95.07

Weak Faithfulness Properties for the Burau Representation

Patrick DEHORNOY

ABSTRACT. We study the components of the matrices that belong to the image of the Burau representation of braids, and establish both algebraic and order constraints for a given Laurent polynomial possibly be a component of such a Burau matrix. As an application partial faithfulness results for the Burau representation are deduced.

AMS Classification: 20F36, 20H25, 15A24, 57M05.

Keywords: Braid groups, Burau representation

The Burau representation, here denoted ρ, is the oldest and presumably the simplest linear representation of the braid groups. Several questions about ρ remain uncompletely solved, concerning in particular its kernel and its image. For the first problem J. Moody proved in [15] that ρ is not faithful on braids with at least 9 strands, a result subsequently improved to 6 strands in [13]. The criterion used there leaves the cases of 4 and 5 strands open as well as the description of the kernel. Little is known about the second problem, excepted a seminal observation of C. Squier that shows in [16] that the Burau matrices are unitary with respect to some sort of Hermitian metric.

In this paper we shall obtain partial results about the above problems and, in particular, establish a seemingly new connection between them. The initial idea is to use the existence for any braid of decompositions where the generator σ_1 does not appear simultaneoulsy with positive and negative powers. Considering decompositions with a bounded number k of σ_1's and a bounded number n of strands gives for ρ a partial faithfulness statement $\mathcal{P}_k(B_n)$ whose strength increases with k and n. We propose to use the double scale formed by the properties $\mathcal{P}_k(B_n)$ as a natural measure for the faithfulness degree of the Burau representation. From the unfaithfulness of ρ one deduces that $\mathcal{P}_5(B_7)$ and $\mathcal{P}_8(B_6)$ fail (Proposition 1.4). On the other hand for small values of k the study of the properties $\mathcal{P}_k(B_n)$ amounts to questions such as whether a given Laurent polynomial may appear or not as a component in a Burau matrix (Lemma 1.5).

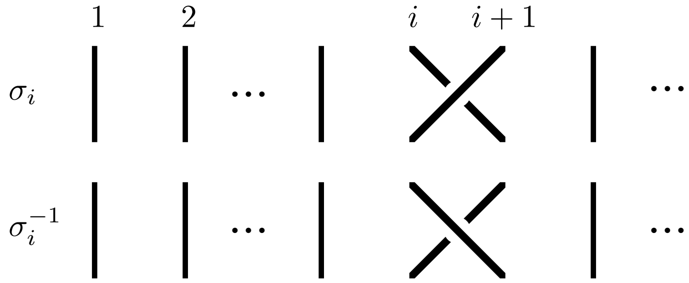
We are thus led to the problem of describing the Burau matrices, with a special interest in the above particular question. To this end we develop and refine in Sections 2 and 3 the study initiated in [16]. *These sections are independent from Section 1.* In Section 2 we give a series of quadratic relations that necessarily connect the components of the Burau matrices (Proposition 2.8). These relations can be exploited in different ways to obtain individual constraints for these components. An algebraic treatment gives strong constraints in the case of B_3 (Proposition 2.9).

In Section 3 we appeal to order considerations. A typical result in this direction (Proposition 3.1) claims that, if the Laurent polynomial p is the $1,1$-component of an $n \times n$ Burau matrix, then for $0 < \theta < \pi/n$ the value of p at $e^{2i\theta}$ has to lie in some (effectively defined) closed disk of the plane. We also obtain linear conditions, and, in particular, the surprisingly simple result (Corollary 3.4) that, if p is the $1,1$-component of a Burau matrix (of any dimension), then the value of the derivative p' at 1 is negative. Such inequalities imply that the groups of Burau matrices are included in some convex polytopes (Proposition 3.5).

In Section 4 the constraints established in Section 2 and 3 are applied to prove some of the weak faithfulness statements $\mathcal{P}_k(B_n)$, namely $\mathcal{P}_3(B_7)$ (Proposition 4.3) and $\mathcal{P}_4(B_4)$ (Proposition 4.4). We finally introduce some conjectures about a family of particular Burau matrices connected with a still poorly understood selfdistributive operation.

1. A measure for the degree of faithfulness of the Burau representation

As usual B_n denotes the group of all n strand braids up to isotopy. Then B_n admits $n-1$ generators $\sigma_1, \ldots, \sigma_{n-1}$ corresponding to the diagrams



and it is wellknown (*cf.* [1]) that the relations

$$\begin{cases} \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} & \\ \sigma_i\sigma_j = \sigma_j\sigma_i & \text{for } |i-j| \geq 2 \end{cases} \tag{1}$$

constitute a presentation of B_n. We denote by B_∞ the direct limit of the groups B_n with respect to the trivial injection of $\{1, \ldots, n\}$ into $\{1, \ldots, n+1\}$, *i.e.*, the group generated by an infinite sequence σ_1, σ_2, ... with defining relations (1).

Let β be any braid in B_∞. We say that a braid word w (*i.e.*, a finite sequence of generators σ_i and σ_i^{-1} viewed as letters) is a decomposition for β in B_n if w involves only letters among σ_1, σ_1^{-1}, ..., σ_{n-1}, σ_{n-1}^{-1} and β is the product of the successive letters of w in B_∞. Our starting point is the following

Theorem 1. *Let β be any braid. Then either β admits a decomposition where σ_1 occurs and σ_1^{-1} does not, or β admits a decomposition where σ_1^{-1} occurs and σ_1 does not, or β admits a decomposition where neither σ_1 nor σ_1^{-1} occurs.*

The first proof of this result in [3] works only in B_∞ (see also [5] for a more general introduction to the subject). The argument given there does not preserve in general the initial number of strands: starting with a braid β in B_n one obtains a 'σ_1-reduced' decomposition for β (*i.e.*, a decomposition where either σ_1^{-1} or σ_1 does not occur) in B_N for some effective but possibly huge number N. Subsequently R. Laver [11], D. Larue in [8], and the present author in [6] have given new proofs where the initial number of strands is preserved, so that Theorem 1 actually holds in each group B_n and not only in their limit B_∞.

One immediately deduces a criterion for establishing that a given representation of braids is faithful. In the sequel we denote by s the *shift* endomorphism of B_∞ that maps every generator σ_i to the corresponding generator σ_{i+1}.

Corollary 2. *Assume that ρ is any representation of B_n (simply a mapping of B_n into any set) that is compatible with the shift endomorphism in the sense that $\rho(s(\beta)) = \rho(1)$ implies $\rho(\beta) = \rho(1)$. Then ρ is faithful if and only if a braid that admits a decomposition where σ_1 occurs but σ_1^{-1} does not cannot have a trivial image under ρ.*

We investigate in this paper how this criterion applies to Burau representation. We shall denote by $\mathbf{Z}[t, t^{-1}]$ the ring of Laurent polynomials with integer coefficients, and by $\mathrm{GL}(\infty, \mathbf{Z}[t, t^{-1}])$ the direct limit of the groups $\mathrm{GL}(n, \mathbf{Z}[t, t^{-1}])$ with respect to the embeddings $i_{n,m}$ arising from

$$i_{n,n+1} : A \mapsto \begin{pmatrix} & & & 0 \\ & A & & \vdots \\ & & & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

In the sequel we shall always identify a matrix in $\mathrm{GL}(n, \mathbf{Z}[t, t^{-1}])$ with its images under $i_{n,m}$ for $n \leq m \leq \infty$. The (unreduced) *Burau representation* of B_∞ is the endomorphism

$$\rho : B_\infty \longrightarrow \mathrm{GL}(\infty, \mathbf{Z}[t, t^{-1}])$$

that maps σ_1 to the matrix

$$\Sigma_1 = \begin{pmatrix} 1-t & t \\ 1 & 0 \end{pmatrix}$$

and commutes with the shift endomorphism, defined (and still denoted s) in the case of matrices by

$$s : A \mapsto \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix}.$$

Corollary 2 naturally suggests that we investigate the Burau images of the braids that admit decompositions where σ_1^{-1} does not occur. To make a precise analysis we consider the following

> Property $\mathcal{P}_k(B_n)$: If β is a braid that admits in B_n a decomposition with no occurrence of σ_1^{-1} and at most k occurrences of σ_1, then the Burau image of β is nontrivial,

and its strengthening

> Property $\mathcal{P}_k^+(B_n)$: If β is a braid that admits in B_n a decomposition with no occurrence of σ_1^{-1} and at most k occurrences of σ_1, then the Burau image of β has a nontrivial first row.

For each pair (k, n), $\mathcal{P}_k(B_n)$ and $\mathcal{P}_k^+(B_n)$ are partial faithfulness properties for the Burau representation, and clearly their strength increases both with k and n. *We propose to measure the degree of faithfulness of ρ by determining which of the properties $\mathcal{P}_k(B_n)$ and $\mathcal{P}_k^+(B_n)$ are true.*

We begin with the upper bound in this measure. By Corollary 2 (which applies since ρ is by very construction compatible with the shift), the Burau representation is faithful on B_n just in case all properties $\mathcal{P}_k(B_n)$ be true. After [15] we know that this cannot happen for n large enough, and that there must exist pairs (k, n) such that $\mathcal{P}_k(B_n)$ (and therefore $\mathcal{P}_k^+(B_n)$) are false. A first observation, due to [13], is

Lemma 3. *If $\mathcal{P}_k^+(B_n)$ is false, so is $\mathcal{P}_k(B_{n+1})$.*

Proof. Assume that the braid β is a counterexample to $\mathcal{P}_k^+(B_n)$. The first row of the matrix $\rho(\beta)$ is trivial, and so is its first column by Corollary 1.2 of [13] (also stated as Proposition 2.5 below). It follows that the matrices Σ_1 and $s(\rho(\beta))$ commute, *i.e.*, that the braid $\sigma_1 s(\beta) \sigma_1^{-1} s(\beta)^{-1}$ belongs to the kernel of ρ. Now the latter braid is also

$$\sigma_2^{-1} \ldots \sigma_n^{-1} \beta \sigma_n \ldots \sigma_2 s(\beta)^{-1},$$

and a decomposition of β in B_n with at most k times σ_1 and no σ_1^{-1} gives for this braid a similar decomposition in B_{n+1}. ■

Now Theorem 1 is effective, and applying a σ_1-reduction process to the counterexamples constructed in [15] or [13] should give counterexamples to some properties $\mathcal{P}_k(B_n)$. The methods of [3], [11] and [8] cannot be applied practically because the involved braids are too complicated. But using the efficient method of [6] one easily finds

Proposition 4. *The properties $\mathcal{P}_5^+(B_6)$, $\mathcal{P}_5(B_7)$ and $\mathcal{P}_8(B_6)$ are false.*

Proof. One can verify that the braid $\psi^{-1}\sigma_5\psi$ of [13], which is shown to have a Burau matrix with trivial first row and column, admits (in B_6) the decomposition

$$\begin{aligned}&\sigma_2\underline{\sigma_1}\sigma_2^{-1}\sigma_4^{-1}\sigma_3^{-1}\sigma_5^{-1}\sigma_4^{-2}\sigma_3^{-1}\sigma_4^{-1}\sigma_5^3\sigma_4^{-1}\sigma_3^{-1}\sigma_2\underline{\sigma_1}\sigma_2^{-4}\sigma_3\sigma_4\sigma_5^{-2}\\ &\qquad\sigma_3\sigma_4\sigma_5\sigma_3\sigma_4\underline{\sigma_1^2}\sigma_5\sigma_4\sigma_3^{-1}\sigma_2^{-1}\underline{\sigma_1},\end{aligned}$$

where σ_1 occurs 5 times and σ_1^{-1} does not occur: so $\mathcal{P}_5^+(B_6)$ is false. By Lemma 3 this implies that $\mathcal{P}_5(B_7)$ is false as well (using additional reductions one can obtain a counterexample with 74 crossings.) Similarly it happens that the braid $[\psi^{-1}\sigma_5\psi, (\sigma_2\sigma_3\sigma_4\sigma_5)^5]$, which is shown in [13] to have a trivial Burau matrix, admits (in B_6) the decomposition

$$\begin{aligned}&\sigma_2\underline{\sigma_1}\sigma_4^{-1}\sigma_3\sigma_2^{-2}\sigma_4\sigma_3^3\sigma_2^{-1}\sigma_5\sigma_4^{-1}\sigma_5^{-1}\sigma_3^{-1}\sigma_4^{-1}\sigma_2^{-2}\sigma_3^{-1}\underline{\sigma_1}\sigma_2^{-4}\sigma_3\sigma_4\underline{\sigma_1^2}\\ &\quad\sigma_5^{-3}\sigma_4\sigma_3\sigma_4\sigma_3\sigma_2^{-1}\sigma_5\sigma_4\sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_5\sigma_4^{-1}\sigma_5^{-1}\sigma_2^{-1}\underline{\sigma_1}\sigma_5^{-1}\sigma_4^{-1}\sigma_3^{-1}\sigma_2^{-1}\\ &\quad\sigma_5^{-1}\sigma_4^{-1}\sigma_3\sigma_5^{-1}\sigma_4\sigma_2^{-2}\underline{\sigma_1}\sigma_3^{-1}\sigma_2\sigma_4^{-1}\sigma_5\sigma_3^{-3}\sigma_4\sigma_5\sigma_4^3\sigma_5^4\sigma_3^{-2}\sigma_2\sigma_3\underline{\sigma_1}\sigma_2^3\\ &\quad\sigma_4^{-1}\sigma_3\sigma_4^2\sigma_3\sigma_2\underline{\sigma_1}\sigma_5^{-1}\sigma_4^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_4^{-1}\sigma_3^{-1}\sigma_2^{-1}\end{aligned}$$

where σ_1 occurs 8 times and σ_1^{-1} does not occur. So $\mathcal{P}_8(B_6)$ is false. ■

We shall not go further here for the upper bound. The rest of the paper deals with establishing lower bounds for the faithfulness of the Burau representation by proving that the properties $\mathcal{P}_k(B_n)$ and $\mathcal{P}_k^+(B_n)$ are true for certain (small) values of k and n.

Assume that A is a matrix. We use $c_j^i(A)$ to denote the i, j-component of A (i-th row, j-th column). Similarly we denote by $c^i(A)$ the i-th row of A, and by $c_j(A)$ the j-th column of A. We shall approach the properties $\mathcal{P}_k(B_n)$ and $\mathcal{P}_k^+(B_n)$ using the following

Lemma 5. *i) The property $\mathcal{P}_2^+(B_n)$ is true for every n.*

ii) If the property $\mathcal{P}_3^+(B_n)$ fails, then there exist braids β^+, β^- in B_{n-1} that satisfy

$$c_1^1(\rho(\beta^+)) = -t^{-1} + 2 - t, \qquad c_1^1(\rho(\beta^-)) = t - t^2.$$

iii) If the property $\mathcal{P}_4^+(B_n)$ fails, then there exist braids β, β' in B_{n-1} that satisfy

$$c_1^1(\rho(\beta)) - t^{-2}c_1^1(\rho(\beta')) = -t^{-1} + 2 - t.$$

Proof. The Burau image of a braid word with k occurrences of σ_1 and no occurrence of σ_1^{-1} has the form

$$M = s(M_0)\Sigma_1 s(M_1)\Sigma_1 \ldots s(M_{k-1})\Sigma_1 s(M_k).$$

We use the facts that $c^1(s(A)B)$ is always equal to $c^1(B)$ and that $c^1(A) = c^1(A')$ is equivalent to $c^1(AB) = c^1(A'B)$ provided that B is inversible, which the Burau matrices always are.

Consider M as above. If k is 1, the equality $c^1(M) = c^1(I)$ (where I is the identity matrix) is equivalent to

$$c^1(\Sigma_1) = c^1(s(M_1^{-1})) = c^1(I),$$

which is clearly false. If k is 2, $c^1(M) = c^1(I)$ becomes

$$c^1(\Sigma_1 s(M_1)) = c^1(\Sigma_1^{-1}),$$

which is also impossible since $c_1^1(\Sigma_1 s(M_1))$ is $1 - t$ while $c_1^1(\Sigma_1^{-1})$ is 0. If k is 3, $c^1(M) = c^1(I)$ becomes

$$c^1(\Sigma_1 s(M_1)\Sigma_1) = c^2(s(M_2^{-1})),$$

which develops into

$$\begin{cases} c_1^1(M_1) = -t^{-1} + 2 - t, & c_1^1(M_2^{-1}) = t - t^2, \\ tc_j^1(M_1) = c_j^1(M_2^{-1}) & \text{for } j \geq 2. \end{cases}$$

Finally if k is 4, $c^1(M) = c^1(I)$ becomes similarly

$$c^1(\Sigma_1 s(M_1)\Sigma_1 s(M_2)) = c^2(s(M_3^{-1})\Sigma_1^{-1}),$$

and the equality for the first components develops into

$$(1-t)^2 + tc_1^1(M_1) = t^{-1}c_1^1(M_3^{-1}). \blacksquare$$

At this point we are left with the question as to whether some particular Laurent polynomial, here the polynomials $-t^{-1}+2-t$ and $t-t^2$, henceforth denoted p_0^+ and p_0^-, may appear as the $1,1$-component of a Burau matrix, or as a given linear combination of such components. A few 'experimental' observations suggest a negative answer to the above questions, but, on the other hand, it is easily verified that the polynomials p_0^+ and p_0^- are the $1,2$-components of the Burau image of braids in B_3, which indicates that a rather precise argument is presumably needed. The subject of the next sections will be to establish some constraints about the components of these matrices, with a special interest in the 'critical' values p_0^+ and p_0^-.

2. The quadratic relations for the components of Burau matrices.

We consider the general question of describing the image of the Burau representation. In this section we establish quadratic relations that connect the components of the rows in a Burau matrix. This study is a development of the approach initiated by C. Squier in [16] and also used in [7] or [13].

The first observation is that one can restrict without loss of generality to the particular case of $1,1$-components and of first rows.

Lemma 1. *i) The Laurent polynomial p is a i,j-component in $\rho(B_n)$) if and only if the polynomial $t^{-j+1}p$ is a $1,1$-component in $\rho(B_n)$).*

ii) The sequence of Laurent polynomials $(p_1, \ldots, p_n)$ is a i-th row in $\rho(B_n)$ if and only if it is a first row in $\rho(B_n)$.

iii) The sequence of Laurent polynomials $(p_1, \ldots, p_n)$ is a j-th column in $\rho(B_n)$ if and only if the sequence $(t^{-j+1}p_1, \ldots, t^{-j+1}p_n)$ is a first column in $\rho(B_n)$ if and only if the sequence $(t^{-j+1}p_1, t^{-j+2}p_2, \ldots, t^{-j+n}p_n)$ is a first row in $\rho(B_n)$.

Proof. For every $n \times n$ matrix M and every i with $2 \leq i \leq n$, one has

$$c^i(\mathit{\Sigma}_{i-1}\ldots\mathit{\Sigma}_2\mathit{\Sigma}_1 M) = c^1(M),$$

which gives (ii). Similarly one has

$$c_j(M\mathit{\Sigma}_1\mathit{\Sigma}_2\ldots\mathit{\Sigma}_{j-1}) = t^{j-1}c_1(M),$$

which gives (i) and the first part of (iii). Then we observe that, if $\mathit{\Theta}$ is the mapping of $\mathrm{GL}(\infty, \mathbf{Z}[t, t^{-1}])$ into itself defined by

$$c^i_j(\mathit{\Theta}(M)) = t^{i-j}c^i_j(M),$$

then $\mathit{\Theta}$ is an automorphism which maps every $\mathit{\Sigma}_i$ to its transpose. It follows that every braid β satisfies the relation

$$\mathit{\Theta}(\rho(\beta)) = \rho(\beta^{\mathrm{rev}})^T,$$

where β^{rev} is the braid obtained from β by considering any representant of β and reversing the order of the generators (and M^T is the transpose of M). So the transposes of Burau matrices are exactly their images under $\mathit{\Theta}$, and this gives the last point in (iii). (Observe that the preceding relation implies, for any braid β, that the diagonal elements of the matrices $\rho(\beta)$ and $\rho(\beta^{\mathrm{rev}})$ are equal.) ■

By a similar easy argument we have

Lemma 2. *If the Laurent polynomial p is a $1,1$-component in $\rho(B_n)$, then the polynomial $t^{-1}p$ is a $1,1$-component in $\rho(B_{n+1})$.*

Proof. Immediate from the equality

$$c^1_1(\rho(\sigma_1^{-1}s(\beta)\sigma_1^{-1})) = t^{-1}c^1_1(\rho(\beta)). \ ■$$

Remark. The preceding result shows that one cannot hope to establish the criterion of Lemma 1.5.ii, *i.e.*, prove that the polynomials p_0^+ and p_0^- are forbidden as $1,1$-components of Burau matrices, by using a uniform specialization argument, at east when the roots of unity are concerned. For z a fixed complex number let ρ_z be the representation of braids obtained from ρ by taking $t = z$. We have mentioned that p_0^+ and

p_0^- belong to $c_2^1(\rho(B_3))$. Similarly $t^{-1}p_0^+$ and $t^{-1}p_0^-$ belong to $c_1^1(\rho(B_3))$. Now Lemma 2 implies that $t^{-k}p_0^+$ and $t^{-k}p_0^-$ belong to $c_1^1(\rho(B_{k+2}))$ for every positive k. So if ω_k is a k-th root of unity, the forbidden values $p_0^+(\omega_k)$ and $p_0^-(\omega_k)$ belong to $c_1^1(\rho_{\omega_k}(B_{k+2}))$. However the properties $\mathcal{P}_k(B_n)$ themselves certainly fail for certain such specializations since for instance the matrix $(\Sigma_1)^k$ is equivalent to the identity matrix *modulo* $t^k - (-1)^k$ and therefore the property $\mathcal{P}_k(B_2)_{t=-\omega_k}$ fails (where for z a fixed complex number $\mathcal{P}_k(B_n)_{t=z}$ denotes the statement similar to $\mathcal{P}_k(B_n)$ involving the representation ρ_z).

We shall now investigate more closely the relations satisfied by the components of a Burau matrix, and, more precisely, some quadratic relations. In the sequel we consider on the ring $\mathbf{Z}[t, t^{-1}]$ the (involutory) conjugacy endomorphism that maps t onto t^{-1}; the image of the polynomial p will be denoted $\overline{p}$. We shall use for that conjugacy some of the notations that are classical in the case of the complex numbers:

Notations. For any Laurent polynomial p, $|p|^2$ stands for $p\overline{p}$, and $2\mathfrak{Re}(p)$ for $p + \overline{p}$. Polynomials that coincide with their conjugate are said to be *real*. The conjugate-transpose of the matrix M is denoted by M^*.

It has been observed in [16] (in the essentially equivalent case of the 'reduced' Burau representation) that for the above notion of conjugacy the Burau matrices are unitary with respect to some Hermitian matrix, *i.e.*, that they satisfy the equality

$$AHA^* = H$$

for some fixed matrix H that does not depend on A. Once this fundamental intuition is acquired, it is actually very easy to systematically find all such matrices H.

Lemma 3. *The matrices H (with entries in $\mathbf{Z}[t, t^{-1}]$) such that the relation $AHA^* = H$ holds for every Burau matrix A are exactly the matrices $H_{q,r}$ defined by*

$$c_j^i(H_{q,r}) = \begin{cases} q & \text{for } i > j, \\ r & \text{for } i = j, \\ r[q] & \text{for } i < j, \end{cases}$$

where q, r are fixed Laurent polynomials and the bracket denotes the barycentric mean $r[q] = (1-t)r + tq$.

Proof. Successively considering the matrices Σ_1, Σ_2, $\ldots$ shows that the relations are necessary. That they are sufficient is then trivial. ■

The matrices $H_{q,r}$ are the $\mathbf{Z}[t, t^{-1}]$-linear combinations of the matrices

$$H_{1,1} = \begin{pmatrix} 1 & 1 & 1 & \cdots \\ 1 & 1 & 1 & \cdots \\ 1 & 1 & 1 & \cdots \\ \vdots & \vdots & \vdots & \end{pmatrix} \qquad H_{1,0} = \begin{pmatrix} 0 & t & t & \cdots \\ 1 & 0 & t & \cdots \\ 1 & 1 & 0 & \ddots \\ \vdots & \vdots & \ddots & \ddots \end{pmatrix}$$

Observe that the fact that the Burau matrices are unitary with respect to the rank 1 matrix $H_{1,1}$ is a consequence of the wellknown property that the sum of each row is 1. Using various possible matrices $H_{q,r}$ gives rise to different types of relations for the components of the Burau matrices. For instance we have the very simple

Proposition 4. *Assume that A is any $n \times n$ Burau matrix. Then the following relations hold between the 'corner' components of A and A^{-1}*

$$\begin{cases} c_1^1(A^{-1}) - 1 = t(\overline{c_1^1(A)} - 1), \qquad c_n^1(A^{-1}) = \overline{c_1^n(A)}, \\ c_1^n(A^{-1}) = \overline{c_n^1(A)}, \qquad c_n^n(A^{-1}) - 1 = t^{-1}(\overline{c_n^n(A)} - 1). \end{cases}$$

Proof. If H satisfies $AHA^* = H$ and is inversible, then A^{-1} is HA^*H^{-1}. Considering the case of $H_{0,1}$, which is upper triangular and certainly inversible, one obtains

$$c_1^1(A^{-1}) = c_1^1(HA^*H^{-1}) = \overline{c_1^1(A)} + (1-t)\overline{c_2^1(A)} + \ldots + (1-t)\overline{c_n^1(A)},$$

which gives the first formula using $c_1^1(A) + \ldots + c_n^1(A) = 1$. Similarly the $n, 1$-component of HA^*H^{-1} is $\overline{c_n^1(A)}$, which implies the third formula. The other two ones are proved in the same way using the matrix $H_{1-t^{-1},1}$, which is lower triangular. ■

Considering the matrix $H_{1-t^{-1},1}$ again we have also the following property, already stated in [13].

Proposition 5. *Assume that A is a Burau matrix and that the first row of A is trivial (i.e., is the first row of the identity matrix). Then the first column of A is trivial.*

The most interesting results appear when we consider matrices H that are Hermitian, *i.e.*, satisfy the equality $\overline{H} = H$. Again such matrices are easily described.

Lemma 6. *For every Laurent polynomial q there exists a unique Laurent polynomial $\widetilde{q}$ satisfying $\widetilde{q}[q] = \overline{q}$. Moreover $\widetilde{q}$ is real (i.e., is equal to its conjugate), and, if r is real, then $\widetilde{rq} = r\widetilde{q}$ holds for every q (and in particular $\widetilde{r} = r$ holds).*

Proof. Since $q(1)$ and $\overline{q}(1)$ are equal, the polynomial $1 - t$ has to divide $\overline{q} - tq$. Then $\widetilde{q}$, which is defined by

$$(1 - t)\widetilde{q} + tq = \overline{q}, \tag{1}$$

must be the corresponding quotient. This gives both existence and uniqueness. Applying conjugacy to (1) shows that $\overline{\widetilde{q}}$ satisfies $\overline{\widetilde{q}}[q] = \overline{q}$, which implies $\overline{\widetilde{q}} = \widetilde{q}$ by uniqueness. Similarly, if r is real, one deduces from (1) the equality

$$(1 - t)r\widetilde{q} + trq = \overline{rq},$$

which shows that $\widetilde{rq}$ is $r\widetilde{q}$. ■

Corollary 7. *The Hermitian matrices H such that the relation $AHA^* = H$ holds for every Burau matrix A are exactly the matrices $H_{q,\tilde{q}}$ where q is any Laurent polynomial.*

The fact that the Burau matrices are unitary with respect to the Hermitian matrices $H_{q,\tilde{q}}$ implies that the components of any row in such a matrix (and of any column as well by Lemma 1) have to satisfy some quadratic relation. A direct translation of the equality

$$AH_{q,\tilde{q}}A^* = H_{q,\tilde{q}}$$

shows that, if $(p_1, \ldots, p_n)$ is a row in an $n \times n$ Burau matrix, then the polynomials p_1, ..., p_n satisfy the equality

$$\sum_{i=1}^{n} \widetilde{q}|p_i|^2 + 2\mathfrak{Re}\Big(\sum_{1 \le j \le i \le n} q p_i \overline{p_j}\Big) = \widetilde{q}. \tag{$\mathcal{Q}_{n,0}(q)$}$$

This can be refined to

Proposition 8. *Assume that $(p_1, \ldots, p_n)$ belongs to $c^1(\rho(B_n))$. Then, for every k with $1 \le k \le n$, the polynomials p_1, …, p_{n-1} satisfy*

$$\sum_{i=1}^{n-k} \widetilde{q_k}|p_i|^2 + 2\mathfrak{Re}(\sum_{1\le j<i\le n-k} q_k p_i \overline{p_j}) - 2\mathfrak{Re}(\sum_{i=1}^{n-k} q_k p_i)$$
$$+ \sum_{j=n-k+1}^{n-1} \widetilde{q_{k-1}}\cdots\widetilde{q_{n-j+1}}|q_{n-j}|^2|F_{n-j,j}(p_1,\ldots,p_j)|^2 + \widetilde{\overline{q_k}} = 0 \quad (\mathcal{Q}_{n,k})$$

where the polynomials q_j are defined by

$$q_1 = 1+t, \qquad q_{j+1} = (t+\ldots+t^j)|q_j|^2,$$

and $F_{\ell,j}(p_1, \ldots, p_j)$ is $p_1 + \ldots + p_{j-1} + (1+\ldots+t^\ell)p_j - 1$.

Proof. We use the notations

$$S_\ell = \sum_{i=1}^{\ell} p_i, \quad Q_\ell = \sum_{i=1}^{\ell} |p_i|^2, \quad R_\ell = \sum_{1\le j<i\le \ell} p_i\overline{p_j}.$$

First one deduces $(\mathcal{Q}_{n,1})$ from $(\mathcal{Q}_{n,0}(t))$ by using the relation $S_n = 1$ to eliminate the variable p_n. The values

$$Q_n = 2Q_{n-1} + 2\mathfrak{Re}(R_{n-1}) - 2\mathfrak{Re}(S_{n-1}) + 1,$$
$$R_n = -Q_{n-1} - \overline{R_{n-1}} + \overline{S_{n-1}},$$

give the desired formula owing to the relation $\widetilde{q} + \widetilde{\overline{q}} = 2\mathfrak{Re}(q)$. The subsequent formulas correspond to a Gauss decomposition into squares for the quadratic form of p_1, …, p_{n-1} involved in $(\mathcal{Q}_{n,1})$. Assume for an induction that $(\mathcal{Q}_{n,k})$ has been established. Isolating the terms involving p_{n-k} leads, after multiplying by the real polynomial $\widetilde{q_k}$, to the formula

$$(\widetilde{q_k}^2 - |q_k|^2)Q_{n-k-1} + 2\mathfrak{Re}((q_k\widetilde{q_k} - |q_k|^2)R_{n-k-1})$$
$$-2\mathfrak{Re}((q_k\widetilde{q_k} - |q_k|^2)S_{n-k-1}) + |P|^2$$
$$+ \sum_{j=n-k+1}^{n-1} \widetilde{q_k}\widetilde{q_{k-1}}\cdots\widetilde{q_{n-j+1}}|q_{n-j}|^2|F_{n-j,j}(p_1,\ldots,p_j)|^2 + \widetilde{q_k}\widetilde{\overline{q_k}} - |q_k|^2 = 0,$$

where P is

$$\overline{q_k}p_1 + \ldots + \overline{q_k}p_{n-k-1} + \widetilde{q_k}p_{n-k} - \overline{q_k}.$$

This is $(\mathcal{Q}_{n,k+1})$ *modulo* the following

Claim. *The polynomials q_k satisfy the relations*

$$(i)\ q_k = t^k\overline{q_k}, \quad (ii)\ \widetilde{q_k} = (1+\ldots+t^k)\overline{q_k}, \quad (iii)\ q_{k+1} = q_k\widetilde{q_k} - |q_k|^2,$$
$$(iv)\ \widetilde{q_{k+1}} = \widetilde{q_k}^{\,2} - |q_k|^2, \quad (v)\ \widetilde{\overline{q_{k+1}}} = \widetilde{q_k}\widetilde{\overline{q_k}} - |q_k|^2.$$

These relations are proved inductively on $k \geq 1$. First (i) for $k=1$ is obvious. Now (i) for k implies

$$(1-t)(1+\ldots+t^k)\overline{q_k} + tq_k = \overline{q_k} - t^{k+1}\overline{q_k} + tq_k = \overline{q_k},$$

which gives (ii) by uniqueness of $\widetilde{q_k}$. Then one has

$$q_{k+1} = (t+\ldots+t^k)|q_k|^2 = (1+\ldots+t^k)\overline{q_k}q_k - |q_k|^2 = q_k\widetilde{q_k} - |q_k|^2,$$

which gives (iii). Then (iv) follows using Lemma 6, and (v) follows from (iii), (iv) and the general relation $\widetilde{\overline{q}} = 2\mathfrak{Re}(q) - \widetilde{q}$. Finally it is obvious that (iii) for k implies (i) for $k+1$. So the proof is complete. ■

Remarks. i) While different polynomials q can give non equivalent relations $\mathcal{Q}_{n,0}(q)$, there is only one (nontrivial) relation $\mathcal{Q}_{n,k}$ for every positive k. Indeed starting with $\mathcal{Q}_{n,0}(q)$ instead of $\mathcal{Q}_{n,0}(t)$ in the proof above amounts to replace $q_1 = 1+t$ by $q_1 = \widetilde{q} - \overline{q}$ and then to use the same induction formulas. Now the polynomial $1+t$ always divides $\widetilde{q} - \overline{q}$ (because $q(-1)$ is real for any q in $\mathbf{Z}[t,t^{-1}]$ and $\widetilde{q}(-1) = q(-1)$ follows from the defining equality of $\widetilde{q}$). It follows that the equality $\mathcal{Q}_{n,k}(q)$ obtained from q is a multiple of the equality $\mathcal{Q}_{n,k} = \mathcal{Q}_{n,k}(t)$.

If one introduces (as in [16]) a new variable s satisfying $s^2 = t$, then the initial choice $q = s$ leads to $q_1 = s$, a sort of 'minimal' value. This choice would not simplify significantly the formulas used here.

ii) If the decomposition into squares is made from $\mathcal{Q}_{n,0}$ rather than from $\mathcal{Q}_{n,1}$, *i.e.*, if one renounces to use the relation $S_n = 1$ at the beginning of the induction, one obtains similar quadratic relations, but they are less precise and in particular less useful in the context of the subsequent sections.

The formulas of Proposition 8 give rise to *algebraic constraints* for the components of the Burau matrices. Let us consider the particular case of the Burau image of B_3. If (p_1, p_2, p_3) is a row in some element of $\rho(B_3)$, then the Laurent polynomials p_1 and p_2 have to verify the equalities $(\mathcal{Q}_{3,k})$ for $1 \leq k \leq 3$, and this in turn gives some necessary conditions for the possible values of p_1.

Proposition 9. *Assume that the Laurent polynomial p belongs to $c_1^1(\rho(B_3))$. Then the polynomial*

$$\Phi(p) = |tp+1|^2 - |tp+p|^2$$

has to be the square of the norm of some polynomial in $\mathbf{Z}[t,t^{-1}]$.

Proof. The explicit development of $(\mathcal{Q}_{3,2})$ is

$$\begin{aligned}|F_{1,2}(p_1,p_2)|^2 &= 1 + tp_1 + t^{-1}\overline{p_1} - (t^{-1}+1+t)|p_1|^2 \\ &= |tp_1+1|^2 - |tp_1+p_1|^2. \blacksquare\end{aligned}$$

We thus obtain an algorithm for finding which polynomials p_2, p_3 could possibly complete a given polynomial p_1 in order to form the first row of a matrix in $\rho(B_3)$:

i) factorize the polynomial $\Phi(p_1)$ in the (factorial) ring $\mathbf{Z}[t,t^{-1}]$ and find the possible values of $F_{1,2}(p_1,p_2)$ by grouping the factors of $\Phi(p_1)$ in pairs of the form $q\overline{q}$ and multiplying by a unit of $\mathbf{Z}[t,t^{-1}]$, *i.e.*, by a polynomial of the form $\pm t^k$;

ii) deduce possible values of p_2 by solving the equation $(1+t)p_2 = 1 - p_1 - q$, where q is one of the values found in step (i);

iii) for each possible pair (p_1,p_2), take $p_3 = 1 - p_1 - p_2$.

Example. Take $p_1 = t^{-1}$. Then $\Phi(p_1)$ is $(1-t)(\overline{1-t})$, and one obtains

$$(1+t)p_2 = 1 - t^{-1} \pm t^k(1-t),$$

which leads to the values

$$p_2 = \begin{cases} -t^{-1} + 2 - 2t + \ldots + 2(-1)^{k-1}t^{k-1} + (-1)^k t^k, & \text{with } k \geq 0, \\ -(-1)^k t^k - 2(-1)^{k+1}t^{k+1} - \ldots - 2t^{-2} + t^{-1}, & \text{with } k \leq -1. \end{cases}$$

One can verify that the latter values are actually obtained: they correspond to the braids $\sigma_1^{-2}\sigma_2^k$.

It is tempting to conjecture that the above constraints, together with the similar ones for the columns deduced using Lemma 1 and the linear relations

$$\begin{cases} c_1^i(A) + c_2^i(A) + c_3^i(A) = 1, \\ c_j^1(A) + tc_j^2(A) + t^2c_j^3(A) = t^j, \end{cases} \qquad (\mathcal{L}_3)$$

completely characterize the image of B_3 under the Burau representation. (Observe that, in the case of B_2, the linear relations $(\mathcal{L}_2)$ that are similar to $(\mathcal{L}_3)$ above entirely characterize the image $\rho(B_2)$ in $\mathrm{GL}(2,\mathbf{Z}[t,t^{-1}])$.)

3. Order constraints on the components of Burau matrices

Assume that the variable t involved in Burau representation is given a fixed complex value z with module 1. Then the conjugacy of Section 2 becomes the usual conjugacy of complex numbers, and, in particular, the value of $|q|^2$ at z is a *nonnegative* real number for every Laurent polynomial q. Then from the quadratic relations of Proposition 2.8 we deduce quadratic inequalities involving the components of the Burau matrices. Our main result in this direction is the following

Proposition 1. (see Figure 1) *Assume that θ is a nonzero real number, and let D_θ be the line from 1 to $-e^{2i\theta}$ in the real plane identified with $\mathbf{C}$. Let N be the maximal integer satisfying $(N–1)|\theta| < \pi$. For $1 \leq n \leq N$ let $z_{\theta,n}$ be the intersection of D_θ with the line from 0 to $e^{-(n-1)i\theta}$ (possibly the infinite point of D_θ), and let $\mathit{\Delta}_{\theta,n}$ be the closed domain of the plane that contains 0 and is limited by the circle that contains 1 and has center $z_{\theta,n}$ (the line through 1 that is perpendicular to D_θ if $z_{\theta,n}$ is at infinity).*

Then if the Laurent polynomial p is the $1,1$-component of the Burau image of a n strand braid with $n \leq N$, the value $p(e^{2i\theta})$ lies in the domain $\mathit{\Delta}_{\theta,n}$.

Proof. Let us assume that $(p_1, \ldots, p_n)$ is a row in the Burau image of an n strand braid. Then the polynomials p_1, …, p_{n-1} satisfy the relation $(\mathcal{Q}_{n,n})$ of Proposition 2.8. This relation has the form

$$\begin{aligned}|q_{n-1}|^2|F_{n-1,1}(p_1)|^2 + \widetilde{q_{n-1}}|q_{n-2}|^2|F_{n-2,2}(p_1,p_2)|^2 + \ldots \\ +\widetilde{q_{n-1}}\ldots\widetilde{q_2}|q_1|^2|F_{1,n-1}(p_1,\ldots,p_{n-1})|^2 + \widetilde{\widetilde{q_n}} = 0 \qquad (1)\end{aligned}$$

When the variable t is given a complex value of module 1, say $e^{2i\theta}$, relation (1) becomes a relation between ordinary modules of complex numbers. So if the real numbers $\widetilde{q_2}(e^{2i\theta})$, …, $\widetilde{q_{n-1}}(e^{2i\theta})$ happen to be all positive, we deduce an order constraint for the value $p_1(e^{2i\theta})$.

Claim. *Assume $0 < |2\theta| \leq \pi$. Then the inequalities*

$$\widetilde{q_2}(e^{2i\theta}) \geq 0, \quad \ldots \quad , \widetilde{q_{n-2}}(e^{2i\theta}) \geq 0$$

hold exactly for $|\theta| \leq \pi/(n-1)$. In this case $q_{n-1}(e^{2i\theta})$ is not 0, and $\widetilde{q_{n-1}}(e^{2i\theta})$ is positive, null or negative respectively for $|\theta| < \pi/n$, $|\theta| = \pi/n$ and $|\theta| > \pi/n$.

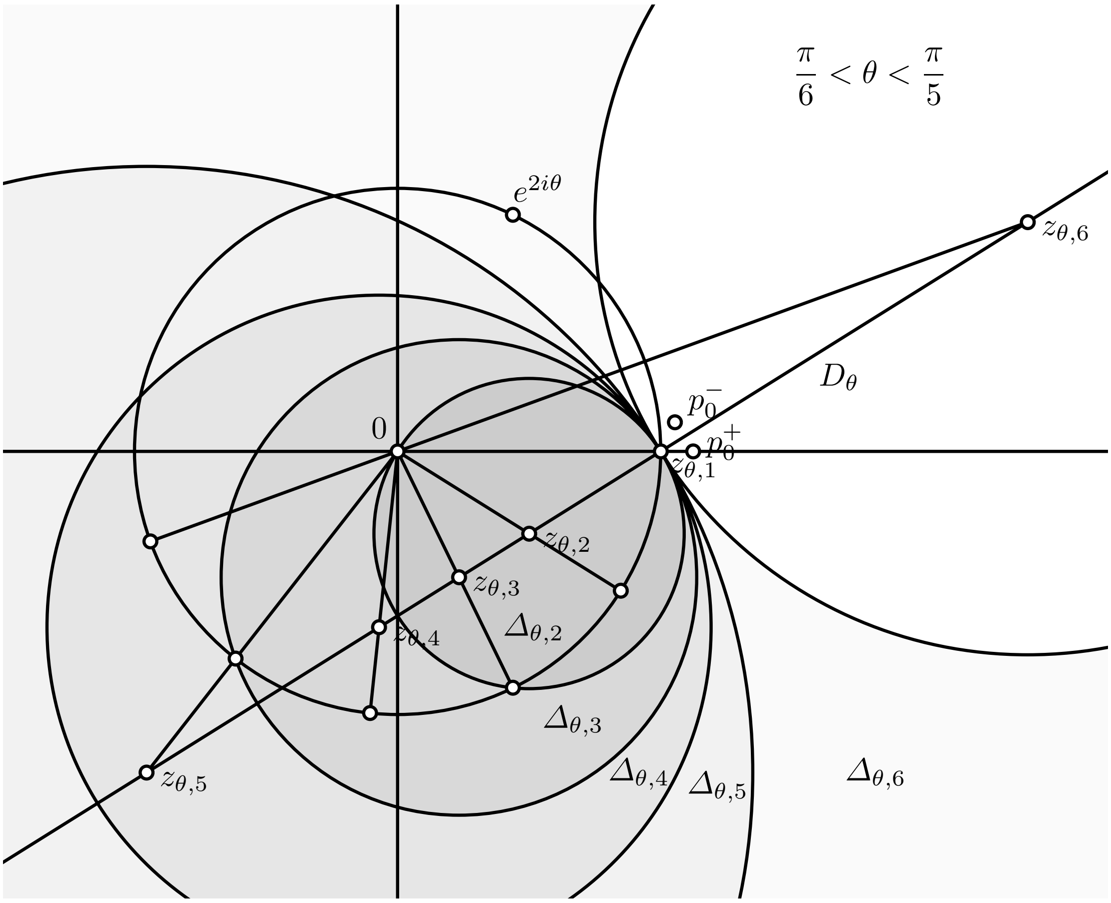


Figure 1

Indeed let μ_1, μ_2, … be the real numbers inductively defined by

$$\mu_1 = \frac{\sin 2\theta}{\sin\theta}, \quad \mu_{k+1} = \frac{\sin k\theta}{\sin\theta}\mu_k^2.$$

Then the formulas

$$q_k(e^{2i\theta}) = \mu_k e^{ki\theta}\ , \quad \widetilde{q_k}(e^{2i\theta}) = \frac{\sin(k+1)\theta}{\sin\theta}\mu_k$$

are easily proved using the inductive definition of the polynomials q_k, and formula (ii) of the Claim in the proof of 2.8. The sign inequalities then follow inductively on $n \geq 3$ using the equalities

$$\begin{aligned} q_k(e^{2i\theta}) &= \frac{\sin(k-1)\theta}{\sin\theta}\mu_{k-1}^2 e^{ki\theta} \\ \widetilde{q_k}(e^{2i\theta}) &= \sin(k+1)\theta\sin(k-1)\theta\mu_{k-1}^2/\sin^2\theta. \end{aligned}$$

This establishes the Claim. At this point three cases are to be distinguished.

Case 1. The absolute value of θ is below π/n.

Then the numbers $\widetilde{q_2}(e^{2i\theta})$, …, $\widetilde{q_{n-1}}(e^{2i\theta})$ are positive, and relation $(\mathcal{Q}_{n,n})$ implies

$$|q_{n-1}(e^{2i\theta})|^2|F_{n-1,1}(p_1)(e^{2i\theta})|^2 \leq -\widetilde{\widetilde{q_n}}(e^{2i\theta}),$$

which develops into

$$\frac{\sin n\theta}{\sin\theta}(|p_1(e^{2i\theta})|^2 - 1) - 2\mathfrak{Re}(e^{(n-1)i\theta}(p_1(e^{2i\theta}) - 1)) \leq 0. \tag{2}$$

This shows that the complex number $p_1(e^{2i\theta})$ has to lie in the interior of a circular disk. One reads on (2) that the point 1 belongs to the frontier circle of that disk, and that the center is the point $z_{\theta,n}$ given by

$$z_{\theta,n} = \frac{\sin\theta}{\sin n\theta}e^{-(n-1)i\theta} \tag{3}$$

We observe that (3) implies

$$1 - z_{\theta,n} = \frac{\sin(n-1)\theta}{\sin n\theta}e^{i\theta}, \tag{4}$$

which shows that $z_{\theta,n}$ lies on the line from 1 to $-e^{2i\theta}$.

Case 2. The absolute value of θ is between π/n and $\pi/(n-1)$.

This case is similar, excepted that the value $\widetilde{q_{n-1}}(e^{2i\theta})$ is negative. So relation $(\mathcal{Q}_{n,n})$ gives rise to the same inequality as (2) above, but with $\geq$ instead of $\leq$. The sequel of the computation is identical, and we conclude that $p_1(e^{2i\theta})$ has to lie in the exterior of the circle that contains the point 1 and whose center $z_{\theta,n}$ is still determined by equations (3) and (4).

Case 3. The absolute value of θ is exactly π/n.

In this case all coefficients in the relation $(\mathcal{Q}_{n,n})$ vanish. But appealing to $(\mathcal{Q}_{n,n-1})$ yields the relation

$$\begin{aligned} -2\mathfrak{Re}(q_{n-1}p_1) + |q_{n-2}|^2|F_{n-2,2}(p_1,p_2)|^2 + \ldots \\ +\widetilde{q_{n-2}}\ldots\widetilde{q_2}|q_1|^2|F_{1,n-1}(p_1,\ldots,p_{n-1})|^2 + \widetilde{q_{n-1}} = 0 \end{aligned}$$

which implies the inequality

$$-2\mathfrak{Re}(q_{n-1}p_1)(e^{2i\theta}) \leq -\widetilde{q_{n-1}}(e^{2i\theta}).$$

Owing to the value of θ, the latter one in turn develops to

$$\mathfrak{Re}(p_1(e^{2i\pi/n})) + \mathrm{cotan}\frac{\pi}{n}\,\mathfrak{Im}(p_1(e^{2i\pi/n})) \leq 1. \tag{5}$$

This shows that the point $p_1(e^{2i\pi/n})$ belongs to the half-plane containing 0 and limited by the line from 1 to $e^{2i\pi/n}$. This result is clearly the limit of the results for cases 1 and 2 when the point $z_{\theta,n}$ goes to infinity on the line from 1 to $-e^{2i\theta}$. This completes the proof of Proposition 1. ■

Figure 1 illustrates the results when θ is chosen (strictly) between $\pi/6$ and $\pi/5$. The circles that limit the domains $\varDelta_{\theta,n}$ belong to a common linear family, and, of course, the sequence $\varDelta_{\theta,2}$, $\varDelta_{\theta,3}$, *etc.* is increasing with respect to inclusion. For the degenerate case of B_1, the result is still true if $\rho(B_1)$ is defined as the size 1 identity matrix and the domain $\varDelta_{\theta,1}$ as the closed disk with center $z_{\theta,1}$ and radius 0.

Remark. The line D_θ is a symmetry axis for the figure, and therefore each domain $\varDelta_{\theta,n}$ is invariant under the corresponding orthogonal symmetry, which is the mapping $z \mapsto 1 + e^{2i\theta}(\overline{z} - 1)$: observe that by Proposition 2.4 this is precisely the transformation that maps $c_1^1(A)$ to $c_1^1(A^{-1})$ for every Burau matrix.

In the case when the ring $\mathbf{Z}[e^{2i\theta}]$ is a discrete lattice of the plane, the inclusions established above imply finiteness results for the corresponding images of the braid groups. We use as above $\rho_z(B_n)$ to denote the group of all matrices obtained by giving the value z to the variable t in the Burau representation of B_n. One obtains the following results (which give a complete description for the classes *modulo* t^2+1 or t^3+1 of the Burau coefficients for B_3 and B_5 respectively)

Corollary 1. *The groups $\rho_i(B_3)$ and $\rho_{\omega_6}(B_5)$ are finite, where i^2 is -1 and ω_6 is a 6-th primitive root of unity.*

Proof. The intersection of the bounded domain $\mathit{\Delta}_{\pi/4,3}$ with the lattice $\mathbf{Z}[i]$ has exactlty 9 points. So there are at most 9 elements in $c_1^1(\rho_i(B_3))$. By Lemma 1 there are similarly at most 9 values for each component of a matrix in $\rho_i(B_3)$, and therefore there are at most 9^9 such matrices. By the linear relations $(\mathcal{L}_3)$ of Section 2, this bound may be lowered to 9^4 elements. Actually the exact values are 9 elements in $c_1^1(\rho_i(B_3))$, 24 elements in $c^1(\rho_i(B_3))$ and 96 elements in $\rho_i(B_3)$. The argument is similar for $\rho_{\omega_6}(B_5)$: the intersection of $\mathit{\Delta}_{\pi/6,5}$ with the lattice $\mathbf{Z}[\omega_6]$ has 13 elements. (One can note that the inclusions thus established are optimal: each element of $\mathit{\Delta}_{\pi/4,3} \cap \mathbf{Z}[i]$ is the $1,1$-component of a matrix in $\rho_i(B_3)$, and similarly each element of $\mathit{\Delta}_{\pi/6,n} \cap \mathbf{Z}[\omega_6]$ is the $1,1$-component of a matrix in $\rho_{\omega_6}(B_n)$ for $2 \leq n \leq 5$. In the limit case of half-planes, $\rho_i(B_4)$ is infinite and seems to fill the half-plane $\mathit{\Delta}_{\pi/4,4}$, but we have no proof.) ■

The special cases where the quadratic relations degenerate to affine inequalities lead to very simple statements. By developing relation (5) above one obtains

Proposition 2. *If the Laurent polynomial $\sum a_k t^k$ is the $1,1$-component of the Burau image of some braid in B_n, then the integers a_k satisfy*

$$\sum_k \sin \frac{(2k+1)\pi}{n}\, a_k \leq sin\frac{\pi}{n}. \qquad (\mathcal{R}_n)$$

Corollary 3. *If the Laurent polynomial p is the $1,1$-component of Burau matrix (of any dimension), then its derivative p' satisfies $2p'(1) + p(1) \leq 1$, and therefore $p'(1)$ is negative.*

Proof. Letting n go to infinity (which is legitimate since there are only finitely many nonzero coefficients in a Laurent polynomial), we first deduce from Proposition 3 that, if $\sum a_k t^k$ belongs to $c_1^1(\rho(B_\infty))$, then the coefficients a_k satisfy

$$\sum_k (2k+1)a_k \leq 1.$$

Then we observe that the only components of the matrices in $\rho_1(B_\infty)$ are 0 and 1 (since these matrices are permutation matrices), and therefore the value of $\sum a_k$ is 0 or 1. This implies $\sum ka_k \le 1/2$, and therefore $p'(1)$ is negative (since it is an integer). ■

Let us come back to the general problem of describing the Burau matrices and not only their components. The constraints given in Proposition 1 for the $1,1$-components show that the set $\rho(B_n)$, viewed as a subset of $(\mathbf{R}[t,t^{-1}])^{n^2}$, is included in some *semi-algebraic set* of degree 2, *i.e.*, in some intersection of domains specified by quadratic inequalities. If we restrict to the linear relations as in Proposition 3, this semi-algebraic set becomes a polytope.

Proposition 4. *Let χ_n be the linear form on $\mathbf{Z}[t,t^{-1}]$ defined by*

$$\chi_n(t^k) = \sin\frac{(2k+1)\pi}{n} / \sin\frac{\pi}{n}.$$

Then the image of B_n under the Burau representation is included in the convex polytope

$$\bigcap_{\beta,\beta'\in B_n} \mathit{\Gamma}_n^{\beta,\beta'},$$

where $\mathit{\Gamma}_n^{\beta,\beta'}$ is the half-space of $(\mathbf{R}[t,t^{-1}])^{n^2}$ whose equation (with respect to the matrix variable A) is

$$\chi_n(c_1^1(\rho(\beta)A\rho(\beta'))) \le 1. \qquad (\mathcal{R}_n^{\beta,\beta'})$$

Proof. Proposition 3 exactly claims that $\rho(B_n)$ is included in $\mathit{\Gamma}_n^{1,1}$. Now for any braids β, β' in B_n, the matrix A belongs to $\rho(B_n)$ if and only if the matrix $\rho(\beta)A\rho(\beta')$ does. ■

Consider for example the case of B_4. One has

$$\chi_4(\sum_k a_k t^k) = \sum_k (-1)^k (a_{2k} + a_{2k+1}).$$

Write $\lceil p \rceil$ and $\lfloor p \rfloor$ for $\chi_4(p)$ and $\chi_4(tp)$ respectively. Then the relations $(\mathcal{R}_4^{\beta,\beta'})$ involve only linear combinations of the expressions $\lceil c_j^i(A) \rceil$ and

$\lfloor c^i_j(M)\rfloor$:

$$\begin{aligned}
(\mathcal{R}_4^{1,1}):&\quad \lceil c^1_1(A)\rceil \leq 1\\
(\mathcal{R}_4^{1,\sigma_1}):&\quad \lceil c^1_1(A)\rceil - \lfloor c^1_1(A)\rfloor + \lceil c^1_2(A)\rceil \leq 1\\
(\mathcal{R}_4^{\sigma_1,1}):&\quad \lceil c^1_1(A)\rceil - \lfloor c^1_1(A)\rfloor + \lfloor c^2_1(A)\rfloor \leq 1\\
(\mathcal{R}_4^{1,\sigma_1^{-1}}):&\ -\lfloor c^1_2(A)\rfloor \leq 1,\\
(\mathcal{R}_4^{\sigma_1^{-1},1}):&\quad \lceil c^2_1(A)\rceil \leq 1, etc.
\end{aligned}$$

Thus all above inequalities hold for any matrix A in the Burau image of B_4.

1. Weak faithfulness properties

We now come back to the statements $\mathcal{P}_k(B_n)$ and $\mathcal{P}^+_k(B_n)$ introduced in Section 1. The constraints established in Sections 2 and 3 enable us to prove some of these partial faithfulness properties of the Burau representation.

In the case $n = 3$, the point is that ρ is faithful and the Burau image of B_2 is completely known.

Proposition 1. *The property $\mathcal{P}^+_k(B_3)$ is true for every k.*

Proof. That $\mathcal{P}_k(B_3)$ is always true is trivial for one knows after [14] that ρ is injective on B_3: it then suffices to appeal to Theorem 1.1, which claims that a braid that admits a decomposition where σ_1 occurs and σ_1^{-1} does not cannot be trivial. For the stronger property $\mathcal{P}^+_k(B_3)$, assume that the matrix A is $\rho(\beta)$ for some 3 strand braid β and that the first row of A is trivial. By Proposition 2.5 the first column of A is trivial as well, so A is $s(B)$ for some 2×2 matrix B. Now A satisfies the linear relations $(\mathcal{L}_3)$ introduced at the end of Section 2, so B satisfies the relations $(\mathcal{L}_2)$ and, therefore, B belongs to $\rho(B_2)$, *i.e.*, is $\rho(\sigma_1^k)$ for some k. It follows that $\rho(\beta\sigma_2^{-k})$ is the identity matrix, and therefore that β is equal to σ_2^k by injectivity of ρ on B_3. ■

We turn to the case $k = 3$. Then we try to apply the condition given by Lemma 1.5, *i.e.*, to prove that the particular polynomials p_0^+ $(= -t^{-1} + 2 - t)$ and p_0^- $(= t - t^2)$ cannot be the $1,1$-components of Burau matrices. (Observe that Proposition 2.5 shows that $c_1^1(A) = p_0^+$ is equivalent to $c_1^1(A^{-1}) = p_0^-$ for any Burau matrix A, and therefore the problem is symmetric.) The algebraic approach of the end of Section 2 gives

Proposition 2. *The property $\mathcal{P}_3^+(B_4)$ is true.*

Proof. Apply Proposition 2.9. One obtains

$$\varPhi(p_0^-) = -t^{-3} + 2t^{-2} - t^{-1} + 1 - t + 2t - t^3,$$

and this Laurent polynomial is irreducible in $\mathbf{Z}[t, t^{-1}]$ (since the polynomial $t^3\varPhi(p_0^-)$ is irreducible over $\mathbf{Z}[t]$). So it is certainly not equal to $q\overline{q}$ for any polynomial q. ■

The order constraints of Section 3 enable to strengthen this result.

Proposition 3. *The property $\mathcal{P}_3^+(B_n)$ is true for $n \leq 7$, i.e., if a braid β admits in B_7 a decomposition with at most three σ_1 and no σ_1^{-1}, then the Burau matrix of β has a nontrivial first row (and a nontrivial first column).*

Proof. (see Figure 1) Consider an angle θ (strictly) between $\pi/6$ and $\pi/5$. The value $p_0^+(e^{2i\theta})$ is $4\sin^2\theta$, which increases from 1 to 1.382 when θ increases from $\pi/6$ to $\pi/5$. On the other hand the intersection of $\varDelta_{\theta,6}$ with the real axis is the complement of the interval $(1, 1+2\sin 5\theta \cos\theta / \sin 6\theta)$. In order to make sure that $p_0^+(e^{2i\theta})$ lies outside $\varDelta_{\theta,6}$ is suffices to have

$$4\sin^2\theta < 1 + 2\frac{\sin 5\theta}{\sin 6\theta}\cos\theta.$$

This is certainly true for $\theta \leq 34^o$ (Figure 1 corresponds to $\theta = 32^o$). So for such an argument θ, it is impossible that $p_0^+(e^{2i\theta})$ belongs to $c_1^1(\rho_{e^{2i\theta}}(B_6))$, and therefore the property $\mathcal{P}_3^+(B_7)_{t=e^{2i\theta}}$ is true, which in turn implies $\mathcal{P}_3^+(B_7)$. ■

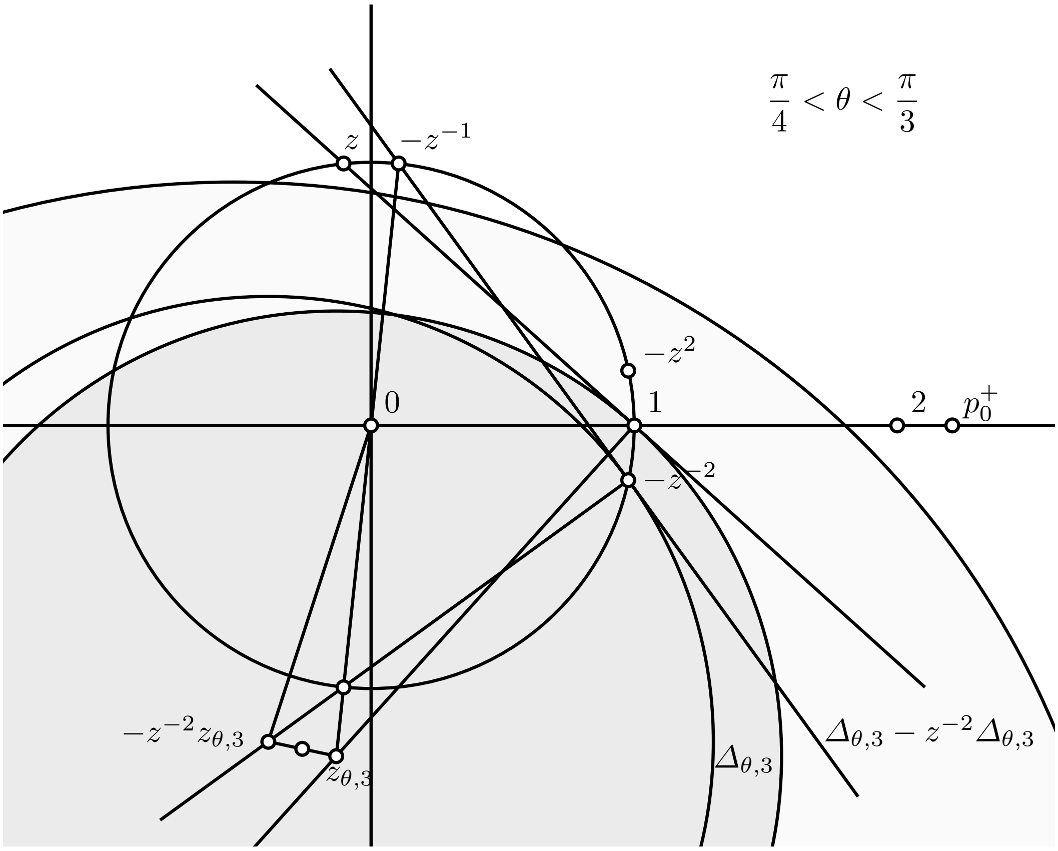


Figure 2

Similarly we have

Proposition 4. *The property $\mathcal{P}_4^+(B_4)$ is true, i.e., if a braid β admits in B_4 a decomposition with at most four σ_1 and no σ_1^{-1}, then the Burau matrix of β has a nontrivial first row (and a nontrivial first column).*

Proof. (see Figure 2) Choose θ between $\pi/4$ and $\pi/3$. We claim that $\mathcal{P}_4^+(B_4)_{t=e^{2i\theta}}$ is true. Write z for $e^{2i\theta}$. By Lemma 1.5.iii it suffices to show that the point $p_0^+(z)$ cannot belong to the domain $\Delta_{\theta,3} - z^{-2}\Delta_{\theta,3}$. Now $p_0^+(z)$ is strictly greater than 2, and it suffices to prove that the intersection of the above domain with the real axis lies of the left of the point 2. So it is enough to show

$$d(2, z_{\theta,3} - z^{-2} z_{\theta,3}) \geq 2R, \tag{1}$$

where $d(z, z')$ denotes the distance of the points z and z' and R is the radius of $\mathit{\Delta}_{\theta,3}$. Now the domain $\mathit{\Delta}_{\theta,3}$ always lies on the left of the line from 1 to z, while, for the present choice of θ, the point $-z^2$ lies on the right of this line, so one certainly has

$$d(-z^2, z_{\theta,3}) \geq R,$$

which implies

$$d(1, -z^{-2} z_{\theta,3}) \geq R,$$

and, because $d(1, z_{\theta,3})$ is R,

$$d(1, (z_{\theta,3} - z^{-2} z_{\theta,3})/2) \geq R.$$

By an homothety we obtain (1). ■

We see that the above method fails for larger dimensions because the forbidden value $p_0^+(e^{2i\theta})$ enters the domain in which we know the coefficients have to lie. Of course this does not give any indication that the forbidden values are actually reached. For instance in the case $\theta = \pi/10$ the value $p_0^+(e^{2i\theta})$ belongs to $\mathit{\Delta}_{\theta,3}$ but not to $c_1^1(\rho_{e^{2i\theta}}(B_3))$ (which is finite with 27 elements), so that $\mathcal{P}_3^+(B_4)_{t=e^{i\pi/5}}$ is still true.

So at this point we have established that in the double scale of $\mathcal{P}_k(B_n)$'s the faithfulness degree of the Burau representation lies somewhere between the lower bounds $\mathcal{P}_3(B_7)$, $\mathcal{P}_4(B_4)$ and the upper bounds $\mathcal{P}_5(B_7)$, $\mathcal{P}_8(B_6)$ of Section 1.

It seems likely that both the lower and the upper bounds are not yet optimal, but we shall leave the task of filling the gap between these values open, and conclude the paper with some remarks about a family of particular Burau matrices. In [3] we have shown that the 'exotic' bracket product defined on B_∞ by

$$\beta[\beta'] = \beta s(\beta')\sigma_1 s(\beta)^{-1}$$

satisfies the left distributivity identity

$$x[y[z]] = x[y][x[z]],$$

and, what is more remarkable, that the closure of any singleton $\{\beta\}$ under this bracket in B_∞ happens to be a *free* left distributive algebra (with one generator). We shall in the sequel denote by $\mathfrak{b}$ the closure of $\{1\}$ in B_∞ under this bracket.

Because ρ is not faithful on B_∞, it is not clear that the bracket on braids induces a welldefined operation on Burau matrices. But a direct verification shows that the bracket defined on $\mathrm{GL}(\infty, \mathbf{Z}[t, t^{-1}])$ by

$$A[B] = As(B)\mathit{\Sigma}_1 s(A^{-1})$$

is left distributive (and left cancellative). Indeed the general condition for the above bracket to be left distributive is that the matrix $\mathit{\Sigma}_1$ satisfies

$$\mathit{\Sigma}_1 s(\mathit{\Sigma}_1)\mathit{\Sigma}_1 = s(\mathit{\Sigma}_1)\mathit{\Sigma}_1 s(\mathit{\Sigma}_1) \tag{1}$$

and, for any matrix M,

$$\mathit{\Sigma}_1 s^2(M) = s^2(M)\mathit{\Sigma}_1. \tag{2}$$

This is clearly true for the present value of $\mathit{\Sigma}_1$. (One can observe that the Burau matrix $\mathit{\Sigma}_1$ is essentially the only 2×2 matrix that satisfies the above requirements. The other ones are its images under some automorphisms or antiautomorphisms, and therefore the corresponding left distributive algebras are isomorphic.)

Let us consider the closure $\mathfrak{b}_t$ of the identity matrix under the above bracket. By construction $\mathfrak{b}_t$ is a left distributive algebra generated by the matrix I. The elements of $\mathfrak{b}_t$ will be called *special* Burau matrices. Simple special Burau matrices are for instance

$$I, \quad I[I] = \mathit{\Sigma}_1, \quad I[I][I] = \mathit{\Sigma}_1^2 \mathit{\Sigma}_2^{-1}, \quad I[I[I]] = \mathit{\Sigma}_2\mathit{\Sigma}_1, \quad \textit{etc.}$$

Applying the Burau representation to the braid decompositions in terms of the elements of $\mathfrak{b}$ obtained in [3] induces the following result

Proposition 5. *i) Every Burau matrix A admits a decomposition of the form*

$$A = \prod_{j=\infty}^{j=1} s^{j-1}(A_j^{-1}) \prod_{j=1}^{j=\infty} s^{j-1}(A'_j),$$

where A_1, A_2, ..., A'_1, A'_2, ... are special Burau matrices.

ii) Every positive Burau matrix A (i.e., any product of matrices $\mathit{\Sigma}_i$) admits a decomposition of the form

$$A = \prod_{j=1}^{j=\infty} s^{j-1}(A'_j),$$

where A'_1, A'_2, ... are special Burau matrices.

It is then a very natural question to ask if the restriction of the Burau representation to the subset $\mathfrak{b}$ of B_∞ is faithful or not, *i.e.*, if the left distributive algebra $\mathfrak{b}_t$ is free or not. By the criterion of [9], it is known that $\mathfrak{b}_t$ is a free left distributive algebra if and only if no equality of the form

$$A = A[C_1]...[C_k] \tag{3}$$

may hold in $\mathfrak{b}_t$ for any positive k. Developing $A^{-1}(A[C_1]...[C_k])$ in terms of A, C_1, ..., C_k shows that the conjunction of all properties $\mathcal{P}_k(B_n)$ would be a sufficient condition for forbidding (3). We know that this conjunction is certainly false for some k, but having no explicit description of the counterexamples to $\mathcal{P}_k(B_n)$ we cannot decide if these counterexamples have the special form needed for (3). Here we shall only establish the following partial result:

Proposition 6. *The mapping $c_1{\circ}\rho$ is not injective on the subset $\mathfrak{b}$ of B_∞.*

Proof. As for Proposition 5 we use the fact that every braid admits a decomposition in terms of the elements of $\mathfrak{b}$. More precisely, it is shown in [3] that, for every positive braid β in B_∞ (a braid that admits a decomposition where the inverses σ_i^{-1} do not occur), there exists a (unique) sequence β_1, β_2, ... of braids belonging to $\mathfrak{b}$ (and eventually equal to 1) such that β is equal to the product of β_1, $s(\beta_2)$, $s^2(\beta_3)$, *etc.* Assume that β, β' are two positive braids satisfying $\rho(\beta) = \rho(\beta')$, and consider the $\mathfrak{b}$-decompositions as above for β and β', say

$$\beta = \prod_{j=1}^{j=\infty} s^{j-1}(\beta_j), \qquad \beta' = \prod_{j=1}^{j=\infty} s^{j-1}(\beta'_j).$$

Then the first column of $\rho(\beta)$ is the first column of $\rho(\beta_1)$, and similarly the first column of $\rho(\beta')$ is the first column of $\rho(\beta'_1)$. If we assume that $c_1{\circ}\rho$ is injective on $\mathfrak{b}$, we conclude that β_1 and β'_1 are equal. Now the second column of $\rho(\beta_1^{-1}\beta)$ is the first column of $\rho(\beta_2)$, the second column of $\rho(\beta_1^{-1}\beta')$ is the first column of $\rho(\beta'_2)$ and, under the same assumption, we have that β_2 and β'_2 are equal. The argument goes on inductively, and finally β and β' are equal. In other words we have shown that ρ is injective on positive braids, which in turn implies that ρ is injective on B_∞ since every braid can be expressed as the quotient of two positive braids. This proves that the injectivity of $c_1{\circ}\rho$ on $\mathfrak{b}$ is a contradictory hypothesis. ∎

We can observe that a similar result for the first rows is trivial (and *not* equivalent): for instance the first rows of $I[I]$ and of $I[I[I]]$ are equal. Owing to Proposition 6 it seems rather unlikely that ρ be faithful on $\mathfrak{b}$. On the other hand the possible counterexamples have to be rather complicated (in particular because $\mathcal{P}_2(B_n)$ is always true). Even the presumably easier question of the unfaithfulness on $\mathfrak{b}$ of the specialization ρ_z of ρ obtained when t is given a fixed complex value z is open. By [2] it is known that ρ_1 is not faithful on $\mathfrak{b}$, but nothing is known even for ρ_{-1}. Observe that a faithfulness result for some representation ρ_z would imply that the question of deciding whether two given bracket words are equivalent or not up to left distributivity be solvable in polynomial time by evaluating the corresponding Burau matrices. (The freeness of $\mathfrak{b}_t$ itself would not give this result for the degree of the polynomials involved in the evaluation of a size n bracket word may increase as an exponential function of n.)

We conclude with an easy formula of linear algebra. There is a (trivial) left distributive algebra made by the natural numbers equipped with the bracket

$$x[y] = y + 1,$$

and 0 is a generator for this algebra. If $\mathfrak{b}_t$ is free (or ‘nearly’ free), the above algebra should be an homomorphic image of $\mathfrak{b}_t$. In other words, there should exist some mapping f from the Burau matrices to the positive integers verifying $f(A[B]) = f(B) + 1$. Actually there are (at least) two such functions. Trivially one has

$$\det(A[B]) = \det(B) \times t.$$

Now some properties of $\rho_1(\mathfrak{b})$ invite the consideration of the sum of the overdiagonal terms, and this leads to the following skew version of the invariance of the trace of a matrix under conjugacy

Proposition 7. *Let* $\mathrm{Tr}^+(M)$ *denote the sum of all components* $c^k_{k+1}(M)$*. Then for any square matrices* A*,* B *with* A *inversible, one has*

$$\mathrm{Tr}^+(As(B)\Sigma_1 s(A^{-1})) = \mathrm{Tr}^+(B) + t.$$

The verification is an undergraduate exercice once the formula is conjectured. It seems to be a much more difficult problem to define a bracket preserving homomorphism of $\mathfrak{b}_t$ (or even of $\mathfrak{b}$) into the finite left distributive algebras of size 2^n introduced in [10] from the theory of large cardinals.

References

[1] J. Birman, *Braids, links, and mapping class groups*, Annals of Math. Studies **82** Princeton Univ. Press (1975).

[2] P. Dehornoy, *Algebraic properties of the shift mapping*, Proc. Amer. Math. Soc. **106-3** (1989) 617–623.

[3] —, *Braid Groups and Left Distributive Operations*, Trans. Amer. Math. Soc **345-1** (1994) 115–151.

[4] —, *Non-commutative Versions of the Burau Representation*, C. R. Acad. Roy. Sci. Canada **17-1** (1995) 53–58.

[5] —, *From Large Cardinals to Braids via Distributive Algebra*, J. Knot Theory & Ramifications **4-1** (1995) 33–79.

[6] —, *A Fast Method for Comparing Braids*, preprint (1995).

[7] D. M. Goldschmidt, *Classical Link Invariants and the Burau Representation*, Pacific Journal of Math. **144-2** (1990) 277–292.

[8] D. Larue, *Left-Distributive and Left-Distributive Idempotent Algebras*, Ph D Thesis, University of Colorado, Boulder (1994);

[9] R. Laver, *The left distributive law and the freeness of an algebra of elementary embeddings*, Advances in Math. **91-2** (1992) 209–231;

[10] —, *On the algebra of elementary embeddings of a rank into itself*, Advances in Math. **110** (1995) 334–346.

[11] —, , Private communication (1993).

[12] D. Long, *On the linear representations of braid groups*, Trans. Amer. Math. Soc. **311** (1989) 535–561.

[13] D. Long & M. Paton, *The Burau representation is not faithful for $n \geq 6$*, Topology **32-2** (1993) 439–447.

[14] W. Magnus & A. Peluso, *On a theorem of V. I. Arnold*, Com. on Pure and Appl. Math. **XXII** (1969) 683–692.

[15] J. Moody, *The Burau representation of the group B_n is unfaithful for large n*, Bull. Americ. Math. Soc. **25-2** (1991) 379–384.

[16] C. Squier, *The Burau representation is unitary*, Proc. Amer. Math. Soc. **90-2** (1984) 199–202.

Mathématiques, Université, 14 032 Caen, France
dehornoy@geocub.greco-prog.fr