Экстракция доказуемо случайной битовой последовательности из траекторий цепи Маркова

И.М. Арбеков, С.Н. Молотков

ООО «СФБ Лаб», МГУ им. М.В Ломоносова

CTCrypt 2024
4 июня 2024

Igor.Arbekov@sfblaboratory.ru

СФБ ЛАБ

Общая схема ФГСЧ

ИСТОЧНИК ШУМА

↓

X — **исходная** 0,1-последовательность

↓

Ψ — **преобразование** (экстракция)

↓

Y — **выходная** 0,1-последовательность

Основной результат

Пусть

X – цепь Маркова порядка $r \geq 1$,

Ψ – алгоритм арифметического кодирования В.Ф. Бабкина,

доказано

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

ℓ – длина последовательности

Основной результат: источники

H. Zhou

Randomness and Noise in Information Systems

2012

В.Ф. Бабкин

Метод универсального кодирования источника независимых сообщений неэкспоненциальной трудоемкости

1971

И.М. Арбеков, С.Н. Молотков

Методические заметки. Квантовые генераторы случайных чисел, экстракция доказуемо случайных битовых последовательностей из траекторий цепей Маркова

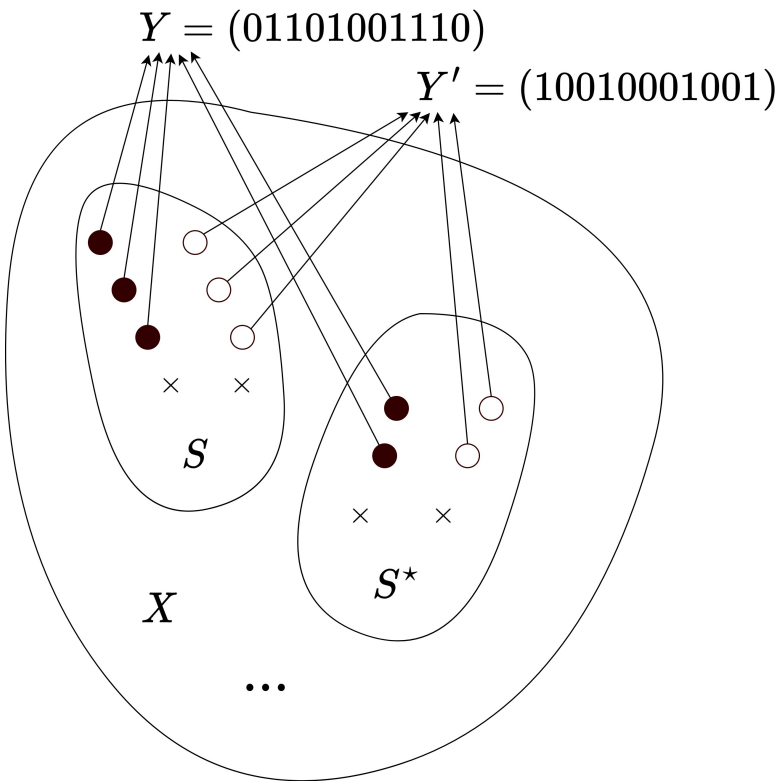
2024

Центральное место доказательства

1. Разбиение последовательности X на классы S *одинаково-вероятных* последовательностей
2. $B_Y = \{X : \Psi(X) = Y\}$

$|S \cap B_Y| = |S \cap B_{Y'}|$ для любых Y, Y'

(следствие алгоритма В.Ф. Бабкина)



Центральное место доказательства

3. Формула полной вероятности

$$P(Y) = P\left(X \in B_Y\right) =$$

$$= \sum_{S \in G} P(X \in S)\, P\left(X \in B_Y \mid X \in S\right) =$$

$$= \sum_{S \in G} P(X \in S)\, \frac{P_S(X) \cdot |S \cap B_Y|}{P_S(X) \cdot |S|} =$$

$$= \sum_{S \in G} P(X \in S)\, \frac{|S \cap B_Y|}{|S|}$$

Из $|S \cap B_Y| = |S \cap B_{Y'}|$ следует $P(Y) = P(Y')$ и $P(Y) = 2^{-\ell}$

Благодарю за внимание!

И.М. Арбеков, С.Н. Молотков

ООО «СФБ Лаб», МГУ им. М.В Ломоносова

CTCrypt 2024

4 июня 2024

Igor.Arbekov@sfblaboratory.ru

СФБ ЛАБ

Алгоритм В.Ф. Бабкина: нумерация

Блок

$$X = x_1, .., x_n, x_i = \{s_1, s_2\},$$

k символов s_1 на местах

$$(i_1, i_2, ..., i_k) \Leftrightarrow$$

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

если $j < i$

Нумерация по ходу появления $i_1, i_2, ..., i_k$

Алгоритм В.Ф. Бабкина: экстракция двоичных последовательностей

СФБ ЛАБ

$$Num(i_1, i_2, ..., i_k) =$$

$$= \varepsilon_{r_m+1} 2^{r_m+1} + \varepsilon_{r_m} 2^{r_m} + \varepsilon_{r_m-1} 2^{r_m-1} + ... + \varepsilon_1 2^1 + \varepsilon_r \in \{0, 1\}$$

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

Алгоритм В.Ф. Бабкина: пример $n = 8, k = 2$

(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
$\mathbf{s_1}\mathbf{s_1}s_2s_2s_2s_2s_2s_2$	0	00000	00
…	1	00001	01
$j = 0$	2	00010	10
	$3 = 2^{r_0} - 1$	00011	11
	4	00100	100
$j = 1$	…	…	…
	10	01010	010
	$11 = 2^{r_1} + 2^{r_0} - 1$	01011	011
	12	01100	1100
	13	01101	1101
$j = 2$	…	…	…
	25	11001	1001
	26	11010	1010
$s_2s_2s_2s_2s_2s_2\mathbf{s_1}\mathbf{s_1}$	$27 = 2^{r_2} + 2^{r_1} + 2^{r_0} - 1$	11011	1011

X – бернуллиевская, классы S

Задающая класс S последовательность

$X = \left(X_1, ..., X_M\right), X_i$ – блоки длины n

$X' = x'_1 x'_2 ... x'_N \in S : \ X'_i \equiv X_i$– перестановка

$$P(X') = P(X)$$

$Y_i = \Psi\left(X_i\right), Y = Y_1 \parallel ... \parallel Y_M$–конкатенация

X – простая цепь Маркова, m состояний, классы S

Задающая класс S траектория
$X = x_1 x_2 ... x_N,\ x_i \in \{s_1, ..., s_m\} \Longleftrightarrow$

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

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

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

$$X' = x'_1 x'_2 ... x'_N \in S :$$

$x'_1 = x_1$ и $x'_N = x_N = s_\chi$ – начало и конец X и X' совпадают,
$\pi_\chi(X') \equiv \pi_\chi(X)$ – любая перестановка,
$\pi_i(X') \overset{\bullet}{\equiv} \pi_i(X),\ i \neq \chi$ – **перестановка с фиксированным хвостом**

$$P(X') = P(X)$$

Алгоритм A

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

$Y = Y_1||...||Y_\chi||..||Y_m$ – конкатенация

$\Psi(...)$ – m-арный алгоритм В.Ф. Бабкина

Алгоритм B (stream)

Задающая класс S траектория

$$X = x_1 x_2 ... x_N,\ x_i,\ x_i \in \{s_1, ..., s_m\} \Longleftrightarrow$$

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

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

$$X' = x'_1 x'_2 ... x'_N \in S\ :$$

$x_1 = x'_1$ и $x_N = x'_N$ – начало и конец X и X' совпадают,

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

$F_{ij} \equiv F'_{ij}$ – перестановка
Блоки F_{ij} наполняются в $\pi_1(X), ..., \pi_m(X)$ **параллельно** по времени

Алгоритм B (stream): важно

СФБ ЛАБ

- Считывание блоков не совпадает с **естественно-временным** порядком, т.е. **не по мере наполнения блоков**
- Обработанный блок $\Psi\left(F_{ik}\right)$ **сразу отправляется на конкатенацию**, если последний элемент в блоке $s_\varpi = s_i$
- Если в блоке F_{ik} последний элемент $s_\varpi \neq s_i$, то обработанный блок $\Psi\left(F_{ik}\right)$ **ждет**, пока в траектории цепи Маркова **не появится** s_i:

$$Y = \Psi\left(F_{i_1,j_1}\right)||\Psi\left(F_{i_2 j_2}\right)||\ldots||\Psi\left(F_{i_L j_L}\right)$$

Алгоритм B (stream): пример

Траектория

$$X = s_1.s_2.s_2.s_1.s_1.s_2.s_2.s_1.s_1.s_2.s_2.s_1.s_1.s_2.s_2. \\ s_1.s_1.s_2.s_2.s_1.s_1.s_2.s_2.s_1.s_1.s_2.s_2.s_1.s_1$$

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

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

Естественно-временной порядок считывания блоков:

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

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

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

$$Y = \Psi(F_{21}) \parallel \Psi(F_{11}) \parallel \Psi(F_{12}) \parallel ..... \parallel \Psi(F_{24})$$

X – цепь Маркова, 2 состояния, порядок $r \geq 2$

СФБ ЛАБ

Траектория цепи Маркова:

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

Переход ***простой цепи Маркова*** порядка $r = 1$:

$$X = \left(\overbrace{\varepsilon_1\varepsilon_2\ldots\varepsilon_r}^{x_1}\right)\left(\overbrace{\varepsilon_2\varepsilon_3\ldots\varepsilon_{r+1}}^{x_2}\right)\left(\overbrace{\varepsilon_3\varepsilon_4\ldots\varepsilon_{r+2}}^{x_3}\right)\ldots\left(\overbrace{\varepsilon_{L-r+1}\varepsilon_{L-r+2}\ldots\varepsilon_L}^{x_N}\right), x_i \in \{0,1\}^r$$

Возможные переходы состояний:

$$s_i = \left(\varepsilon_1\varepsilon_2\ldots\varepsilon_r\right) \rightarrow s_i' = \left(\varepsilon_2\ldots\varepsilon_r, 0\right) \text{ и } s_i'' = \left(\varepsilon_2\ldots\varepsilon_r, 1\right)$$

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

Пример

Траектория

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

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

Вверху – укрупненные состояния

$$00 = 1, 01 = 2, 10 = 3, 11 = 4$$

внизу – такты

$$\pi_{00}(X) = 1{\cdot}2{\cdot}3\,\overbrace{2_{4{\cdot}5{\cdot}6{\cdot}7{\cdot}8{\cdot}9{\cdot}10{\cdot}11}2_{12{\cdot}13{\cdot}14{\cdot}15{\cdot}16{\cdot}17}2_{18}}^{F_{11}}{\cdot}19{\cdot}20{\cdot}21{\cdot}22\,\overbrace{1_{23}2_{24{\cdot}25{\cdot}26{\cdot}27{\cdot}28}1_{29}}^{F_{12}}\overbrace{1_{30}2_{31{\cdot}32{\cdot}33{\cdot}34}2_{35}}^{E_1}{\cdot}36$$

$$\pi_{01}(X) = 1\,\overbrace{3_{2{\cdot}3{\cdot}4}3_{5{\cdot}6}4_7}^{F_{21}}{\cdot}8{\cdot}9\,\overbrace{3_{10{\cdot}11{\cdot}12}4_{13{\cdot}14{\cdot}15{\cdot}16{\cdot}17{\cdot}18}3_{19}}^{F_{22}}{\cdot}20\,\overbrace{3_{21{\cdot}22{\cdot}23{\cdot}24}4_{25{\cdot}26{\cdot}27{\cdot}28{\cdot}29{\cdot}30{\cdot}31}4_{32}}^{F_{23}}{\cdot}33{\cdot}34{\cdot}35\,\overbrace{3_{36}}^{E_2}$$

$$\pi_{10}(X) = 1{\cdot}2\,\overbrace{1_{3{\cdot}4{\cdot}5}2_{6{\cdot}7{\cdot}8}2_9}^{F_{31}}{\cdot}10\,\overbrace{1_{11{\cdot}12{\cdot}13{\cdot}14{\cdot}15{\cdot}16}1_{17{\cdot}18{\cdot}19}2_{20}}^{F_{32}}{\cdot}21\,\overbrace{1_{22{\cdot}23{\cdot}24{\cdot}25{\cdot}26{\cdot}27}1_{28{\cdot}29{\cdot}30{\cdot}31{\cdot}32{\cdot}33}1_{34}}^{F_{33}}{\cdot}35{\cdot}36$$

$$\pi_{11}(X) = 1{\cdot}2{\cdot}3{\cdot}4{\cdot}5{\cdot}6{\cdot}7\,\overbrace{3_{8{\cdot}9{\cdot}10{\cdot}11{\cdot}12{\cdot}13}4_{14}4_{15}}^{F_{41}}\overbrace{3_{16{\cdot}17{\cdot}18{\cdot}19{\cdot}20{\cdot}21{\cdot}22{\cdot}23{\cdot}24{\cdot}25}4_{26}3_{27}}^{F_{42}}{\cdot}28{\cdot}29{\cdot}30{\cdot}31{\cdot}32\,\overbrace{3_{33}}^{E_4}{\cdot}34{\cdot}35{\cdot}36$$

Пример

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

$$F_{21}.....F_{31}.....F_{41}.....F_{22}.....F_{32}.....F_{11}.....F_{12}.....F_{42}.....F_{23}.....F_{33}$$

$$Y = \Psi\left(F_{21}\right) \| \Psi\left(F_{31}\right) \| \Psi\left(F_{41}\right) \| ..... \| \Psi\left(F_{33}\right).$$