Volume 12 Number 4
Journal of Advances in Mathematics

Basis of Hecke algebras - associated to Coxeter groups - via matrices of inversion for permutations

E. A. Elrifai and Redha. A. Alghamdi
Princess Nourah Bint Abdul Rahman University, Kingdom of Saudi Arabia:
1- Department of Mathematical Sciences, College of Science.
2- Deanship of Scientific Research.
eaelrifai@pnu.edu.sa, rdh.ashour24@hotmail.com

Abstract

Applying the matrices of inversion for permutations, we show that every element of S_n associates a unique canonical word in the Hecke algebra $H_{n-1}(z)$. That provides an effective and simple algorithm for counting a linear basis of Hecke algebra H_n, as binary matrices.

Keywords: braid groups; Hecke algebras; Symmetric group; Representation theory of groups; matrix of inversions for a permutation.

Mathematics Subject Classification 2000: 20F36, 20C30, 05A05.

1 Introduction

The Hecke algebra has nontrivial important properties and applications. We apply the matrices of inversion for permutations, for constructing a linear basis of Hecke algebra.In section two we give a brief knowledge on braid groups B_n in point of view of an algebraic and geometric presentations. And how braid group is related to symmetric group S_n. The positive braids B_n^+, where each word is a product of positive generators, has a specific subset of positive braids which is known by positive permutation braids, PPBs S_n^+, where each pair of strings cross in a positive sense at most once. The set S_n^+ has interested properties and useful applications for solving the word and conjugacy problems in braid groups. Also we mention the good relation between braids and knots. We explore the relation between braid groups and a specific type of Hecke algebras $H_n(z)$ based on symmetric groups.In section three, we will give an explicit set of generators for H_n, that is in view of matrices of inversions for permutations.

2 Background and notations

In this section we remind some basics from symmetric groups, braid groups, knot theory and Hecke algebras as representation of braid groups.

2.1 Braid groups and symmetric groups

Braid groups are very powerful and useful in various areas of mathematics such as representation theory of groups, group algebras, dynamical systems, algebraic geometry, algebraic topology and cryptography [1, 2]. It were first introduced by Emil Artin in 1925, as a group B_n with presentation of $n-1$ generators $\sigma_i, i=1,2,...,n-1$ subject to the relations $\sigma_i\sigma_{i+1}\sigma_i=\sigma_{i+1}\sigma_i\sigma_{i+1}, i=1,2,...,n-2$ and $\sigma_i\sigma_j=\sigma_j\sigma_i, |i-j|\geq 2$ [3].

The geometric approach is a good tool for understanding braids, think of an n braid as a collection of n strands in space. The strands are disjoint and monotone in the z-direction. The endpoints of the strands are fixed. Two braids are considered to be equivalent if they are homotopic relative to top and bottom endpoints. Fig. 1 illustrates the graphs of the generator σ_i, the inverse generator σ_i^{-1} in B_n and a braid word in B_4.

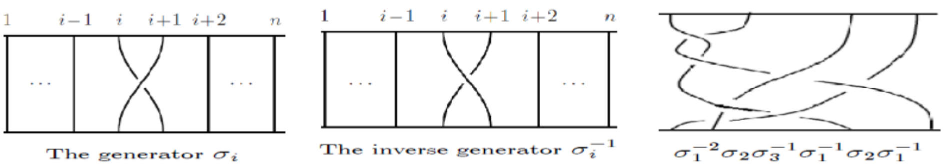

Figure1: a b c

ISSN 2347-1921
Volume 12 Number 4
Journal of Advances in Mathematics

The symmetric group S_n has a quite similar presentation of $n-1$ generators $\tau_i = (i\,i+1)$, $i = 1,2,...,n-1,$ subject to the relations $\tau_i \tau_{i+1} \tau_i = \tau_{i+1} \tau_i \tau_{i+1}$, $i = 1,2,...,n-2$, $\tau_i \tau_j = \tau_j \tau_i, |i-j| \geq 2$ and $\tau_i^2 = id., i = 1,2,...,n-1,$ the first two relations are braid relations [4]. In fact this presentation makes the symmetric group S_n as a Coxeter group with Coxeter matrix and Dynkin diagram, as in Fig. 2:

$$M = \begin{bmatrix} 1 & 3 & 2 & 2 & . & . & & 2 \\ 3 & 1 & 3 & 2 & & & & 2 \\ 2 & 3 & . & . & 2 & & & . \\ . & & . & . & & 2 & & \\ & & & & & . & 2 & \\ & & & & & . & 3 & 2 \\ & & & & & 3 & 1 & 3 \\ 2 & 2 & . & & . & 2 & 3 & 1 \end{bmatrix}$$

Figure 2: Dynkin diagram

This suggests a natural homomorphism $\phi : B_n \to S_n, \phi(\sigma_i) = \tau_i, i = 1,2,...,n-1$, hence we have a relation between braids and permutations. In fact, each n braid defines a permutation of n points, which can be read at the bottom line of the braid. For example, in Fig. 1, the two graphs (a), (b) have permutation $(i\,i+1)$ in S_n, while the graph (c) has permutation (3421) in S_4. It is remarkable that the homomorphism $\phi : B_n \to S_n$ is surjective but not injective.

A braid is said to be positive if it can be written as a product of elements $\sigma_i^k, k \in \mathbb{N}$ without involving negative powers. The positive braids B_n^+ form a semi-group [1]. Braid in Fig. 1a is positive, in Fig. 1b is negative while in Fig. 1c neither positive nor negative. A positive braid is called a positive permutation braid, PPB, if each pair of its strings cross in a positive sense at most once. Let S_n^+ be the set of all positive permutation braids, then $S_n^+ \subset B_n^+ \subset B_n$. A specific PPB where each two strings cross each other exactly once in a positive sense is called the fundamental braid. It was introduced by F. A. Garside [5] and denoted Δ_n, with

$$\Delta_1 = I, \Delta_2 = \sigma_1, \Delta_3 = \sigma_1.\sigma_2\sigma_1, \Delta_n = \Delta_{n-1}\sigma_{n-1}\sigma_{n-2}...\sigma_2\sigma_1$$
$$i.e.\ \Delta_n = (\sigma_1)(\sigma_2\sigma_1)...(\sigma_{n-2}...\sigma_2\sigma_1)(\sigma_{n-1}\sigma_{n-2}...\sigma_2\sigma_1)$$

This can be described as a geometric n braid by imagining the strings attached to a rod which is given a positive half-twist, as in Fig. 3. The PPB Δ_n has the permutation representation $\phi(\Delta_n) = \delta = (n\,n-1\,n-2\,...\,2\,1).$ In fact the center $Z(B_n)$ of the group B_n is generated by Δ_n^2 [1].

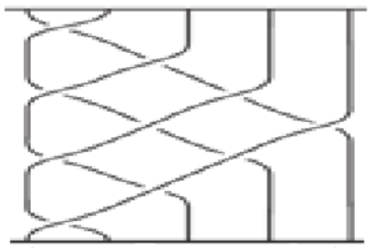

Figure 3: The fundamental braid Δ_5

The set S_n^+ of PPBs has many interested properties and so many useful applications. Garside showed that every element β in B_n can be represented by a word $\beta = \Delta^{2r}P$, where r is an integer and P is a positive word, and r is maximal for all such representations [5]. Elrifai improved Graside algorithm, he showed that P can be factorized as a product of PPBs $P_1, P_2, ..., P_s$. Elrifai's form is a unique representation in which the integer s is minimal for all representations of P as a product of PPBs. Also, each P_i is the longest possible PPB in the factorization [6]. The results in [6] were rewritten and modified by Elrifai and Morton [7]. Also independently, Thurston improved Graside's algorithm [8].

2.2 Braid groups and knots

A knot is an embedding $K : S^1 \to S^3$ of 1-sphere into 3-sphere, while a link is a finite collection of disjoint knots $L : S^1 \cup S^1 ... \cup S^1 \to S^3$. In fact, any oriented knot can be viewed as a closed braid. A closed braid can be formed by connecting opposite ends of the strands of the braid, as in Fig. 4. A comprehensive details about knot and link theory can be found in [9].

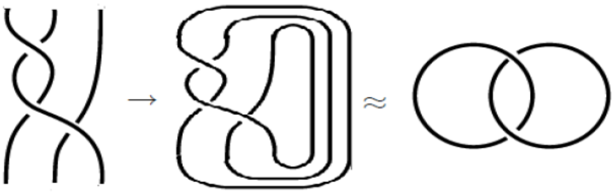

Figure 4: The Hopf link as a closed braid

2.3 Hecke algebras and representation of braid groups

A classical Hecke algebra $H(z)$ for some $z \in \mathbb{C}$, is the algebra generated by $c_i, i \in \mathbb{N}$ subject to the relations; $c_i^2 = zc_i + 1, i \geq 1, c_i c_j = c_j c_i, |i - j| > 1$ and $c_i c_{i+1} c_i = c_{i+1} c_i c_{i+1}, i \geq 1.$ For an integer n the finitely generated Hecke algebra $H_n(z)$ is a subalgebra of $H(z),$ with the presentation,

$$H_n(z) = \left\{ c_i, i = 1,2,...,n \;\middle|\; \begin{array}{c} c_i^2 = zc_i + 1, 1 \leq i \leq n \\ c_i c_j = c_j c_i, |i - j| > 1 \\ c_i c_{i+1} c_i = c_{i+1} c_i c_{i+1}, 1 \leq i \leq n-1 \end{array} \right\}$$

In fact is the symmetric group S_{n+1} when $z = 0.$ Also H_n can be viewed as a vector space with dimension $n!$ [10].

Since B_n has $n-1$ generators and $c_i^{-1} = c_i - z,$ then the braid group B_{n+1} can be represented in the Hecke algebra $H_n,$ with $\rho_v : B_{n+1} \to H_n, \rho_v(\sigma_i) = vc_i$ for any $v \in$ □.

3Basis of Hecke algebra via matrices of inversions for permutations

An inversion of a permutation $\pi = (\pi_1 \pi_2 ... \pi_n)$ in S_n is a pair (i, j) with $i < j$ and $\pi_i > \pi_j.$ Any permutation $\pi = (\pi_1 \pi_2 ... \pi_n)$ in S_n has a matrix invariant for its inversion $M_\pi = (m_{ij})_{n \times n}$, where $m_{ij} = 1$ if $i < j$ and $\pi_i > \pi_j,$ otherwise $m_{ij} = 0.$ In fact the notion "matrix of inversions for a permutation" is introduced and analyzed in [12], [13]. We refer to example 9, for many operations on matrices of inversions for permutations.

Remark 1 In this remark, we summarize some of its properties which will be needed in this work:

1. The set $M_n(F) = \{M_\pi : \pi \in S_n, m_{ij} \in F = \{0,1\}\}$ of all possible matrices of inversions for permutations over S_n is a group with the operation $M_\alpha + M_\beta = M_\alpha \underset{mod 2}{+} \alpha^{-1}(M_\beta)$, for each α, β in $S_n,$ and if $M_\alpha = (m_{ij}),$ then

$$\beta(M_\alpha) = \beta(m_{ij}) = \begin{Bmatrix} 0 & ,i \geq j \\ m_{\beta(i)\beta(j)} & ,i < j, \beta(i) < \beta(j) \\ m_{\beta(j)\beta(i)} & ,i < j, \beta(i) > \beta(j) \end{Bmatrix}$$

2. The set $M_n(F)$ with the above operation is a group and it is isomorphic to S_n, with an isomorphism $\psi : S_n \to M_n(F), \psi(\pi) = M_\pi$.for every π in S_n.

3. In fact, not every binary matrix is a matrix of inversion for a permutation. A recognition algorithm for such these matrices is given in [13].

4. An algorithm for writing a canonical word W_π of a permutation π in S_n is given by using its matrix of inversions. Given π in S_n, find the matrix of inversion M_π for π. Each row in M_π will contributes by a word as a product of transpositions $\tau_i, i = 1,2,...,n-1$. The row that all its entries are zeros will contribute by the identity word. If the number of ones in the entries of the i[th]row is $m_i, 0 \leq m_i \leq n-i$, the corresponding word will be $w_i = \tau_i \tau_{i+1} ... \tau_{i+m_i-1}, 1 \leq i \leq n-1, w_n = id.$, hence $W_\pi = w_n w_{n-1} ... w_1$. The canonical word W_π of the permutation π can be represented diagrammatically, in Fig. 5, as a tower of $n-1$ floors. The j^{th} floor contains a word $\tau_j \tau_{j+1} ... \tau_{j+i_j-1}$ starts by τ_j, if $i_j \geq 1$, while it will be the identity if $i_j = 0$.

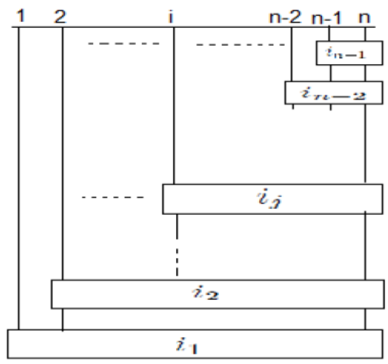

Figure 5: Diagram of a canonical word

Lemma 2 $M_{\pi^{-1}} = \pi(M_\pi)$, for every π in S_n.

Proof. From the relation $M_{\alpha\beta} = M_\alpha + M_\beta = M_\alpha +_{mod 2} \alpha^{-1}(M_\beta)$, for $\alpha = \pi^{-1}, \beta = \pi$ we have $M_I = M_{\pi^{-1}\pi} = M_{\pi^{-1}} + M_\pi = M_{\pi^{-1}} +_{mod2} \pi(M_\pi)$ the zero matrix, then $M_{\pi^{-1}} = \pi(M_\pi) \ mod 2$.

Lemma 3 In S_n, the expression $W_\pi = w_{n-1} ... w_1$ for a permutation π is unique.

Proof. The two groups $M_n(F)$, of all possible matrices of inversions for permutations over S_n, and S_n are isomorphic [12]. And every matrix of inversions for a permutation induces a unique canonical word $W_\pi = w_{n-1} ... w_1$. Therefore the given associated canonical word W_π, for every π in S_n, is unique

Definition 4 Since the symmetric group S_n is generated by the transpositions $\tau_i, i = 1,2,...,n-1$. For a permutation π in S_n, the number $l(\pi) = \sum_{i=1}^{n-1} l(w_i)$ is called the length of π, where W_π is the associated canonical word for π, and $l(w_i)$ is the number of transpositions in w_i. In fact $l(\pi)$ is the number of inversions of the permutation π.

Now we are ready to give a different version of the Hecke algebra $H_n(z)$. Instead of S_n, consider its isomorphic version

council for Innovative Research
www.cirworld.com

$M_n(F)$. So we have the Coxeter system $(M_n(F), S)$, with the operation given in remark 1, where the group $M_n(F)$ is generated by

$$S = \{M_{\tau_i} : \tau_i = (i \ \ i+1), 1 \le i \le n-1\}$$

Definition 5 For a permutation π and for its associated canonical word $W_\pi = w_{n-1}...w_1$ in S_n. Let T_π be the word in $H_n(z)$ by replacing each τ_i in W_π by c_i, and $BH_n = \{T_\pi : \pi \in S_{n+1}\} \subseteq H_n(z)$. Then we have a $1-1$ correspondence,

$$f : M_{n+1}(F) \to BH_n = \{H_\pi : \pi \in S_n\}, f\ (M_\pi) = T_\pi \ \forall \pi \in S_{n+1}$$

Now we are going to prove that the set BH_n is a linear basis for $H_n(z)$.

Definition 6 The starting set for a permutation π in S_n, is a subset $S(\pi)$ of the generators of S_n, such that $S(\pi) = \{\tau_i : \pi = \tau_i \pi', \pi' \in S_n, i = 1,2,...,n-1\}$.

Theorem 7 The Hecke algebra H_n can be viewed as an algebra with basis $M_n(F)$, as a vector space, via the operations

$$\mathrm{T}_{\tau_i}\mathrm{T}_\pi = \begin{cases} T_{(\tau_i \pi)} = M_{\tau_i} +_{\mathrm{mod}\,2} \tau_i(M_\pi) & , l(\tau_i \pi) = l(\pi)+1 \\ T_{(\tau_i \pi)} + (q - q^{-1}) M_\pi = M_{\tau_i} +_{\mathrm{mod}\,2} \tau_i(M_\pi) + (q - q^{-1}) M_\pi & , \text{otherwise} \end{cases}$$

Proof. For a permutation $\pi = (\pi_1 \pi_2 ... \pi_{i-1} \underline{\pi_i \pi_{i+1}} \pi_{i+2} ... \pi_n)$ in S_n and for a transposition τ_i, we have $\tau_i \pi = (\pi_1 \pi_2 ... \pi_{i-1} \underline{\pi_{i+1} \pi_i} \pi_{i+2} ... \pi_n)$. If τ_i does not in $S(\pi)$, then $\pi_i < \pi_{i+1}$ and $(\tau_i \pi)(i) = \pi_{i+1} > \pi_i = (\tau_i \pi)(i+1)$. Therefore $l(\tau_i \pi) = l(\pi) + 1$. While, if τ_i in $S(\pi)$, then $\pi_i > \pi_{i+1}$ and $(\tau_i \pi)(i) = \pi_{i+1} < \pi_i = (\tau_i \pi)(i+1)$, hence we missed one inversion. So $l(\tau_i \pi) = l(\pi) - 1 < l(\pi)$, where $\pi = \tau_i \pi', \pi' \in S_n$. Then $\tau_i \pi = \tau_i \tau_i \pi'$, which gives $c_i T_\pi = c_i^2 T_{\pi'} = (zc_i + 1) T_{\pi'}$

Example 8 Consider the permutation $\pi = (613254)$ in S_6, then we are going to apply the operations above,

$$M_\pi = (m_{ij}) = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

the rows in M_π from the first to the sixth contributes by the words $w_1 = \tau_1\tau_2\tau_3\tau_4\tau_5$, $w_2 = Id.$, $w_3 = \tau_3$, $w_4 = Id.$, $w_5 = \tau_5$ and $w_6 = Id.$, respectively. Then the associated canonical word for π, in S_6, is

$$W_\pi = w_6 w_5 w_4 w_3 w_2 w_1 = Id.Id.\tau_5 Id.\tau_3 Id.\tau_1\tau_2\tau_3\tau_4\tau_5 = \tau_5.\tau_3.\tau_1\tau_2\tau_3\tau_4\tau_5$$

which can be diagrammatically represented as in Fig. 6, and can be read from top to bottom. From the diagram which is the unique canonical word for π.

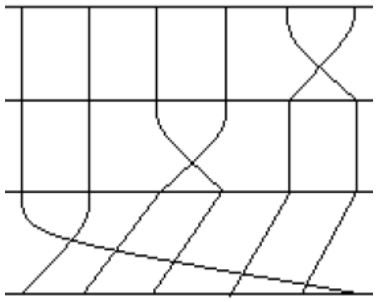

Figure 6: A diagram of π

The corresponding word for W_π in $H_5(z)$ is $H_\pi = c_5.c_3.c_1c_2c_3c_4c_5$ with $T_\pi = M_\pi$, the matrix above. To find the starting set for this permutation, apply the relations of the given presentation for S_n on $W_\pi = \tau_5.\tau_3.\tau_1\tau_2\tau_3\tau_4\tau_5$, then

$$\pi = \tau_5.\tau_3.\tau_1\tau_2\tau_3\tau_4\tau_5 = \tau_3.\tau_5.\tau_1\tau_2\tau_3\tau_4\tau_5 = \tau_1.\tau_5.\tau_3.\tau_2\tau_3\tau_4\tau_5$$

So $S(\pi) = \{\tau_1, \tau_3, \tau_5\}$. For τ_2, τ_4 which do not in $S(\pi)$, to have $\tau_2\pi$ and $\tau_4\pi$ just interchange by π_2, π_3 and by π_4, π_5 in π, respectively. So $\tau_2\pi = (631254)$, $\tau_4\pi = (613524)$, and

$$M_{\tau_2\pi} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \; M_{\tau_4\pi} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

We can directly compute the matrix $M_{\tau_2\pi}$ by interchanging between the second and the third rows in the M_π, then add 1 in the entry m_{23}, in the resulting matrix. Also compute the matrix $M_{\tau_4\pi}$ by interchanging between the fourth and the fifth rows in the M_π, then add 1 in the entry m_{45}, in the resulting matrix. While, the permutations $\tau_1\pi, \tau_3\pi, \tau_5\pi$ can be computed just by interchanging between $\pi_1, \pi_2; \pi_3, \pi_4$, and by π_5, π_6 in π, respectively. So $\tau_1\pi = (163254)$, $\tau_3\pi = (612354)$, $\tau_5\pi = (613245)$. To find their matrices of inversions, we put 0 instead of 1, in the entrees m_{12}, m_{34}, m_{56} of M_π, then, in the resulting matrix, interchanging between the first and the second, the third and the fourth, the fifth and the sixth, rows respectively, then

$$M_{\tau_1\pi} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, M_{\tau_3\pi} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, M_{\tau_5\pi} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

4Conclusion and future work

We hope that the given basis BH_n for $H_n(z)$ offers a simple method for calculating polynomial invariants of knots. Also it might provide a way for ordering or enumerating permutations.

5 Acknowledgements

The authors would like to express their gratitude to the deanship of scientific research at Princess Noura Bint Abdulrahman university for supporting and funding this work No. 36-s-132. The deanship of scientific research owns the intellectual property rights.

References

[1] A Jon Berrick, Frederick R Cohen, Elizabeth Hanbury, Yan-Loi Wong, Jie Wu, "Braids" Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore, Vol. 19, World Scientific, 2009.

[2] Kassel, Christian, Turaev, Vladimir, "Braid Groups" Graduate Texts in Mathematics, Vol. 247, 2008.

[3] E. Artin "Theory of braids" Ann. of Math. (2) 48, 101–126, (1947).

[4] R. McWeeny, "An introduction to group theory and its applications" Dover Publications, USA, 2002.

[5] F. A. Garside, "The braid group and other groups" Quart. J. Math. Oxford 20, No. 78 (1969), 235 254.

[6] E. A. El-Rifai, " Positive braids and Lorenz links" Liverpool University, UK, Ph.D. Thesis, 1988.

[7] E. A. El-Rifai and H. Morton " Algorithms for positive braids" Quart. J. Math. Oxford (2), 45 (1994), 479-497.

[8] D. B. A. Epstein (with Cannon, Holt, Levey, Patterson and Thurston) " Word Processing in Groups" Jones and Bartlett, Boston, Amazon (1992).

[9] Kunio Murasugi "Knot Theory and Its Applications" Birkhauser (Boston), 1996.

[10] N. Bourbaki " Groupes et algebres de Lie" Chapters 4-6, Hermann, Paris, 1968.

[11] P. Freyd, D. Yetter, J. Hoste, W. B. R. Lickorish, K. Millett and A. Ocneanu "A new polynomial invariant of knots and links" Bull. Amer. Math. Soc. (N.S.) 12 (1985), no. 2, 239–246.

[12] E. A. Elrifai, M. Anis, "Positive permutation braids and permutation inversions with some applications" Journal of knot theory and its ramifications, Vol. 21, No. 10, 2012.

[13] E. A. Elrifai, Redha. A. Alghamdi " Matrices of inversions for permutations: Recognition and Applications" Journal of Advances in Mathematics, Vol 9, No 1, 2014.

[14] Mathas. A "Iwahori-Hecke Algebras and schur Algebras of the symmetric groups" University Lecture Series, Vol. 14, AMS, 1999.