cyclic permutation

Canonical name	CyclicPermutation
Date of creation	2013-03-22 17:33:54
Last modified on	2013-03-22 17:33:54
Owner	CWoo (3771)
Last modified by	CWoo (3771)
Numerical id	13
Author	CWoo (3771)
Entry type	Definition
Classification	msc 94B15
Classification	msc 20B99
Classification	msc 03-00
Classification	msc 05A05
Classification	msc 11Z05
Classification	msc 94A60
Synonym	Caesar cipher
Related topic	CyclicCode
Related topic	SubgroupsWithCoprimeOrders
Defines	Caesar shift cipher
Defines	cyclic conjugate

Let $A = \{a_0, a_1, \ldots, a_{n-1}\}$ be a finite set indexed by $i = 0, \ldots, n-1$. A *cyclic permutation* on A is a permutation π on A such that, for some integer k,

$$\pi(a_i) = a_{(i+k)(\mathrm{mod}\ n)},$$

where $a\,(\mathrm{mod}\ b) := a - \lfloor a/b \rfloor b$, the remainder of a when divided by b, and $\lfloor\cdot\rfloor$ is the floor function.

For example, if $A = \{1, 2, \ldots, m\}$ such that $a_i = i + 1$. Then a cyclic permutation π on A has the form

$$\begin{array}{rcl}
\pi(1) & = & r \\
\pi(2) & = & r+1 \\
& \vdots & \\
\pi(m-r+1) & = & m \\
\pi(m-r+2) & = & 1 \\
& \vdots & \\
\pi(m) & = & r-1.
\end{array}$$

In the usual permutation notation, it looks like

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & m-r+1 & m-r+2 & \cdots & m \\ r & r+1 & \cdots & m & 1 & \cdots & r-1 \end{pmatrix}$$

Remark. For every finite set of cardinality n, there are n cyclic permutations. Each non-trivial cyclic permutation has order n. Furthermore, if n is a prime number, the set of cyclic permutations forms a cyclic group.

Cyclic permutations on words

Given a word $w = a_1 a_2 \cdots a_n$ on a set Σ (may or may not be finite), a *cyclic conjugate* of w is a word v derived from w based on a cyclic permutation. In other words, $v = \pi(a_1)\pi(a_2)\cdots\pi(a_n)$ for some cyclic permutation π on $\{a_1, \ldots, a_n\}$. Equivalently, v and w are cyclic conjugates of one another iff $w = st$ and $v = ts$ for some words s, t.

For example, the cyclic conjugates of the word $ababa$ over $\{a, b\}$ are

$$baba^2, \quad aba^2b, \quad ba^2ba, \quad a^2bab, \quad \text{and itself.}$$

Strictly speaking, π is a cyclic permutation on the *multiset* $A = \{a_1, \dots, a_n\}$, which can be thought of as a cyclic permutation on the set $A' = \{(1, a_1), \dots, (n, a_n)\}$. Furthermore, π can be extended to a function on A^*: for every word $w = a_{\phi(1)} \cdots a_{\phi(m)}$, $\pi(w) := \pi(a_{\phi(1)}) \cdots \pi(a_{\phi(m)})$, where ϕ is a permutation on A.

Given any word $w = a_1 a_2 \cdots a_n$ on Σ, two cyclic permutations π_1, π_2 on $\{a_1, \dots, a_n\}$ are said to be the *same* if $\pi_1(w) = \pi_2(w)$. For example, with the word *abab*, then the cyclic permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

is the same as the identity permutation. There is a one-to-one correspondence between the set of all cyclic conjugates of w and the set of all *distinct* cyclic permutations on $\{a_0, a_1, \dots, a_n\}$.

Remarks.

- In a group G, if two elements u, v are cyclic conjugates of one another, then they are conjugates: for if $u = st$ and $v = ts$, then $v = t(st)t^{-1} = tut^{-1}$.

- Cyclic permutations were used as a ciphering scheme by Julius Caesar. Given an alphabet with letters, say $a, b, c, \dots, x, y, z$, messages in letters are encoded so that each letter is shifted by three places. For example, the name

  "Julius Caesar" becomes "Mxolxv Fdhvdu".

  A ciphering scheme based on cyclic permutations is therefore also known as a *Caesar shift cipher*.