The Forth Scientific Conference of the College of Science University of Kerbala 2016

Journal of University of Kerbala

Software package to implement operations on the permutation

Ahmed Saleem Abbas
ahmed.saleam@uokerbala.edu.iq
Univ. of Karbala / college of science

Amjad Hamead Alhusiny
amjad.alhusini@uokerbala.edu.iq
Univ. of Karbala / college of science

Ashwak Alabaichi
ashwakalabaichi2007@yahoo.com
Univ. of Karbala / college of science

Abstract

Informally, a permutation of the elements is rearrangement of those elements into a specific order. In mathematics, the notion of the permutation is used with a little different meaning, all related to the act of rearranging in an ordered fashion of those elements or values. Many operations can be performed on the elements of the permutation such as composition which is used to combine two permutations to produce a third one. In this paper software package is implemented to generate all possible of the permutations on a set of n elements, where the number of these possible permutations are the factorial of n. Then composition on the permuted set is conducted. As well as deducting some properties of the composition such as inverse of each element and power the element that can be used to produce the identity element. Where power element is the element has been multiplied by itself m times, where m is the power. Java language (NetBeans IDE 7.2) is used to implement this package.

Keywords: Permutation, Composition, Power and the Inverse.

الخلاصة

تعرف التباديل على العناصر بشكل عام على أنها إعادة ترتيب محدد لهذه العناصر. وتستخدم فكرة التباديل في الرياضيات بمعنى مختلفاً قليلاً نسبة إلى طريقة إعادة الترتيب لتلك العناصر. ويمكن تعريف أنواع كثيرة من العمليات الثنائية على التباديل كعناصر ومنها التركيب حيث يربط بين تبديلين لينتج تبديل آخر. في هذا البحث قمنا بتنفيذ حزمة برمجية لتوليد كل التباديل المحتملة على مجموعة تتألف من n من العناصر، والتي يكون عددها مساوياً إلى مضروب n. وقمنا بالتحقق من بعض خواص التركيب بعد تنفيذه على التباديل كالمعكوس لكل عنصر والقوة المرفوعة لعنصر والتي ينتج عنها العنصر المحايد، إذ يتم ضرب العنصر في نفسه m من المرات، و m هي القوة. وقد قمنا باستخدام لغة جافا (NetBeans IDE 7.2) لتنفيذ هذه الحزمة.

1-Introduction

Linear ordering on a fixed set of the objects is known as Permutations. These objects are permuting without consider what kind of them. The number of the permutations on the n elements is the factorial of n [1], where the permutation is a function which gives different order of the elements position.

The permutation can be applied on a matrix, where the result from this operation can be used in several applications as security, image processing, games, data compression and lottery.

One of the most important operations on the permutation is the composition, where the Composition is used to combine two permutations to produce another one within the same set.

Some of The benefits of composition are to decrease the number of mathematical steps, to enable the process to go back to the specified step by using the inverse element, and to increase the probabilities of the permutations.

There are seven sections in this paper. While section 1 introduces the topic, then section 2 present the related works, next, section 3 presents the permutations with their types and how can be presented, section 4, provides a brief of the composition on the permutation with some of the composition benefits, section 5 presents some properties of the composition such as the inverse, identity, power element, after this section 6 provides a description of the software with some examples and the results, and finally, section 7 includes suggestion for the future works.

2. Related Works

Zakablukov (2015) discussed various applications of permutation group theory in the synthesis of reversible logic circuits, consisting of Toffoli gates with negative control lines. Permutations, corresponding to all the gates NOT, CNOT and 2-CNOT, generate the alternating group A($\mathbb{Z}_2^n$) and permutations, corresponding to all the gates k-CNOT, generate the symmetric group. This indicates the permutation group theory can be used to successfully synthesize a reversible circuit for a given reversible specification.

Lee et al. (2001) defined four permutation methodologies and created innovative permutation instructions for performing arbitrary n-bit permutations efficiently with software running on programmable processors. As well as characterized the

performance of these different permutation methodologies and the tradeoffs between them is performed. Also described how arbitrary permutations could be specified in high-level software by means of an array of integers, in a processor-independent way. This can be used by compilers or macro assemblers to generate efficient sequences of permutation instructions to achieve any arbitrary permutation, using the permutation instructions available in the target processor.

Shi and Lee (2000) proposed two instructions, PPERM3R and GRP for efficient software implementation of arbitrary permutations. The PPERM3R instruction can be used for dynamically specified permutations; the GRP instruction can be used to do arbitrary n-bit permutations with up to n lg(n) instructions. In addition, a systematic method for determining the instruction sequence for performing an arbitrary permutation is defined.

Sedgewlck (1977) presented surveys the numerous methods that have been proposed for permutation enumeration by computer. It is not only as a survey of permutation generation methods, but also as a tutorial on how to compare a number of different algorithms for the same task.

3. Permutations

A permutation on a set X is a bijection $f: X \to X$. Recall that a bijection is a mapping which is 1-1 and onto. If $X = \{1,2,3, \dots, n\}$, a permutation of X is called a permutation on n letters. The set of permutation of X will be denoted by $\mathrm{Perm}(X)$.

The permutation can be applied on a set of elements or a matrix as follow:
The permutation on the set is implemented by swapping every element with another element in the set. The following example illustrates it.

- Example: the six permutations of the set {1, 2, 3} are 123, 132, 213, 231, 312, and 321.

- A permutation on a matrix M can effects on the position of its elements, for example consider the matrix $M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$, and $P(M) = \begin{pmatrix} 7 & 8 & 9 \\ 4 & 5 & 6 \\ 1 & 2 & 3 \end{pmatrix}$, this statement can be written as

$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 9 & 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$, the set of all permutations on the matrix M is S_9 which contains $factorial\ \ which\ is\ 362880$ elements [6].

In this paper we implemented the permutation on the matrix of two rows, where the first row represents the original positions of the elements while the second row represents the new positions of the elements.

4. Composition on Permutation

A composition functions can be defined as one the function inside another the function. For example, the function $h(x)=(2x-1)^2$. This function, h(x) was formed by the composition of the two other functions, the inside function which is 2x–1 while the outside function which is z^2. The notation used for the composition of the functions is $(f\circ g)(x) = f(g(x))$. This mean the composition of the function f with g which is function g is inside of the function f. The order is very important in the composite functions where $(f\circ g)(x)$ is not the same as $(g\circ f)(x)$ [7].

Composition on the permutation is used to combine two permutations set to produce a third set. The composition is opposite to the way functions were combined in mathematics. In most branches of mathematics, the composition, $(f \circ g)(x)$ read from right-to-left: $f(g(x))$. While the composition of permutations is combined from the left-to-right as shown in the figure 1[9].

Let $\boldsymbol{\alpha} = \begin{pmatrix}1&2&3&4&5\\5&3&1&4&2\end{pmatrix}$ and $\boldsymbol{\beta} = \begin{pmatrix}1&2&3&4&5\\5&3&2&1&4\end{pmatrix}$, Then

$$\boldsymbol{\alpha\beta} = \begin{pmatrix}1&2&3&4&5\\5&3&1&4&2\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\5&3&2&1&4\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\4&2&5&1&3\end{pmatrix}.$$

Figure 1 composition on the permutation

5. Properties of Composition

An operation on any set can objected with some properties as associativity, identity element and the inverse, but there are other properties which we are interested with such as power element of a permutation P_i^n which is difficult to find manually, and the order of the permutation when the power element of the permutation equal to the identity. Sometimes finding the inverse of a permutation with respect to composition is difficult. However it is consider as part of finding the element order.

5.1 Power element

Composing an element $P_i \in S_n$ by itself several times is called the power element of P_i denoted by P_i^m, which of cares represent another element say $P_j \in S_n$. It can be defined as perm [8].

$$P_j = P_i^m = P_i \circ P_i \circ \dots \circ P_i \; m \; times \qquad \text{(eq.1)}$$

5.2 The order

If a power element $\mathrm{P_i^r}$ of a permutation $\mathrm{P_i} \in \mathrm{S_n}$ is equal to the identity element e, then r is called the order of $\mathrm{P_i}$. That is

$$\mathrm{P_i^r = e = \begin{pmatrix} 1 & 2\cdots & \cdots n \\ 1 & 2\cdots & \cdots n \end{pmatrix}} \qquad \text{(eq.2)}$$

5.3 Inverse

Every permutation has an inverse that is undoes the operation. In other words, when the permutation on the set of element with its inverse are applied, the result will be the original element. If P is a permutation and P-1is its inverse, the PP-1=e. As well as the same is right for the composition of the permutation which is define mathematically as follow

Let $\mathrm{P_i} \in \mathrm{S_n}$, which permutation is the inverse of $\mathrm{P_i}$, that $\exists \mathrm{P_i^{-1}} \in \mathrm{S_n}$

where

$$\mathrm{P_i \circ P_i^{-1} = e = \begin{pmatrix} 1 & 2\cdots & \cdots n \\ 1 & 2\cdots & \cdots n \end{pmatrix}} \qquad \text{(eq.3)}$$

And since $\mathrm{P_i^r = e}$, then$\mathrm{P_i \circ P_i^{r-1} = e}$, and hence

$$\mathrm{P_i \circ P_i^{r-1} = P_i \circ P_i^{-1} = e}, \text{ then } \mathrm{P_i^{-1} = P_i^{(r-1)}} \qquad \text{(eq.4)}$$

6. Software Packages

This section describes the Software packages and presents the results from them which are implemented for permutation and composition as well as other properties that will be explained in details in the following sections

6.1 Description

The main window of this program was shown in figure (2) and figure (3) that contains two menus and seven buttons to help users to use all the functions of the program. The about windows was shown in figure (4) that contain the name of program and the names of development team.
The general activities of software package can be presented by the following steps:

- The first step: Dealing with the matrix which is determined by user and permute its elements with all probabilities.
- The second step: compute composition of any two matrixes which is determined by user.
- The third step: verify of the associative property will be explained in section 6.2.
- The fourth step: applying property of the order which is mentioned in section 5.2. Compose of the matrix which is applied for n times till getting the identity matrix.

The output of all these steps will be shown in next section.

6.2 Results

This section shows the output of the steps in above section that have been obtained through the implementation of software package as following:
➢ For the first step the following example will be present:

Example 1: first of all, the user has to click on Permutation button then the program ask him to enter the dimensions of the matrix to show all the elements of its permutation that produced by the program, where the matrix in this example has five elements so 120 different sequences will be produced as shown below:

Enter the number of rows and columns of matrix
2 5
Enter the elements of second row
1 2 3 4 5
The resulted elements are shown in table (1).

Table (1): the outputs from example 1

P1 1,2,3,4,5 1,2,3,4,5	P21 1,2,3,4,5 1,5,4,3,2	P41 1,2,3,4,5 2,4,5,1,3	P61 1,2,3,4,5 3,4,1,2,5	P81 1,2,3,4,5 4,3,1,2,5	P101 1,2,3,4,5 5,2,1,4,3
P2 1,2,3,4,5 1,2,3,5,4	P22 1,2,3,4,5 1,5,4,2,3	P42 1,2,3,4,5 2,4,5,3,1	P62 1,2,3,4,5 3,4,1,5,2	P82 1,2,3,4,5 4,3,1,5,2	P102 1,2,3,4,5 5,2,1,3,4
P3 1,2,3,4,5 1,2,4,3,5	P23 1,2,3,4,5 1,5,2,4,3	P43 1,2,3,4,5 2,5,3,4,1	P63 1,2,3,4,5 3,4,2,1,5	P83 1,2,3,4,5 4,3,5,1,2	P103 1,2,3,4,5 5,3,2,4,1
P4 1,2,3,4,5 1,2,4,5,3	P24 1,2,3,4,5 1,5,2,3,4	P44 1,2,3,4,5 2,5,3,1,4	P64 1,2,3,4,5 3,4,2,5,1	P84 1,2,3,4,5 4,3,5,2,1	P104 1,2,3,4,5 5,3,2,1,4
P5 1,2,3,4,5 1,2,5,4,3	P25 1,2,3,4,5 2,1,3,4,5	P45 1,2,3,4,5 2,5,4,3,1	P65 1,2,3,4,5 3,4,5,2,1	P85 1,2,3,4,5 4,1,3,2,5	P105 1,2,3,4,5 5,3,4,2,1
P6 1,2,3,4,5 1,2,5,3,4	P26 1,2,3,4,5 2,1,3,5,4	P46 1,2,3,4,5 2,5,4,1,3	P66 1,2,3,4,5 3,4,5,1,2	P86 1,2,3,4,5 4,1,3,5,2	P106 1,2,3,4,5 5,3,4,1,2
P7 1,2,3,4,5 1,3,2,4,5	P27 1,2,3,4,5 2,1,4,3,5	P47 1,2,3,4,5 2,5,1,4,3	P67 1,2,3,4,5 3,5,1,4,2	P87 1,2,3,4,5 4,1,2,3,5	P107 1,2,3,4,5 5,3,1,4,2
P8 1,2,3,4,5 1,3,2,5,4	P28 1,2,3,4,5 2,1,4,5,3	P48 1,2,3,4,5 2,5,1,3,4	P68 1,2,3,4,5 3,5,1,2,4	P88 1,2,3,4,5 4,1,2,5,3	P108 1,2,3,4,5 5,3,1,2,4
P9 1,2,3,4,5 1,3,4,2,5	P29 1,2,3,4,5 2,1,5,4,3	P49 1,2,3,4,5 3,2,1,4,5	P69 1,2,3,4,5 3,5,4,1,2	P89 1,2,3,4,5 4,1,5,2,3	P109 1,2,3,4,5 5,4,3,2,1
P10 1,2,3,4,5 1,3,4,5,2	P30 1,2,3,4,5 2,1,5,3,4	P50 1,2,3,4,5 3,2,1,5,4	P70 1,2,3,4,5 3,5,4,2,1	P90 1,2,3,4,5 4,1,5,3,2	P110 1,2,3,4,5 5,4,3,1,2
P11 1,2,3,4,5 1,3,5,4,2	P31 1,2,3,4,5 2,3,1,4,5	P51 1,2,3,4,5 3,2,4,1,5	P71 1,2,3,4,5 3,5,2,4,1	P91 1,2,3,4,5 4,5,3,1,2	P111 1,2,3,4,5 5,4,2,3,1

P12 1,2,3,4,5 1,3,5,2,4	P32 1,2,3,4,5 2,3,1,5,4	P52 1,2,3,4,5 3,2,4,5,1	P72 1,2,3,4,5 3,5,2,1,4	P92 1,2,3,4,5 4,5,3,2,1	P112 1,2,3,4,5 5,4,2,1,3
P13 1,2,3,4,5 1,4,3,2,5	P33 1,2,3,4,5 2,3,4,1,5	P53 1,2,3,4,5 3,2,5,4,1	P73 1,2,3,4,5 4,2,3,1,5	P93 1,2,3,4,5 4,5,1,3,2	P113 1,2,3,4,5 5,4,1,2,3
P14 1,2,3,4,5 1,4,3,5,2	P34 1,2,3,4,5 2,3,4,5,1	P54 1,2,3,4,5 3,2,5,1,4	P74 1,2,3,4,5 4,2,3,5,1	P94 1,2,3,4,5 4,5,1,2,3	P114 1,2,3,4,5 5,4,1,3,2
P15 1,2,3,4,5 1,4,2,3,5	P35 1,2,3,4,5 2,3,5,4,1	P55 1,2,3,4,5 3,1,2,4,5	P75 1,2,3,4,5 4,2,1,3,5	P95 1,2,3,4,5 4,5,2,1,3	P115 1,2,3,4,5 5,1,3,4,2
P16 1,2,3,4,5 1,4,2,5,3	P36 1,2,3,4,5 2,3,5,1,4	P56 1,2,3,4,5 3,1,2,5,4	P76 1,2,3,4,5 4,2,1,5,3	P96 1,2,3,4,5 4,5,2,3,1	P116 1,2,3,4,5 5,1,3,2,4
P17 1,2,3,4,5 1,4,5,2,3	P37 1,2,3,4,5 2,4,3,1,5	P57 1,2,3,4,5 3,1,4,2,5	P77 1,2,3,4,5 4,2,5,1,3	P97 1,2,3,4,5 5,2,3,4,1	P117 1,2,3,4,5 5,1,4,3,2
P18 1,2,3,4,5 1,4,5,3,2	P38 1,2,3,4,5 2,4,3,5,1	P58 1,2,3,4,5 3,1,4,5,2	P78 1,2,3,4,5 4,2,5,3,1	P98 1,2,3,4,5 5,2,3,1,4	P118 1,2,3,4,5 5,1,4,2,3
P19 1,2,3,4,5 1,5,3,4,2	P39 1,2,3,4,5 2,4,1,3,5	P59 1,2,3,4,5 3,1,5,4,2	P79 1,2,3,4,5 4,3,2,1,5	P99 1,2,3,4,5 5,2,4,3,1	P119 1,2,3,4,5 5,1,2,4,3
P20 1,2,3,4,5 1,5,3,2,4	P40 1,2,3,4,5 2,4,1,5,3	P60 1,2,3,4,5 3,1,5,2,4	P80 1,2,3,4,5 4,3,2,5,1	P100 1,2,3,4,5 5,2,4,1,3\	P120 1,2,3,4,5 5,1,2,3,4

➢ Second step illustrated by another example.

Example 2: from this example the composition operation will be applied between to permutations to produce another one as shown below:

Enter the elements of first matrix:

1 2 3 4 5

1 3 4 5 2

Enter the elements of second matrix:

1 2 3 4 5

5 3 4 1 2

The output from the composition between the entered matrices is:-

1 2 3 4 5

2 4 5 1 3

- The associative property of the composed matrixes is proven as illustrated in example 3.

Example 3: let take three elements from the permutations of (2 x 3) matrix, where these elements are shown below then applying the composition on them to prove that it is associative then by that the user can trust on the results of this program.

Let :

$$p1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$p2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$p3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$p1\ o\ (p2\ o\ p3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$(p1\ o\ p2)\ o\ p3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

From that we can see:

$(p1\ o\ p2)\ o\ p3 = p1\ o\ (p2\ o\ p3)$ then it is associative and the program is reliable and trusted.

- The fourth step the matrix is powered for n times till getting the identity matrix as in example (4) , where the user have to press on power button then he has to enter the array, after that the program will produce the power of it.

Example 4:

Enter the elements of a matrix

1 2 3 4 5

2 4 5 1 3

The power is:-

5

This number resulted from that the matrix composed with itself five times until produce the Identity element, all these times of composition listed below:

- ✓ First one:

  1,2,3,4,5

  4,1,3,2,5

==========

- ✓ Second one:

  1,2,3,4,5

  1,2,5,4,3

==========

- ✓ Third one:

  1,2,3,4,5

  2,4,3,1,5

==========

- ✓ Forth one:

  1,2,3,4,5

  4,1,5,2,3

==========

- ✓ Fifth one:

  1,2,3,4,5

  1,2,3,4,5

==========

From that we can see the last one produce the identity element, so the power is five.

7. Future Works

In the future work, we will focus on applying permutation on matrixes. The software selects the permutation depending on the requirements. In addition the software will be classified permutation base on application requirements

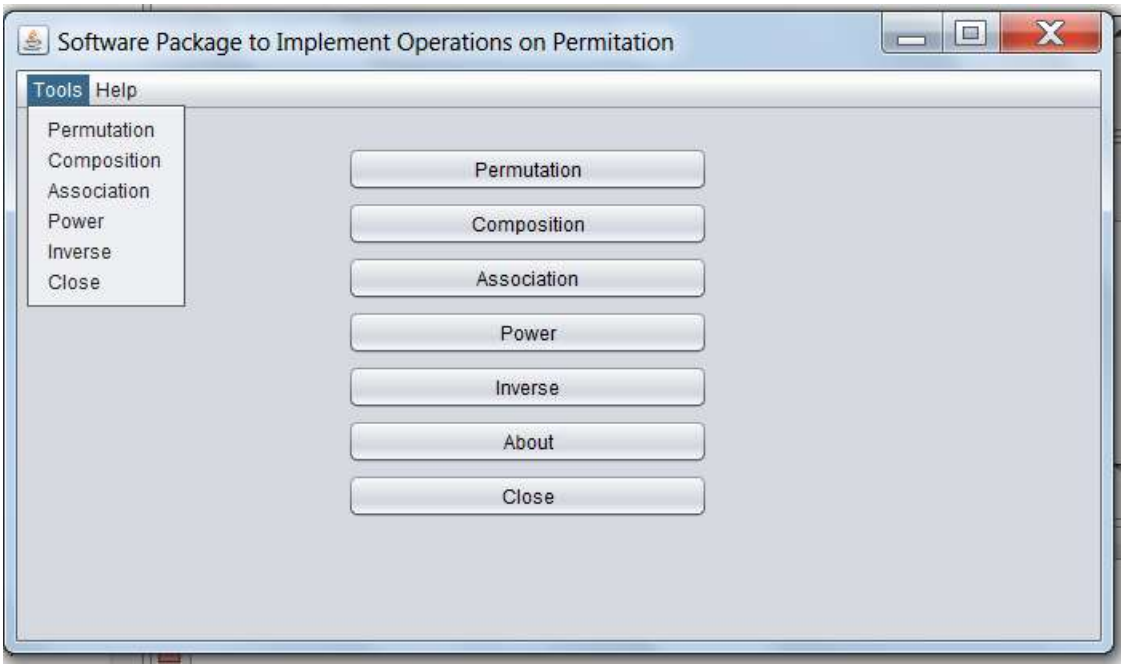

Figure (2): The main window (Tool menu)

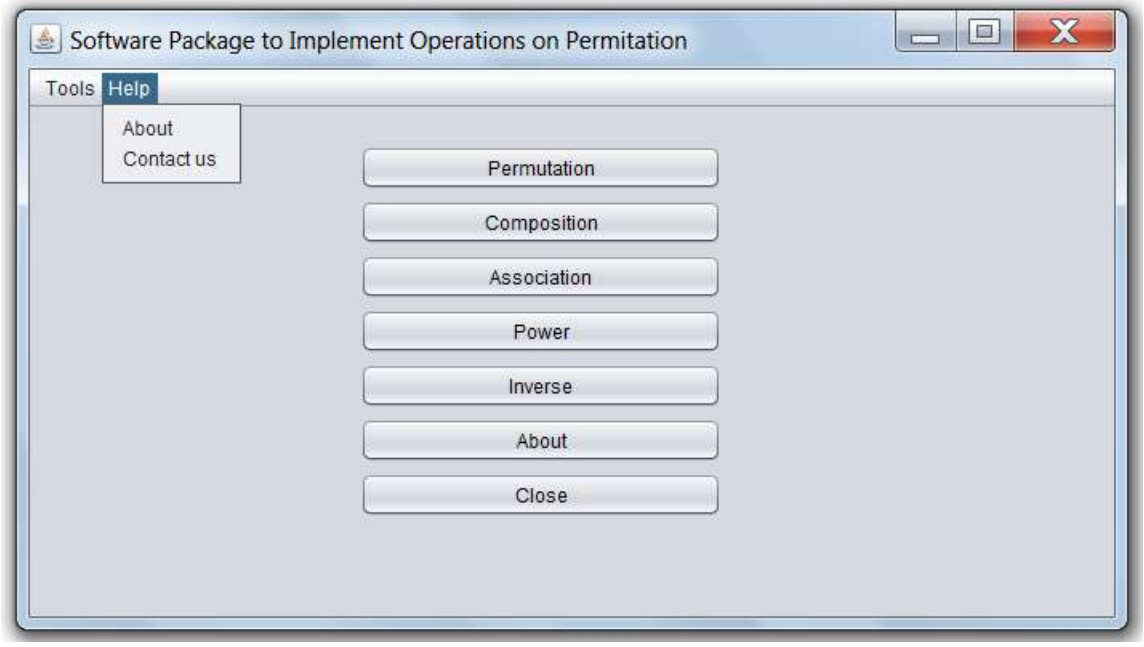

Figure (3): The main window (Help menu)

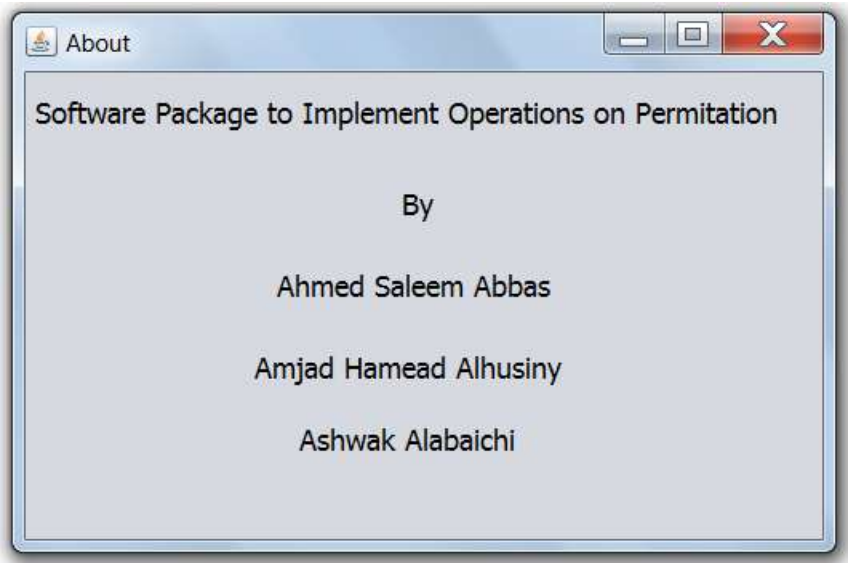

Figure (4): The About window

References

[1] E. Ouchterlony, "On Young tableau involutions and patterns in permutations," arXiv preprint arXiv:0908.0255, 2009.

[2] D. Zakablukov, "Application of Permutation Group Theory in Reversible Logic Synthesis," *arXiv preprint arXiv:1507.04309*, 2015.

[3] R. B. Lee, et al., "Efficient permutation instructions for fast software cryptography," Micro, IEEE, vol. 21, pp. 56-69, 2001.

[4] Z. Shi and R. B. Lee, "Bit permutation instructions for accelerating software cryptography," in Application-Specific Systems, Architectures, and Processors, 2000. Proceedings. IEEE International Conference on, 2000, pp. 138-148.

[5] R. Sedgewick, "Permutation generation methods," *ACM Computing Surveys (CSUR)*, vol. 9, pp. 137-164, 1977.

[6] T. Davis, "Permutation Groups," no. 3, pp. 1–12, 2003.

[7] "Composite functions," *Read*, no. x, pp. 22–25, Retrieved from www.mesacc.edu/~pikeu/.../**composition/composite_functions**_intro.**pdf**.

[8] D. Joyce, "Permutations and determinants Math 130 Linear Algebra," pp. 1–3, 2015.

[9] J. Mulholland, "Permutation Puzzles: A Mathematical Perspective 15," 2015.