On the Burau representation modulo a small prime

D Cooper
D D Long

Abstract  We discuss techniques for analysing the structure of the group obtained by reducing the image of the Burau representation of the braid group modulo a prime. The main tools are a certain sesquilinear form rst introduced by Squier and consideration of the action of the group on a Euclidean building.

AMS Classification  20F36; 57M07 57M25

Keywords  Burau representation, braid group, Euclidean building, Squier form

1 Introduction

Despite the work of many authors, the group theoretic image of linear representations of the braid groups remains mysterious in most cases. The rst nontrivial example, the Burau representation is not at all well understood. This representation

\[ n: B_n \to \text{GL}(n-1; \mathbb{Z}[t;t^{-1}]) \]

is known not to be faithful for \( n \geq 6 \) ([5] and [6]) but the nature of the image group and in particular, a presentation for the image group has not been found. In [3], we simplified the problem by composing \( n \) with the map which reduces coefficients modulo 2. In this way, we were able to give a presentation for the image of the simplified representation \( 4 \otimes \mathbb{Z}_2 \). (Throughout this paper we use the notation \( \mathbb{Z}_p \) for the finite field with \( p \) elements.) Of course, the motivation for this approach comes from the classical problem of whether the representation \( 4 \) is faithful and to this end we pose the question:

Question 1.1 Is there any prime \( p \) for which the representation

\[ 4 \otimes \mathbb{Z}_p: B_4 \to \text{GL}(3; \mathbb{Z}_p[t; t^{-1}]) \]

is faithful?

Copyright Geometry and Topology
It is a consequence of some results of this note that the representation is not faithful in the case $p = 3$, (below we exhibit a braid word in the kernel) however the program for attacking the problem runs into difficulty at the final stage when $p = 5$. This case remains open and has some features which suggest it may be different to the first two primes.

In order to describe our approach, we recall that the group $GL(3; \mathbb{Z}_p[t; t^{-1}])$ acts on a certain contractible two dimensional simplicial complex, $\mathcal{K}$, which is a so-called Euclidean building (see [2]). This is defined by embedding $GL(3; \mathbb{Z}_p[t; t^{-1}]) \hookrightarrow GL(3; \mathbb{Z}_p(t))$ where $\mathbb{Z}_p(t)$ is the field of fractions of the ring $\mathbb{Z}_p[t; t^{-1}]$. This target group admits a discrete rank one valuation defined by $(p/q) = \deg(q) - \deg(p)$. A standard construction now yields the complex $\mathcal{K}$. We briefly outline how this building and action are defined, restricting our attention to the case $n = 4$, since this is the only case in which we shall subsequently be interested. This will serve the additional purpose of establishing notation. Standard properties imply that

$$O = f \times 2 \mathbb{Z}_p(t) \quad (x) \quad 0g$$

is a subring of $\mathbb{Z}_p(t)$, the valuation ring associated to $\mathcal{K}$. This is a local ring and the unique maximal ideal is easily seen to be $M = f \times 2 \mathbb{Z}_p(t) \quad (x) > 0g$, a principal ideal. Choose some generator for this ideal. This element is called a uniformizing parameter and by construction we have that $(\ ) = 1$. Since $M$ is maximal, the quotient $k = \mathbb{Z}_p(t)/M$ is a field, the residue class field. One sees easily that in this case, the residue class field is $\mathbb{Z}_p$.

Now let $V$ be the vector space $\mathbb{Z}_p(t)^3$. By a lattice in $V$ we shall mean an $O$-submodule, $L$, of the form $L = Ox_1 \oplus Ox_2 \oplus Ox_3$ where $f(x_1; x_2; x_3)g$ is some basis for $V$. Thus the columns of a non-singular $3 \times 3$ matrix with entries in $\mathbb{Z}_p(t)$ define a lattice. The standard lattice is the one corresponding to the identity matrix. We denote two lattices $L$ and $L^0$ to be equivalent, if for some $2 \mathbb{Z}_p(t)$ we have $L = L^0$. We denote equivalence class by $[L]$. The building $\mathcal{K}$ is defined as a flag complex in the following way. The points are equivalence classes of lattices, and $[L_0]; \ldots; [L_k]$ span a $k$-simplex (in our situation $k = 0; 1; 2$ are the only possibilities) and only if one can find representatives so that $L_0 \sim L_1 \sim \ldots \sim L_k \sim L_0$.

All $2$-simplices are of the form $[(x_1; x_2; x_3); (x_1; x_2; x_3); (x_1; x_2; x_3); (x_1; x_2; x_3)]g$; this is usually referred to as a chamber and denoted by $C$. Clearly the group $GL_3(\mathbb{Z}_p(t))$ acts on lattices and one sees easily that incidence is preserved, so that the group acts simplicially on $\mathcal{K}$. It is shown in [2] that this building...
is a so-called Euclidean building, in particular, it is contractible and can be equipped with a metric which makes it into a CAT(0) space and for which $\text{GL}_3(\mathbb{Z}p(t))$ acts as a group of isometries. The metric is such that each 2 dimensional simplex is isometric to a unit Euclidean equilateral triangle.

We now return to our situation. One of the difficulties of dealing with representations of braid groups is that it is extremely difficult to determine exactly which matrices are in the image. We bypass this by dealing with a group which contains $\text{im}(\phi \circ \mathbb{Z}_p)$. To define this group, we recall that it was shown by Squier [7] that the Burau representation is unitary in the sense that there is a matrix $J$ with the property that $A J A = J$ for all $A \in \text{im}(\phi)$. Here the involution $t \mapsto 1+t$ to the matrix group by $(a_{i,j}) = (a_{j,i})$, where $s^2 = t$.

We define the subgroup $\text{Isom}_J(\mathbb{Z}_p(t))$ to be those matrices with Laurent polynomial entries which are unitary for the form $J$. The advantage of dealing with this subgroup is that the condition that a matrix lies inside $\text{Isom}_J(\mathbb{Z}_p(t))$ is easily used.

The strategy now is to examine the action of $\text{Isom}_J(\mathbb{Z}_p(t))$ on $\mathbb{Z}_p(t)$ as a finite group. This is interesting in its own right. Moreover, the greater ease of dealing with this subgroup means that we are able to compute the complex $\phi \circ \text{Isom}_J(\mathbb{Z}_p(t))$ together with all vertex, edge and 2-simplex stabilisers. We then appeal to results of Haefliger [4] to compute a presentation for the group $\text{Isom}_J(\mathbb{Z}_p(t))$.

Now recall that homotheties act trivially on $\mathbb{Z}_p(t)$ so that the presentation for $\text{Isom}_J(\mathbb{Z}_p(t))$ is to be compared with the following presentation of $B_4 = \text{centre}(B_4)$:

**Lemma 1.2** The group $B_4 = \text{centre}(B_4)$ is presented as

$$\langle x, y | x^4 = y^3 = 1, [x^2, yxy] = 1 \rangle$$

where $x = 1 2 3$ and $y = x_1$.

This is presumably well known to the experts; it is derived in [3]. The starting point for this work is:

**Lemma 1.3** The group $\text{stab}_J(\phi)$ acts on $\mathbb{Z}_p(t)$ as a finite group.
**Sketch of proof** If \( A \) stabilizes \((I)\), then its action on \( J(I) \) is unchanged by homothety and it's easily seen that we can adjust any such \( A \) by applying \( t^k \) so that \( A \in SL(3;O) \). Rewriting the unitary condition as \( A = J(A^{-1})^{-1} A^{-1} \) and noting that \( J \in GL(3;O) \), we see that \( A \in SL(3;O) \). However the only matrices with Laurent polynomial entries for which \( A \) and \( A^{-1} \) have all entries valuing positively are the constant matrices.

Thus we have shown that the only such \( A \) have constant entries up to homothety. In particular, they are unchanged by setting \( t = 1 \), so that stabilizer \((I)\) can be regarded as a subgroup of the finite group \( GL(3;Z_p) \), completing the proof.

This has the immediate corollary:

**Corollary 1.4** For every vertex \( v \in \mathcal{B} \), \( J(v) \) is a finite group.

**Proof** The building \( \mathcal{B} \) is locally finite, in fact the link of every vertex is the flag manifold in the vector space \( Z_p^3 \). The stabilizer of any vertex acts on this set as a group of permutations, so by passing to a subgroup of finite index in \( J(v) \) we obtain a subgroup which acts as the identity on all vertices in the link. Since every vertex is connected to \( I \) by some chain of vertices, we see that for every \( v \), there is a subgroup of finite index which lies inside \( J(v) \), a finite group.

We now focus on the case \( p = 3 \). In this case one finds by calculation:

**Theorem 1.5** At the prime \( 3 \), group \( J(I) \) acts on \( Z_4 = \langle x \rangle \).

**Remark 1.6** For \( p = 2; 3; 5 \), the group \( J(I) \) acts as the cyclic group \( Z_4 \). For \( p = 7 \) it is cyclic of order 8 and for \( p = 11 \), cyclic of order 12.

One important difference between the case \( p = 2 \) and that of the larger primes is that it is one of the consequences of the results of [3] that \( Isom(\mathcal{B}(2)) = \text{im}(4 \otimes Z_2) \), this is not so for (at least some and conjecturally all) primes \( p \neq 3 \). In particular, for \( p = 3 \), we are able to construct (see below) an element \( u \in Isom(\mathcal{B}(3)) \) which has order 6; it is easy to see that this element does not lie in the subgroup \( \text{im}(4 \otimes Z_3) \). Its matrix is given by:

\[
0 \quad 2 + t + t^2 \quad 2 + t^2 \quad 2 + 2t + 2t^2 \\
2 + t \quad 2 + 2t^2 \quad 2 + t + 2t^2 \quad 2 + t + t^2 \quad A \\
2 + t \quad 2 + t \quad 2 + 2t
\]
However, having noted this difference, the qualitative picture of the quotient complex is very similar to the case $p = 2$; the complex consists of a compact piece coming from behaviour of groups close to the identity lattice, together with a single annular end. Application of Haefliger's methods yields the following group theoretic result:

**Theorem 1.7** When $p = 3$, the group $\text{Isom}_J(\ )$ is presented as:

Generators: $x; y; u$

Relations:

1. $x^4 = y^3 = u^6 = 1$
2. $[x^2; yxy] = 1$
3. $[x; u^{-1}x^{-1}y^{-1}xyxy] = 1$
4. $[yxy; u^{-1}x^{-1}y^{-1}xyxy] = 1$
5. $[xy; u^2] = 1$
6. $[x^2yx; u^3] = 1$
7. $(u^2x^2yx)^2 = (x^2yxu^2)^2$
8. Infinitely many other relations to do with nilpotence.

Of course the verification that these relations hold is a trivial matter of multiplying matrices modulo 3. We remark that the relations contained in (8) are explicitly known.

We claim that a computer application of the Reidemeister–Schröer algorithm contained in the computer program GAP applied to the presentation involving the first seven relations proves:

**Corollary 1.8** The index $[\text{Isom}_J(\ ) : hx; y]i$ is finite.

This index is a divisor of 162. The corollary already implies that $\text{im}(4 \otimes Z_3)$ is not faithful. One way to see this is that one sees easily (for example from the matrix representation) that the element $w = u^{-1}x^{-1}y^{-1}xyxy$ has in finite order. The presentation implies that it commutes with $x$. However, since $[\text{Isom}_J(\ ) : hx; y]$ is finite, some power of $w$ lies in the subgroup generated by $x$ and $y$ and this gives an unexpected element commuting with $x$. Alternatively, in the course of the proof, one discovers that $\text{Isom}_J(\ )$ contains arbitrarily large soluble subgroups and this can also be used to show that the representation is not faithful. In fact, one can be more specific: the computer can be used to...
give a presentation for the subgroup generated by $hx; yi$; one finds for example, that there is a relation (where $x = x^{-1}$ and $y = y^{-1}$):

Of course the fact that these are all group points is immediate and the fact that they are distance one from \( I \) is a calculation. The content of the lemma is that there are no more group points. This proved by noting that the lattice
\[
\begin{pmatrix}
0 & 1 \\
1 & 0 \\
\end{pmatrix}
\]

is in the link of the identity and is stabilised by the element \( u \). Thus it cannot be a group point as its stabiliser contains an element of order 6. The action of known group elements now accounts for all the other elements in \( \text{Link}(I) \).

We indicate briefly how one can construct any isometries which may exist in the stabiliser of \( M_{19} \), in particular, how one can find the element \( u \). This involves an elaboration of the method used in Lemma 1.3.

Suppose that \( g \in \text{Isom}_J(\ ) \) has \( g[M_{19}] = [M_{19}] \). The definition shows that this is the same as the existence of an element \( \in \text{GL}_3(\mathbb{O}) \) with \( g \cdot M_{19} = M_{19} \).

The form of the elements \( M_{19} \) and \( g \) means that \( g \) has Laurent polynomial entries. Then
\[
(M_{19}, M_{19}) = (M_{19} \cdot J ; M_{19} \cdot J) = (g \cdot M_{19} \cdot J ; g \cdot M_{19} \cdot J) = M_{19} \cdot J ; M_{19}
\]
since \( g \) is an isometry. It follows that \( g \) is an isometry of the form \( M_{19} \cdot J ; M_{19} \) and although unlike Lemma 1.3, this form does not have its matrix lying in \( \text{GL}_3(\mathbb{O}) \), we have a bound on the valuations of its entries, so that exactly as in the lemma, we have a bound on the valuations possible for the entries of \( g \). Since we are dealing with a finite field, it follows that there are only a finite number of possibilities for the entries of \( g \) and one can check by direct enumeration which of these make \( M_{19} \cdot J ; M_{19}^{-1} \) into a \( J \)-isometry. (In fact sharper, more practical methods exist, but this would take us too far afield.)

We now give some indication of how one can give complete descriptions of all vertex stabilisers. The idea is to work outwards from the identity; it turns out that we need no more elements than those we have already introduced.

Recalling the notation defined above, a calculation shows that that action of \( u \) on its link is given by the permutation
\[
(7)(11)(18)(23)(3,13)(6,8)(14,24,26)(17,21,20)
(1,5,12,22,19,10)(4,16,25,15,2,9)
\]

where \( x \) is shorthand for \( M_{19} \cdot x \). The two six cycles consist of 12 group points, \( (I = 2) \), there are 14 points in the orbit of \( M_{19} \) and two remaining, as yet

---

*Geometry and Topology Monographs, Volume 1 (1998)*
unidentified points, 7 and 11. Points in the orbit of \( M_{19} \) we refer to as \( n \) points. Observe that neither of the unidentified points can be group points as they contain an element of order 6 in their stabiliser.

Using this information we now show:

**Lemma 2.2** The group \( \text{stab}_J(M_{19}) \) acts on \( \text{Link}(M_{19}) \) as a finite group \( \mathbb{Z}_6 = \langle u \rangle \).

**Sketch of Proof** First consider the map \( i_0: \text{stab}_J(M_{19}) \to \text{Aut}(\text{Link}(M_{19})) \). We begin by noting that this map is injective, for any element of the kernel must fix every vertex in \( \text{Link}(M_{19}) \), in particular the vertex \( I \), so that the kernel can only consist of powers of the element \( x \). However, one checks that no element of the group \( \langle x \rangle \) other than the identity fixes \( M_{19} \) proving the assertion.

We refer to the above permutation, where we recall the vertex 2 is the identity vertex. Pick an element \( \gamma \) in \( \text{stab}_J(M_{19}) \); it is type-preserving so that it must map the group points in \( \text{Link}(M_{19}) \) which correspond to lines back to lines, and those which correspond to planes to planes. Since \( u \) acts transitively on this orbit, we can find some power of \( u \) so that \( u^k: \gamma \) fixes the vertex 2. Now exactly as in the previous paragraph, we deduce that \( u^k: \gamma = 1 \), so that \( \gamma \) is a power of \( u \) as required.

We now analyse the two new points 7 and 11. We have already shown that these are not group points; we now show that they are not \( n \) points.

Firstly, one finds that \( xxyx(7) = 11 \), so that this is only one orbit of point and moreover that \( u \) acts as an element of order two on \( \text{Link}(7) \). Moreover, we can construct a potentially new element in \( \text{stab}_J(7) \) namely \( u_1 = (xxyx)^{-1}:u:xxxy \). A calculation reveals that the action of the group \( \langle u; u_1 \rangle \) on \( \text{Link}(7) \) is the dihedral group \( D_3 \). It now follows from 1.5 and 2.2 that the orbit of 7 is distinct from that of the group and \( n \) points.

In fact, the stabiliser is larger than this and one finds that there is an element \( h \) of order 3 which commutes with this dihedral group.

\[
0 \
1 + t^4 \
1 + t^2 + t^4 \
1 + t + 2t^2 + 2t^3 \
1 + t + 2t^3 + t^4 \
2 + 2t + t^2 + t^3 \
2t + 2t^2 + 2t^3 \
2t^2 + 2t^3 + 2t^4 \
0 \
0 \
2 \t^2
\]

We omit the arguments which identify the stabilisers of these two points, as this is slightly special, however the results are that one shows successively:

**Lemma 2.3** The map \( i_1: \text{stab}_J(7) \to \text{Aut}(\text{Link}(7)) \) has \( \text{im}(i_1) = \mathbb{Z}_3 \times D_3 \).

*Geometry and Topology Monographs, Volume 1 (1998)*
Theorem 2.4 The group $\text{stab}(7)$ has order 54 with structure given by the nonsplit central extension:

$$1! \big\langle h \big| Z_3 \big\rangle \big\langle Z_3 \big\rangle \big\langle D_3 \big| 1 \big\rangle$$

The orbit type for the action of $\text{stab}(7)$ acting on its stabiliser is $9; 9; 3; 3; 1; 1$, where the orbits of size 9 are points, the orbits of size 3 are of type 7 and there are two points as yet unaccounted for, namely $M_{19} : M_7 : M_7$ and $M_{19} : M_7 : M_{11}$ for which we adopt the notational shorthand $7^{(2)}$ and $11^{(2)}$. As above, $\text{xyx}(7^{(2)}) = 11^{(2)}$.

This is the point at which the behaviour stabilises. For later use, it is more convenient to define for $i \geq 0$, a sequence of elements $u_1 = (\text{xyx})^{-i} u_1 \text{xyx}^i$. Then we have

$$\text{Theorem 2.5} \quad \text{For } k \geq 2, \text{ the map } i_k : \text{stab}(7^{(k)}) \mapsto \text{Aut}(\text{Link}(7^{(k)})) \text{ has image of order 54.}$$

Moreover, $\text{stab}(7^{(k)})$ is generated by the elements $u, h, 1, \ldots, k$.

**Sketch Proof** The argument is inductive; we explain the step $k = 2$ which contains all the essential ingredients. We set $H(2) = \big\langle h; 1 \big| 2 \big\rangle \text{stab}(7^{(2)})$. Note that every element of $H(2)$ stabilises $7^{(3)}$ and $11^{(3)}$. We refer to Figure 1, which shows the hexagon $\text{Link}(7^{(2)}) = H(2)$. Our claim is that no element of $2 \text{stab}(7^{(2)})$ can move $7^{(3)}$.

---

*Figure 1*
We argue as follows. Note that since elements in vertex stabilisers are type preserving, the only possibilities for \((7^{(3)})\) (assuming that it is moved) are the \(H(2)\) orbit of \(1^{(3)}\) or the \(H(2)\) orbit of \(3^{(3)}\).

However, the former orbit contains 9 elements and the latter 3, so that in any case, \(\gamma\) must move some element in the \(H(2)\) orbit of \(1^{(3)}\) back into this orbit. By composing with an element of \(H(2)\), we see that this implies the existence of an element moving \(7^{(3)}\) lying in \(\text{stab}(1^{(3)})\) or \(\text{stab}(3^{(3)})\). An examination of the generating elements shows that no element of this latter group moves \(7^{(3)}\), a contradiction.

A similar argument establishes that \(\text{stab}(7^{(2)})\) stabilises \(11^{(3)}\).

We now show that \(\text{im}(i_2)\) is a group of order at most 54. The reason is this: All of \(\text{im}(i_2)\) stabilises \(7^{(3)}\) hence permutes the four points in the link adjacent to it, however one of these points is \(11^{(3)}\), which is also fixed by the whole group. Therefore by passing to a subgroup of \(\text{im}(i_2)\) of index at most 3 we stabilise the point \(3^{(3)}\). Arguing similarly for \(3^{(3)}\), we deduce that \(\text{im}(i_2)\) contains a subgroup of index at most 9 which stabilises \(2^{(3)} = 7\). This is a group whose structure is already completely determined and one finds that \(\text{stab}(7)\) acts on \(\text{Link}(7^{(2)})\) as a group of order 6, proving the claim.

Now the group \(H(2)\) is easily analysed; in particular, one shows easily that it acts on the link as a group of order 54. This establishes that \(i_2(H(2)) = \text{im}(i_2)\) as required.

The kernel of the map \(i_2\) is a subgroup of \(\text{stab}(7^{(2)})\) and \(\text{Aut}(\text{Link}(7^{(2)}))\) is a subgroup of \(\text{stab}(7)\). Recalling that \(H(2)\) is generated by \(u_1\) and \(u_2\), it follows that \(u_1h_1\) and \(h_2\) generate \(\text{stab}(7)\), completing the first step of the induction.

Given this theorem, one can now give a complete description of the groups \(\text{stab}(7^{(k)})\) by analysing how \(\ker(i_k)\) acts on \(\text{Link}(7^{(k)})\). As a consequence, one proves that the group \(\text{stab}(7^{(k)})\) has order \(2^{3k+1}\). It follows immediately that the orbits \(7^{(k)}\) are all distinct.

We recap our progress so far. From the information that the stabiliser of the lattice \(I\) is a cyclic group of order four, we have identified the stabiliser of every vertex in the building; this information success to deduce that the orbits for the action of \(\text{Isom}(\gamma)\) on \(\gamma\) are precisely \(I; M_{22}; 7^{(k)}\) for \(k = 1\). Moreover, this already shows:

**Corollary 2.6** The group \(\text{Isom}(\gamma)\) is generated by \(x, y\) and \(u\).
The construction of the entire complex \( \text{Isom}_J \) rests largely on the work set forth above and we shall not go into it in detail. Broadly it involves two steps: The identification of a candidate set of orbits of edges and triangles coming from the action of fairly short elements, followed by the proof that no further identifications are possible. This latter step is accomplished by the detailed understanding we have developed of the vertex stabilisers. This task gets easier as one moves further away from the group points, as stabilisers get larger and there are less orbits to be considered; eventually the action of stabilisers on links becomes constant. As a result, the complex has a fairly natural decomposition into two pieces; a compact part and some "tubes". We refer the reader to [3] for details in the case \( p = 2 \). For example, a picture of the tube comes from the concatenation of hexagons shown in Figure 2.

3 The case \( p = 5 \)

The analysis in this case follows the same outline as indicated above, though of course the details become much more complicated. Nonetheless, one obtains a presentation of the group \( \text{Isom}_J \) \((5)\). The quotient complex has interesting features not present in the first two cases; for example in contrast to the cases \( p = 2 \) and \( p = 3 \), the complex which emerges has three annular ends. Once again one finds extra elements in \( \text{Isom}_J \) \((5)\) which it turns out do not
lie in the group generated by \( x \) and \( y \). The simplest of these is the element \( \gamma \) shown below:

\[
\gamma = \begin{align*}
0 & \quad 1 + 2t + 2t^2 & \quad 3 + t \\
4 & \quad 1 + t & \quad 4 + 2t & \quad 2 + 2t & \quad A \\
1 & \quad 4 + 3t + 4t^2 & \quad 2 + 2t
\end{align*}
\]

This is an element of order 4 and one finds that:

**Theorem 3.1** The group \( \text{Isom}_J((5)) \) is generated by \( x, y \) and \( \gamma \).

In fact, we are able to complete all the analysis up until the very last step and in particular, we are able to find a presentation of the group \( \text{Isom}_J((5)) \). It is rather complicated and GAP was unable to show that the index \([ \text{Isom}_J((5)) : h_x; y_i] \) was finite. We have been unable to prove that it is finite and unable to analyse the situation sufficiently to prove or disprove that \( h_x; y_i \) contains no extra relations.

**Acknowledgment** Both authors are supported in part by the NSF.

**References**


Department of Mathematics
University of California
Santa Barbara, CA 93106, USA

Email: cooper@math.ucsb.edu, long@math.ucsb.edu

Received: 26 August 1997