

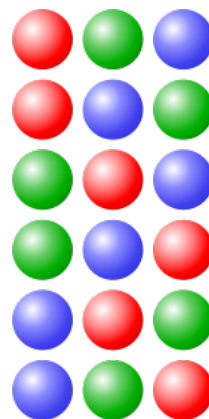
WIKIPEDIA

# Permutation

---

In mathematics, a **permutation** of a set is, loosely speaking, an arrangement of its members into a sequence or linear order, or if the set is already ordered, a rearrangement of its elements. The word "permutation" also refers to the act or process of changing the linear order of an ordered set.<sup>[1]</sup>

Permutations differ from combinations, which are selections of some members of a set regardless of order. For example, written as tuples, there are six permutations of the set  $\{1, 2, 3\}$ , namely  $(1, 2, 3)$ ,  $(1, 3, 2)$ ,  $(2, 1, 3)$ ,  $(2, 3, 1)$ ,  $(3, 1, 2)$ , and  $(3, 2, 1)$ . These are all the possible orderings of this three-element set. Anagrams of words whose letters are different are also permutations: the letters are already ordered in the original word, and the anagram is a reordering of the letters. The study of permutations of finite sets is an important topic in the fields of combinatorics and group theory.



Each of the six rows is a different permutation of three distinct balls

Permutations are used in almost every branch of mathematics, and in many other fields of science. In computer science, they are used for analyzing sorting algorithms; in quantum physics, for describing states of particles; and in biology, for describing RNA sequences.

The number of permutations of  $n$  distinct objects is  $n$  factorial, usually written as  $n!$ , which means the product of all positive integers less than or equal to  $n$ .

Technically, a permutation of a set  $S$  is defined as a bijection from  $S$  to itself.<sup>[2][3]</sup> That is, it is a function from  $S$  to  $S$  for which every element occurs exactly once as an image value. This is related to the rearrangement of the elements of  $S$  in which each element  $s$  is replaced by the corresponding  $f(s)$ . For example, the permutation (3, 1, 2) mentioned above is described by the function  $\alpha$  defined as

$$\alpha(1) = 3, \quad \alpha(2) = 1, \quad \alpha(3) = 2.$$

The collection of all permutations of a set form a group called the symmetric group of the set. The group operation is the composition (performing two given rearrangements in succession), which results in another rearrangement. As properties of permutations do not depend on the nature of the set elements, it is often the permutations of the set  $\{1, 2, \dots, n\}$  that are considered for studying permutations.

In elementary combinatorics, the  $k$ -permutations, or partial permutations, are the ordered arrangements of  $k$  distinct elements selected from a set. When  $k$  is equal to the size of the set, these are the permutations of the set.

## Contents

---

### History

### Permutations without repetitions

### Definition

### Notations

Two-line notation

One-line notation

Cycle notation

Canonical cycle notation

Composition of permutations

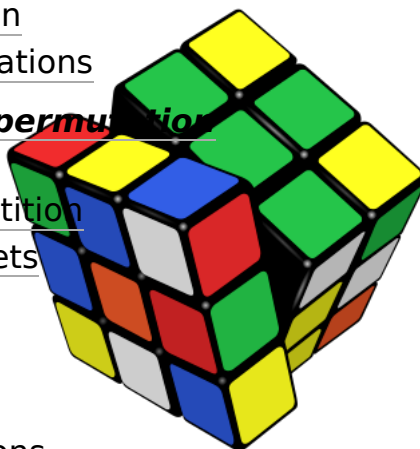
## **Other uses of the term *permutation***

$k$ -permutations of  $n$

Permutations with repetition

Permutations of multisets

Circular permutations



## **Properties**

Permutation type

Conjugating permutations

Permutation order

Parity of a permutation

Matrix representation

Foata's transition lemma

In the popular puzzle Rubik's cube invented in 1974 by Ernő Rubik, each turn of the puzzle faces creates a permutation of the surface colors.

## **Permutations of totally ordered sets**

Ascents, descents, runs and excedances

Inversions

## **Permutations in computing**

Numbering permutations

Algorithms to generate permutations

Random generation of permutations

Generation in lexicographic order

Generation with minimal changes

Meandric permutations

Applications

## **See also**

## **Notes**

## **References**

## Bibliography

## Further reading

## External links

# History

---

Permutations called hexagrams were used in China in the I Ching (Pinyin: Yi Jing) as early as 1000 BC.

Al-Khalil (717–786), an Arab mathematician and cryptographer, wrote the *Book of Cryptographic Messages*. It contains the first use of permutations and combinations, to list all possible Arabic words with and without vowels.<sup>[4]</sup>

The rule to determine the number of permutations of  $n$  objects was known in Indian culture around 1150. The *Lilavati* by the Indian mathematician Bhaskara II contains a passage that translates to:

The product of multiplication of the arithmetical series beginning and increasing by unity and continued to the number of places, will be the variations of number with specific figures.<sup>[5]</sup>

In 1677, Fabian Stedman described factorials when explaining the number of permutations of bells in change ringing. Starting from two bells: "first, *two* must be admitted to be varied in two ways", which he illustrates by showing 1 2 and 2 1.<sup>[6]</sup> He then explains that with three bells there are "three times two figures to be produced out of three" which again is illustrated. His explanation involves "cast away 3, and 1.2 will remain; cast away 2, and 1.3 will remain; cast away 1, and 2.3 will remain".<sup>[7]</sup> He then moves on to four bells and repeats the casting away argument showing that there will be four different

sets of three. Effectively, this is a recursive process. He continues with five bells using the "casting away" method and tabulates the resulting 120 combinations.<sup>[8]</sup> At this point he gives up and remarks:

Now the nature of these methods is such, that the changes on one number comprehends the changes on all lesser numbers, ... insomuch that a compleat Peal of changes on one number seemeth to be formed by uniting of the compleat Peals on all lesser numbers into one entire body;<sup>[9]</sup>

Stedman widens the consideration of permutations; he goes on to consider the number of permutations of the letters of the alphabet and of horses from a stable of 20.<sup>[10]</sup>

A first case in which seemingly unrelated mathematical questions were studied with the help of permutations occurred around 1770, when Joseph Louis Lagrange, in the study of polynomial equations, observed that properties of the permutations of the roots of an equation are related to the possibilities to solve it. This line of work ultimately resulted, through the work of Évariste Galois, in Galois theory, which gives a complete description of what is possible and impossible with respect to solving polynomial equations (in one unknown) by radicals. In modern mathematics, there are many similar situations in which understanding a problem requires studying certain permutations related to it.

## Permutations without repetitions

---

The simplest example of permutations is permutations without repetitions where we consider the number of possible ways of arranging  $n$  items into  $n$  places. The factorial has special application in defining the number of permutations in a set which does not include repetitions. The number  $n!$ , read "n factorial", is precisely the

number of ways we can rearrange  $n$  things into a new order. For example, if we have three fruits: an orange, apple and pear, we can eat them in the order mentioned, or we can change them (for example, an apple, a pear then an orange). The exact number of permutations is then  $3! = 1 \cdot 2 \cdot 3 = 6$ . The number gets extremely large as the number of items ( $n$ ) goes up.

In a similar manner, the number of **arrangements** of  $k$  items from  $n$  objects is sometimes called a partial permutation or a  $k$ -permutation. It can be written as  $nPk$  (which reads "n permute k"), and is equal to the number  $n(n-1) \cdots (n-k+1)$  (also written as  $n!/(n-k)!$ ).<sup>[11][12]</sup>

## Definition

---

In mathematics texts it is customary to denote permutations using lowercase Greek letters. Commonly, either  $\alpha$  and  $\beta$ , or  $\sigma$ ,  $\tau$  and  $\pi$  are used.<sup>[13]</sup>

Permutations can be defined as bijections from a set  $S$  onto itself. All permutations of a set with  $n$  elements form a symmetric group, denoted  $S_n$ , where the group operation is function composition. Thus for two permutations,  $\pi$  and  $\sigma$  in the group  $S_n$ , the four group axioms hold:

1. Closure: If  $\pi$  and  $\sigma$  are in  $S_n$  then so is  $\pi\sigma$ .
2. Associativity: For any three permutations  $\pi, \sigma, \tau \in S_n$ ,  $(\pi\sigma)\tau = \pi(\sigma\tau)$ .
3. Identity: There is an identity permutation, denoted  $\text{id}$  and defined by  $\text{id}(x) = x$  for all  $x \in S$ . For any  $\sigma \in S_n$ ,  $\text{id}\sigma = \sigma\text{id} = \sigma$ .
4. Invertibility: For every permutation  $\pi \in S_n$ , there exists  $\pi^{-1} \in S_n$  so that  $\pi\pi^{-1} = \pi^{-1}\pi = \text{id}$ .

In general, composition of two permutations is not commutative, that is,  $\pi\sigma \neq \sigma\pi$ .

As a bijection from a set to itself, a permutation is a function that *performs* a rearrangement of a set, and is not a rearrangement itself. An older and more elementary viewpoint is that permutations are the rearrangements themselves. To distinguish between these two, the identifiers *active* and *passive* are sometimes prefixed to the term *permutation*, whereas in older terminology *substitutions* and *permutations* are used.<sup>[14]</sup>

A permutation can be decomposed into one or more disjoint *cycles*, that is, the orbits, which are found by repeatedly tracing the application of the permutation on some elements. For example, the permutation  $\sigma$  defined by  $\sigma(7) = 7$  has a 1-cycle,  $(7)$  while the permutation  $\pi$  defined by  $\pi(2) = 3$  and  $\pi(3) = 2$  has a 2-cycle  $(23)$  (for details on the syntax, see § Cycle notation below). In general, a cycle of length  $k$ , that is, consisting of  $k$  elements, is called a  $k$ -cycle.

An element in a 1-cycle  $(x)$  is called a fixed point of the permutation. A permutation with no fixed points is called a derangement. 2-cycles are called transpositions; such permutations merely exchange two elements, leaving the others fixed.

## Notations

---

Since writing permutations elementwise, that is, as piecewise functions, is cumbersome, several notations have been invented to represent them more compactly. *Cycle notation* is a popular choice for many mathematicians due to its compactness and the fact that it makes a permutation's structure transparent. It is the notation used in this article unless otherwise specified, but other notations are still widely used, especially in application areas.

## Two-line notation

In Cauchy's two-line notation,<sup>[15]</sup> one lists the elements of  $S$  in the first row, and for each one its image below it in the second row. For instance, a particular permutation of the set  $S = \{1, 2, 3, 4, 5\}$  can be written as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix};$$

this means that  $\sigma$  satisfies  $\sigma(1) = 2$ ,  $\sigma(2) = 5$ ,  $\sigma(3) = 4$ ,  $\sigma(4) = 3$ , and  $\sigma(5) = 1$ . The elements of  $S$  may appear in any order in the first row. This permutation could also be written as:

$$\sigma = \begin{pmatrix} 3 & 2 & 5 & 1 & 4 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix},$$

or

$$\sigma = \begin{pmatrix} 5 & 1 & 4 & 3 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

## One-line notation

If there is a "natural" order for the elements of  $S$ ,<sup>[a]</sup> say  $x_1, x_2, \dots, x_n$ , then one uses this for the first row of the two-line notation:

$$\sigma = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ \sigma(x_1) & \sigma(x_2) & \sigma(x_3) & \cdots & \sigma(x_n) \end{pmatrix}.$$

Under this assumption, one may omit the first row and write the permutation in *one-line notation* as



$$(\sigma(x_1) \sigma(x_2) \sigma(x_3) \cdots \sigma(x_n)),$$

that is, as an ordered arrangement of the elements of  $S$ .<sup>[16][17]</sup> Care must be taken to distinguish one-line notation from the cycle notation described below. In mathematics literature, a common usage is to omit parentheses for one-line notation, while using them for cycle notation. The one-line notation is also called the *word representation* of a permutation.<sup>[18]</sup> The example above would then be 2 5 4 3 1 since the natural order 1 2 3 4 5 would be assumed for the first row. (It is typical to use commas to separate these entries only if some have two or more digits.) This form is more compact, and is common in elementary combinatorics and computer science. It is especially useful in applications where the elements of  $S$  or the permutations are to be compared as larger or smaller.

## Cycle notation

Cycle notation describes the effect of repeatedly applying the permutation on the elements of the set. It expresses the permutation as a product of cycles; since distinct cycles are disjoint, this is referred to as "decomposition into disjoint cycles".

To write down the permutation  $\sigma$  in cycle notation, one proceeds as follows:

1. Write an opening bracket then select an arbitrary element  $x$  of  $S$  and write it down:  $(x$
2. Then trace the orbit of  $x$ ; that is, write down its values under successive applications of  $\sigma$ :  
 $(x \sigma(x) \sigma(\sigma(x)) \dots$
3. Repeat until the value returns to  $x$  and write down a closing parenthesis rather than  $x$ :  
 $(x \sigma(x) \sigma(\sigma(x)) \dots)$
4. Now continue with an element  $y$  of  $S$ , not yet

written down, and proceed in the same way:

$$(x \sigma(x) \sigma(\sigma(x)) \dots)(y \dots)$$

5. Repeat until all elements of  $S$  are written in cycles.

So the permutation 2 5 4 3 1 (in one-line notation) could be written as  $(125)(34)$  in cycle notation.

While permutations in general do not commute, disjoint cycles do; for example,

$$(125)(34) = (34)(125).$$

In addition, each cycle can be written in different ways, by choosing different starting points; for example,

$$(125)(34) = (512)(34) = (251)(43).$$

One may combine these equalities to write the disjoint cycles of a given permutation in many different ways.

1-cycles are often omitted from the cycle notation, provided that the context is clear; for any element  $x$  in  $S$  not appearing in any cycle, one implicitly assumes  $\sigma(x) = x$ .<sup>[19]</sup> The identity permutation, which consists only of 1-cycles, can be denoted by a single 1-cycle  $(x)$ , by the number 1,<sup>[b]</sup> or by  $id$ .<sup>[20][21]</sup>

A convenient feature of cycle notation is that cycle notation of the inverse of a permutation is given by reversing the order of the elements in the permutation's cycles. For example,

$$[(125)(34)]^{-1} = (521)(43).$$

## Canonical cycle notation

In some combinatorial contexts it is useful to fix a certain order for the elements in the cycles and of the (disjoint) cycles themselves. Miklós Bóna calls the following ordering choices the *canonical cycle notation*:

- in each cycle the *largest* element is listed first
- the cycles are sorted in *increasing* order of their first element

For example,  $(312)(54)(8)(976)$  is a permutation in canonical cycle notation.<sup>[22]</sup> The canonical cycle notation does not omit one-cycles.

Richard P. Stanley calls the same choice of representation the "standard representation" of a permutation.<sup>[23]</sup> and Martin Aigner uses the term "standard form" for the same notion.<sup>[18]</sup> Sergey Kitaev also uses the "standard form" terminology, but reverses both choices; that is, each cycle lists its least element first and the cycles are sorted in decreasing order of their least, that is, first elements.<sup>[24]</sup>

## Composition of permutations

There are two ways to denote the composition of two permutations.  $\sigma \cdot \pi$  is the function that maps any element  $x$  of the set to  $\sigma(\pi(x))$ . The rightmost permutation is applied to the argument first,<sup>[25]</sup> because of the way the function application is written.

Since function composition is associative, so is the composition operation on permutations:  $(\sigma\pi)\tau = \sigma(\pi\tau)$ . Therefore, products of more than two permutations are usually written without adding parentheses to express grouping; they are also usually written without a dot or other sign to indicate composition.

Some authors prefer the leftmost factor acting first,<sup>[26][27][28]</sup> but to that end permutations must be written to the *right* of their argument, often as an exponent, where  $\sigma$  acting on  $x$  is written  $x^\sigma$ ; then the

product is defined by  $x^{\sigma\pi} = (x^\sigma)^\pi$ . However this gives a *different* rule for multiplying permutations; this article uses the definition where the rightmost permutation is applied first.

## Other uses of the term *permutation*

---

The concept of a permutation as an ordered arrangement admits several generalizations that are not permutations, but have been called permutations in the literature.

### ***k*-permutations of *n***

A weaker meaning of the term *permutation*, sometimes used in elementary combinatorics texts, designates those ordered arrangements in which no element occurs more than once, but without the requirement of using all the elements from a given set. These are not permutations except in special cases, but are natural generalizations of the ordered arrangement concept. Indeed, this use often involves considering arrangements of a fixed length *k* of elements taken from a given set of size *n*, in other words, these ***k*-permutations of *n*** are the different ordered arrangements of a *k*-element subset of an *n*-set (sometimes called **variations** or **arrangements** in older literature<sup>[c]</sup>). These objects are also known as **partial permutations** or as **sequences without repetition**, terms that avoid confusion with the other, more common, meaning of "permutation". The number of such *k*-permutations of *n* is denoted variously by such symbols as  $P_k^n$ ,  ${}_n P_k$ ,  ${}^n P_k$ ,  $P_{n,k}$ , or  $P(n, k)$ , and its value is given by the product<sup>[29]</sup>

$$P(n, k) = n \cdot (n - 1) \cdot (n - 2) \cdots (n - k + 1),$$

*k* factors

which is 0 when  $k > n$ , and otherwise is equal to

$$\frac{n!}{(n-k)!}.$$

The product is well defined without the assumption that  $n$  is a non-negative integer, and is of importance outside combinatorics as well; it is known as the Pochhammer symbol  $(n)_k$  or as the  $k$ -th falling factorial power  $n^{\underline{k}}$  of  $n$ .

This usage of the term *permutation* is closely related to the term combination. A  $k$ -element combination of an  $n$ -set  $S$  is a  $k$  element subset of  $S$ , the elements of which are not ordered. By taking all the  $k$  element subsets of  $S$  and ordering each of them in all possible ways, we obtain all the  $k$ -permutations of  $S$ . The number of  $k$ -combinations of an  $n$ -set,  $C(n,k)$ , is therefore related to the number of  $k$ -permutations of  $n$  by:

$$C(n,k) = \frac{P(n,k)}{P(k,k)} = \frac{\frac{n!}{(n-k)!}}{\frac{k!}{0!}} = \frac{n!}{(n-k)!k!}.$$

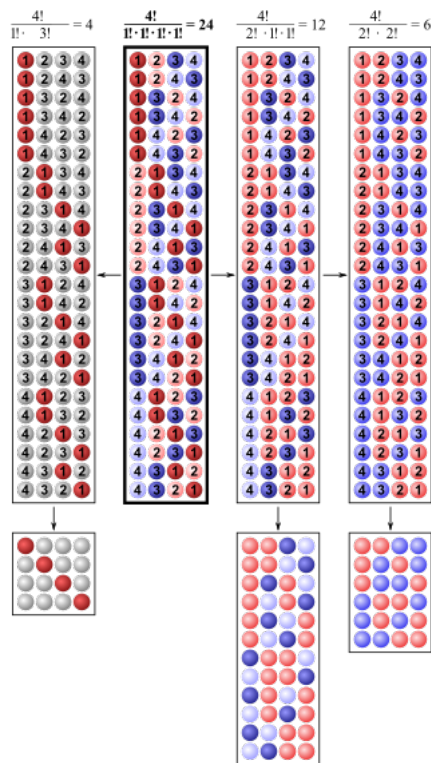
These numbers are also known as binomial coefficients and are denoted by  $\binom{n}{k}$ .

## Permutations with repetition

Ordered arrangements of  $k$  elements of a set  $S$ , where repetition is allowed, are called  $k$ -tuples. They have sometimes been referred to as **permutations with repetition**, although they are not permutations in general. They are also called words over the alphabet  $S$  in some contexts. If the set  $S$  has  $n$  elements, the number of  $k$ -tuples over  $S$  is  $n^k$ . There is no restriction on how often an element can appear in an  $k$ -tuple, but if restrictions are placed on how often an element can appear, this formula is no longer valid.

## Permutations of multisets

If  $M$  is a finite multiset, then a **multiset permutation** is an ordered arrangement of elements of  $M$  in which each element appears a number of times equal exactly to its multiplicity in  $M$ . An anagram of a word having some repeated letters is an example of a multiset permutation.<sup>[d]</sup> If the multiplicities of the elements of  $M$  (taken in some order) are  $m_1, m_2, \dots, m_l$  and their sum (that is, the size of  $M$ ) is  $n$ , then the number of multiset permutations of  $M$  is given by the multinomial coefficient,<sup>[30]</sup>



Permutations of multisets

$$\binom{n}{m_1, m_2, \dots, m_l} = \frac{n!}{m_1! m_2! \dots m_l!} = \frac{\left(\sum_{i=1}^l m_i\right)!}{\prod_{i=1}^l m_i!}.$$

For example, the number of distinct anagrams of the word MISSISSIPPI is:<sup>[31]</sup>

$$\frac{11!}{1! 4! 4! 2!} = 34650.$$

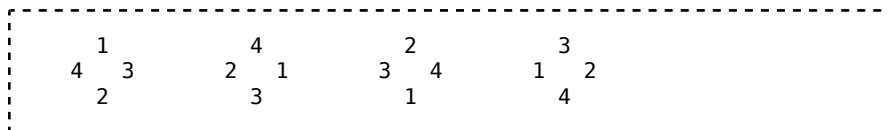
A  **$k$ -permutation** of a multiset  $M$  is a sequence of length  $k$  of

elements of  $M$  in which each element appears *a number of times less than or equal to* its multiplicity in  $M$  (an element's *repetition number*).

## Circular permutations

Permutations, when considered as arrangements, are sometimes referred to as *linearly ordered* arrangements. In these arrangements there is a first element, a second element, and so on. If, however, the objects are arranged in a circular manner this distinguished ordering no longer exists, that is, there is no "first element" in the arrangement, any element can be considered as the start of the arrangement. The arrangements of objects in a circular manner are called **circular permutations**.<sup>[32][e]</sup> These can be formally defined as equivalence classes of ordinary permutations of the objects, for the equivalence relation generated by moving the final element of the linear arrangement to its front.

Two circular permutations are equivalent if one can be rotated into the other (that is, cycled without changing the relative positions of the elements). The following four circular permutations on four letters are considered to be the same.



The circular arrangements are to be read counter-clockwise, so the following two are not equivalent since no rotation can bring one to the other.



The number of circular permutations of a set  $S$  with  $n$  elements is  $(n - 1)!$ .

## Properties

---

The number of permutations of  $n$  distinct objects is  $n!$ .

The number of  $n$ -permutations with  $k$  disjoint cycles is the signless Stirling number of the first kind, denoted by  $c(n, k)$ .<sup>[33]</sup>

## Permutation type

The cycles (including the fixed points) of a permutation  $\sigma$  of a set with  $n$  elements partition that set; so the lengths of these cycles form a partition of  $n$ , which is called the cycle type of  $\sigma$ . There is a "1" in the cycle type for every fixed point of  $\sigma$ , a "2" for every transposition, and so on. The cycle type of  $\beta = (1\,2\,5)(3\,4)(6\,8)(7)$  is  $(3, 2, 2, 1)$ .

This may also be written in a more compact form as  $[1^1 2^2 3^1]$ . More precisely, the general form is  $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$ , where  $\alpha_1, \dots, \alpha_n$  are the numbers of cycles of respective length. The number of permutations of a certain type is<sup>[34]</sup>

$$\frac{n!}{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n} \alpha_1! \alpha_2! \dots \alpha_n!}.$$

## Conjugating permutations

In general, composing permutations written in cycle notation follows no easily described pattern – the cycles of the composition can be different from those being composed. However the cycle structure is



preserved in the special case of conjugating a permutation  $\sigma$  by another permutation  $\pi$ , which means forming the product  $\pi\sigma\pi^{-1}$ . Here,  $\pi\sigma\pi^{-1}$  is the *conjugate* of  $\sigma$  by  $\pi$  and its cycle notation can be obtained by taking the cycle notation for  $\sigma$  and applying  $\pi$  to all the entries in it.<sup>[35]</sup> It follows that two permutations are conjugate exactly when they have the same type.

## Permutation order

The order of a permutation  $\sigma$  is the smallest positive integer  $m$  so that  $\sigma^m = \text{id}$ . It is the least common multiple of its cycles lengths. For example, the order of  $(1\ 3\ 2)(4\ 5)$  is  $2 \cdot 3 = 6$ .

## Parity of a permutation

Every permutation of a finite set can be expressed as the product of transpositions.<sup>[36]</sup> Although many such expressions for a given permutation may exist, either they all contain an even or an odd number of transpositions. Thus all permutations can be classified as even or odd depending on this number.

This result can be extended so as to assign a *sign*, written **sgn**  $\sigma$ , to each permutation. **sgn**  $\sigma = +1$  if  $\sigma$  is even and **sgn**  $\sigma = -1$  if  $\sigma$  is odd. Then for two permutations  $\sigma$  and  $\pi$

$$\mathbf{sgn}(\sigma\pi) = \mathbf{sgn}\ \sigma \cdot \mathbf{sgn}\ \pi.$$

It follows that  $\mathbf{sgn}(\sigma\sigma^{-1}) = +1$ .

## Matrix representation

A *permutation matrix* is an  $n \times n$  matrix that has exactly one entry 1 in each column and in each row, and all other entries are 0. There are

several different conventions that one can use to assign a permutation matrix to a permutation of  $\{1, 2, \dots, n\}$ . One natural approach is to associate to the permutation  $\sigma$  the matrix  $\mathbf{M}_\sigma$  whose  $(i, j)$  entry is 1 if  $i = \sigma(j)$  and is 0 otherwise. This convention has two attractive properties: first, the product of matrices and of permutations is in the same order, that is,  $\mathbf{M}_\sigma \mathbf{M}_\pi = \mathbf{M}_{\sigma \circ \pi}$  for all permutations  $\sigma$  and  $\pi$ . Second, if  $\mathbf{e}_i$  represents the standard  $n \times 1$  column vector (the vector with  $i$ th entry equal to 1 and all other entries equal to 0), then  $\mathbf{M}_\sigma \mathbf{e}_i = \mathbf{e}_{\sigma(i)}$ .

For example, with this convention, the matrix associated to the

permutation  $\sigma(1, 2, 3) = (2, 1, 3)$  is  $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$  and the matrix

associated to the permutation  $\pi(1, 2, 3) = (2, 3, 1)$  is  $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ .

Then the composition of permutations is  $(\sigma \circ \pi)(1, 2, 3) = \sigma(2, 3, 1) = (1, 3, 2)$ , and the corresponding matrix product is

$$\mathbf{M}_{(2,1,3)} \mathbf{M}_{(2,3,1)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

It is also common in the literature to find the inverse convention, where a permutation  $\sigma$  is associated to the matrix  $\mathbf{P}_\sigma = (\mathbf{M}_\sigma)^{-1} = (\mathbf{M}_\sigma)^T$  whose  $(i, j)$  entry is 1 if  $j = \sigma(i)$  and is 0 otherwise. In this convention, permutation matrices multiply in the opposite order from permutations, that is,  $\mathbf{P}_\sigma \mathbf{P}_\pi = \mathbf{P}_{\pi \circ \sigma}$  for all permutations  $\sigma$  and  $\pi$ . In this correspondence, permutation matrices act by permuting indices of standard  $1 \times n$  row vectors  $(\mathbf{e}_i)^T$ : one

has  $(\mathbf{e}_i)^T P_\sigma = (\mathbf{e}_{\sigma(i)})^T$ .

The Cayley table on the right shows these matrices for permutations of 3 elements.

## Foata's transition lemma

There is a relationship between the one-line and the canonical cycle notation. Consider the permutation  $(2)(31)$ , in canonical cycle notation, if we erase its cycle parentheses, we obtain the permutation  $(2,3,1)$  in one-line notation. Foata's transition lemma establishes the nature of this correspondence as a bijection on the set of  $n$ -permutations (to itself).<sup>[37]</sup> Richard P. Stanley calls this correspondence the *fundamental bijection*.<sup>[23]</sup>

Let  $f$  be the parentheses-erasing transformation. The inverse of  $q = f(p)$  is a bit less intuitive. Starting with the one-line notation  $q = q_1 q_2 \cdots q_n$ , the first cycle in canonical cycle notation must start with  $q_1$ . As long as the subsequent elements are smaller than  $q_1$ , we are in the same cycle. The second cycle starts at the smallest index  $j$  such that  $q_j > q_1$ . In other words,  $q_j$  is larger than everything else to its left, so it is called a *left-to-right maximum*. Every cycle in the canonical cycle notation starts with a left-to-right maximum.<sup>[37]</sup>

For example, in the one-line notation  $(3, 1, 2, 5, 4, 8, 9, 7, 6)$ , 5 is the first element larger than 3, so the first cycle must be  $(3\ 1\ 2)$ . Then 8 is the next element larger than 5, so the second cycle is  $(5\ 4)$ . Since

Composition of permutations corresponding to a multiplication of permutation matrices.

9 is larger than 8, **(8)** is a cycle by itself. Finally, 9 is larger than all the remaining elements to its right, so the last cycle is **(976)**.

The six permutations of **123** with their canonical cycle maps are:

**123(1)(2)(3), 132(1)(32), 213(21)(3), 231(312), 312(321), 321(231)**

As a first corollary, the number of  $n$ -permutations with exactly  $k$  left-to-right maxima is also equal to the signless Stirling number of the first kind,  **$c(n, k)$** . Furthermore, Foata's mapping takes an  $n$ -permutation with  $k$ -weak excedances to an  $n$ -permutations with  $k - 1$  ascents.<sup>[37]</sup> For example,  $(2)(31) = 321$  has two weak excedances (at index 1 and 2), whereas  $f(321) = 231$  has one ascent (at index 1; that is, from 2 to 3).

## Permutations of totally ordered sets

---

In some applications, the elements of the set being permuted will be compared with each other. This requires that the set  $S$  has a total order so that any two elements can be compared. The set  $\{1, 2, \dots, n\}$  is totally ordered by the usual " $\leq$ " relation and so it is the most frequently used set in these applications, but in general, any totally ordered set will do. In these applications, the ordered arrangement view of a permutation is needed to talk about the *positions* in a permutation.

There are a number of properties that are directly related to the total ordering of  $S$ .

## Ascents, descents, runs and excedances

An *ascent* of a permutation  $\sigma$  of  $n$  is any position  $i < n$  where the following value is bigger than the current one. That is, if

$\sigma = \sigma_1\sigma_2\dots\sigma_n$ , then  $i$  is an ascent if  $\sigma_i < \sigma_{i+1}$ .

For example, the permutation 3452167 has ascents (at positions) 1, 2, 5, and 6.

Similarly, a *descent* is a position  $i < n$  with  $\sigma_i > \sigma_{i+1}$ , so every  $i$  with  $1 \leq i < n$  either is an ascent or is a descent of  $\sigma$ .

An *ascending run* of a permutation is a nonempty increasing contiguous subsequence of the permutation that cannot be extended at either end; it corresponds to a maximal sequence of successive ascents (the latter may be empty: between two successive descents there is still an ascending run of length 1). By contrast an *increasing subsequence* of a permutation is not necessarily contiguous: it is an increasing sequence of elements obtained from the permutation by omitting the values at some positions. For example, the permutation 2453167 has the ascending runs 245, 3, and 167, while it has an increasing subsequence 2367.

If a permutation has  $k - 1$  descents, then it must be the union of  $k$  ascending runs.<sup>[38]</sup>

The number of permutations of  $n$  with  $k$  ascents is (by definition) the Eulerian number  $\left\langle n \atop k \right\rangle$ ; this is also the number of permutations of  $n$  with  $k$  descents. Some authors however define the Eulerian number  $\left\langle n \atop k \right\rangle$  as the number of permutations with  $k$  ascending runs, which corresponds to  $k - 1$  descents.<sup>[39]</sup>

An *excedance* of a permutation  $\sigma_1\sigma_2\dots\sigma_n$  is an index  $j$  such that  $\sigma_j > j$ . If the inequality is not strict (that is,  $\sigma_j \geq j$ ), then  $j$  is called a *weak excedance*. The number of  $n$ -permutations with  $k$  excedances coincides with the number of  $n$ -permutations with  $k$  descents.<sup>[40]</sup>

## Inversions

An *inversion* of a permutation  $\sigma$  is a pair  $(i, j)$  of positions where the entries of a permutation are in the opposite order:  $i < j$  and  $\sigma_i > \sigma_j$ .<sup>[42]</sup> So a descent is just an inversion at two adjacent positions. For example, the permutation  $\sigma = 23154$  has three inversions:  $(1, 3)$ ,  $(2, 3)$ , and  $(4, 5)$ , for the pairs of entries  $(2, 1)$ ,  $(3, 1)$ , and  $(5, 4)$ .

Sometimes an inversion is defined as the pair of values  $(\sigma_i, \sigma_j)$  whose order is reversed; this makes no difference for the *number* of inversions, and this pair (reversed) is also an inversion in the above sense for the inverse permutation  $\sigma^{-1}$ . The number of inversions is an important measure for the degree to which the entries of a permutation are out of order; it is the same for  $\sigma$  and for  $\sigma^{-1}$ . To bring a permutation with  $k$  inversions into order (that is, transform it into the identity permutation), by successively applying (right-multiplication by) adjacent transpositions, is always possible and requires a sequence of  $k$  such operations. Moreover, any reasonable choice for the adjacent transpositions will work: it suffices to choose at each step a transposition of  $i$  and  $i + 1$  where  $i$  is a descent of the permutation as modified so far (so that the transposition will remove this particular descent, although it might create other descents). This is so because applying such a transposition reduces the number of inversions by 1; as long as this number is not zero, the permutation is not the identity, so it has at least one descent. Bubble sort and insertion sort can be



In the 15 puzzle the goal is to get the squares in ascending order. Initial positions which have an odd number of inversions are impossible to solve.<sup>[41]</sup>

interpreted as particular instances of this procedure to put a sequence into order. Incidentally this procedure proves that any permutation  $\sigma$  can be written as a product of adjacent transpositions; for this one may simply reverse any sequence of such transpositions that transforms  $\sigma$  into the identity. In fact, by enumerating all sequences of adjacent transpositions that would transform  $\sigma$  into the identity, one obtains (after reversal) a *complete* list of all expressions of minimal length writing  $\sigma$  as a product of adjacent transpositions.

The number of permutations of  $n$  with  $k$  inversions is expressed by a Mahonian number,<sup>[43]</sup> it is the coefficient of  $X^k$  in the expansion of the product

$$\prod_{m=1}^n \sum_{i=0}^{m-1} X^i = 1 (1 + X) (1 + X + X^2) \cdots (1 + X + X^2 + \cdots$$

which is also known (with  $q$  substituted for  $X$ ) as the  $q$ -factorial  $[n]_q!$ . The expansion of the product appears in Necklace (combinatorics).

Let  $\sigma \in S_n, i, j \in \{1, 2, \dots, n\}$  such that  $i < j$  and  $\sigma(i) > \sigma(j)$ . In this case, say the weight of the inversion  $(i, j)$  is  $\sigma(i) - \sigma(j)$ . Kobayashi (2011) proved the enumeration formula

$$\sum_{i < j, \sigma(i) > \sigma(j)} (\sigma(i) - \sigma(j)) = |\{\tau \in S_n \mid \tau \leq \sigma, \tau \text{ is bigrassmanian}\}|$$

where  $\leq$  denotes Bruhat order in the symmetric groups. This graded partial order often appears in the context of Coxeter groups.

## Permutations in computing

---

## Numbering permutations

One way to represent permutations of  $n$  things is by an integer  $N$  with  $0 \leq N < n!$ , provided convenient methods are given to convert between the number and the representation of a permutation as an ordered arrangement (sequence). This gives the most compact representation of arbitrary permutations, and in computing is particularly attractive when  $n$  is small enough that  $N$  can be held in a machine word; for 32-bit words this means  $n \leq 12$ , and for 64-bit words this means  $n \leq 20$ . The conversion can be done via the intermediate form of a sequence of numbers  $d_n, d_{n-1}, \dots, d_2, d_1$ , where  $d_i$  is a non-negative integer less than  $i$  (one may omit  $d_1$ , as it is always 0, but its presence makes the subsequent conversion to a permutation easier to describe). The first step then is to simply express  $N$  in the *factorial number system*, which is just a particular mixed radix representation, where, for numbers less than  $n!$ , the bases (place values or multiplication factors) for successive digits are  $(n-1)!, (n-2)!, \dots, 2!, 1!$ . The second step interprets this sequence as a Lehmer code or (almost equivalently) as an inversion table.

In the **Lehmer code** for a permutation  $\sigma$ , the number  $d_n$  represents the choice made for the first term  $\sigma_1$ , the number  $d_{n-1}$  represents the choice made for the second term  $\sigma_2$  among the remaining  $n-1$  elements of the set, and so forth. More precisely, each  $d_{n+1-i}$  gives the number of *remaining* elements strictly less than the term  $\sigma_i$ . Since those remaining elements are bound to turn up as some later term  $\sigma_j$ , the digit  $d_{n+1-i}$  counts the *inversions*  $(i, j)$  involving  $i$  as smaller index (the number of values  $j$  for which  $i < j$  and  $\sigma_i > \sigma_j$ ). The **inversion table** for  $\sigma$  is quite similar, but here  $d_{n+1-k}$  counts the number of inversions  $(i, j)$  where  $k = \sigma_j$  occurs as the smaller of the two values appearing in inverted order.<sup>[44]</sup> Both encodings can be visualized by an  $n$  by  $n$  **Rothe diagram**<sup>[45]</sup> (named after Heinrich August Rothe) in which dots at  $(i, \sigma_i)$  mark the entries of the permutation, and a cross at  $(i, \sigma_j)$  marks the inversion  $(i, j)$ ; by the definition of inversions a cross appears in any square that comes both before the dot  $(j, \sigma_j)$  in its



Rothe diagram for  $\sigma = (6, 3, 8, 1, 4, 9, 7, 2, 5)$ 

$i$	$\sigma_i$	1	2	3	4	5	6	7	8	9	Lehmer code
1		×	×	×	×	×	•				$d_9 = 5$
2		×	×	•							$d_8 = 2$
3		×	×		×	×		×	•		$d_7 = 5$
4		•									$d_6 = 0$
5			×		•						$d_5 = 1$
6			×			×		×		•	$d_4 = 3$
7			×			×		•			$d_3 = 2$
8			•								$d_2 = 0$
9						•					$d_1 = 0$
<b>Inversion table</b>		3	6	1	2	4	0	2	0	0	

column, and before the dot  $(i, \sigma_i)$  in its row. The Lehmer code lists the numbers of crosses in successive rows, while the inversion table lists the numbers of crosses in successive columns; it is just the Lehmer code for the inverse permutation, and vice versa.

To effectively convert a Lehmer code  $d_n, d_{n-1}, \dots, d_2, d_1$  into a permutation of an ordered set  $S$ , one can start with a list of the elements of  $S$  in increasing order, and for  $i$  increasing from 1 to  $n$  set  $\sigma_i$  to the element in the list that is preceded by  $d_{n+1-i}$  other ones, and remove that element from the list. To convert an inversion table  $d_n, d_{n-1}, \dots, d_2, d_1$  into the corresponding permutation, one can traverse the numbers from  $d_1$  to  $d_n$  while inserting the elements of  $S$  from largest to smallest into an initially empty sequence; at the step using the number  $d$  from the inversion table, the element from  $S$  inserted into the sequence at the point where it is preceded by  $d$  elements

already present. Alternatively one could process the numbers from the inversion table and the elements of  $S$  both in the opposite order, starting with a row of  $n$  empty slots, and at each step place the element from  $S$  into the empty slot that is preceded by  $d$  other empty slots.

Converting successive natural numbers to the factorial number system produces those sequences in lexicographic order (as is the case with any mixed radix number system), and further converting them to permutations preserves the lexicographic ordering, provided the Lehmer code interpretation is used (using inversion tables, one gets a different ordering, where one starts by comparing permutations by the *place* of their entries 1 rather than by the value of their first entries). The sum of the numbers in the factorial number system representation gives the number of inversions of the permutation, and the parity of that sum gives the signature of the permutation. Moreover, the positions of the zeroes in the inversion table give the values of left-to-right maxima of the permutation (in the example 6, 8, 9) while the positions of the zeroes in the Lehmer code are the positions of the right-to-left minima (in the example positions the 4, 8, 9 of the values 1, 2, 5); this allows computing the distribution of such extrema among all permutations. A permutation with Lehmer code  $d_n, d_{n-1}, \dots, d_2, d_1$  has an ascent  $n - i$  if and only if  $d_i \geq d_{i+1}$ .

## Algorithms to generate permutations

In computing it may be required to generate permutations of a given sequence of values. The methods best adapted to do this depend on whether one wants some randomly chosen permutations, or all permutations, and in the latter case if a specific ordering is required. Another question is whether possible equality among entries in the given sequence is to be taken into account; if so, one should only generate distinct multiset permutations of the sequence.

An obvious way to generate permutations of  $n$  is to generate values

for the Lehmer code (possibly using the factorial number system representation of integers up to  $n!$ ), and convert those into the corresponding permutations. However, the latter step, while straightforward, is hard to implement efficiently, because it requires  $n$  operations each of selection from a sequence and deletion from it, at an arbitrary position; of the obvious representations of the sequence as an array or a linked list, both require (for different reasons) about  $n^2/4$  operations to perform the conversion. With  $n$  likely to be rather small (especially if generation of all permutations is needed) that is not too much of a problem, but it turns out that both for random and for systematic generation there are simple alternatives that do considerably better. For this reason it does not seem useful, although certainly possible, to employ a special data structure that would allow performing the conversion from Lehmer code to permutation in  $O(n \log n)$  time.

## Random generation of permutations

For generating random permutations of a given sequence of  $n$  values, it makes no difference whether one applies a randomly selected permutation of  $n$  to the sequence, or chooses a random element from the set of distinct (multiset) permutations of the sequence. This is because, even though in case of repeated values there can be many distinct permutations of  $n$  that result in the same permuted sequence, the number of such permutations is the same for each possible result. Unlike for systematic generation, which becomes unfeasible for large  $n$  due to the growth of the number  $n!$ , there is no reason to assume that  $n$  will be small for random generation.

The basic idea to generate a random permutation is to generate at random one of the  $n!$  sequences of integers  $d_1, d_2, \dots, d_n$  satisfying  $0 \leq d_i < i$  (since  $d_1$  is always zero it may be omitted) and to convert it to a permutation through a bijjective correspondence. For the latter correspondence one could interpret the (reverse) sequence as a Lehmer code, and this gives a generation method first published in

1938 by Ronald Fisher and Frank Yates.<sup>[46]</sup> While at the time computer implementation was not an issue, this method suffers from the difficulty sketched above to convert from Lehmer code to permutation efficiently. This can be remedied by using a different bijective correspondence: after using  $d_i$  to select an element among  $i$  remaining elements of the sequence (for decreasing values of  $i$ ), rather than removing the element and compacting the sequence by shifting down further elements one place, one swaps the element with the final remaining element. Thus the elements remaining for selection form a consecutive range at each point in time, even though they may not occur in the same order as they did in the original sequence. The mapping from sequence of integers to permutations is somewhat complicated, but it can be seen to produce each permutation in exactly one way, by an immediate induction. When the selected element happens to be the final remaining element, the swap operation can be omitted. This does not occur sufficiently often to warrant testing for the condition, but the final element must be included among the candidates of the selection, to guarantee that all permutations can be generated.

The resulting algorithm for generating a random permutation of  $a[0], a[1], \dots, a[n - 1]$  can be described as follows in pseudocode:

```

for  $i$  from  $n$  downto 2 do
   $d_i \leftarrow$  random element of  $\{ 0, \dots, i - 1 \}$ 
  swap  $a[d_i]$  and  $a[i - 1]$ 

```

This can be combined with the initialization of the array  $a[i] = i$  as follows

```

for  $i$  from 0 to  $n-1$  do
   $d_{i+1} \leftarrow$  random element of  $\{ 0, \dots, i \}$ 
   $a[i] \leftarrow a[d_{i+1}]$ 
   $a[d_{i+1}] \leftarrow i$ 

```

If  $d_{i+1} = i$ , the first assignment will copy an uninitialized value, but the second will overwrite it with the correct value  $i$ .

However, Fisher-Yates is not the fastest algorithm for generating a permutation, because Fisher-Yates is essentially a sequential algorithm and "divide and conquer" procedures can achieve the same result in parallel.<sup>[47]</sup>

## Generation in lexicographic order

There are many ways to systematically generate all permutations of a given sequence.<sup>[48]</sup> One classic, simple, and flexible algorithm is based upon finding the next permutation in lexicographic ordering, if it exists. It can handle repeated values, for which case it generates each distinct multiset permutation once. Even for ordinary permutations it is significantly more efficient than generating values for the Lehmer code in lexicographic order (possibly using the factorial number system) and converting those to permutations. It begins by sorting the sequence in (weakly) increasing order (which gives its lexicographically minimal permutation), and then repeats advancing to the next permutation as long as one is found. The method goes back to Narayana Pandita in 14th century India, and has been rediscovered frequently.<sup>[49]</sup>

The following algorithm generates the next permutation lexicographically after a given permutation. It changes the given permutation in-place.

1. Find the largest index  $k$  such that  $a[k] < a[k + 1]$ . If no such index exists, the permutation is the last permutation.
2. Find the largest index  $l$  greater than  $k$  such that  $a[k] < a[l]$ .
3. Swap the value of  $a[k]$  with that of  $a[l]$ .
4. Reverse the sequence from  $a[k + 1]$  up to and

including the final element  $a[n]$ .

For example, given the sequence  $[1, 2, 3, 4]$  (which is in increasing order), and given that the index is zero-based, the steps are as follows:

1. Index  $k = 2$ , because 3 is placed at an index that satisfies condition of being the largest index that is still less than  $a[k + 1]$  which is 4.
2. Index  $l = 3$ , because 4 is the only value in the sequence that is greater than 3 in order to satisfy the condition  $a[k] < a[l]$ .
3. The values of  $a[2]$  and  $a[3]$  are swapped to form the new sequence  $[1, 2, 4, 3]$ .
4. The sequence after  $k$ -index  $a[2]$  to the final element is reversed. Because only one value lies after this index (the 3), the sequence remains unchanged in this instance. Thus the lexicographic successor of the initial state is permuted:  $[1, 2, 4, 3]$ .

Following this algorithm, the next lexicographic permutation will be  $[1, 3, 2, 4]$ , and the 24th permutation will be  $[4, 3, 2, 1]$  at which point  $a[k] < a[k + 1]$  does not exist, indicating that this is the last permutation.

This method uses about 3 comparisons and 1.5 swaps per permutation, amortized over the whole sequence, not counting the initial sort.<sup>[50]</sup>

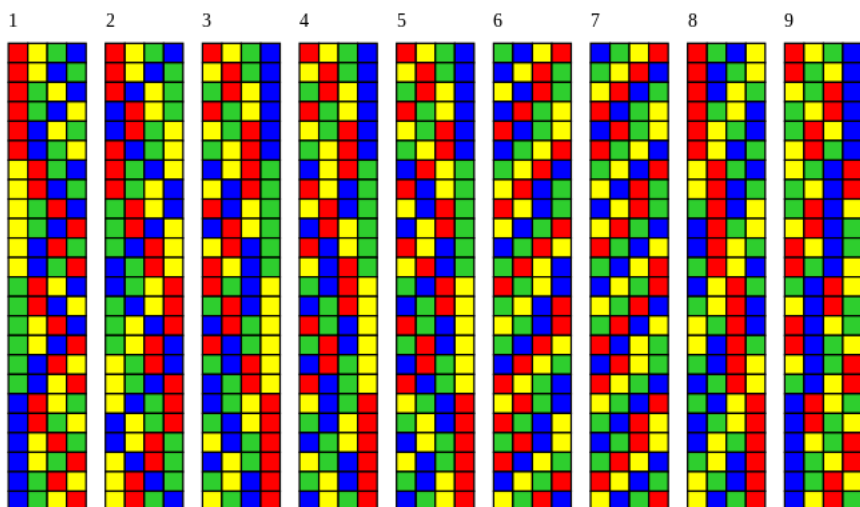
## Generation with minimal changes

An alternative to the above algorithm, the Steinhaus–Johnson–Trotter algorithm, generates an ordering on all the permutations of a given sequence with the property that any two consecutive permutations in

its output differ by swapping two adjacent values. This ordering on the permutations was known to 17th-century English bell ringers, among whom it was known as "plain changes". One advantage of this method is that the small amount of change from one permutation to the next allows the method to be implemented in constant time per permutation. The same can also easily generate the subset of even permutations, again in constant time per permutation, by skipping every other output permutation.<sup>[49]</sup>

An alternative to Steinhaus–Johnson–Trotter is Heap's algorithm,<sup>[51]</sup> said by Robert Sedgewick in 1977 to be the fastest algorithm of generating permutations in applications.<sup>[48]</sup>

The following figure shows the output of all three aforementioned algorithms for generating all permutations of length  $n = 4$ , and of six additional algorithms described in the literature.



Ordering of all permutations of length  $n = 4$  generated by different algorithms. The permutations are color-coded, where   1,   2,   3,   4.<sup>[52]</sup>

1. Lexicographic ordering;

2. Steinhaus–Johnson–Trotter algorithm;
3. Heap's algorithm;
4. Ehrlich's star-transposition algorithm:<sup>[49]</sup> in each step, the first entry of the permutation is exchanged with a later entry;
5. Zaks' prefix reversal algorithm:<sup>[53]</sup> in each step, a prefix of the current permutation is reversed to obtain the next permutation;
6. Sawada-Williams' algorithm:<sup>[54]</sup> each permutation differs from the previous one either by a cyclic left-shift by one position, or an exchange of the first two entries;
7. Corbett's algorithm:<sup>[55]</sup> each permutation differs from the previous one by a cyclic left-shift of some prefix by one position;
8. Single-track ordering:<sup>[56]</sup> each column is a cyclic shift of the other columns;
9. Single-track Gray code:<sup>[56]</sup> each column is a cyclic shift of the other columns, plus any two consecutive permutations differ only in one or two transpositions.

## Meandric permutations

Meandric systems give rise to *meandric permutations*, a special subset of *alternate permutations*. An alternate permutation of the set  $\{1, 2, \dots, 2n\}$  is a cyclic permutation (with no fixed points) such that the digits in the cyclic notation form alternate between odd and even integers. Meandric permutations are useful in the analysis of RNA secondary structure. Not all alternate permutations are meandric. A modification of Heap's algorithm has been used to generate all alternate permutations of order  $n$  (that is, of length  $2n$ ) without generating all  $(2n)!$  permutations.<sup>[57]</sup> Generation of these alternate



permutations is needed before they are analyzed to determine if they are meandric or not.

The algorithm is recursive. The following table exhibits a step in the procedure. In the previous step, all alternate permutations of length 5 have been generated. Three copies of each of these have a "6" added to the right end, and then a different transposition involving this last entry and a previous entry in an even position is applied (including the identity; that is, no transposition).

Previous sets	Transposition of digits	Alternate permutations
1-2-3-4-5-6		1-2-3-4-5-6
	4, 6	1-2-3-6-5-4
	2, 6	1-6-3-4-5-2
1-2-5-4-3-6		1-2-5-4-3-6
	4, 6	1-2-5-6-3-4
	2, 6	1-6-5-4-3-2
1-4-3-2-5-6		1-4-3-2-5-6
	2, 6	1-4-3-6-5-2
	4, 6	1-6-3-2-5-4
1-4-5-2-3-6		1-4-5-2-3-6
	2, 6	1-4-5-6-3-2
	4, 6	1-6-5-2-3-4

## Applications

Permutations are used in the interleaver component of the error detection and correction algorithms, such as turbo codes, for example 3GPP Long Term Evolution mobile telecommunication standard uses

these ideas (see 3GPP technical specification 36.212<sup>[58]</sup>). Such applications raise the question of fast generation of permutations satisfying certain desirable properties. One of the methods is based on the permutation polynomials. Also as a base for optimal hashing in Unique Permutation Hashing.<sup>[59]</sup>

## See also

---

- Alternating permutation
- Convolution
- Cyclic order
- Even and odd permutations
- Josephus permutation
- Levi-Civita symbol
- List of permutation topics
- Major index
- Permutation category
- Permutation group
- Permutation pattern
- Permutation representation (symmetric group)
- Probability
- Rencontres numbers
- Sorting network
- Substitution cipher
- Superpattern
- Superpermutation
- Twelvefold way
- Weak order of permutations

## Notes

---

- a. The order is often implicitly understood. A set of integers is naturally written from smallest to largest; a set of letters is written in lexicographic order. For other sets, a natural order needs to be specified explicitly.
- b. 1 is frequently used to represent the identity element in a non-commutative group
- c. More precisely, *variations without repetition*. The term is still common in other languages and appears in modern English most often in translation.
- d. The natural order in this example is the order of the letters in the original word.
- e. In older texts *circular permutation* was sometimes used as a synonym for cyclic permutation, but this is no longer done. See Carmichael (1956, p. 7)

## References

---

1. Webster (1969)
2. McCoy (1968, p. 152)
3. Nering (1970, p. 86)
4. Broemeling, Lyle D. (1 November 2011). "An Account of Early Statistical Inference in Arab Cryptology". *The American Statistician*. **65** (4): 255–257. doi:10.1198/tas.2011.10191 (<https://doi.org/10.1198%2Ftas.2011.10191>). S2CID 123537702 (<https://api.semanticscholar.org/CorpusID:123537702>).
5. Biggs, N. L. (1979). "The Roots of Combinatorics" (<https://doi.org/10.1016%2F0315-0860%2879%2990074-0>). *Historia Math.* **6** (2): 109–136. doi:10.1016/0315-0860(79)90074-0 (<https://doi.org/10.1016%2F0315-0860%2879%2990074-0>).

6. Stedman 1677, p. 4.
7. Stedman 1677, p. 5.
8. Stedman 1677, pp. 6–7.
9. Stedman 1677, p. 8.
10. Stedman 1677, pp. 13–18.
11. "Combinations and Permutations" (<https://www.mathsisfun.com/combinatorics/combinations-permutations.html>). *www.mathsisfun.com*. Retrieved 2020-09-10.
12. Weisstein, Eric W. "Permutation" (<https://mathworld.wolfram.com/Permutation.html>). *mathworld.wolfram.com*. Retrieved 2020-09-10.
13. Scheinerman, Edward A. (March 5, 2012). "Chapter 5: Functions" (<https://books.google.com/books?id=DZBHGD2sEYwC&pg=PA188>). *Mathematics: A Discrete Introduction* (3rd ed.). Cengage Learning. p. 188. ISBN 978-0840049421. Archived (<https://web.archive.org/web/20200205212843/https://books.google.com/books?id=DZBHGD2sEYwC&pg=PA188>) from the original on February 5, 2020. Retrieved February 5, 2020. "It is customary to use lowercase Greek letters (especially  $\pi$ ,  $\sigma$ , and  $\tau$ ) to stand for permutations."
14. Cameron 1994, p. 29, footnote 3.
15. Wussing, Hans (2007), *The Genesis of the Abstract Group Concept: A Contribution to the History of the Origin of Abstract Group Theory* (<https://books.google.com/books?id=Xp3JymnfAq4C&pg=PA94>), Courier Dover Publications, p. 94, ISBN 9780486458687, "Cauchy used his permutation notation—in which the arrangements are written one below the other and both are enclosed in parentheses—for the first time in 1815."
16. Bogart 1990, p. 17

17. [Gerstein 1987](#), p. 217
18. Aigner, Martin (2007). *A Course in Enumeration* ([https://archive.org/details/courseenumeratio00aign\\_007](https://archive.org/details/courseenumeratio00aign_007)). Springer GTM 238. pp. 24 ([https://archive.org/details/courseenumeratio00aign\\_007/page/n32](https://archive.org/details/courseenumeratio00aign_007/page/n32))-25. ISBN 978-3-540-39035-0.
19. [Hall 1959](#), p. 54
20. [Rotman 2002](#), p. 41
21. [Bogart 1990](#), p. 487
22. [Bona 2012](#), p.87 [Note that the book has a typo/error here, as it gives (45) instead of (54).]
23. Stanley, Richard P. (2012). *Enumerative Combinatorics: Volume I, Second Edition*. Cambridge University Press. p. 23. ISBN 978-1-107-01542-5.
24. Kitaev, Sergey (2011). *Patterns in Permutations and Words*. Springer Science & Business Media. p. 119. ISBN 978-3-642-17333-2.
25. Biggs, Norman L.; White, A. T. (1979). *Permutation groups and combinatorial structures*. Cambridge University Press. ISBN 978-0-521-22287-7.
26. Dixon, John D.; Mortimer, Brian (1996). *Permutation Groups* (<https://archive.org/details/permutationgroup0000dixo>). Springer. ISBN 978-0-387-94599-6.
27. Cameron, Peter J. (1999). *Permutation groups* (<https://archive.org/details/permutationgroup0000came>). Cambridge University Press. ISBN 978-0-521-65302-2.
28. Jerrum, M. (1986). "A compact representation of permutation groups". *J. Algorithms*. **7** (1): 60–78. doi:10.1016/0196-6774(86)90038-6 (<https://doi.org/10.1016%2F0196-6774%2886%2990038-6>). S2CID 18896625 (<https://api.semanticscholar.org/CorpusID:18896625>).

29. Charalambides, Ch A. (2002). *Enumerative Combinatorics* (<https://books.google.com/books?id=PDMGA-v5G54C&pg=PA42>). CRC Press. p. 42. ISBN 978-1-58488-290-9.
30. Brualdi 2010, p. 46, Theorem 2.4.2
31. Brualdi 2010, p. 47
32. Brualdi 2010, p. 39
33. Bona 2012, pp. 97–103.
34. Sagan, Bruce (2001), *The Symmetric Group* (2 ed.), Springer, p. 3
35. Humphreys 1996, p. 84.
36. Hall 1959, p. 60
37. Bona 2012, pp. 109–110.
38. Bóna 2004, p. 4f.
39. Bona 2012, pp. 4–5.
40. Bona 2012, p. 25.
41. Slocum, Jerry; Weisstein, Eric W. (1999). "15 – puzzle" (<http://mathworld.wolfram.com/15Puzzle.html>). *MathWorld*. Wolfram Research, Inc. Retrieved October 4, 2014.
42. Bóna 2004, p. 43.
43. Bóna 2004, pp. 43ff.
44. Knuth 1973, p. 12.
45. H. A. Rothe, *Sammlung combinatorisch-analytischer Abhandlungen* **2** (Leipzig, 1800), 263–305. Cited in Knuth 1973, p. 14
46. Fisher, R.A.; Yates, F. (1948) [1938]. *Statistical tables for biological, agricultural and medical research* (3rd ed.). London: Oliver & Boyd. pp. 26–27. OCLC 14222135 (<https://www.worldcat.org/oclc/14222135>).

47. Bacher, A.; Bodini, O.; Hwang, H.K.; Tsai, T.H. (2017). "Generating Random Permutations by Coin Tossing: Classical Algorithms, New Analysis, and Modern Implementation" (ACM Trans. Algorithms 13(2): 24:1–24:43 ed.). pp. 24–43.
48. Sedgewick, R (1977). "Permutation generation methods" (<http://www.math.uiowa.edu/~goodman/22m150.dir/2007/Permutation%20Generation%20Methods.pdf>) (PDF). *Computing Surveys*. **9** (2): 137–164. doi:10.1145/356689.356692 (<https://doi.org/10.1145%2F356689.356692>). S2CID 12139332 (<https://api.semanticscholar.org/CorpusID:12139332>).
49. Knuth 2005, pp. 1–26.
50. "std::next\_permutation" ([http://en.cppreference.com/w/cpp/algorithm/next\\_permutation](http://en.cppreference.com/w/cpp/algorithm/next_permutation)). *cppreference.com*. 4 December 2017. Retrieved 31 March 2018.
51. Heap, B. R. (1963). "Permutations by Interchanges" (<https://doi.org/10.1093/comjnl/6.3.293>). *The Computer Journal*. **6** (3): 293–298. doi:10.1093/comjnl/6.3.293 (<https://doi.org/10.1093%2Fcomjnl%2F6.3.293>).
52. Mütze, Torsten; Sawada, Joe; Williams, Aaron. "Generate permutations" (<http://combos.org/perm>). *Combinatorial Object Server*. Retrieved May 29, 2019.
53. Zaks, S. (1984). "A new algorithm for generation of permutations". *BIT Numerical Mathematics*. **24** (2): 196–204. doi:10.1007/BF01937486 (<https://doi.org/10.1007%2FBF01937486>). S2CID 30234652 (<https://api.semanticscholar.org/CorpusID:30234652>).

54. Sawada, Joe; Williams, Aaron (2018). "A Hamilton path for the sigma-tau problem". *Proceedings of the 29th Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2018*. New Orleans, Louisiana: Society for Industrial and Applied Mathematics (SIAM). pp. 568–575.  
[doi:10.1137/1.9781611975031.37](https://doi.org/10.1137/1.9781611975031.37) (<https://doi.org/10.1137/1.9781611975031.37>).
55. Corbett, P. F. (1992). "Rotator graphs: An efficient topology for point-to-point multiprocessor networks". *IEEE Transactions on Parallel and Distributed Systems*. **3** (5): 622–626.  
[doi:10.1109/71.159045](https://doi.org/10.1109/71.159045) (<https://doi.org/10.1109/71.159045>).
56. Arndt, Jörg (2011). *Matters Computational. Ideas, Algorithms, Source Code*. Springer.  
[doi:10.1007/978-3-642-14764-7](https://doi.org/10.1007/978-3-642-14764-7) (<https://doi.org/10.1007/978-3-642-14764-7>).  
ISBN 978-3-642-14763-0.
57. Alexiou, A.; Psiha, M.; Vlamos, P. (2011). "Combinatorial permutation based algorithm for representation of closed RNA secondary structures" (<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3174042>). *Bioinformatics*. **7** (2): 91–95.  
[doi:10.6026/97320630007091](https://doi.org/10.6026/97320630007091) (<https://doi.org/10.6026/97320630007091>). PMC 3174042 (<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3174042>). PMID 21938211 (<https://pubmed.ncbi.nlm.nih.gov/21938211>).
58. "3GPP TS 36.212" (<http://www.3gpp.org/ftp/Specs/html-info/36212.htm>).
59. Dolev, Shlomi; Lahiani, Limor; Haviv, Yinnon (2013). "Unique permutation hashing" (<https://doi.org/10.1016/j.tcs.2012.12.047>). *Theoretical Computer Science*. **475**: 59–65. [doi:10.1016/j.tcs.2012.12.047](https://doi.org/10.1016/j.tcs.2012.12.047) (<https://doi.org/10.1016/j.tcs.2012.12.047>).



## Bibliography

---

- Bogart, Kenneth P. (1990), *Introductory Combinatorics* (2nd ed.), Harcourt Brace Jovanovich, ISBN [978-0-15-541576-8](#)
- Bóna, Miklós (2004), *Combinatorics of Permutations*, Chapman Hall-CRC, ISBN [978-1-58488-434-7](#)
- Bona, Miklos (2012), *Combinatorics of Permutations* (2nd ed.), CRC Press, ISBN [978-1-4398-5051-0](#)
- Brualdi, Richard A. (2010), *Introductory Combinatorics* (5th ed.), Prentice-Hall, ISBN [978-0-13-602040-0](#)
- Cameron, Peter J. (1994), *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, ISBN [978-0-521-45761-3](#)
- Carmichael, Robert D. (1956) [1937], *Introduction to the theory of Groups of Finite Order*, Dover, ISBN [978-0-486-60300-1](#)
- Fraleigh, John B. (1976), *A First Course In Abstract Algebra* (2nd ed.), Reading: Addison-Wesley, ISBN [0-201-01984-1](#)
- Gerstein, Larry J. (1987), *Discrete Mathematics and Algebraic Structures* (<https://archive.org/details/diskretemathemat0000gers>), W.H. Freeman and Co., ISBN [978-0-7167-1804-8](#)
- Hall, Marshall, Jr. (1959), *The Theory of Groups*, MacMillan
- Humphreys, J. F. (1996), *A course in group theory* ([https://books.google.com/books?id=2p3\\_ngEACAAJ&pg=PA84&dq=%22conjugate+permutations+have+the+same+cycle+type%22](https://books.google.com/books?id=2p3_ngEACAAJ&pg=PA84&dq=%22conjugate+permutations+have+the+same+cycle+type%22)), Oxford University Press, ISBN [978-0-19-853459-4](#)

- Knuth, Donald (1973), *Sorting and Searching*, The Art of Computer Programming, vol. 3 This book mentions the Lehmer code (without using that name) as a variant  $C_1, \dots, C_n$  of inversion tables in exercise 5.1.1–7 (p. 19), together with two other variants.
- Knuth, Donald (2005), *Generating All Tuples and Permutations*, The Art of Computer Programming, vol. 4, Addison–Wesley, ISBN 978-0-201-85393-3 Fascicle 2, first printing.
- McCoy, Neal H. (1968), *Introduction To Modern Algebra, Revised Edition*, Boston: Allyn and Bacon, LCCN 68015225 (<https://lccn.loc.gov/68015225>)
- Nering, Evar D. (1970), *Linear Algebra and Matrix Theory* (2nd ed.), New York: Wiley, LCCN 76091646 (<https://lccn.loc.gov/76091646>)
- Rotman, Joseph J. (2002), *Advanced Modern Algebra*, Prentice-Hall, ISBN 978-0-13-087868-7
- Stedman, Fabian (1677), *Campanalogia*, London The publisher is given as "W.S." who may have been William Smith, possibly acting as agent for the Society of College Youths, to which society the "Dedicatory" is addressed. *In quotations the original long "S" has been replaced by a modern short "s".*
- *Webster's Seventh New Collegiate Dictionary*, Springfield: G. & C. Merriam Company, 1969

## Further reading

---

- Biggs, Norman L. (2002), *Discrete Mathematics* (2nd ed.), Oxford University Press, ISBN 978-0-19-850717-8
- Foata, Dominique; Schützenberger, Marcel-Paul

(1970), *Théorie Géométrique des Polynômes Eulériens* (<http://irma.math.unistra.fr/~foata/paper/pub14.html>), Lecture Notes in Mathematics, vol. 138, Berlin, Heidelberg: Springer-Verlag, ISBN 978-3-540-04927-2. The link is to a freely available retyped (LaTeX'ed) and revised version of the text originally published by Springer-Verlag.

- Knuth, Donald (1998), *Sorting and Searching*, The Art of Computer Programming, vol. 3 (Second ed.), Addison-Wesley, ISBN 978-0-201-89685-5. Section 5.1: Combinatorial Properties of Permutations, pp. 11–72.
- Sedgewick, Robert (1977). "Permutation generation methods". *ACM Computing Surveys*. **9** (2): 137–164. doi:10.1145/356689.356692 (<https://doi.org/10.1145%2F356689.356692>). S2CID 12139332 (<https://api.semanticscholar.org/CorpusID:12139332>).
- Masato, Kobayashi (2011). "Enumeration of bigrassmannian permutations below a permutation in Bruhat order". *Order*. **1**: 131–137.

## External links

---

- "Permutation" (<https://www.encyclopediaofmath.org/index.php?title=Permutation>), *Encyclopedia of Mathematics*, EMS Press, 2001 [1994]
- 

Retrieved from "<https://en.wikipedia.org/w/index.php?title=Permutation&oldid=1090481467>"

---

**This page was last edited on 29 May 2022, at 19:06 (UTC).**

Text is available under the Creative Commons Attribution-ShareAlike License 3.0; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.