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 $i+s \pmod k$.*

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

Лемма 1. *Пары перестановок вида xy и yx пробегают в том числе всевозможные пары циклических перестановок длины k с произвольным шагом.*

Доказательство. Зафиксируем произвольные s и t из $\{0, .., k-1\}$ и докажем, что найдутся такие перестановки x и y из k элементов, что xy будет циклической перестановкой с шагом s, а yx - циклической перестановкой с шагом t.

Пусть элемент i переходит под действием перестановки x в элемент x_i. Потребуем, чтобы x_i под действием перестановки y перешел в $i+s \pmod k$. $i+s$ в свою очередь под действием x переходит в x_{i+s}, потребуем, чтобы $x_{i+s} = x_i + t \pmod k$.

$$i \xrightarrow{x} x_i \xrightarrow{y} i+s \xrightarrow{x} x_{i+s} = x_i + t \tag{1}$$

Поскольку $\{x_i\} = \{x_{i+s}\}$ - множество всех остатков от деления на k, то $\{x_i+t\} \pmod k$ - также множество всех остатков от деления на k. Все x_i и x_i+t различны. Получим систему из k равенств вида $x_{i+s} = x_i+t \pmod k$, $i \in \{0, ..., k-1\}$, где $x_i, x_{i+s} \in \{0, ..., k-1\}$ и каждое такое число встречается по разу в левой и в правой части. Такая система имеет k решений.

□

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

Доказательство. Зафиксируем произвольные s, $t \in \{0, ..., k-1\}$. По Лемме 1 существуют такие перестановки x и y, что xy и yx - это циклические перестановки с шагами s и t соответственно. 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

$$as + bt + cs \equiv ct + bs + at \pmod k \tag{2}$$

что эквивалентно

$$(a-b+c)(s-t) \equiv 0 \pmod k \tag{3}$$

Поскольку s и t принимают произвольные значения $\{0, ..., k-1\}$, их разность по модулю k также принимает различные значения из $\{0, ..., k-1\}$. Найдутся такие s и t, $s-t$ будет взаимно просто с k. Откуда $a-b+c$ должно делиться на 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 x переводит $a-1$ в b, $b-1$ в a, а любой другой элемент в следующий, то есть

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

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

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

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. Тогда выполняется хотя бы одно из следующих правил:*

$$k|a \quad \text{и} \quad k|(b-c)$$

$$k|c \quad \text{и} \quad k|(b-a)$$

$$k|b \quad \text{и} \quad k|(a+c)$$

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.

1. $a + b \neq 0 \mod k$

   Рассмотрим перестановочный автомат 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 $a+c$ (см. Рис. 1). $a+b$ и $a+c$ не равны 0 по модулю k, $a+b \neq a+c$, так как $b-c$ не делится на k. (Существование такого автомата доказывает Лемма 3). Начальное состояние 0.

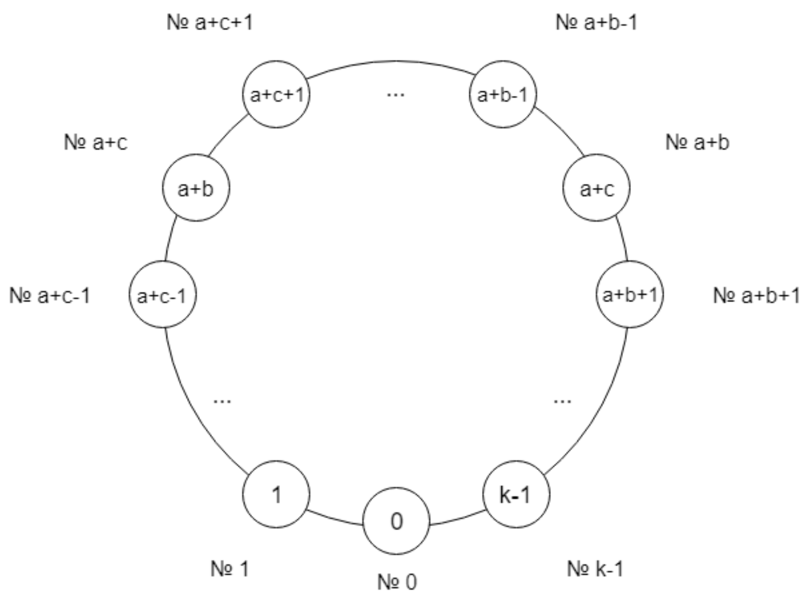

Рис. 1: Перестановка yx

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

Автомат закончит читать слово $(xy)^a(yx)^b(xy)^c$ в состоянии $a+2c$ (см. Рис 2). Корректность переходов:

- $a \neq a+b$, так как $b \not\equiv 0 \mod k$; $a \neq a+c$, так как $c \not\equiv 0 \mod k$.

$\square$

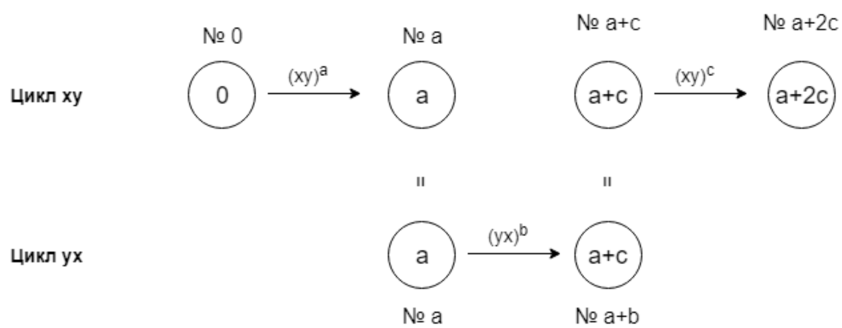

Рис. 2: Чтение автоматом слова $(xy)^a(yx)^b(xy)^c$