldsymbol{P}\left(\varepsilon_{i+r} \mid \varepsilon_i, ..., \varepsilon_{i+r-1}\right).$$

Перейти к ***простой цепи Маркова X*** порядка **1** можно путем ***укрупнения*** алфавита, где число состояний $\boldsymbol{m = 2^r}$.

Введем новый алфавит $\{\boldsymbol{s_1, ..., s_m}\} = \left\{\boldsymbol{s_1 = \left(\underbrace{0...0}_{r}\right), ..., s_m = \left(\underbrace{1...1}_{r}\right)}\right\}$, объединяя соседние $\boldsymbol{r}$ битов в траектории $\boldsymbol{E_L = \varepsilon_1\varepsilon_2...\varepsilon_L}$ (с зацеплением на 1 бит) в *один* символ, получим траекторию длины $\boldsymbol{N = L - r}$.

Пусть

$$\boldsymbol{E = \varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_3...\varepsilon_r\varepsilon_{r+1}\varepsilon_{r+2}...\varepsilon_L, \varepsilon_i \in \{0,1\}},$$

тогда

$$\boldsymbol{X = \left(\overbrace{\varepsilon_1\varepsilon_2...\varepsilon_r}^{x_1}\right)\left(\overbrace{\varepsilon_2\varepsilon_3...\varepsilon_{r+1}}^{x_2}\right)\left(\overbrace{\varepsilon_3\varepsilon_4...\varepsilon_{r+2}}^{x_3}\right)...\left(\overbrace{\varepsilon_{L-r+1}\varepsilon_{L-r+2}...\varepsilon_L}^{x_N}\right) = x_1x_2...x_N,}$$

$$\boldsymbol{x_i \in \{0,1\}^r}.$$

.

.

.

.

.

.

.

.

.

.

Для любого состояния $\boldsymbol{s_i = (\epsilon_1, \epsilon_2, ..., \epsilon_r)}$ возможен переход только в два состояния: $\boldsymbol{(\epsilon_2, ..., \epsilon_r, 0)}$ и $\boldsymbol{(\epsilon_2, ..., \epsilon_r, 1)}$.

Пример

	00 (1)	**01 (2)**	**10 (3)**	**11 (4)**
00 (1)	$\boldsymbol{P(1 \mid 1)}$	$\boldsymbol{P(2 \mid 1)}$	**0**	**0**
01 (2)	**0**	**0**	$\boldsymbol{P(3 \mid 2)}$	$\boldsymbol{P(4 \mid 2)}$
10 (3)	$\boldsymbol{P(1 \mid 3)}$	$\boldsymbol{P(2 \mid 3)}$	**0**	**0**
11 (4)	**0**	**0**	$\boldsymbol{P(3 \mid 4)}$	$\boldsymbol{P(4 \mid 4)}$

Получаемые π-последовательности $\boldsymbol{\{\pi_i(X) = F_{i1}F_{i2}...F_{i\alpha_i}E_i, 1 \leq i \leq m, \}}$ ***бинарные***, применять сложный 2^r-арный алгоритм В.Ф. Бабкина не потребуется.

Пример. Алгоритм B при $\boldsymbol{r=2, N=36, m=2^r=4, \varpi=3.}$

$$\boldsymbol{E = 01_1^2 0_2^3 0_3^1 1_4^2 0_5^3 1_6^2 1_7^4 0_8^3 1_9^2 0_{10}^3 0_{11}^1 1_{12}^2 1_{13}^4 1_{14}^4 1_{15}^4 0_{16}^3 0_{17}^1 1_{18}^2 0_{19}^3 1_{20}^2}$$

$$\boldsymbol{0_{21}^3 0_{22}^1 0_{23}^1 1_{24}^2 1_{25}^4 1_{26}^4 0_{27}^3 0_{28}^1 0_{29}^1 0_{30}^1 1_{31}^2 1_{32}^4 0_{33}^3 0_{34}^1 1_{35}^2 0_{36}^3},$$

Индексация в $\boldsymbol{E}$: внизу - *номер* такта, вверху – номер укрупненного состояния.

$$\boldsymbol{\pi_1(X) = {}_{1\cdot2\cdot3}\overbrace{2_{4\cdot5\cdot6\cdot7\cdot8\cdot9\cdot10\cdot11}2_{12\cdot13\cdot14\cdot15\cdot16\cdot17}2_{18}}^{F_{11}}{}_{\cdot19\cdot20\cdot21\cdot22}\overbrace{1_{23}2_{24\cdot25\cdot26\cdot27\cdot28}1_{29}}^{F_{12}}\overbrace{1_{30}2_{31\cdot32\cdot33\cdot34}2_{35}}^{E_1}{}_{\cdot36}}$$

$$\boldsymbol{\pi_2(X) = {}_1\overbrace{3_{2\cdot3\cdot4}3_{5\cdot6}4_7}^{F_{21}}{}_{\cdot8\cdot9}\overbrace{3_{10\cdot11\cdot12}4_{13\cdot14\cdot15\cdot16\cdot17\cdot18}3_{19}}^{F_{22}}{}_{\cdot20}\overbrace{3_{21\cdot22\cdot23\cdot24}4_{25\cdot26\cdot27\cdot28\cdot29\cdot30\cdot31}4_{32}}^{F_{23}}{}_{\cdot33\cdot34\cdot35}\overbrace{3_{36}}^{E_2}}$$

$$\boldsymbol{\pi_3(X) = {}_{1\cdot2}\overbrace{1_{3\cdot4\cdot5}2_{6\cdot7\cdot8}2_9}^{F_{31}}{}_{\cdot10}\overbrace{1_{11\cdot12\cdot13\cdot14\cdot15\cdot16}1_{17\cdot18\cdot19}2_{20}}^{F_{32}}{}_{\cdot21}\overbrace{1_{22\cdot23\cdot24\cdot25\cdot26\cdot27}1_{28\cdot29\cdot30\cdot31\cdot32\cdot33}1_{34}}^{F_{33}}{}_{\cdot35\cdot36}}$$

$$\boldsymbol{\pi_4(X) = {}_{1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7}\overbrace{3_{8\cdot9\cdot10\cdot11\cdot12\cdot13}4_{14}4_{15}}^{F_{41}}\overbrace{3_{16\cdot17\cdot18\cdot19\cdot20\cdot21\cdot22\cdot23\cdot24\cdot25}4_{26}3_{27}}^{F_{42}}{}_{\cdot28\cdot29\cdot30\cdot31\cdot32}\overbrace{3_{33}}^{E_4}{}_{\cdot34\cdot35\cdot36}}$$

Порядок считывания **Алгоритмом** B

$$\boldsymbol{F_{21} = (334), F_{31} = (122), F_{41} = (344), F_{22} = (343), F_{32} = (112),}$$
$$\boldsymbol{F_{11} = (222), F_{12} = (121), F_{42} = (343), F_{23} = (344), F_{33} = (111)}$$