

«Асимптотическая локальная **обратимость**  
последовательности случайных **автоматов** с  
растущим числом внутренних состояний»

Академия криптографии В. И. Винокуров  
CTCrypt 2026 02.06.2026

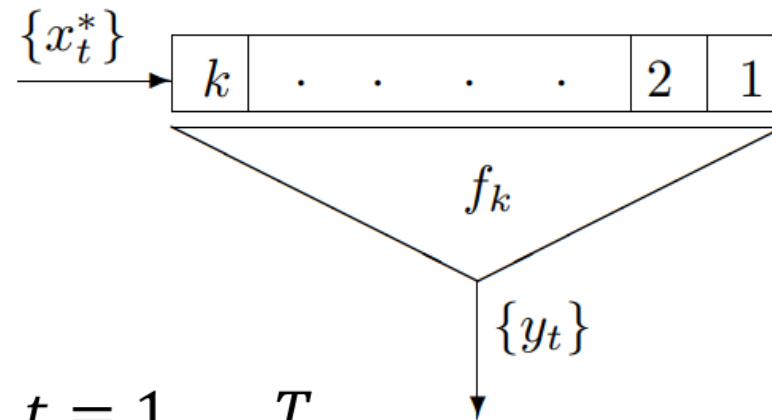


# Кратное содержание предыдущих серий





# Проходной накопитель



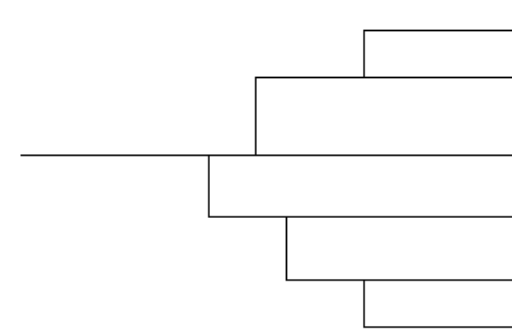
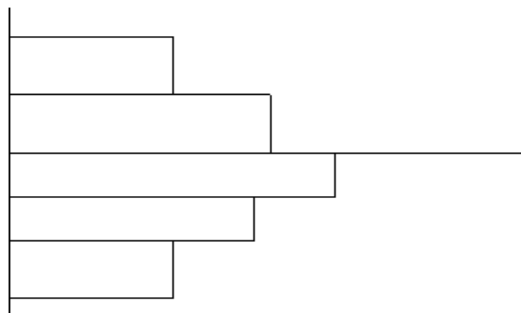
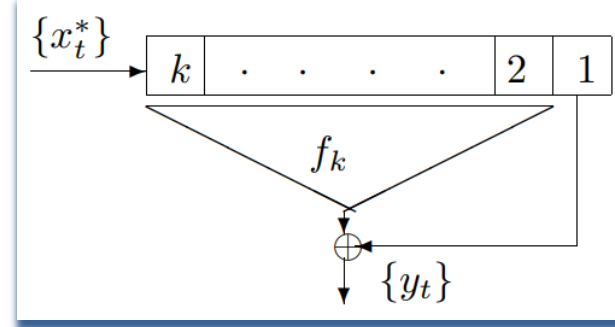
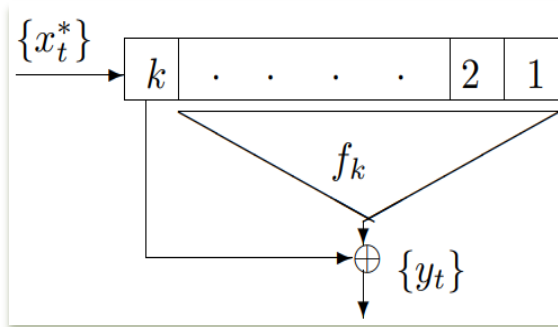
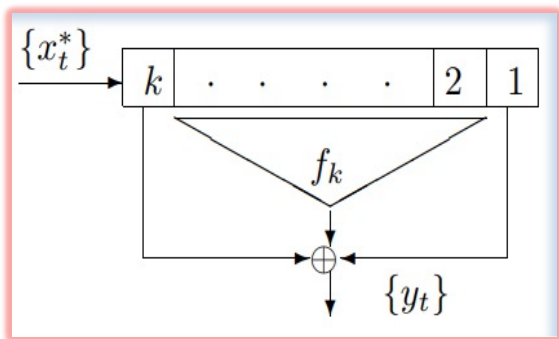
$$f_k(x_{t+k-1}^*, \dots, x_{t+1}^*, x_t^*) = y_t \quad t = 1, \dots, T$$

Найти все решения?  $(x_{T+k-1}, \dots, x_1)$

$$\left[ \begin{array}{l} f_k(x_k, \dots, x_1) = y_1 \\ f_k(x_{k+1}, \dots, x_1) = y_2 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ f_k(x_{T+k-1}, \dots, x_T) = y_T \end{array} \right.$$



# Функции **без запретов**

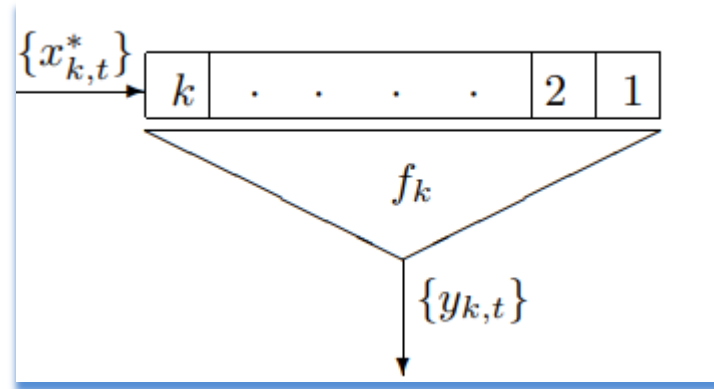


С. Н. Сумароков

О. А. Логачев, Г. В. Проскурин,  
В. В. Яценко, А. А. Курмит



## Функции с запретами



?

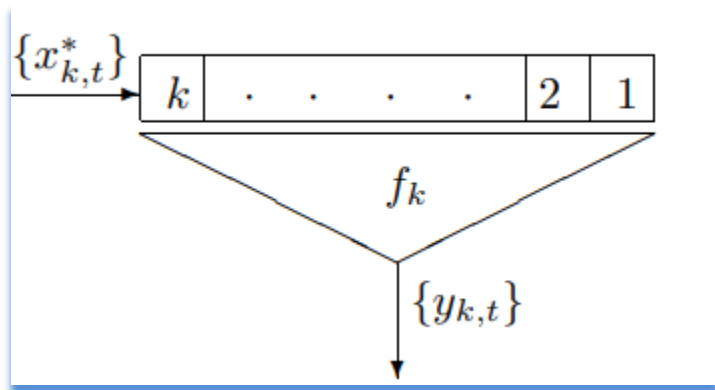
Число решений растёт экспоненциально  $\lambda^T$  ( $\lambda > 1$ )  
с ростом  $T$ .

(Б.А. Севастьянов, В.П. Чистяков, В.А. Копытцев, В.Г. Михайлов,  
А.Е. Жуков, С.В. Полин)

Логарифм числа решений  $\sim N(a_T, \sigma_T)$   
(В.Г. Михайлов)



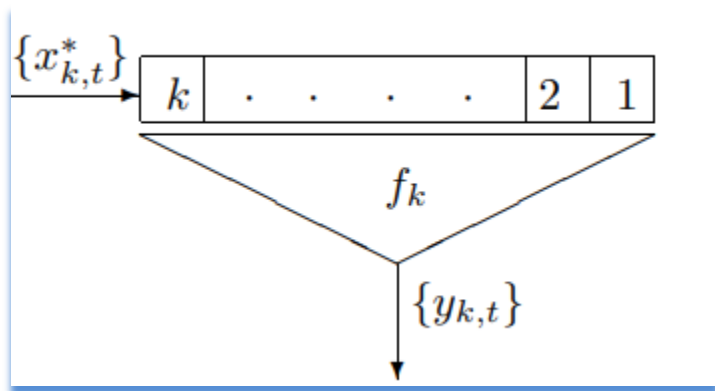
# Структура последовательностей



*А.А. Тюкин,  
Г.В. Проскурин,  
Ю.Г. Воронов,  
В.И. Винокуров*

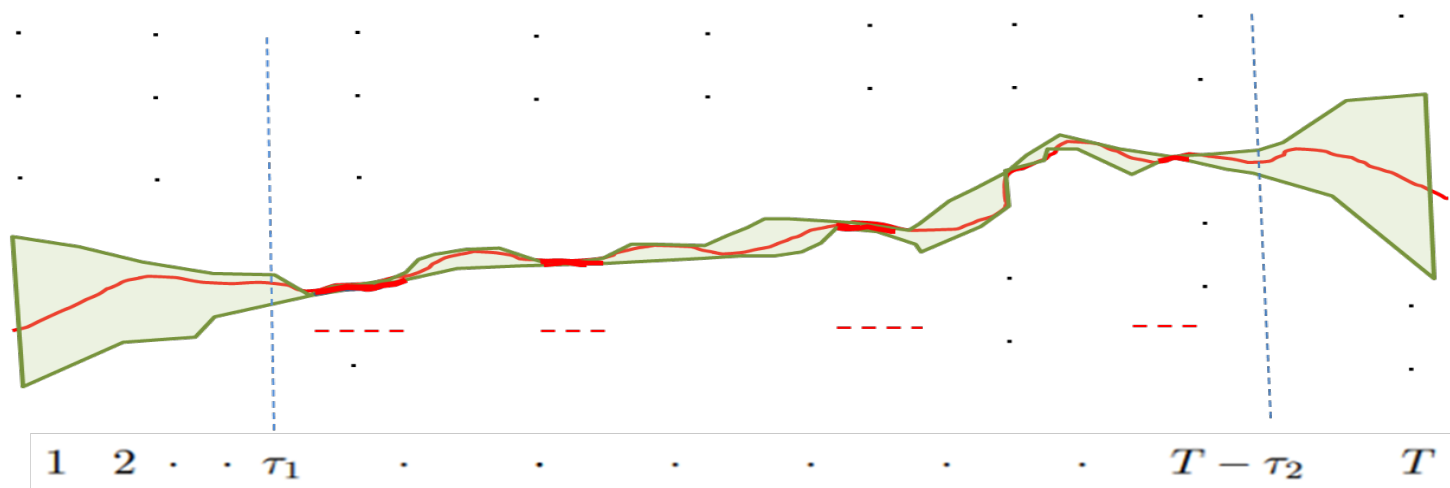


# Структура последовательностей

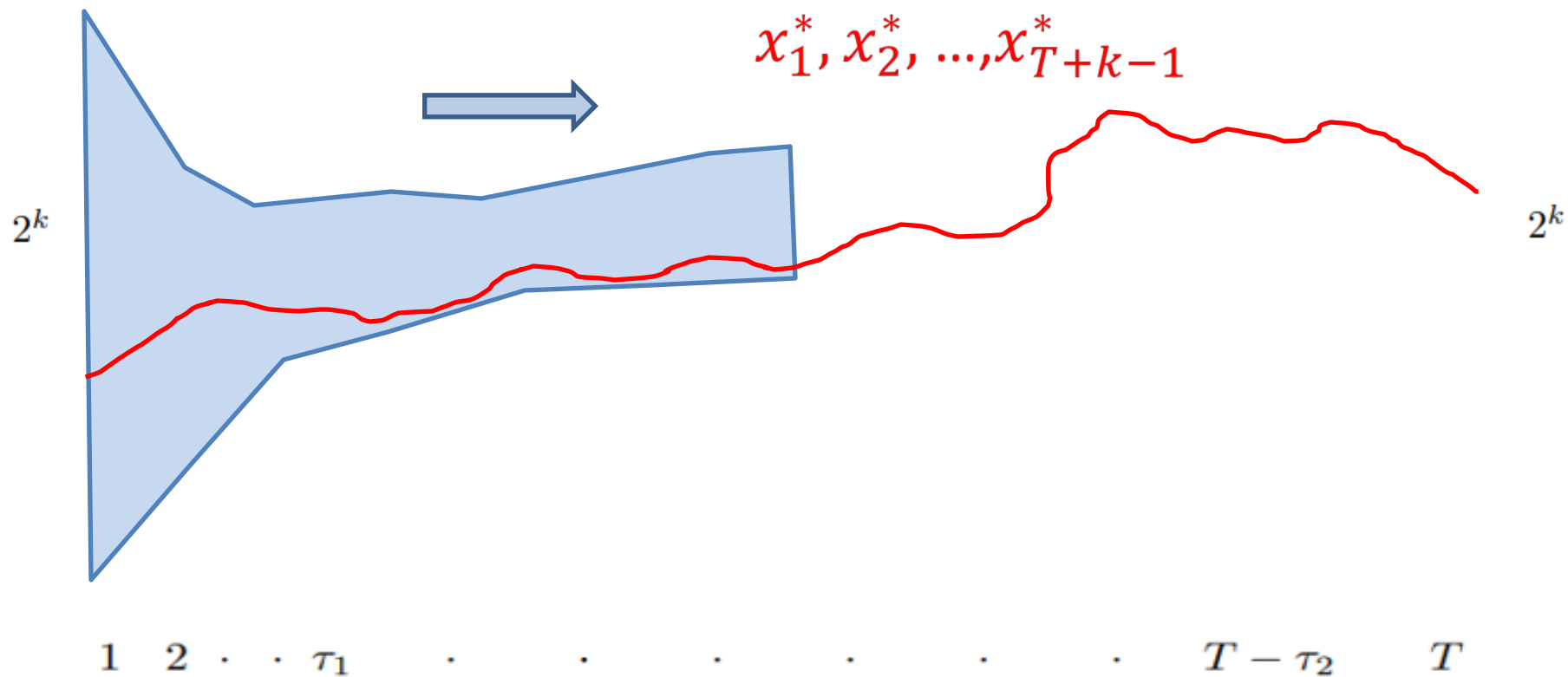


А.А. Тюкин,  
Г.В. Проскурин,  
Ю.Г. Воронов,  
В.И. Винокуров

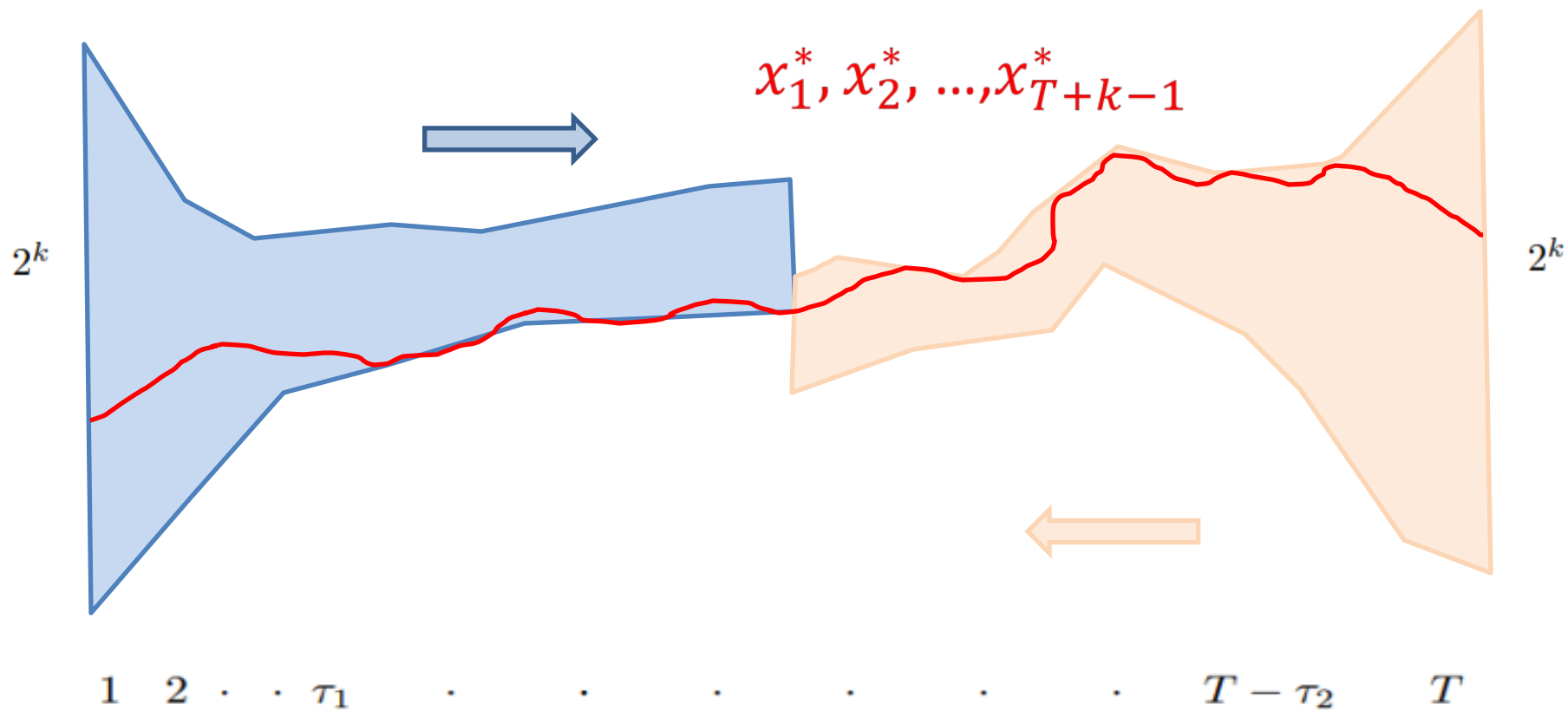
## Гипотеза Обратимости



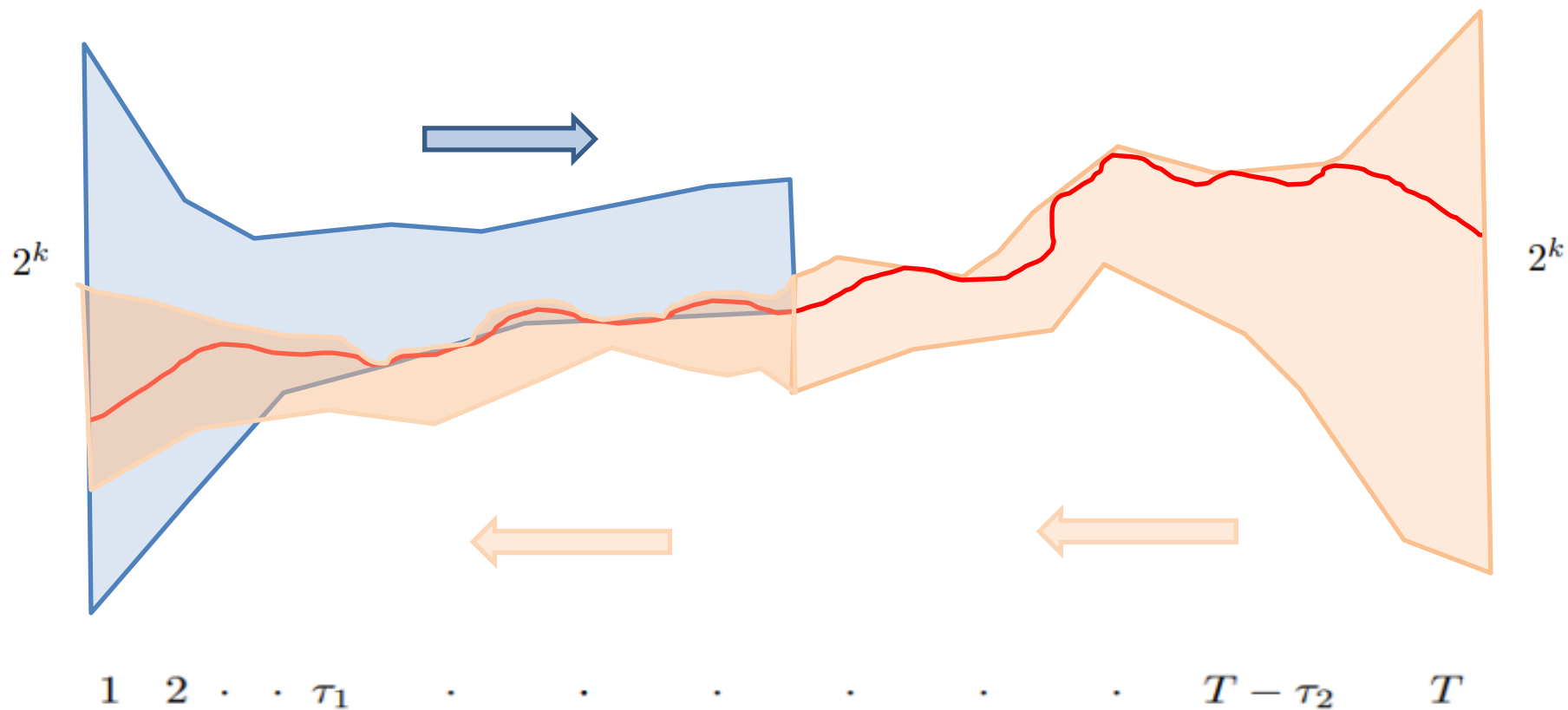
# Ветвление входного слова



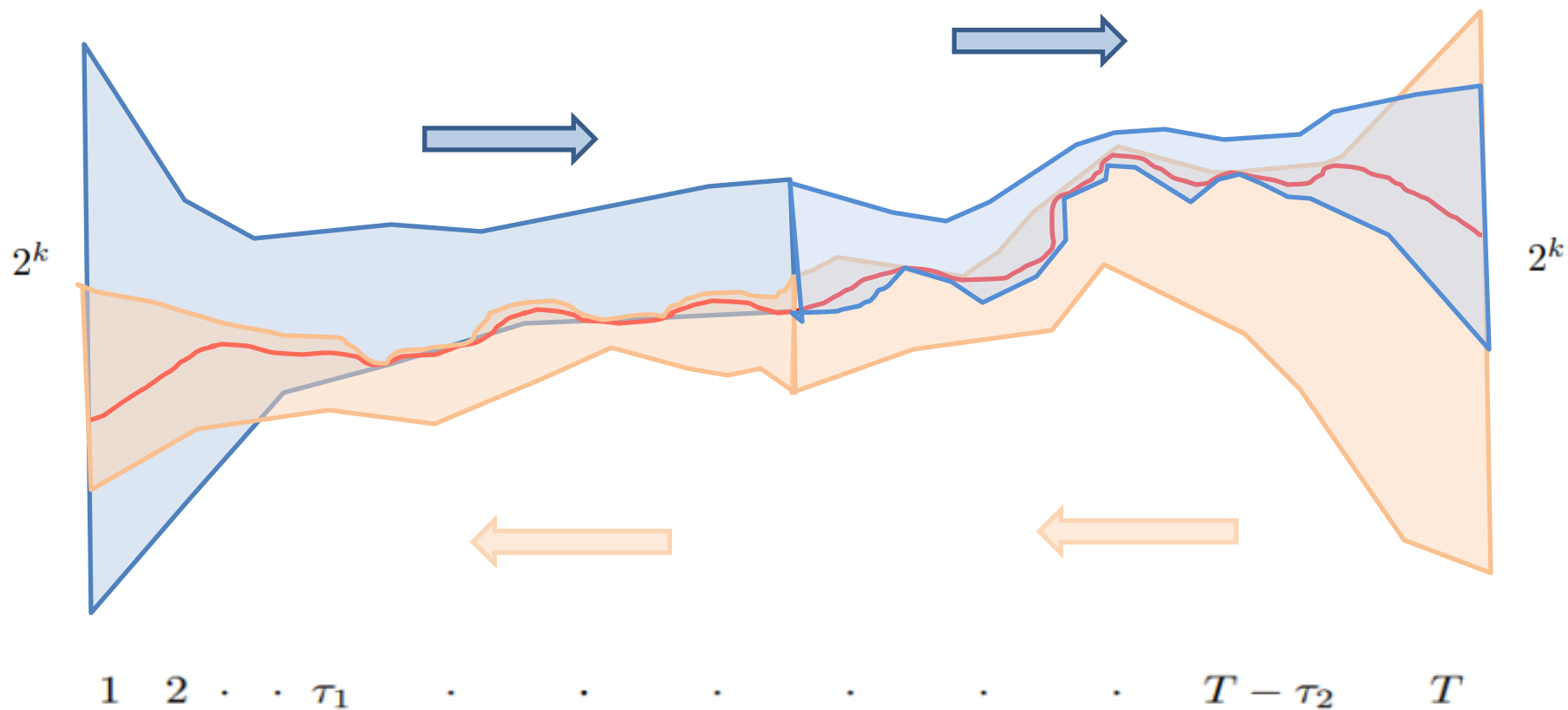
# Встреча двух процессов ветвления



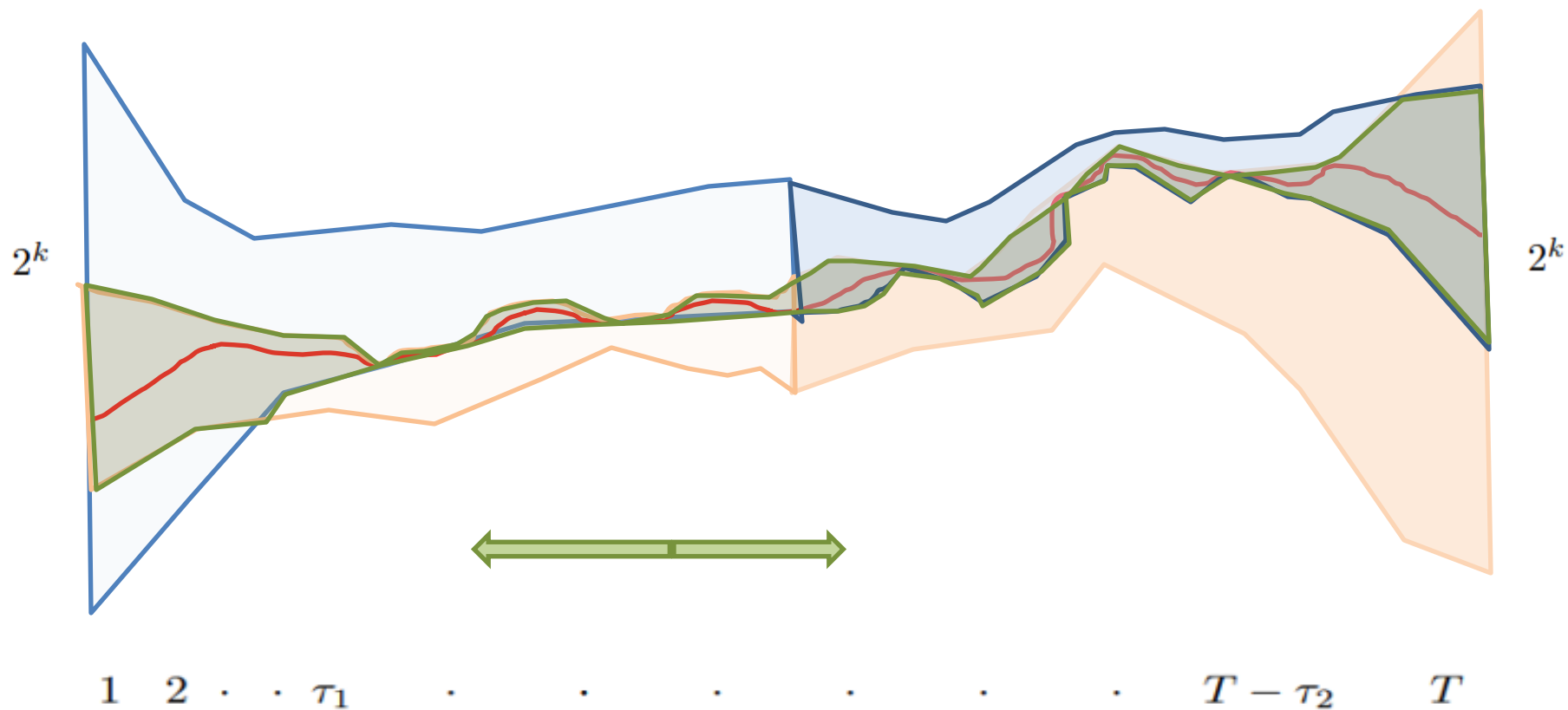
# Встреча двух процессов ветвления



# Встреча двух процессов ветвления

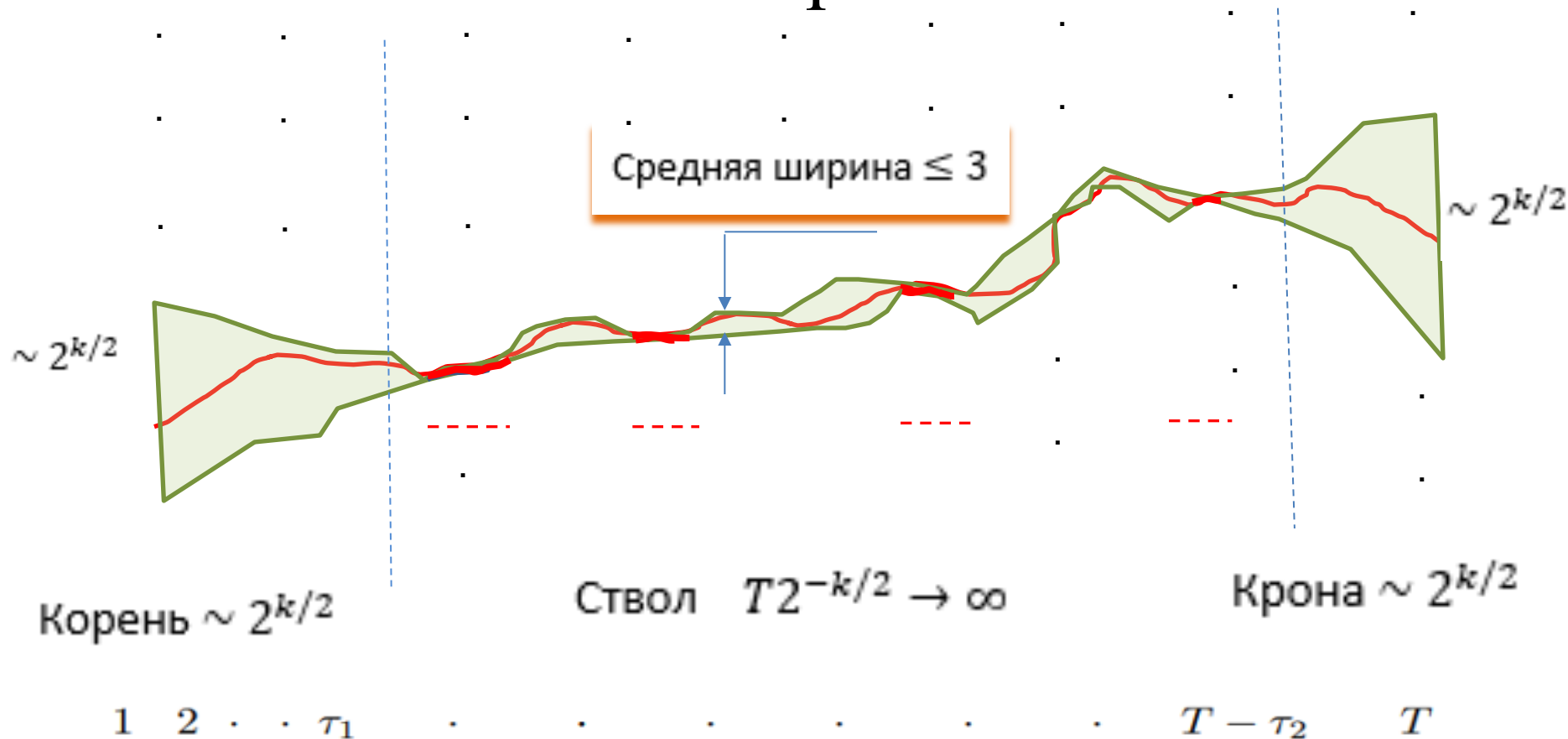


# Встреча двух процессов ветвления





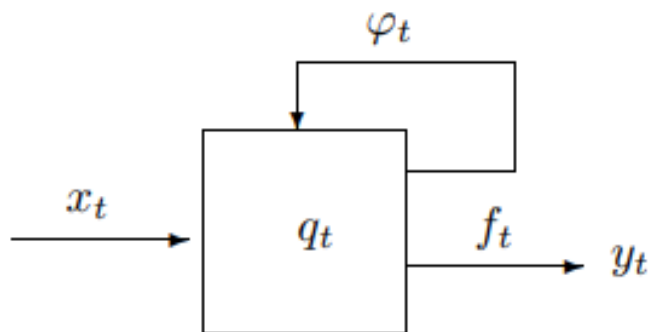
# Обратимость в рамках модели и экспериментально



На Стволе с вероятностью  $\geq 1/3$  ширина равна 1  $\rightarrow$  Локальное обращение

**TO BE  
CONTINUED** →

## Случайный (вероятностный) автомат



$$\begin{cases} y_t = f_t(x_t, q_t), \\ q_{t+1} = \varphi_t(x_t, q_t). \end{cases} \quad t = 1, 2, \dots, T$$

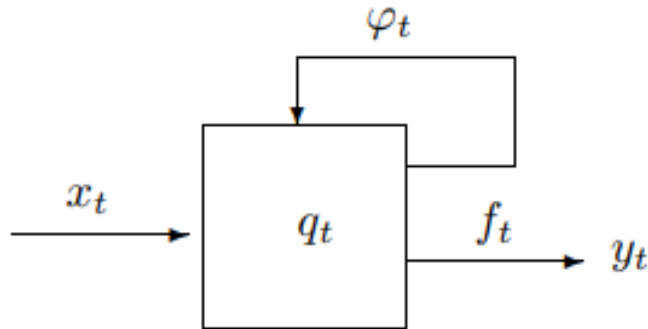
$$x_t \in \{1, 2, \dots, m\} = X, \quad y_t \in \{1, 2, \dots, m\} = Y$$

$$q_t \in \{1, 2, \dots, n\} = Q$$

$$f_t: X \times Q \rightarrow Y$$

$$\varphi_t: X \times Q \rightarrow Q$$

## Случайный (вероятностный) автомат



$$\begin{cases} y_t = f_t(x_t, q_t), \\ q_{t+1} = \varphi_t(x_t, q_t). \end{cases} \quad t = 1, 2, \dots, T$$

$$x_t \in \{1, 2, \dots, m\} = X, \quad y_t \in \{1, 2, \dots, m\} = Y$$

$$q_t \in \{1, 2, \dots, n\} = Q$$

$$f_t: X \times Q \rightarrow Y$$

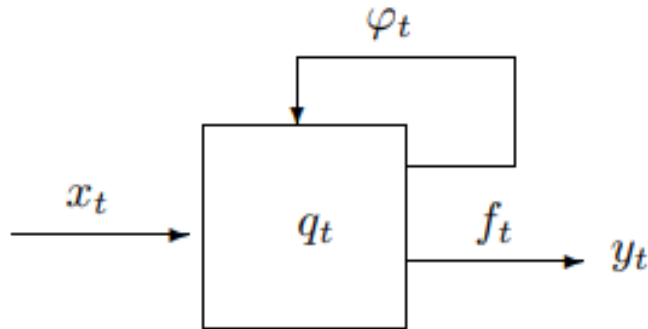
$$\varphi_t: X \times Q \rightarrow Q$$

Начальное состояние автомата, входная последовательность и последовательности функций

$$q_1, \quad \{x_t\}_{t=1}^T, \quad \{f_t\}_{t=1}^T, \quad \{\varphi_t\}_{t=1}^T$$

– случайны и равновероятны!

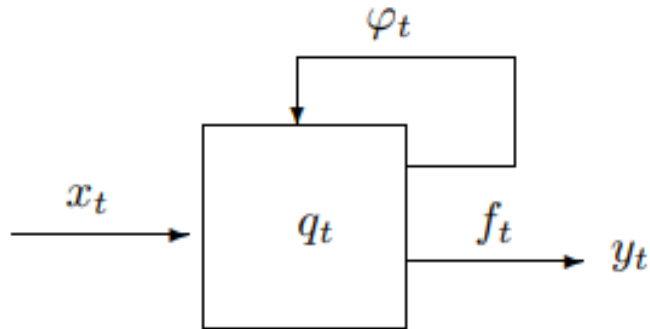
## Возможные приложения



$$\begin{cases} y_t = f_t(x_t, q_t), \\ q_{t+1} = \varphi_t(x_t, q_t). \end{cases} \quad t = 1, 2, \dots, T$$

1. Работа автомата зависит от раундовых ключей.
2. Используются Твики.
3. Модель сложного автомата.

# Случайный (вероятностный) автомат

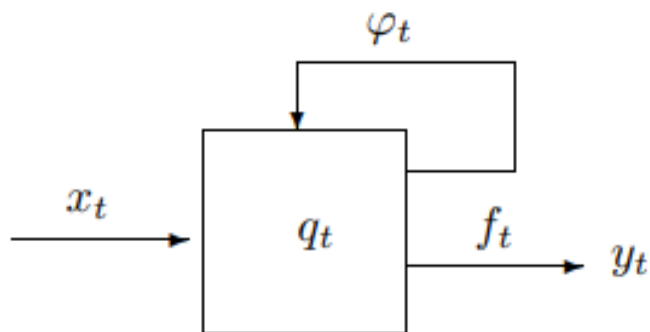


$$\begin{cases} y_t = f_t(x_t, q_t), \\ q_{t+1} = \varphi_t(x_t, q_t). \end{cases} \quad t = 1, 2, \dots, T$$

Постановка задачи

TO BE  
CONTINUED...

## Случайный (вероятностный) автомат



$$\begin{cases} y_t = f_t(x_t, q_t), \\ q_{t+1} = \varphi_t(x_t, q_t). \end{cases} \quad t = 1, 2, \dots, T$$

### Постановка задачи

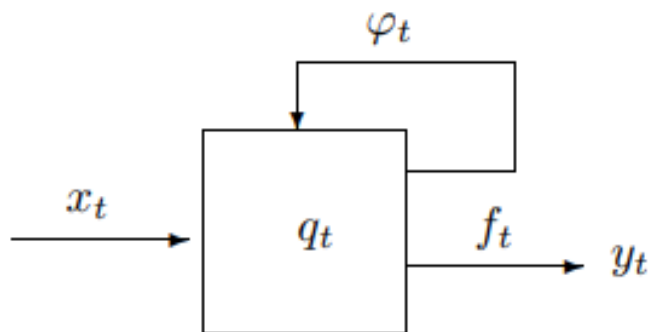
$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$

Структура прообразов известного выхода  $\{y_t\} \quad t=1,2,\dots,T$   
автомата,  
полученного при случайных и равновероятных

$$q_1, \quad \{x_t\}_{t=1}^T, \quad \{f_t\}_{t=1}^T, \quad \{\varphi_t\}_{t=1}^T$$

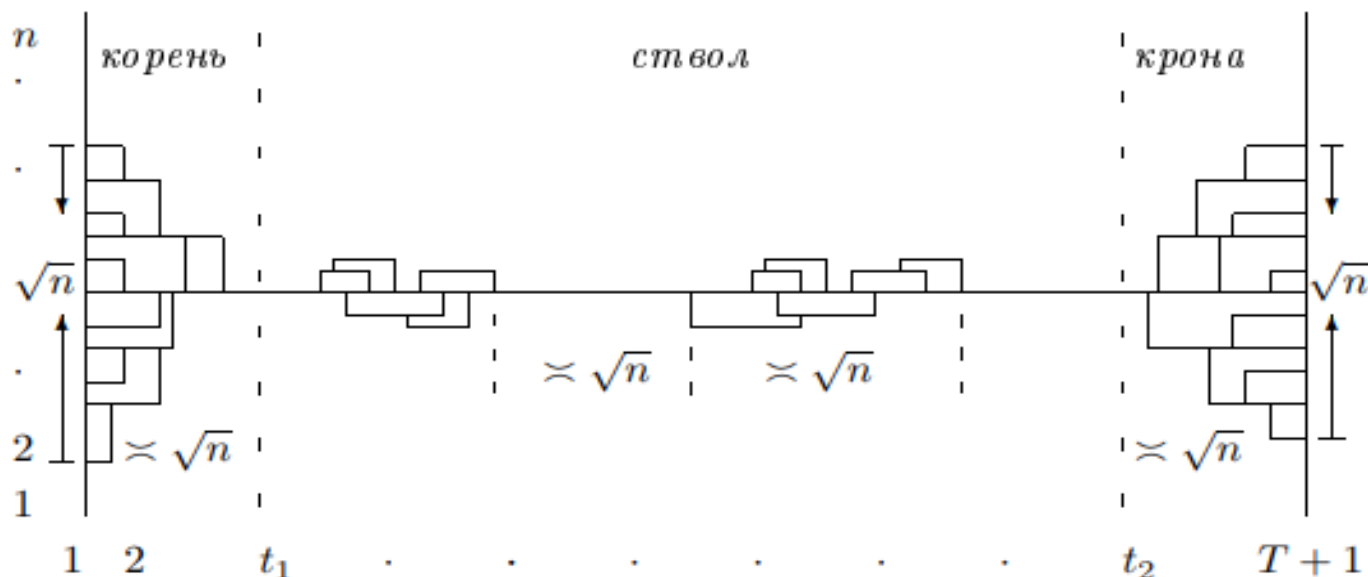
?

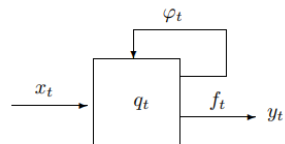
# Структура входных последовательностей



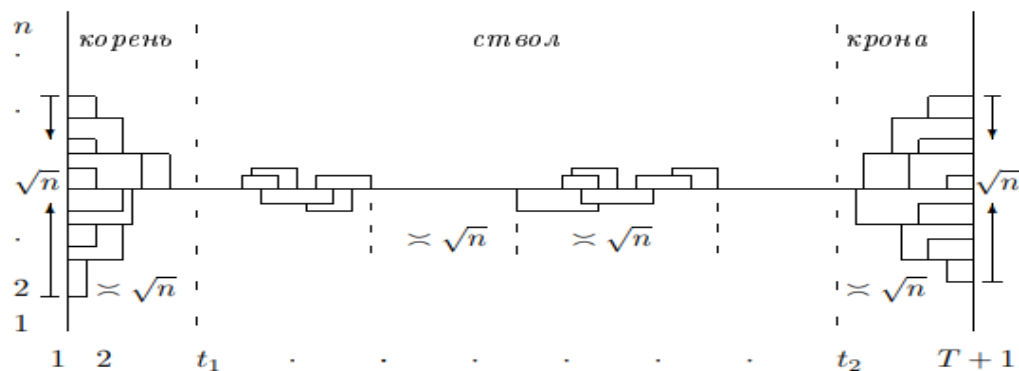
$$\begin{cases} y_t = f_t(x_t, q_t), \\ q_{t+1} = \varphi_t(x_t, q_t). \end{cases}$$

$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$



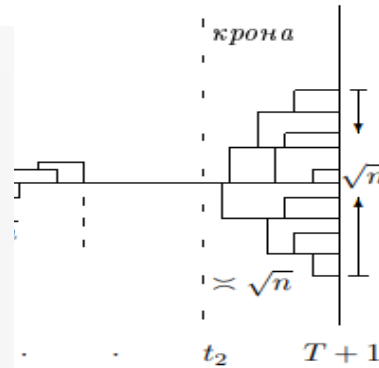
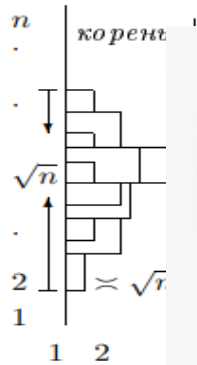
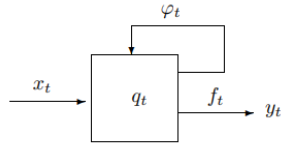


# Структура входных последовательностей



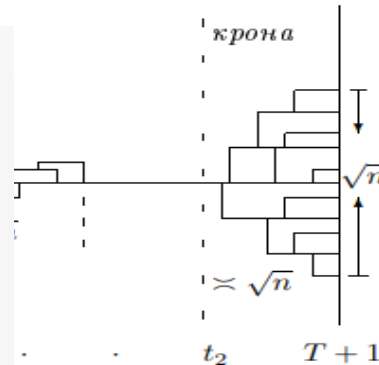
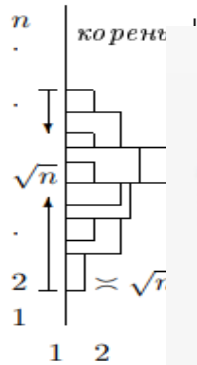
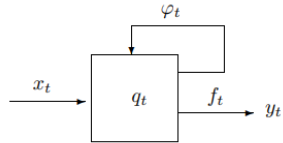
$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$

# Структура входных последовательностей

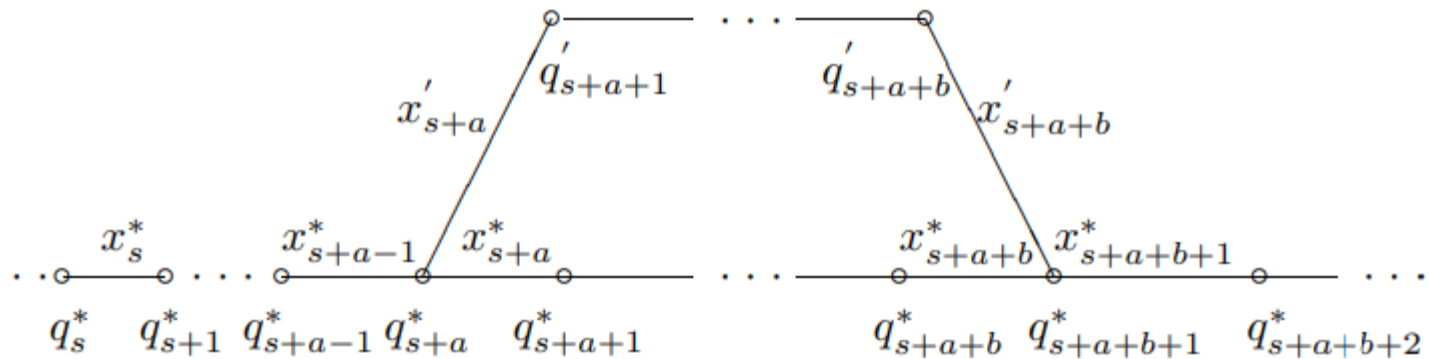


$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$

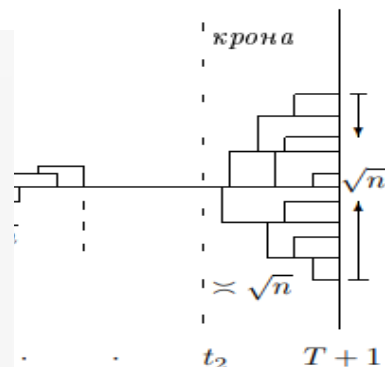
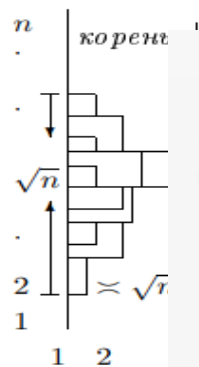
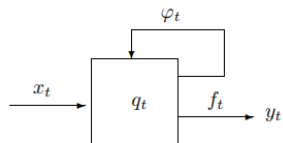
# Структура входных последовательностей



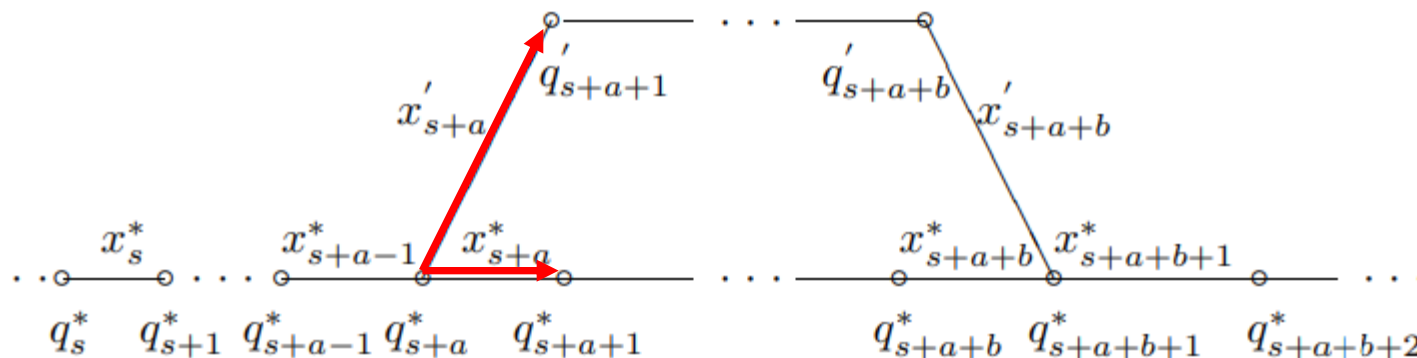
$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$



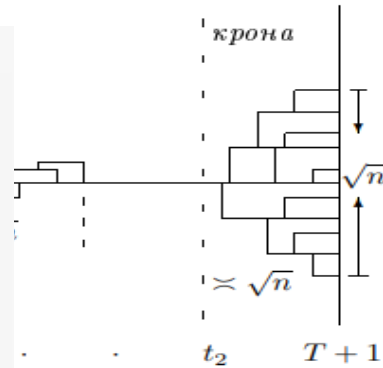
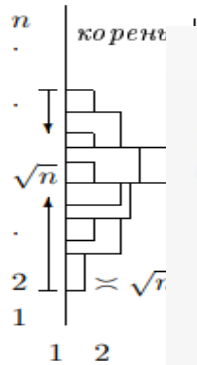
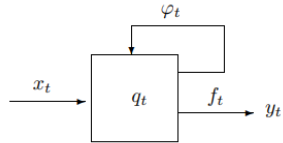
# Структура входных последовательностей



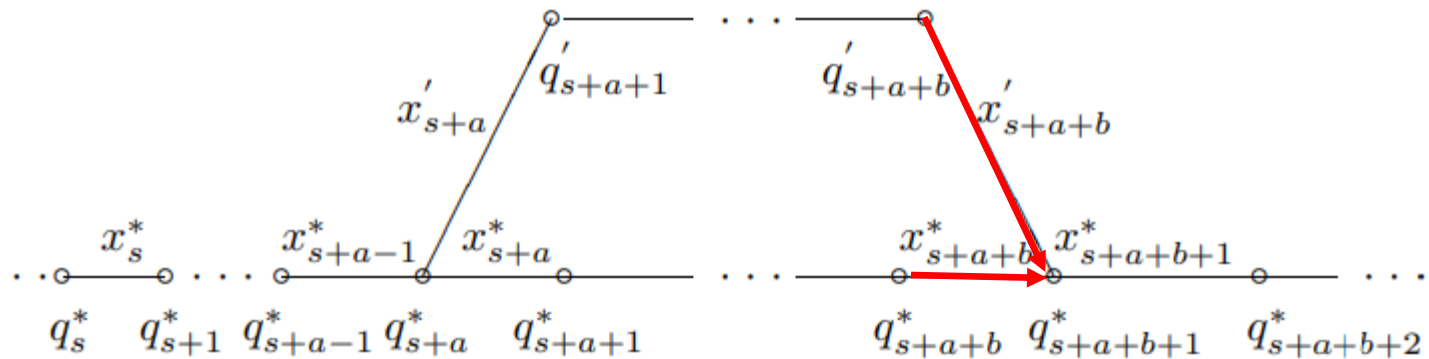
$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$

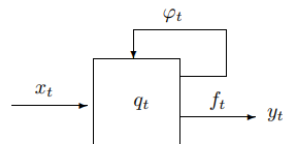


# Структура входных последовательностей

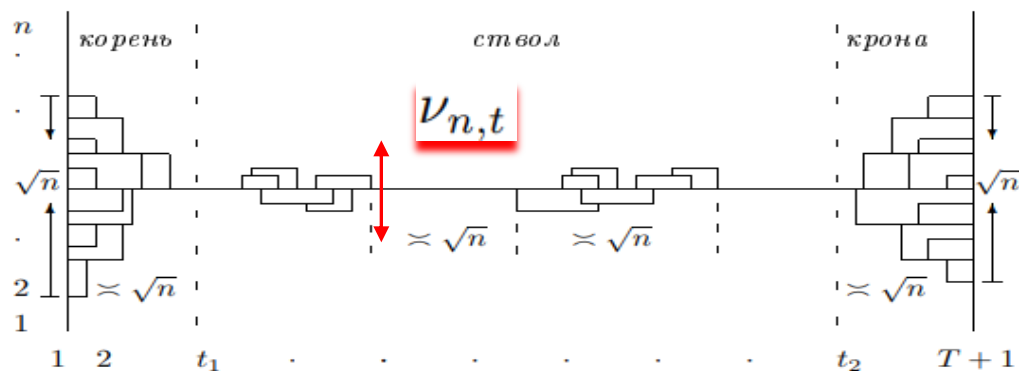


$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$

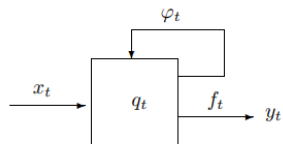




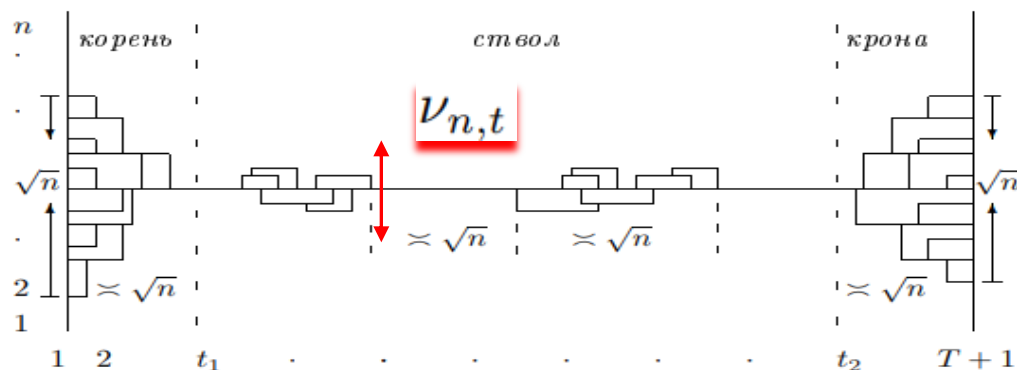
# Структура входных последовательностей



$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$



# Структура входных последовательностей

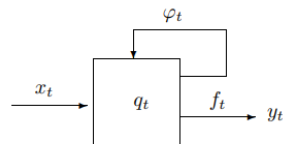


$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$

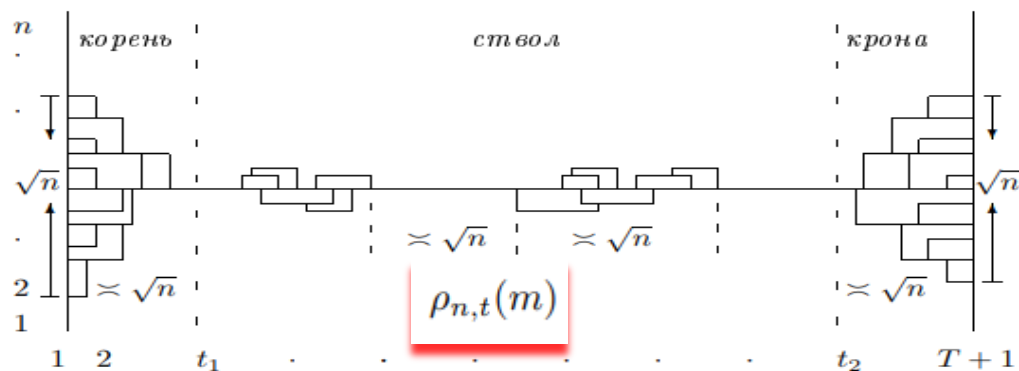
$$\mathbf{P}(\nu_{n,t} = k) \rightarrow \mathbf{P}(\nu = k) = \int_0^\infty \int_0^\infty \frac{(xy)^k}{(k-1)!} e^{-\frac{(x+y)^2}{2}} dx dy, \quad k = 1, 2, \dots$$

$$\mathbf{E}\nu = 1 + \frac{\pi}{2} \approx 2.5707\dots, \quad \mathbf{D}\nu = 2 + \frac{\pi}{2} - \frac{\pi^2}{4} \approx 1.2033\dots$$

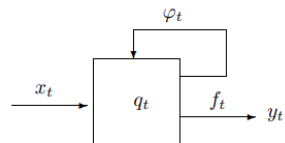
$$\mathbf{P}(\nu = 1) = \frac{1}{3}$$



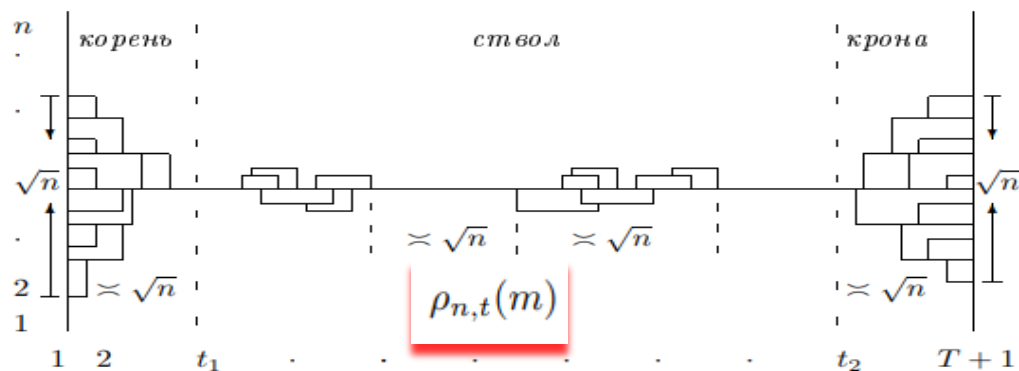
# Структура входных последовательностей



$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$

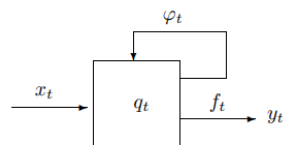


# Структура входных последовательностей

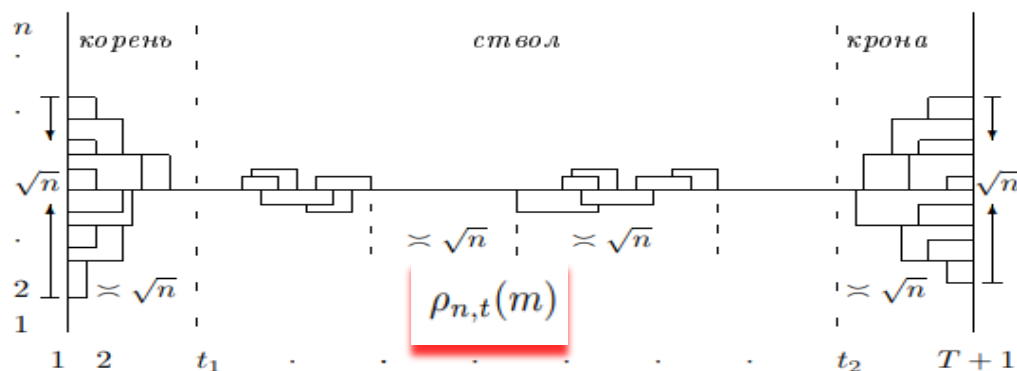


$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$

$$\rho_{n,t}(m) = mF(1/m)(1 + o(1))$$



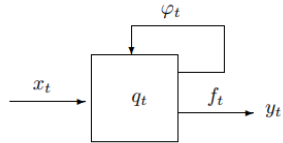
# Структура входных последовательностей



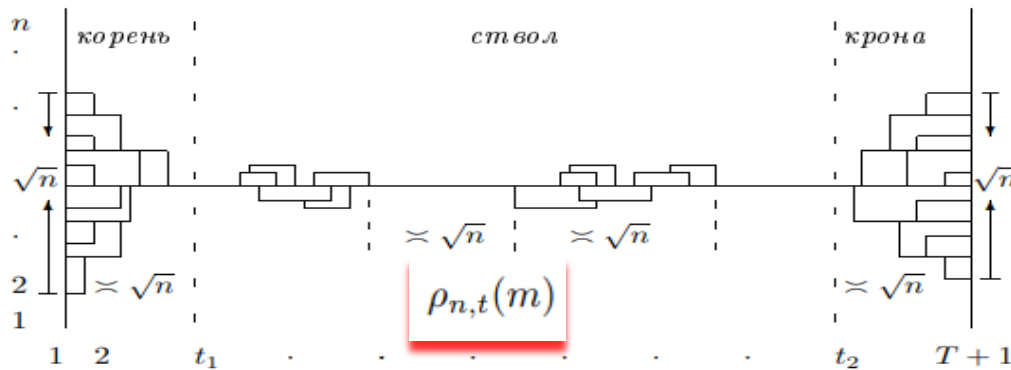
$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$

$$\rho_{n,t}(m) = mF(1/m)(1 + o(1))$$

$$F(z) = \mathbf{E}z^\nu = \frac{1}{2-z} \left( 1 - \frac{1-z}{\sqrt{z(2-z)}} \left( \frac{\pi}{2} - \arcsin(1-z) \right) \right)$$



# Структура входных последовательностей



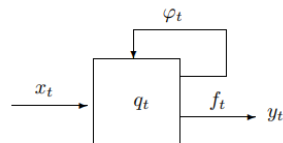
$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$

$$\rho_{n,t}(m) = mF(1/m)(1 + o(1))$$

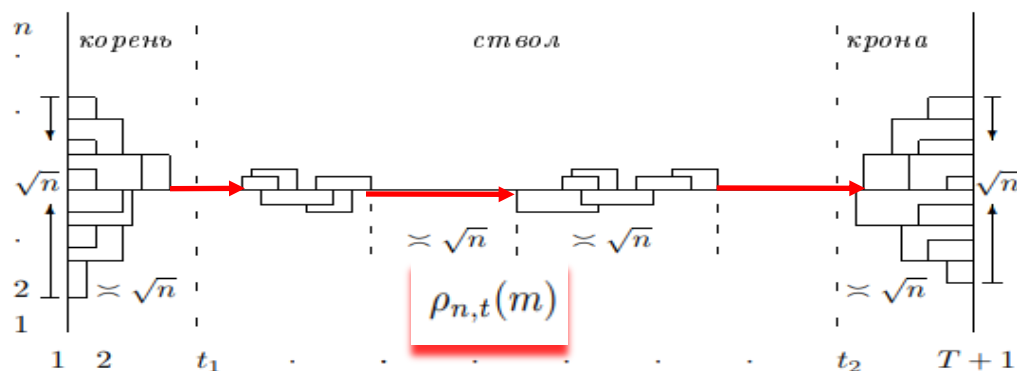
$$F(z) = \mathbf{E}z^\nu = \frac{1}{2-z} \left( 1 - \frac{1-z}{\sqrt{z(2-z)}} \left( \frac{\pi}{2} - \arcsin(1-z) \right) \right)$$

$$\rho_{n,t}(2) \sim 0.5272, \quad \rho_{n,t}(3) \sim 0.4444, \quad \rho_{n,t}(4) \sim 0.4125, \quad \rho_{n,t}(5) \sim 0.3944.$$

$$\rho_{n,t}(m) \rightarrow 1/3$$



## Обратимость автомата



$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$

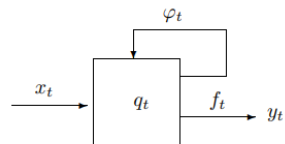
$$\rho_{n,t}(m) = mF(1/m)(1 + o(1))$$

$$F(z) = \mathbf{E}z^\nu = \frac{1}{2-z} \left( 1 - \frac{1-z}{\sqrt{z(2-z)}} \left( \frac{\pi}{2} - \arcsin(1-z) \right) \right)$$

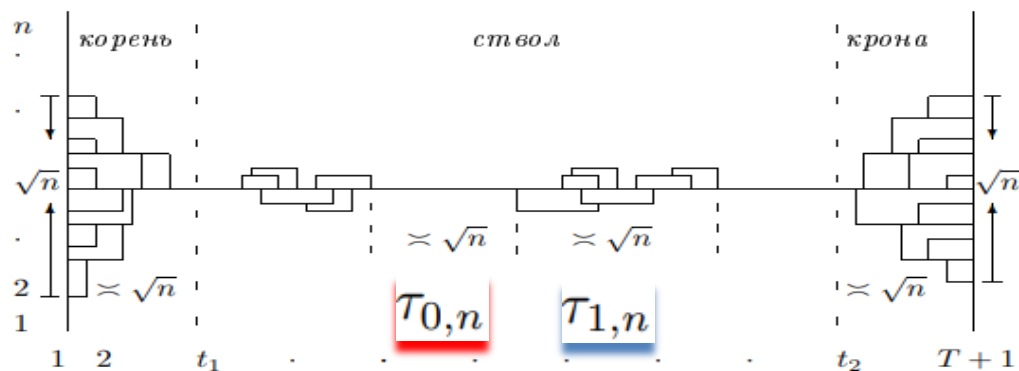
$$\rho_{n,t}(2) \sim 0.5272, \quad \rho_{n,t}(3) \sim 0.4444, \quad \rho_{n,t}(4) \sim 0.4125, \quad \rho_{n,t}(5) \sim 0.3944. \quad . \quad . \quad .$$

$$\rho_{n,t}(m) \rightarrow 1/3$$

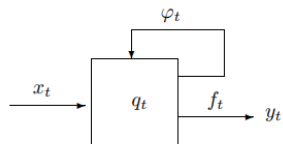
Обратимость – 33%



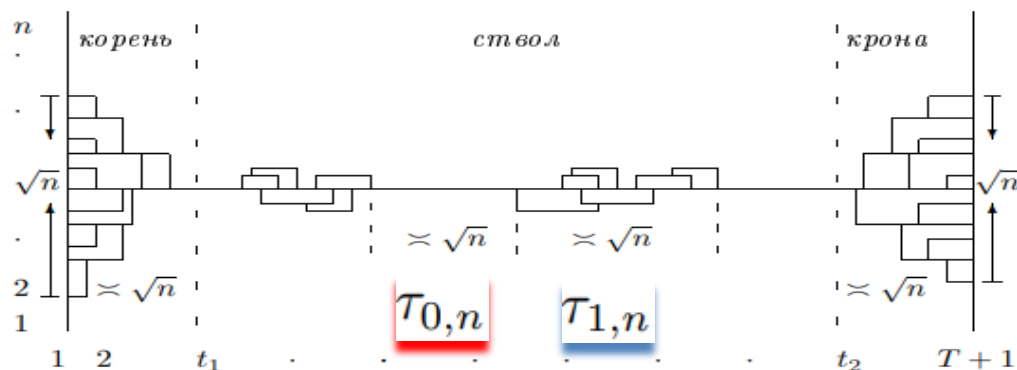
# Структура входных последовательностей



$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$



# Структура входных последовательностей

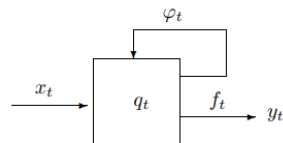


$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$

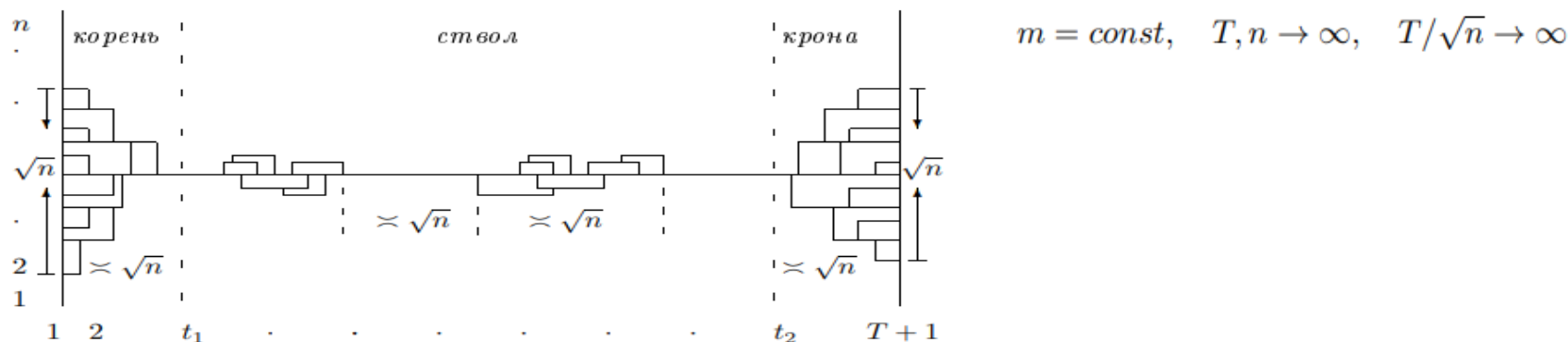
$$\mathbf{P}(\tau_{0,n}/\sqrt{n} \geq x) \geq (1 + \lambda x)e^{-\lambda x}(1 + o(1))$$

$$\mathbf{P}(\tau_{1,n}/\sqrt{n} \geq x) \geq e^{-3\lambda x}(1 + o(1))$$

$$\lambda = \sqrt{\frac{\pi(m-1)}{2m}}$$



## Качественные оценки

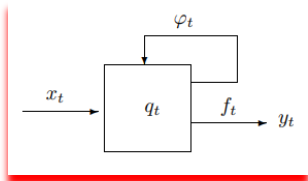


Найдутся такие  $\alpha, \beta > 0$ , что при  $T, n \rightarrow \infty, T/\sqrt{n} \rightarrow \infty$  для общего числа допустимых входных последовательностей автомата  $\aleph_n$  справедлива нижняя асимптотическая оценка

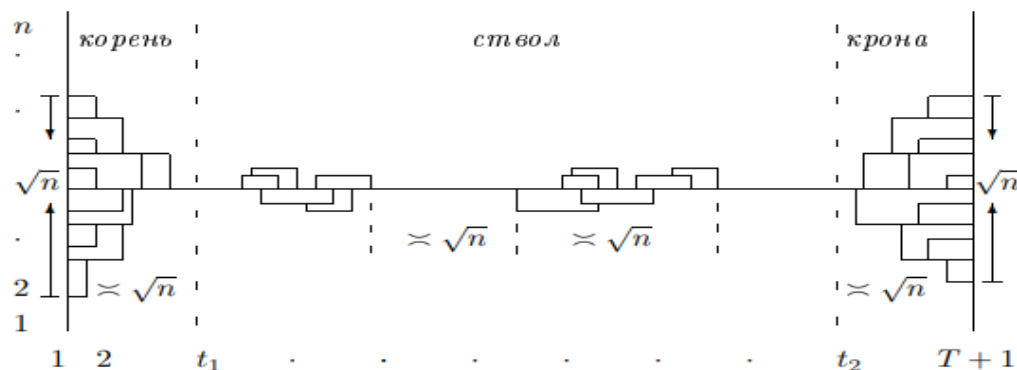
$$X_{n,T} \geq \alpha n \exp\left(\beta \frac{T}{\sqrt{n}}\right).$$

При  $T, n \rightarrow \infty, T/\sqrt{n} \rightarrow \infty$  случайное число  $X_{n,t}$  входных последовательностей  $\{x_{n,t}\}_{t=1}^T$  дающих на выходе известную последовательность  $\{y_{n,t}\}_{t=1}^T$  имеет логнормальное распределение

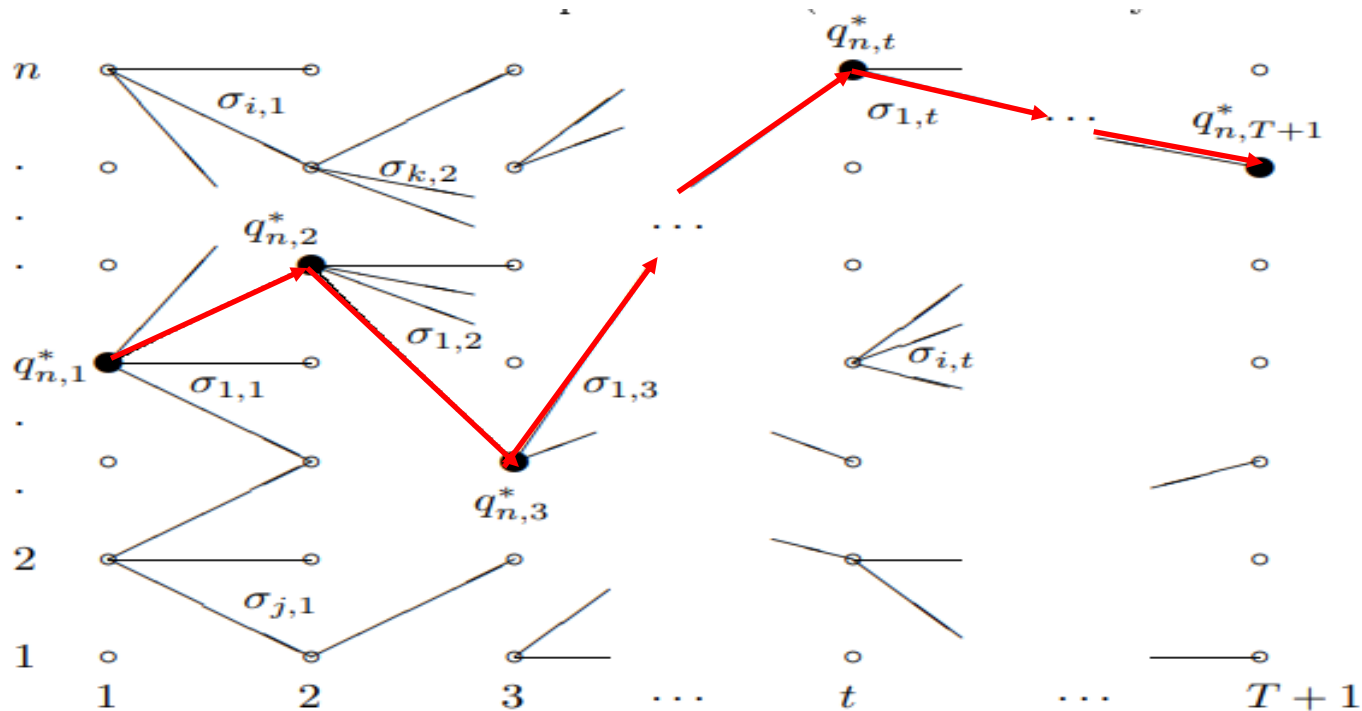
$$\frac{n^{1/4}}{\sqrt{T}} \cdot \ln X_{n,T} \sim N(a, b)$$

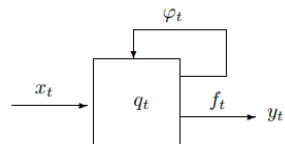


# Два слова при технику доказательств

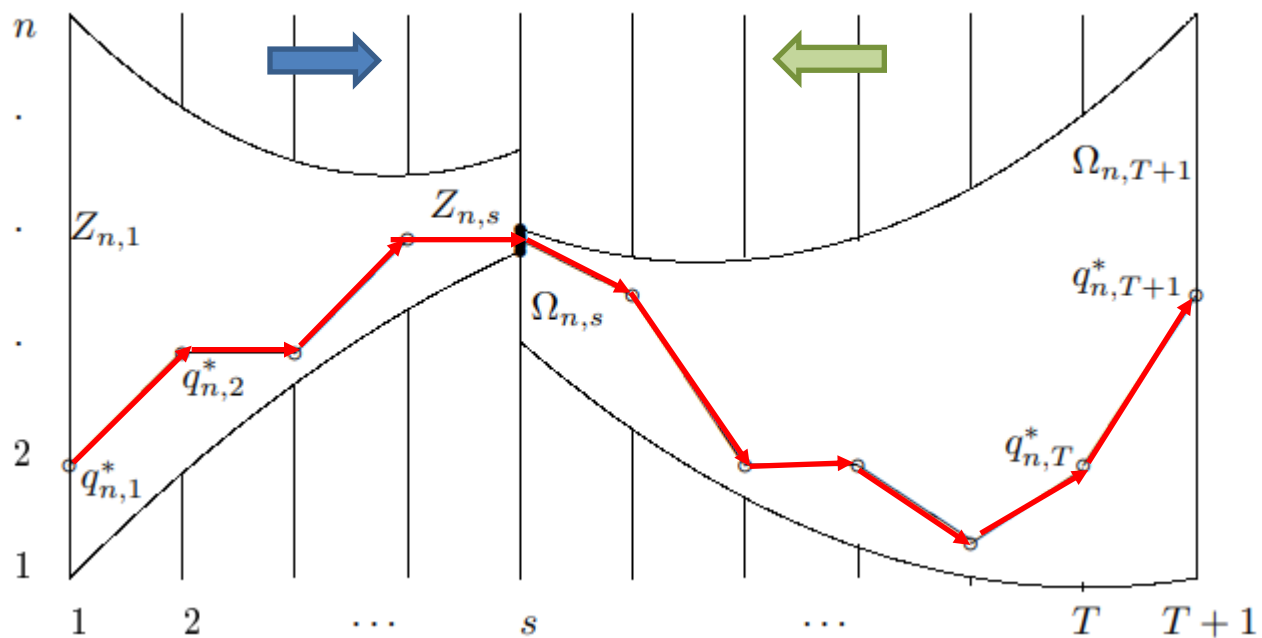
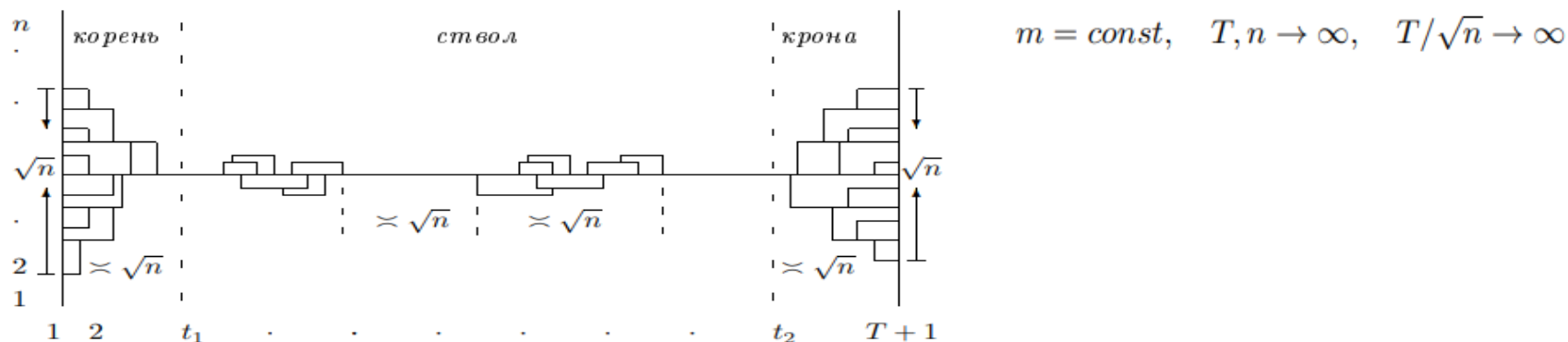


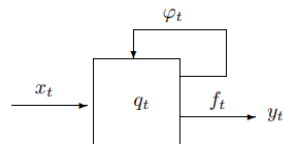
$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$



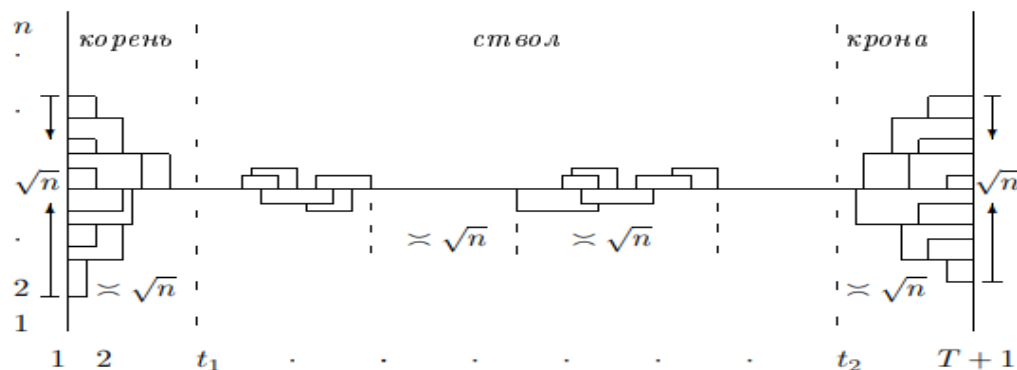


# Идущие навстречу друг другу процессы





## Две конечные цепи Маркова



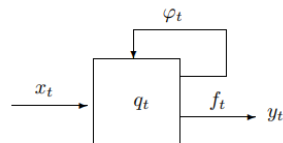
$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$



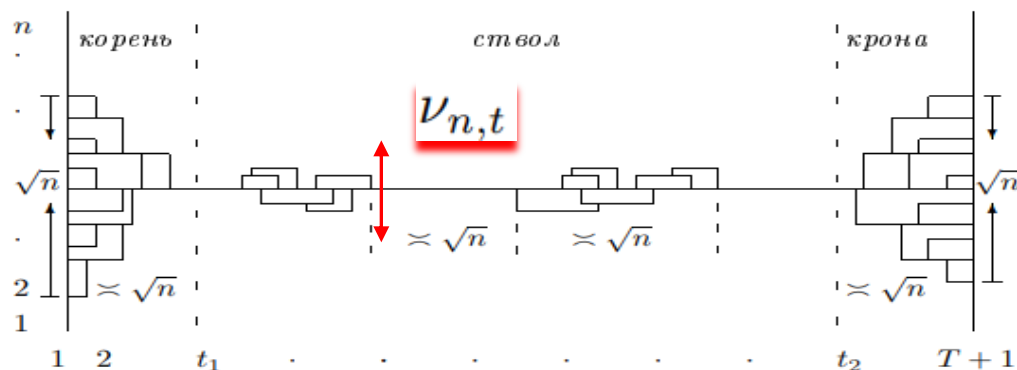
$$\zeta_{n,t+1} = n - \mu_{0,t} \left( \sum_{i=2}^{\zeta_{n,t}} \sigma_{i,t} + \sigma_{1,t,n} \right), \quad \zeta_{n,1} = n,$$

$$\omega_{n,t} = \sum_{i=2}^n \varepsilon_{i,n,t}(\omega_{n,t+1}, \sigma_{i,t}) + 1, \quad \omega_{n,T+1} = n,$$





# Пересечение цепей Маркова



$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$



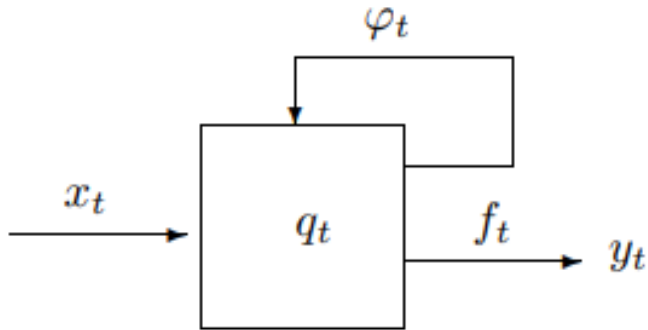
$$\zeta_{n,t+1} = n - \mu_{0,t} \left( \sum_{i=2}^{\zeta_{n,t}} \sigma_{i,t} + \sigma_{1,t,n} \right), \quad \zeta_{n,1} = n,$$

$$\omega_{n,t} = \sum_{i=2}^n \varepsilon_{i,n,t}(\omega_{n,t+1}, \sigma_{i,t}) + 1, \quad \omega_{n,T+1} = n,$$



$$\nu_{n,t} = 1 + \mu_{2,t}(\zeta_{n,t} - 1, \omega_{n,t} - 1, n - 1).$$

## Возможные приложения

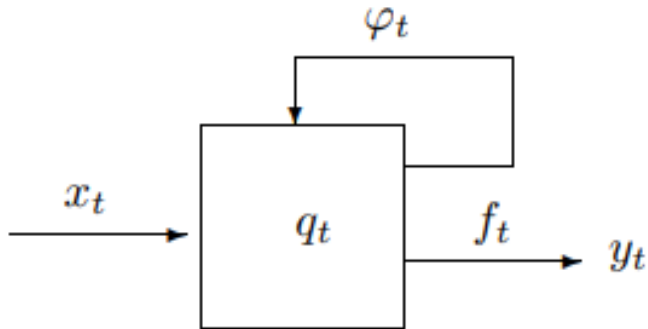


$$\begin{cases} y_t = f_t(x_t, q_t), \\ q_{t+1} = \varphi_t(x_t, q_t). \end{cases} \quad t = 1, 2, \dots, T$$

1. Работа автомата зависит от раундовых ключей.
2. Используются Твики.
3. Модель сложного автомата.

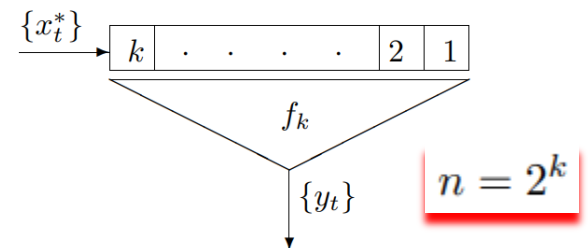
$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$

# Возможные приложения



$$\begin{cases} y_t = f_t(x_t, q_t), \\ q_{t+1} = \varphi_t(x_t, q_t). \end{cases} \quad t = 1, 2, \dots, T$$

1. Работа автомата зависит от раундовых ключей.
2. Используются Твики.
3. Модель сложного автомата.

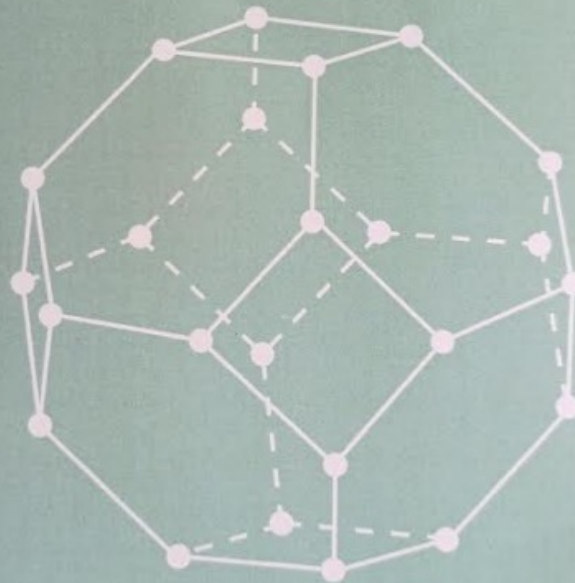


$$m = \text{const}, \quad T, n \rightarrow \infty, \quad T/\sqrt{n} \rightarrow \infty$$

Российская академия наук  
Математический институт им. В.А. Стеклова  
Российской академии наук

ISSN 0234-0860

# Дискретная математика



---

том **37** выпуск **4** \* **2025**



Спасибо за внимание