Определение 1. *Циклической перестановкой из k элементов с шагом s будем называть такую циклическую перестановку, в которой элемент с номером i переходит в элемент с номером $i + s$ ($\mod k$).*

Далее будем считать, что элементы перестановки длины k - это числа от 0 до $k - 1$.

Лемма 1. *Существуют такие перестановки x и y из S_k, что xy - циклическая перестановка с шагом -1, а yx - циклическая перестановка с шагом 1.*

Доказательство. Рассмотрим перестановку x: $i \to -i(\mod k)$ и y: $i \to -i + 1(\mod k)$.

$$x = \begin{pmatrix} 0 & 1 & 2 & 3 & ... & k-3 & k-2 & k-1 \\ 0 & k-1 & k-2 & k-3 & ... & 3 & 2 & 1 \end{pmatrix}$$

$$y = \begin{pmatrix} 0 & 1 & 2 & 3 & ... & k-3 & k-2 & k-1 \\ 1 & 0 & k-1 & k-2 & ... & 4 & 3 & 2 \end{pmatrix}$$

Тогда
xy: $i \xrightarrow{y} (-i+1) \xrightarrow{x} (-(-i+1)) == i - 1$,
yx: $i \xrightarrow{x} (-i) \xrightarrow{y} (-(-i)+1) == i + 1$

□

Лемма 2. *Пусть $(xy)^a(yx)^b(xy)^c = (yx)^c(xy)^b(yx)^a$ - тождество в S_k, где k - нечетное. Тогда $a - b + c \equiv 0 \pmod k$.*

Доказательство. Зафиксируем перестановки xy и yx из Леммы 1. Рассмотрим перестановочный автомат, в котором переход по символам осуществляется соответствующими перестановками x и y. Тогда, чтобы $(xy)^a(yx)^b(xy)^c = (yx)^c(xy)^b(yx)^a$ было тождеством для такого автомата, требуется, чтобы автомат закончил читать обе части равенства в одном состоянии, то есть

$$(-a) + b + (-c) \equiv c + (-b) + a \pmod k \tag{1}$$

что эквивалентно

$$2(a - b + c) \equiv 0 \pmod k \tag{2}$$

Из того, что k нечетно, следует

$$(a - b + c) \equiv 0 \pmod k$$

. □

Лемма 3. *Существуют такие перестановки x и y, что xy - циклическая перестановка с шагом 1, а yx - циклическая перестановка с шагом 1, в которой поменяли местами элементы a и b.*

Доказательство. Без ограничения общности $a < b$. Требуется, чтобы $xy = (0, 1, 2, ..., k-1)$, а $yx = (0, 1, ..., a-1, b, a+1, ..., b-1, a, b+1, ..., k-1)$.

Пусть y переводит $a-1$ в b, $b-1$ в a, а любой другой элемент в следующий, то есть

$$y = \begin{pmatrix} 0 & ... & a-2 & a-1 & a & ... & b-2 & b-1 & b & ... \\ 1 & ... & a-1 & b & a+1 & ... & b-1 & a & b+1 & ... \end{pmatrix}$$

а x переводит a в b и наоборот, а остальные элементы оставляет на месте:

$$x = \begin{pmatrix} 0 & ... & a-1 & a & a+1 & ... & b-1 & b & b+1 & ... \\ 0 & ... & a-1 & b & a+1 & ... & b-1 & a & b+1 & ... \end{pmatrix}$$

Откуда получим

$$xy = \begin{pmatrix} 0 & ... & a-2 & a-1 & a & ... & b-2 & b-1 & b & ... \\ 1 & ... & a-1 & a & a+1 & ... & b-1 & b & b+1 & ... \end{pmatrix}$$

$$yx = \begin{pmatrix} 0 & ... & a-2 & a-1 & a & ... & b-2 & b-1 & b & ... \\ 1 & ... & a-1 & b & b+1 & ... & b-1 & a & a+1 & ... \end{pmatrix}$$

Что и требовалось найти. □

Теорема 1. *Пусть* $(xy)^a(yx)^b(xy)^c = (yx)^c(xy)^b(yx)^a$ *- тождество в* S_k, k *- нечетное число,* $k > 3$. *Тогда выполняется хотя бы одно из следующих правил:*

$$k|a \quad u \quad k|(b-c)$$
$$k|c \quad u \quad k|(b-a)$$
$$k|b \quad u \quad k|(a+c)$$

Доказательство. От противного. Допустим, ни одно из перечисленных правил не выполняется, то есть ни одно из чисел a, b, c не делится на k. Тогда с учетом Леммы 2 на k не делятся и числа $b-a$, $b-c$, $a+c$. Тогда найдутся автоматы, различающие строки справа и слева от знака равенства. Рассмотрим несколько случаев.

В представленных ниже автоматах удобно будет оперировать не только значением состояния в автомате, но и номером этого состояния в цикле. Существование рассматриваемых автоматов доказано Леммой 3.

1. $a + b \not\equiv 0 (\mod k)$

   Рассмотрим перестановочный автомат $\mathscr{A}$ такой, что xy действует на него как циклическая перестановка из k элементов с шагом 1, а yx - как циклическая перестановка из k элементов с шагом 1, в которой поменяли местами элементы $a+b$ и b (см. Рис. 1). $a+b$ и b не равны 0 по модулю k, $a+b \neq b$, так как a не делится на k. Начальное состояние 0.

   Покажем, что такой автомат различит слова $(xy)^a(yx)^b(xy)^c$ и $(yx)^c(xy)^b(yx)^a$.

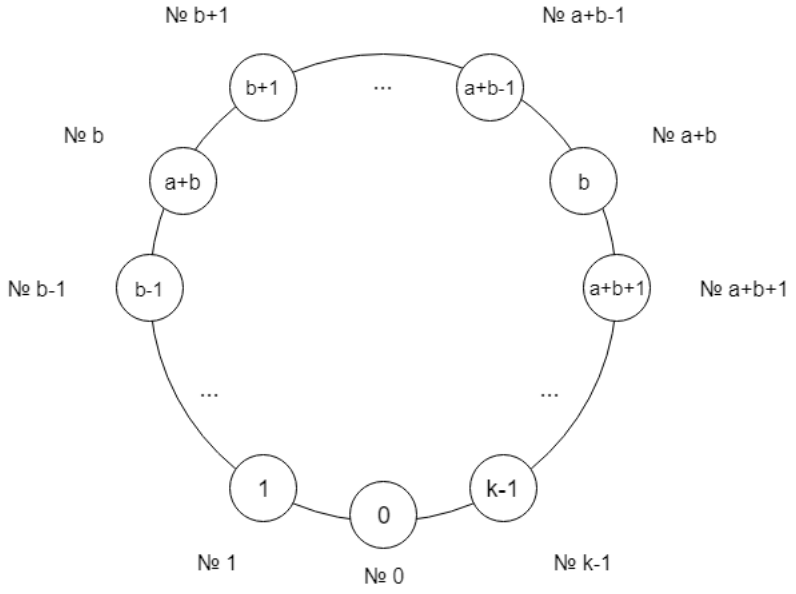

Рис. 1: Перестановка yx автомата $\mathscr{A}$

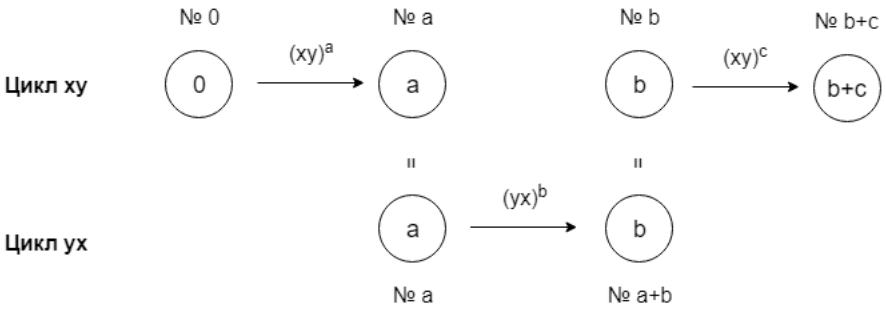

Рис. 2: Чтение автоматом $\mathscr{A}$ слова $(xy)^a(yx)^b(xy)^c$

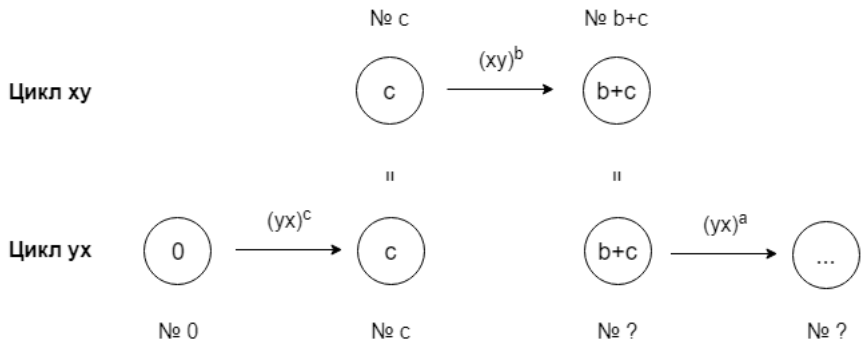

Рис. 3: Чтение автоматом $\mathscr{A}$ слова $(yx)^c(xy)^b(yx)^a$

Автомат $\mathscr{A}$ закончит читать слово $(xy)^a(yx)^b(xy)^c$ в состоянии $b+c$ (см. Рис 2).

Корректность переходов при чтении $(xy)^a(yx)^b(xy)^c$:

- $0 \xrightarrow{(xy)^a} a$
  - $a \not\equiv a+b$, так как $b \not\equiv 0 \mod k$
  - $a \not\equiv b$, так как $b-a \not\equiv 0 \mod k$
- $a \xrightarrow{(yx)^b} b$
  - Из состояния с номером a делаем b шагов, оказываемся в состоянии с номером $a+b$, которым в данном цикле является b, т.к. мы так задали автомат.

Теперь покажем, что $\mathscr{A}$ не закончит читать слово $(yx)^c(xy)^b(yx)^a$ в состоянии $b+c$ (см. Рис 3).

Корректность переходов при чтении $(yx)^c(xy)^b(yx)^a$:

- $0 \xrightarrow{(yx)^c} c$
  - $c \not\equiv a+b$.
    От противного. Пусть $c \equiv a+b \pmod k$. Тогда $a+b-c \equiv 0 \pmod k$ и $a-b+c \equiv 0 \pmod k$ по Лемме 2. Сложив оба равенства получим $2a \equiv 0 \pmod k$. Но k нечетно, поэтому $a \equiv 0 \pmod k$. Противоречие.
  - $c \not\equiv b$, так как $b-c \not\equiv 0 \mod k$
- Переход $c \xrightarrow{(xy)^b} b+c$ осуществляется в обычном цикле без ловушки. Последний переход выполняется из состояния $b+c$. Поскольку $a \not\equiv 0 \pmod k$, переход по $(yx)^a$ не вернет автомат обратно в состояние $b+c$.

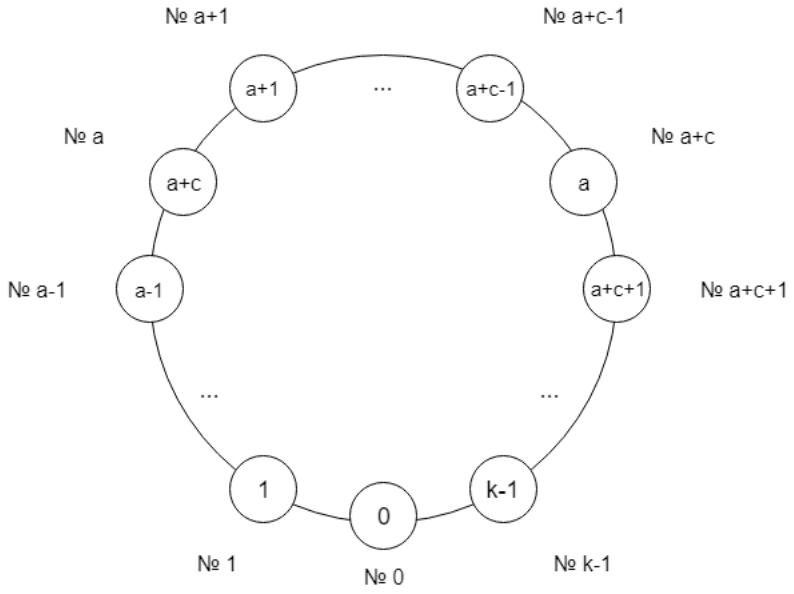

Рис. 4: Перестановка yx автомата $\mathscr{B}$

2. $a + b \equiv 0(\mod k)$ и $a \not\equiv c(\mod k)$

   Из того, что $a + b \equiv 0(\mod k)$, следует $a + c \not\equiv 0(\mod k)$ (иначе, выразив a из первого утверждения и подставив его во второе, получили бы $c - b \equiv 0(\mod k)$, что противоречит нашему предположению).

   Рассмотрим перестановочный автомат $\mathscr{B}$, в котором перестановка xy - это циклическая перестановка из k элементов с шагом 1, а yx - циклическая перестановка из k элементов с шагом 1, в которой состояния a и $a + c$ поменяли местами (см. Рис. 4). Начальное состояние 0.

   Покажем, что такой автомат различит слова $(xy)^a(yx)^b(xy)^c$ и $(yx)^c(xy)^b(yx)^a$.

   Автомат $\mathscr{B}$ закончит читать слово $(xy)^a(yx)^b(xy)^c$ в состоянии $2c$ (см. Рис. 5).

   Корректность переходов:

   - $a \xrightarrow{(yx)^b} c$
     - $a + c + b \equiv c(\mod k)$ потому что $a + b \equiv 0(\mod k)$
     - $c \not\equiv a(\mod k)$ по выбранному ограничению
     - $c \not\equiv a + c(\mod k)$ потому что $a \not\equiv 0(\mod k)$

   Теперь покажем, что автомат $\mathscr{B}$ закончит читать слово $(yx)^c(xy)^b(yx)^a$ в состоянии c, которое, очевидно, не совпадает с состоянием $2c$ (см. Рис. 6)

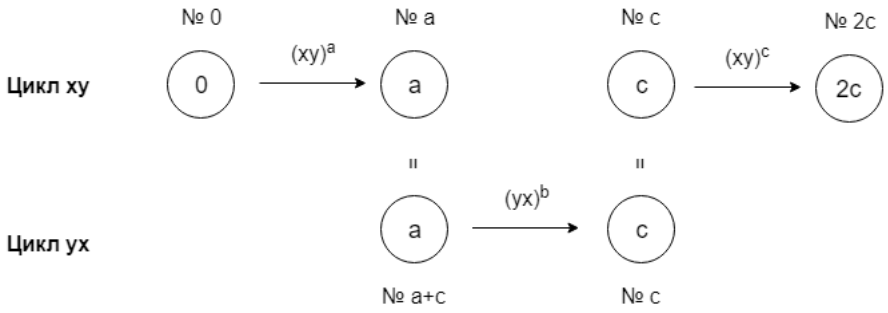

Рис. 5: Чтение автоматом $\mathscr{B}$ слова $(xy)^a(yx)^b(xy)^c$

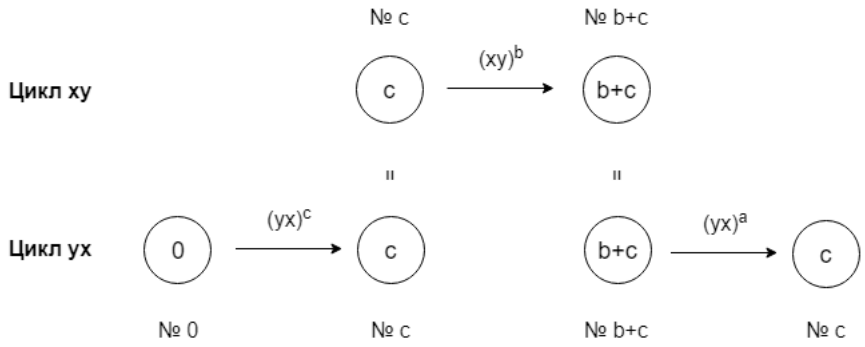

Рис. 6: Чтение автоматом $\mathscr{B}$ слова $(yx)^c(xy)^b(yx)^a$

Корректность переходов:

- $0 \xrightarrow{(yx)^c} c$
  - $c \not\equiv a(\mod k)$ по выбранному ограничению
  - $c \not\equiv a + c(\mod k)$ потому что $a \not\equiv 0(\mod k)$, поэтому не попадаем в "ловушку"
- $c \xrightarrow{(xy)^b} b + c$
  - $b+c \not\equiv a+c(\mod k)$, т.к. $b-a \not\equiv 0(\mod k)$ по предположению
  - $b + c \not\equiv a(\mod k)$
    От противного. Пусть $b + c \equiv a(\mod k)$, тогда $b + c - a \equiv 0(\mod k)$. Сложим с $a - b + c \equiv 0(\mod k)$, получим $2c \equiv 0(\mod k)$. Поскольку k нечетное, имеем $c \equiv 0(modk)$ и получаем противоречие.
- $b + c \xrightarrow{(yx)^a} c$
  - $b+c+a \equiv c(\mod k)$, т.к. $a+b \equiv 0(\mod k)$ по ограничению. А c не попадает в "ловушку".

3. $a + b \equiv 0(\mod k)$ и $a \equiv c(\mod k)$

   Из того, что $a + b \equiv 0(\mod k)$ следует, что $b \equiv -a(\mod k)$.

   Из того, что $a-b+c \equiv 0(\mod k)$ и $a \equiv c(\mod k)$ следует, что $b \equiv 2a(\mod k)$.

   То есть $2a \equiv -a$ или $3a \equiv 0(\mod k)$.

   Если k не делится на 3, получаем $a \equiv 0(\mod k)$, что противоречит предположению.

   Пусть $k = 3m$, $m \in \mathbb{N}$. Тогда $a \equiv c \equiv m(\mod k)$, $b \equiv 2m(\mod k)$.

   Рассмотрим перестановочный автомат $\mathscr{C}$ с начальным состоянием m, такой, что xy - циклическая перестановка из k элементов с шагом 1, а yx - циклическая перестановка из k элементов с шагом 1, в которой поменяли местами состояния $2m$ и z, где $z \not\equiv 0(\mod k)$, $z \not\equiv m(\mod k)$ и $z \not\equiv 2m(\mod k)$ (см. Рис. 7). Такое z существует, если $k > 3$.

   Покажем, что автомат $\mathscr{C}$ закончит читать слова $(xy)^a(yx)^b(xy)^c$ и $(yx)^c(xy)^b(yx)^a$ в разных состояниях.

   При чтении слова $(xy)^a(yx)^b(xy)^c$ автомат $\mathscr{C}$ остановится в состоянии z (см. Рис. 8)

   Корректность переходов:

   - $2m \xrightarrow{(yx)^b} 2m + z$
     - $2m + z \not\equiv x(\mod k)$, т.к. $2m < k$, а значит $2m \not\equiv 0(\mod k)$
     - $2m + z \not\equiv 2m(\mod k)$ по выбору z

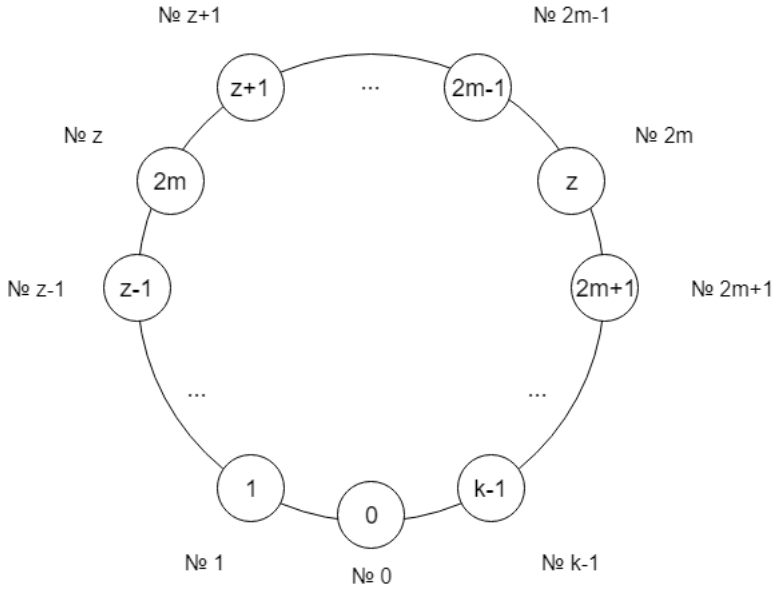

Рис. 7: Цикл yx автомата $\mathscr{C}$

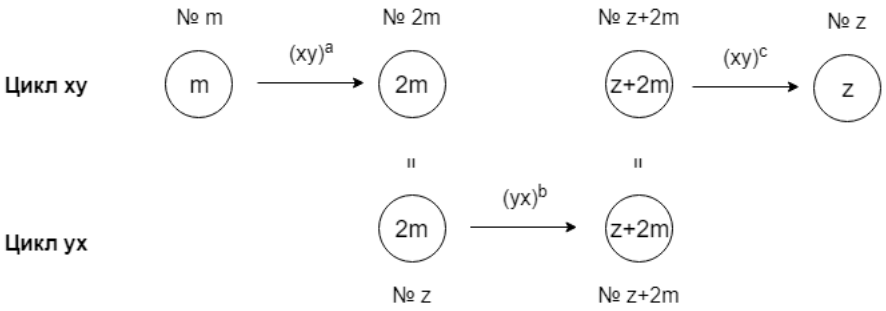

Рис. 8: Чтение слова $(xy)^a(yx)^b(xy)^c$ автоматом $\mathscr{C}$

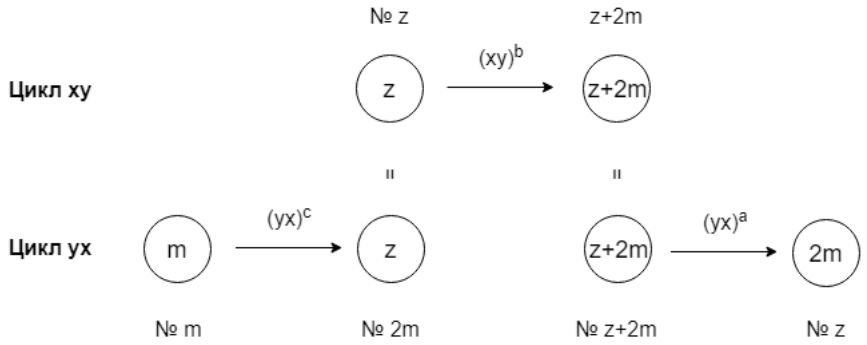

Рис. 9: Чтение слова $(yx)^c(xy)^b(yx)^a$ автоматом $\mathscr{C}$

- $z + 2m \xrightarrow{(xy)^c} z$
  - $z + 2m + m \equiv z + k \equiv z(\mod k)$

При чтении слова $(yx)^c(xy)^b(yx)^a$ автомат $\mathscr{C}$ остановится в состоянии $2m$, которое не совпадает с z (см. Рис. 9)

Корректность переходов:

- $z + 2m \xrightarrow{(yx)^c} 2m$
  - $z + 2m + m \equiv z + k \equiv z(\mod k)$
  - Под номером z в цикле yx находится состояние $2m$ по выбору автомата

В итоге, три рассмотренных случая покрывают всевохможные варианты a, b и c, и ни один не привел к успеху. Значит, наше предположение о невыполнении правил было ложным. □