Unitary braid representations with finite image

Michael Larsen
Eric Rowell

We characterize unitary representations of braid groups B_n of degree linear in n and finite images of such representations of degree exponential in n.

20F36; 20C15

1 Introduction

In this paper, we prove two loosely connected results about unitary representations of the braid group $\phi\colon B_n \to U(d)$, when n is sufficiently large and the degree d is not too large compared to n. The original motivation goes back to the work of Jones on images of Braid groups in Hecke algebra representations $H(q,n)$. Jones showed [10] that when $q = i$, the image of B_n in every irreducible factor of the Hecke algebra is finite; more explicitly, each such image is an extension of a symmetric group by a 2–group. This is in sharp contrast to the usual behavior of irreducible factors of Hecke algebra representations, in which the closure of the image of B_n contains all unimodular unitary matrices (see Freedman, Larsen and Wang [8]). Birman and Wajnryb showed [2] that when $q = e^{2\pi i/6}$, certain factors of $H(q,n)$ give rise to representations whose images are extensions of symplectic groups $\mathrm{Sp}(2r,\mathbb{F}_3)$ by 3–groups, where $n \approx 2r$ (see also Goldschmidt and Jones [9]). It seems to be known by some experts, though so far as we know it has not appeared in print, that some other factors of $H(e^{2\pi i/6},n)$ give rise to image groups which are extensions of $\mathrm{SU}(r+1,\mathbb{F}_2)$ by 2–groups. Other (extensions of) symplectic groups appear as quotients of the braid group; Wajnryb [19] has found explicit relations exhibiting $\mathrm{Sp}(2r,\mathbb{F}_p)$ as a quotient of B_{2r+1} for all p. We would like to explain in some sense or at least characterize the possibilities for finite images in such representations. Such a characterization is given in Theorem 4.5.

It appears to be typically the case that a finite image of B_n in $U(d)$ can be regarded as a linear group, whose rank is comparable to n, over a finite field. We would therefore like to systematically study all representations of B_n of dimension $O(n)$ over all fields. Such a study has been initiated for complex representations of degree $\leq n$ by Formanek and his coworkers in [6; 7; 17]. In Theorem 3.3, we extend these results to

Published: 5 November 2008 DOI: 10.2140/agt.2008.8.2063

higher multiples of n, but only for unitary representations. For general representations, we have only the very soft result Theorem 2.10, which is used to relate n and r in Theorem 4.5.

Acknowledgements We would like to thank the referee for suggesting several substantive improvements to the paper. Michael Larsen was partially supported by NSF grant DMS-0354772 and Eric Rowell was partially supported by NSA grant H98230-08-1-0020.

2 Braid groups

In this section we establish some basic facts concerning the braid groups B_n and their *representations* in the general sense of homomorphisms $\phi\colon B_n \to G$ where G is any group. Proposition 2.2 and Proposition 2.9 can be found in [6], but we include full proofs for the reader's convenience.

For each braid group B_n we fix generators $x_1, \dots, x_{n-1}$ such that

$$x_i x_j x_i = x_j x_i x_j \quad \text{if } |i-j| = 1, \tag{2–1}$$

$$x_i x_j = x_j x_i \quad \text{if } |i-j| \neq 1. \tag{2–2}$$

Definition 2.1 We say a homomorphism $\phi\colon B_n \to G$ is *constant* if

$$\phi(x_1) = \phi(x_2) = \cdots = \phi(x_{n-1}).$$

Proposition 2.2 *If $\phi\colon B_n \to G$ is a homomorphism and $\phi(x_i)$ commutes with $\phi(x_{i+1})$ for some $i \leq n-2$, then ϕ is constant.*

Proof Applying (2–1) when $j = i+1$, we get

$$\phi(x_i)^2 \phi(x_{i+1}) = \phi(x_{i+1})^2 \phi(x_i),$$

which implies $\phi(x_i) = \phi(x_{i+1})$. As x_i commutes with x_{i+2}, $\phi(x_{i+1}) = \phi(x_i)$ commutes with $\phi(x_{i+2})$. By induction on i,

$$\phi(x_i) = \phi(x_{i+1}) = \cdots = \phi(x_{n-1}).$$

Likewise, $\phi(x_{i-1})$ and $\phi(x_i) = \phi(x_{i+1})$ commute, so $\phi(x_i) = \phi(x_{i-1})$, and by downward induction,

$$\phi(x_i) = \phi(x_{i-1}) = \cdots = \phi(x_1). \qquad \square$$

Corollary 2.3 *If $\phi(x_i) \in Z(G)$ for some i, then ϕ is constant.*

Corollary 2.4 *If $\phi(x_i) = \phi(x_{i+1})$ for some i, then ϕ is constant.*

If $j \geq i$, we use the notation $X_{[i,j]}$ for the product $x_i x_{i+1} \cdots x_j$; if $j < i$, we define $X_{[i,j]}$ to be the identity.

Lemma 2.5 *For $k \geq 3$ and $1 \leq i \leq k-2$, we have*

$$X_{[1,k]} x_i X_{[1,k]}^{-1} = x_{i+1}.$$

Proof The lemma holds by the following computation:

$$\begin{aligned}
X_{[1,k]} x_i X_{[1,k]}^{-1} &= X_{[1,i-1]} x_i x_{i+1} X_{[i+2,k]} x_i X_{[i+2,k]}^{-1} x_{i+1}^{-1} x_i^{-1} X_{[1,i-1]}^{-1} \\
&= X_{[1,i-1]} x_i x_{i+1} x_i x_{i+1}^{-1} x_i^{-1} X_{[1,i-1]}^{-1} \\
&= X_{[1,i-1]} x_{i+1} X_{[1,i-1]}^{-1} \\
&= x_{i+1}.
\end{aligned}$$

□

Lemma 2.6 *If $1 \leq i, j, k, l \leq n-1$, $|i-j| \geq 2$, $|k-l| \geq 2$, then there exists $z = z_{i,j,k,l} \in B_n$ such that*

$$z x_i z^{-1} = x_k, \; z x_j z^{-1} = x_l.$$

Proof First we assume $i < j$ and $k < l$. By Lemma 2.5, without loss of generality we may assume $j = l = n-1$. As $X_{[1,n-3]}$ commutes with x_{n-1}, the ordered pair (x_i, x_{n-1}) can be conjugated to (x_{i+1}, x_{n-1}) as long as $1 \leq i \leq n-4$. By induction on i, all the (x_i, x_{n-1}) with $i \leq n-3$ are conjugate.

To treat the case that $i > j$ or $k > l$, it suffices to prove that (x_1, x_3) can be conjugated to (x_3, x_1). Letting

$$y = x_1 x_2 x_3 x_1 x_2 x_1 = x_1 x_2 x_1 x_3 x_2 x_1,$$

we have

$$\begin{aligned}
y x_1 &= x_1 x_2 x_3 x_1 x_2 x_1 x_1 = x_1 x_2 x_3 x_2 x_1 x_2 x_1 = x_1 x_3 x_2 x_3 x_1 x_2 x_1 = x_3 y; \\
y x_3 &= x_1 x_2 x_1 x_3 x_2 x_3 x_1 = x_1 x_2 x_1 x_2 x_3 x_2 x_1 = x_1 x_1 x_2 x_1 x_3 x_2 x_1 = x_1 y.
\end{aligned}$$

□

Now let $0 \to A \to G \to H \to 0$ be a central extension. We write $[h_1, h_2]^{\sim}$ for the commutator $g_1 g_2 g_1^{-1} g_2^{-1} \in G$, where g_i is any element mapping to h_i. As the extension is central, this is well-defined.

Lemma 2.7 *If $0 \to A \to G \xrightarrow{\pi} H \to 0$ is a central extension and $\phi\colon B_n \to G$ is a homomorphism such that $\pi \circ \phi$ is constant, then ϕ is constant.*

Proof Any two elements of G which map to the same element of H must commute. The lemma therefore follows from Proposition 2.2. $\square$

Proposition 2.8 *If $0 \to A \to G \xrightarrow{\pi} H \to 0$ is a central extension and $\phi\colon B_n \to H$ is a homomorphism such that $[\phi(x_i), \phi(x_j)]^{\sim} = 1$ for some i, j with $|i-j| \geq 2$, then ϕ lifts to a homomorphism $\widetilde{\phi}\colon B_n \to G$.*

Proof As $[\,]^{\sim}$ respects conjugation, Lemma 2.6 implies

$$[\phi(x_i), \phi(x_j)]^{\sim} = 1$$

for all i, j with $|i-j| \geq 2$. Fix an element $\widetilde{x}_1 \in G$ with $\pi(\widetilde{x}_1) = \phi(x_1)$ and an element $\widetilde{y} \in G$ with $\pi(\widetilde{y}) = \phi(X_{[1,n-1]})$. By Lemma 2.5,

$$\pi(\widetilde{y}^k \widetilde{x}_1 \widetilde{y}^{-k}) = \phi(x_{k+1}),\ k = 0, 1, \dots, n-2.$$

Let
$$g_i = \widetilde{y}^{i-1} \widetilde{x}_1 \widetilde{y}^{1-i}.$$

Thus g_i and g_j commute when $|i-j| \neq 1$, and the elements

$$a_i := g_i g_{i+1} g_i g_{i+1}^{-1} g_i^{-1} g_{i+1}^{-1}$$

are all conjugate in G and lie in A. Thus, they all coincide; denoting this common element a, and setting $\widetilde{x}_i = a^i g_i$, we have $\pi(\widetilde{x}_i) = \phi(x_i)$, and the $\widetilde{x}_i$ satisfy the relations (2–1) and (2–2). Defining a homomorphism $\widetilde{\phi}$ by the equations $\widetilde{\phi}(x_i) = \widetilde{x}_i$, we see that $\widetilde{\phi}$ is a lift of ϕ. $\square$

Proposition 2.9 *If $n \geq 5$, then every homomorphism from B_n to a solvable group G is constant.*

Proof We use induction on the length of the derived series. The proposition follows immediately from Corollary 2.3 when G is abelian, so without loss of generality we may assume that the last nontrivial term A in the derived series of G is a proper subgroup of G. By the induction hypothesis, any homomorphism $B_n \to G/A$ is constant. We therefore choose an element $g \in G$ and a sequence $a_1, \dots, a_{n-1} \in Z$ such that $\phi(x_i) = a_i g$ for $i = 1, \dots, n-1$. Writing a^g for gag^{-1}, we have

$$a_i a_j^g g^2 = \phi(x_i x_j) = \phi(x_j x_i) = a_j a_i^g g^2$$

and therefore

$$a_i^{-1} a_i^g = a_j^{-1} a_j^g$$

whenever $|i-j|\ge 2$. The graph on the vertex set $\{1,2,\dots,n-1\}$ defined by the relation $|i-j|\ge 2$ is connected for $n\ge 5$. Thus,

$$a_1^{-1}a_1^g=\cdots=a_{n-1}^{-1}a_{n-1}^g=a$$

for some $a\in A$. The braid relation (2–1) for $j=i+1$ implies

$$a^3a_i^2a_{i+1}=a_ia_{i+1}^ga_i^{g^2}=a_{i+1}a_i^ga_{i+1}^{g^2}=a^3a_ia_{i+1}^2,$$

so $a_1=\cdots=a_{n-1}$, and ϕ is constant as claimed. □

We are indebted to the referee for useful suggestions which simplified the proof and improved the constant in the following theorem:

Theorem 2.10 *If $\mathcal{G}$ is a linear algebraic group over a field K with solvable component group, and $n\ge \max(5,2\sqrt{\dim\mathcal{G}}+4)$, then every homomorphism $B_n\to\mathcal{G}(K)$ is constant.*

Proof We assume without loss of generality that K is algebraically closed. We use induction on $\dim\mathcal{G}$, the cases $\dim\mathcal{G}\le 2$ being immediate from Proposition 2.9. We may therefore assume $n\ge 7$. Proposition 2.9 implies also that the composition of $\phi\colon B_n\to\mathcal{G}(K)$ with the quotient map $\mathcal{G}(K)\to\mathcal{G}(K)/\mathcal{G}^\circ(K)$ is constant. We may therefore assume that $\mathcal{G}/\mathcal{G}^\circ$ is cyclic. Assuming without loss of generality that $B_n\to\mathcal{G}/\mathcal{G}^\circ$ is surjective, all generators of B_n map into the same generator of this cyclic group. If $\mathcal{U}$ denotes the unipotent radical of $\mathcal{G}^\circ$, then $\mathcal{U}$ is a normal algebraic subgroup of $\mathcal{G}$. If the composition homomorphism $B_n\to(\mathcal{G}/\mathcal{U})(K)$ is constant, then B_n maps to a solvable subgroup of $\mathcal{G}(K)$, namely, an extension of the (cyclic) image of this homomorphism by $\mathcal{U}(K)$. By Proposition 2.9, this implies that ϕ is constant. Without loss of generality, therefore, we may assume that $\mathcal{G}$ is reductive. Likewise, composing ϕ with the quotient of $\mathcal{G}$ by the center of $\mathcal{G}^\circ$, we may assume without loss of generality that $\mathcal{G}^\circ$ is adjoint semisimple.

If there exist positive dimensional normal subgroups $\mathcal{N}_1,\dots,\mathcal{N}_t$ of $\mathcal{G}$ such that $\mathcal{N}_1(K)\cap\cdots\cap\mathcal{N}_t(K)=\{1\}$, then the compositions of ϕ with the projections $\mathcal{G}(K)\to(\mathcal{G}/\mathcal{N}_i)(K)$ are all constant, and therefore ϕ is constant. If $\mathcal{G}^\circ$ has at least two nonisomorphic simple factors, then the product of all factors of any one type is a proper normal subgroup of $\mathcal{G}$. We may therefore assume that $\mathcal{G}^\circ\cong\mathcal{H}^k$ for some positive integer k and some (adjoint) simple algebraic group $\mathcal{H}$. Moreover, conjugation by a generator of $\mathcal{G}/\mathcal{H}^k$ induces a well-defined outer automorphism of $\mathcal{H}^k$ and therefore a permutation σ of the factors, which are the minimal nontrivial normal subgroups of $\mathcal{H}^k$. Without loss of generality we may assume that this permutation is a k–cycle, since otherwise, each orbit of σ determines a product of factors $\mathcal{H}$ which is a normal subgroup of $\mathcal{G}$.

We assume first that $k=1$, so $\mathcal{G}^\circ = \mathcal{H}$ is simple. Let $x=\phi(x_{n-1})$, and let B_{n-2} denote the subgroup of B_n generated by $x_1,\dots,x_{n-3}$. Thus, $\phi(B_{n-3})$ lies in the centralizer of x in $\mathcal{G}(K)$. If x is semisimple, setting $\mathcal{K} := Z_{\mathcal{G}}(x)$, a well-known theorem of Springer and Steinberg [16, Theorem 9.1] implies that the component group of $\mathcal{G}^\circ\cap\mathcal{K}$ is commutative and therefore that the component group of $\mathcal{K}$ itself is solvable. If not, let $x_u\neq 1$ denote the unipotent factor in the Jordan decomposition $x=x_ux_s$. Then $x_u\in\mathcal{G}^\circ(K)$. By the Borel–Tits theorem [3, Proposition 3.1], there exists a parabolic subgroup $\mathcal{P}$ of $\mathcal{G}^\circ$ which contains $Z_{\mathcal{G}^\circ}(x_u)$ and which is fixed by every automorphism of $\mathcal{G}^\circ$ which fixes x_u. In particular,

$$Z_{\mathcal{G}}(x_u)\subset N_{\mathcal{G}}(\mathcal{P}).$$

As $\mathcal{P}$ is self-normalizing in $\mathcal{G}$, the group $\mathcal{K} := N_{\mathcal{G}}(\mathcal{P})$ has a solvable component group. In every case, therefore, $\phi(B_{n-3})$ lies in $\mathcal{K}$, where $\mathcal{K}/\mathcal{K}^\circ$ solvable and $\mathcal{K}^\circ\subsetneq\mathcal{G}^\circ$. Replacing $\mathcal{K}$ with its quotient by the radical of $\mathcal{K}^\circ$, we may assume that $\mathcal{K}^\circ$ is a semisimple subquotient of $\mathcal{G}^\circ$ From the classification of maximal subgroups by Seitz [14; 15] it follows (with some examination of cases) that

$$\sqrt{\dim\mathcal{K}}\le\sqrt{\dim\mathcal{G}}-1,$$

so $n-2\le\max(5,2\sqrt{\dim\mathcal{K}}+4)$, and the theorem follows by induction.

Finally, we consider the case $k\ge 2$. Conjugation by x induces an action on $\mathcal{H}^k$ given by

$$(h_1,\dots,h_k)\mapsto(\sigma_1(h_2),\sigma_2(h_3),\dots,\sigma_n(h_1)).$$

Therefore, the centralizer of x in $\mathcal{G}$ is contained in

$$\mathcal{K} := \{x^i(h,\sigma_1^{-1}(h),\dots,\sigma_n^{-1}\cdots\sigma_1^{-1}(h))\mid 0\le i<k,\ h\in\mathcal{H}\}.$$

Again $\mathcal{K}$ has solvable component group, and

$$\sqrt{\dim\mathcal{K}}=\sqrt{\dim\mathcal{H}}\le\frac{\sqrt{\dim\mathcal{K}}}{\sqrt{2}}<\sqrt{\dim\mathcal{G}}-1.$$

Again, the theorem follows by induction. □

A variant of this idea which will be useful later is the following:

Proposition 2.11 *Let G and H be finite groups, and k and n positive integers, such that G contains a normal subgroup*

$$N \cong \underbrace{H \times H \times \cdots \times H}_{k}.$$

Suppose the conjugation action of G on N preserves this factorization, and G/N is solvable. If $n \geq \max(5, 2\log_2 |G|)$, then every representation $\phi\colon B_n \to G$ is constant.

Proof Let $f(k) = -2$ for $k = 1$ and $f(k) = 0$ for $k \geq 2$. We prove that if

$$n \geq \max(5, 2\log_2 |G| + f(k))$$

then every G–representation of B_n is constant. If G is solvable, the theorem is immediate. Otherwise, $|G| \geq 60$, so we may assume $n \geq 9$. We suppose that the ordered quadruple (G, H, k, n) is given and that the proposition is known for all groups of order less than $|G|$. As in the proof of Theorem 2.10, we may assume that G/N is a cyclic group of order k and that $x := \phi(x_{n-1})$ maps to a generator of this quotient. If $k=1$, then $G=H$, and the centralizer Z_x of x in G satisfies $\log_2 |Z_x| \leq \log_2 |G| - 1$. As $\phi(B_{n-2}) \subset Z_x$, and the proposition is known for the quadruple $(Z_x, Z_x, 1, n-2)$, we conclude that $\phi|_{B_{n-2}}$ is constant, from which it follows that ϕ is constant.

If $k \geq 2$, as conjugation by x preserves the decomposition $N \cong H^k$, we can write

$$x(h_1, \ldots, h_k)x^{-1} = (\sigma_1(h_2), \sigma_2(h_3), \ldots, \sigma_n(h_1))$$

for automorphisms σ_i. It follows that the centralizer of x is contained in a group K which is an extension of $\mathbb{Z}/k\mathbb{Z}$ by H. Applying the induction hypothesis to the quadruple $(K, K, 1, n-2)$, the proposition holds. □

3 Representations of linearly bounded degree

In this section, we examine the possible degrees of low-dimensional unitary representations of a braid group B_n. The complex irreducible representations of degree $\leq n$ of B_n have been completely described by Formanek et al [7] and Sysoeva [17]. The constant representations have degree 1, and the nonconstant representations in this range have degree $n-2$, $n-1$, or n. Sysoeva [17] has announced that there are no irreducible representations of degree $n+1$ for n sufficiently large, and has conjectured that such a statement holds for degree $n+k$ as well.

In this section, we consider the irreducible unitary representations of B_n of degree $\leq ln$ where l is a fixed integer and n is sufficiently large in terms of l.

We say that a sequence $d_0, d_1, d_2, \ldots$ is *weakly convex* if the sequence of differences $d_1 - d_2, d_2 - d_3, \ldots$ is nonincreasing.

Lemma 3.1 *If $d_0, d_1, \ldots$ is a weakly convex sequence and $i < j < k$, then there exists an integer s such that*

$$\frac{d_j - d_i}{j - i} \leq s \leq \frac{d_k - d_j}{k - j}.$$

Proof Setting $s = d_{j+1} - d_j$, the lemma follows immediately. □

Lemma 3.2 *Let V be a finite-dimensional vector space, $W \subset V$ a subspace, and $T\colon V \to V$ an invertible linear transformation. The sequence $d_0, d_1, d_2, \ldots$ defined by $d_0 := \dim V$ and*

$$d_k := \dim W \cap T(W) \cap T^2(W) \cap \cdots \cap T^{k-1}(W), \; k \geq 1$$

is weakly convex.

Proof Define $W_0 = V$, and

$$W_k := W \cap T(W) \cap T^2(W) \cap \cdots \cap T^{k-1}(W), \; k \geq 1.$$

Then $$d_k - d_{k+1} = \dim W_k - \dim W_{k+1} = \dim W_k / W_{k+1}$$

As T^{-1} maps to W_{k+1} to W_k and W_{k+2} to W_{k+1}, it induces a map

$$W_{k+1}/W_{k+2} \to W_k / W_{k+1}.$$

As $$W_{k+1} \cap T(W_{k+1}) = W_{k+2},$$

this linear transformation is injective, so

$$d_k - d_{k+1} \geq d_{k+1} - d_{k+2}.$$ □

We apply this lemma in the following way. Let V be a finite-dimensional complex vector space endowed with a Hermitian inner product, and $\phi\colon B_n \to U(V)$ an irreducible unitary representation. For each $\lambda \in \mathbb{C}$, we define $W = W^\lambda$ to be the λ–eigenspace of $\phi(x_1)$. By Lemma 2.5 there exists $y \in B_n$ such that $y x_i y^{-1} = x_{i+1}$ for $1 \leq i \leq n-2$. We set $T = \phi(y)$. Now, $w \in W^\lambda$, if and only if

$$(\phi(x_1) - \lambda)(w) = 0.$$

For any k, this is equivalent to

$$(\phi(y^{1-k}x_k y^{k-1}) - \lambda)(w) = 0,$$

or to
$$(\phi(x_k) - \lambda)(\phi(y^{k-1})(w)) = 0.$$

Thus, the λ–eigenspace of $\phi(x_k)$ is $T^{k-1}(W^\lambda)$.

We say that an irreducible representation $\phi\colon B_n \to U(m)$ is of *level* k if one of the following is true:

(1) $k = 0$ and $m = 1$.

(2) $k \geq 1$ and $kn - (k^2 + 3k - 2) \leq m \leq kn$.

Theorem 3.3 *For every integer $l \geq 1$ and every integer n sufficiently large in terms of l, every irreducible unitary representation of the braid group B_n of degree $\leq ln$ is of some (unique) level $k \leq l$.*

Proof As
$$(k-1)n < kn - (k^2 + 3k - 2)$$
when n is sufficiently large, uniqueness is clear. For existence, we use induction on l, the $l = 1$ case being known [7]. For given $l \geq 2$, let $\phi\colon B_n \to \mathrm{Aut}(V)$ be an irreducible unitary representation of degree $\leq ln$. We may therefore assume that

$$(l-1)n + 1 \leq \dim V \leq ln - (l^2 + 3l - 1). \tag{3–1}$$

We write B_{n-1} and B_{n-2} for the subgroups of B_n generated by x_i with $1 \leq i \leq n-2$ and $1 \leq i \leq n-3$ respectively.

For each eigenvalue μ of $\phi(x_{n-1})$, let X^μ denote the μ–eigenspace. As B_{n-2} commutes with x_{n-1}, $\phi(B_{n-2})$ acts on X^μ. We say that X^μ *splits* if it is a direct sum of constant representations of B_{n-2}. A sufficient condition that X^μ splits is

$$\dim X^\mu \leq n-5,$$

as the minimum degree of a nonconstant representation of B_{n-2} is $n-4$. Let X denote the direct sum of all irreducible 1–dimension factors of B_{n-2} in V, so X contains the sum of all split X^μ. Let $\lambda_1, \ldots, \lambda_r$ be the constants appearing in X regarded as a B_{n-2}–representation, and let W^{λ_i} denote the λ_i–eigenspace of $\phi(x_1)$ on V, which of course contains the λ_i–eigenspace of $\phi(x_1)$ on X. Thus $W_j^{\lambda_i}$ is the intersection of the λ_i–eigenspaces of $\phi(x_1), \ldots, \phi(x_j)$. As $W_{n-1}^{\lambda_i} = \{0\}$, Lemma 3.2 implies

$$\dim W_j^{\lambda_i} \geq \frac{n-1-j}{2} \dim W_{n-3}^{\lambda_i},$$

for $1 \le j \le n-3$. If $\dim X \ge 2l+1$,

$$ln \ge \sum_i \dim W_1^{\lambda_i} \ge \frac{n-2}{2} \dim X \ge ln + (n/2 - 2l - 1).$$

Assuming $n > 4l+2$, we may therefore conclude that $\dim X \le 2l$.

We consider first the case that there are at least two different eigenvalues μ_i such that X^{μ_i} does not split. For each $\mu \in \{\mu_1, \ldots, \mu_r\}$, let X_{ns}^{μ} denote the orthogonal complement in X^{μ} of the direct sum of all constant representations of B_{n-2}. Then

$$\begin{aligned}\dim V - \dim X_{ns}^{\mu} &\le ln - (l^2 + 3l - 1) - (n-4)\\ &= (l-1)(n-2) - (l^2 + l - 3)\\ &< (l-1)(n-2),\end{aligned}$$

so $\bigoplus_{\mu_i \ne \mu} X_{ns}^{\mu_i}$ satisfies the induction hypothesis for representations of B_{n-2}, and the same is true of each irreducible factor of each $X_{ns}^{\mu_i}$. Each irreducible factor of $X_{ns}^{\mu_i}$ therefore has a level. Letting $k_1, k_2, \ldots, k_s \ge 1$ denote the sequence of levels, we have

$$\dim V = \dim X + \sum_{i=1}^{s} \dim X_{ns}^{\mu_i},$$

so $(k_1 + \cdots + k_s)(n-2) - \sum_{i=1}^{s} (k_i^2 + 3k_i - 2) \le \dim V \le 2l + (k_1 + \cdots + k_s)(n-2)$.

For n sufficiently large in terms of l, this, together with (3–1) implies $k_1 + \cdots + k_s = l$. As $x^2 + 3x - 2$ is convex, for any fixed values of $s \ge 2$ and l, the sum of $k_i^2 + 3k_i - 2$ is minimized, subject to the constraints $k_i \ge 1$ and $k_1 + \cdots + k_s = l$, when all but one value of k_i is 1. As the difference between values of $x^2 + 3x - 2$ for consecutive positive integers exceeds the value at $x = 1$, if s is constrained to be greater than 1 but otherwise can be chosen freely, the sum of $k_i^2 + 3k_i - 2$ is maximized when $s = 2$. Thus,

$$\begin{aligned}\dim V &\ge (k_1 + \cdots + k_s)(n-2) - \sum_{i=1}^{s}(k_i^2 + 3k_i - 2)\\ &\ge ln - 2l - (l-1)^2 - 3(l-1) + 2 - 2\\ &= ln - (l^2 + 3l - 2).\end{aligned}$$

This leaves the case that there exists a unique μ such that X_{ns}^{μ} is not zero. Let X_i^{μ} denote the intersection of the μ–eigenspaces of $x_{n-1}, x_{n-2}, \ldots, x_{n-i}$. By Lemma 3.2, applying Lemma 3.1 for $0 < i < j$,

$$\dim X_i^\mu - \dim X_j^\mu \le (j-i)\left\lfloor \frac{\dim V - \dim X_i^\mu}{i} \right\rfloor.$$

If
$$\dim V - \dim X_l^\mu < l^2,$$
then setting $j = n-1$ and $i = l$, we have

$$\begin{aligned}\dim V &\le l^2 - 1 + \dim X_l^\mu \le l^2 - 1 + \dim X_l^\mu - \dim X_{n-1}^\mu \\ &\le l^2 - 1 + (n-l-1)\left\lfloor \frac{l^2-1}{l} \right\rfloor \\ &= (l-1)n,\end{aligned}$$

which for n sufficiently large is inconsistent with (3–1). On the other hand,

$$\dim V - \dim X^\mu \le 2l,$$
so
$$\dim V - \dim X_l^\mu \le 2l^2.$$

Assuming that $2l^2 \le n-l-6$, this implies that the orthogonal complement of X_l^μ is a split representation of B_{n-l-1}, the subgroup of B_n generated by $x_1, \dots, x_{n-l-2}$. Let λ_i denote the eigenvalues of this representation. We have

$$\sum_i \dim W_{n-l-2}^{\lambda_i} \ge l^2.$$

On the other hand, $\dim W_{n-1}^{\lambda_i} = 0$. By Lemma 3.1 and Lemma 3.2,

$$\dim W_1^{\lambda_i} - \dim W_{n-l-2}^{\lambda_i} \ge (n-l-3)\left\lceil \frac{\dim W_{n-l-2}^{\lambda_i}}{l+1} \right\rceil.$$

As $\lceil x/(l+1) \rceil$ is superadditive in x and $\lceil l^2/(l+1) \rceil = l$,

$$\begin{aligned}\sum_i \dim W_1^{\lambda_i} &\ge \sum_i \dim W_{n-l-2}^{\lambda_i} + (n-l-3)\left\lceil \frac{\dim W_{n-l-2}^{\lambda_i}}{l+1} \right\rceil \\ &\ge l^2 + (n-l-3)l = nl - 3l,\end{aligned}$$

contrary to (3–1). □

In particular by the proof of Theorem 3.3 we see that B_n has no irreducible $(n+1)$–dimensional unitary representations for $n \ge 16$. The actual lower bound is at least 8 as

B_7 has irreducible 8–dimensional unitary representations (factoring over the Hecke algebra $H(i,7)$; see Jones [10]).

Theorem 3.3 can be extended to projective unitary representations. In fact, we have the following proposition:

Proposition 3.4 *Every irreducible projective unitary representation of B_n of degree $d \le 2^{n/6}$ lifts to a linear representation of B_n.*

Proof The proposition is trivial for $n \le 5$. We may therefore assume $n \ge 6$. Thus there exists a sequence $a_1 < \cdots < a_{2m}$ of positive odd integers less than n, with $m \ge n/6$. Let $y_i = x_{a_i}$. The generators y_i commute with one another. The central extension

$$0 \to U(1) \to U(d) \xrightarrow{\pi} \mathrm{PSU}(d) \to 0$$

defines a commutator map $[\,]^\sim$. By Lemma 2.6, $[\phi(x_i),\phi(x_j)]^\sim$ is independent of the pair (i,j) provided $|i-j| \ge 2$. It is therefore symmetric as well as antisymmetric and consequently takes values ± 1. If $[\phi(x_i),\phi(x_j)]^\sim = 1$ for some (and therefore all) (i,j) with $|i-j| \ge 2$, then by Lemma 2.7, ϕ lifts to a homomorphism to $U(m)$.

We therefore assume that $[\phi(y_i),\phi(y_j)]^\sim = -1$ for all $i \ne j$. Let

$$a_i = y_1 y_2 \cdots y_{2i-1}, \; b_i = y_1 y_2 \cdots y_{2i-2} y_{2i}.$$

Then
$$[a_i,a_j]^\sim = [b_i,b_j]^\sim = 1, \; [a_i,b_j]^\sim = (-1)^{\delta_{ij}}.$$

Let
$$G_i := \pi^{-1}(\phi(\langle a_i, b_i\rangle)).$$

Clearly, the restriction of the standard representation of $U(m)$ to G_i has no 1–dimensional components. The subgroups $G_1,\dots,G_m \subset U(d)$ commute in pairs and give rise to a homomorphism $G_1 \times \cdots \times G_m \to U(d)$. The restriction of the standard representation of $U(m)$ to this product decomposes as a sum of irreducible representations of $G_1 \times \cdots \times G_m$, each of which is an external tensor product of representations of the G_i, each of degree > 1. Therefore, $d \ge 2^m$. □

4 Representations of exponentially bounded degree

In this section we fix a constant c and consider nonconstant unitary representations of B_n, $n \ge 5$, of degree $d \le c^n$ with finite image. We are interested in the behavior of $G := \rho(B_n)$. By Proposition 2.9, G cannot be solvable.

Definition 4.1 We say a finite group G is *almost characteristically simple* if there exists a (nonabelian) finite simple group H and a positive integer k such that $H^k < G < \mathrm{Aut}(H^k)$. We say G is *of permutation type* if H is isomorphic to the alternating group A_n for some $n \geq 5$.

Proposition 4.2 *If G is any finite group which is not solvable and K is maximal among normal subgroups of G such that G/K is not solvable, then G/K is almost characteristically simple.*

Proof Replacing G by G/K, we may assume that G is not solvable but every nontrivial quotient group of G is. In particular, G has no nontrivial normal abelian subgroup. Every minimal normal subgroup L is characteristically simple, ie, of the form H^k where H is simple or cyclic of prime order. However, L cannot be abelian, so H cannot be cyclic. If M is any other minimal normal subgroup, it is also a power of a simple group, and $L \cap M = \{1\}$ since L and M are minimal. This implies that the solvable group G/M contains a simple subgroup isomorphic to H, which is impossible. It follows that L is the unique minimal normal subgroup, and therefore the conjugation map $G \to \mathrm{Aut}(L)$ is injective, which proves that G is almost characteristically simple. □

Definition 4.3 If G is a finite group which is not solvable, a *minimal quotient* is any group of the form G/K where K is maximal among normal subgroups of G such that G/K is not solvable.

Definition 4.4 A finite group is of *classical type of rank r* if it is a finite simple group of the form $A_r(q)$, ${}^2A_r(q), B_r(q)$, $C_r(q)$, $D_r(q)$, or ${}^2D_r(q)$.

Roughly speaking, a finite simple group is of classical type if it is a linear, unitary, orthogonal, or symplectic group over a finite field.

Theorem 4.5 *For every constant c there exist positive constants A, B, K, N, and Q such that for all $n > N$ and all ρ: $B_n \to U(d)$ with $d \leq c^n$ and finite image G, every minimal quotient of G is either of permutation type or of the form $H^k \rtimes \mathbb{Z}/m\mathbb{Z}$, where H is a finite simple group of classical type of rank r. In the latter case, $1 \leq k \leq K$, $2 \leq q \leq Q$, and $An \leq r \leq Bn$.*

Proof A minimal quotient is of the form $H^k \rtimes C$, where C is solvable and H is simple. By hypothesis, H is not an alternating group. By Proposition 2.11, if n is sufficiently large, then $|H|$ can be taken to be as large as we wish; in particular, we exclude that case that H is sporadic. By Theorem 2.10, if n is sufficiently large and H is of Lie type, the dimension of the underlying simple algebraic group must be $> \epsilon n^2$ for some absolute constant $\epsilon > 0$, so the rank r of the group must be greater than An for some absolute constant $A > 0$. Thus, we may assume that H is a perfect group whose universal central extension is $\mathcal{H}(\mathbb{F})$, where $\mathcal{H}$ is a simply connected semisimple algebraic group over $\mathbb{F}$ which is absolutely simple modulo its center and of rank $r \geq 9$.

Let G_0 denote the inverse image of $H^k \subset H^k \rtimes C$ in G. We have a short exact sequence

$$0 \to J \to G_0 \to H^k \to 0,$$

which we pull back to a short exact sequence

$$0 \to J \to \tilde{G}_0 \to \mathcal{H}(\mathbb{F})^k \to 0. \tag{4–1}$$

As $\tilde{G}_0$ is a central extension of G_0, the faithful representation $G_0 \to U(d)$ gives rise to an almost faithful d–dimensional representation of $\tilde{G}_0$. We claim that this implies that d is greater than or equal to the degree of the minimal nontrivial representation of $\mathcal{H}(\mathbb{F})$. Let $X \subset \mathrm{Hom}(Z(J), \mathbb{C}^\times)$ denote the set of characters obtained by restricting $\tilde{G}_0 \to U(d)$ to the abelian group $Z(J)$. Thus $\mathcal{H}(\mathbb{F})^k$ acts on X. If this action is nontrivial, then the permutation representation of $\mathcal{H}(\mathbb{F})^k$ acting on X is nontrivial and therefore contains a nontrivial factor. The minimal degree for a nontrivial representation of $\mathcal{H}(\mathbb{F})^k$ is the same as that for $\mathcal{H}(\mathbb{F})$. We may therefore assume that $\mathcal{H}(\mathbb{F})^k$ acts trivially on X. This implies that the action of $\mathcal{H}(\mathbb{F})^k$ on $Z(J)$ preserves both $Z(\tilde{G}_0) \subset Z(J)$ and $Z(\tilde{G}_0)/Z(J)$ pointwise. As $\mathcal{H}(\mathbb{F})^k$ is perfect, any action of this group on an abelian group which fixes a subgroup and quotient group pointwise is trivial. It follows that $Z(J)$ lies in the center of $\tilde{G}_0$. The nonabelian cohomology class which determines whether (4–1) splits lies in $H^2(\mathcal{H}(\mathbb{F})^k, J)$, which is a principal homogeneous space of $H^2(\mathcal{H}(K)^k, Z(J))$. The latter is trivial since $\mathcal{H}(K)^k$ is centrally closed. Therefore, G_0 contains a subgroup isomorphic to $\mathcal{H}(\mathbb{F})^k$, and restricting V to this subgroup, we see that our claim holds.

The Seitz–Landazuri bound [12] on the minimal degree projective representations of finite simple groups of Lie types now implies that $q^{kr/n}$ is bounded in terms of c. Given that $r/n > A$, this gives upper bounds Q and K for q and k, and given that $q \geq 2$, $k \geq 1$, this gives an upper bound B for r/n. □

We remark that the theorem can be extended in two ways without essentially modifying the proof. On the one hand, we need not assume that the representation V is unitary. On the other hand, if V is unitary, we need not assume that $\rho(B_n)$ is finite; we can take the closure of the image, obtain a compact Lie group, and characterize the *group of components* of this Lie group without assuming that the identity component is trivial.

5 An application

We would like to describe a general setting in which one obtains sequences of unitary representations of the braid group of exponentially bounded degree. Let $\mathcal{C}$ be any unitary premodular (= ribbon fusion) category (see Turaev [18, Chapter II.5]). In particular this means that $\mathcal{C}$ is semisimple with finitely many (isomorphism classes of) simple objects $\{X_0, \cdots, X_r\}$ and the morphism spaces are finite dimensional $\mathbb{C}$–vector spaces. Moreover, such a category is equipped with a conjugation and a positive definite Hermitian form with respect to which each $\mathrm{End}(X^{\otimes n})$ is a Hilbert space. The braiding isomorphisms $c_{X,Y}\colon X \otimes Y \cong Y \otimes X$ induce unitary representations $\rho_n^X\colon B_n \to U(\mathrm{End}(X^{\otimes n}))$ via:

$$\rho_n^X(\sigma_i) f = \mathrm{Id}_X^{\otimes i-1} \otimes c_{X,X} \otimes \mathrm{Id}_X^{\otimes n-i-1} \circ f$$

for any object X, where the B_n–invariance of the Hermitian form is included in the axioms. By semisimplicity of $\mathrm{End}(X^{\otimes n})$ the spaces $\mathrm{Hom}(X_j, X^{\otimes n})$ for simple X_j are equivalent to (potentially reducible) unitary B_n subrepresentations of $\mathrm{End}(X^{\otimes n})$.

We will show that $\dim \mathrm{Hom}(X_j, X^{\otimes n})$ is exponentially bounded. For simplicity of notation we assume that $X = X_i$ is a simple object and each object is isomorphic to its dual; the general case is essentially the same. For each simple object X_i we define a (symmetric) matrix N_i whose (j,k)–entry is $\dim \mathrm{Hom}(X_k, X_i \otimes X_j)$. The matrices N_i, $0 \leq i \leq r$ pairwise commute, and are clearly nonnegative. Let d_i be the Perron–Frobenius eigenvalue of N_i, ie the largest eigenvalue. Setting $D = \max\{d_i\}$ we will show that $\dim \mathrm{Hom}(X_j, X^{\otimes n}) \leq D^n$. First observe that $d_i \geq 1$, since $|\lambda| \leq d_i$ for all other eigenvalues λ and clearly $(N_i)^n \neq 0$ for all n. It follows from the Perron–Frobenius Theorem that the vector $\mathbf{d} = (d_0, d_1, \cdots, d_r)^T$ is a strictly positive eigenvector with eigenvalue d_i for each N_i, uniquely determined up to rescaling (one applies the Perron–Frobenius Theorem to the strictly positive matrix $M := \sum_i N_i$; see eg Etingof, Nikshych and Ostrik [4]). Now denoting by $\mathbf{e}_i$ the i–th standard basis vector for $\mathbb{R}^r$, we see that $\dim(X_j, X_i^{\otimes n})$ is the j–th entry of $(N_i)^{n-1}\mathbf{e}_i$ which is less than or equal to the j–th entry of $(N_i)^{n-1}\mathbf{d} = (d_i)^{n-1}\mathbf{d}$ which in turn is bounded by D^n.

There are two well-known constructions of unitary premodular categories. The first is $\mathrm{Rep}(D^\omega G)$: the representation category of the twisted quantum double of a finite group G. $D^\omega G$ is a semisimple $|G|^2$–dimensional quasi-triangular quasi-Hopf algebra (see Bakalov and Kirillov [1]), and $\mathrm{Rep}(D^\omega G)$ is a modular category. The braid group representations were studied by Etingof, Rowell and Witherspoon [5] and found to have finite images. In particular the image of ρ_n^H where $H = D^\omega G$ is the left regular representation of $D^\omega G$ is found to be a subgroup of the full monomial group $S_n \ltimes \mathbb{Z}_s^n$

for some s and hence of permutation type. Since any simple object appears as a subobject of H, it follows that all images are of permutation type. The second set of examples come from representations of quantum groups at roots of unity (see eg Rowell [13]) or, equivalently, from fixed level representations of affine Kac–Moody algebras. Quantum groups of type A_k at 4–th and 6–th roots of unity yield modular categories supporting braid group representations with finite images. In fact, these representations factor over quotients of Hecke algebras $H(q,n)$ and are precisely those alluded to in the introduction. Quantum groups of type C_2 at 10–th roots of unity also yield finite braid group images [11], with images $\mathrm{Sp}(n-1,\mathbb{F}_5)$. Here the object X of interest has $d_X=\sqrt{5}$, and for B_n with n odd, $\dim\mathrm{End}(X^{\otimes n})=(\sqrt{5})^{n-1}$ and is the metaplectic representation of $\mathrm{Sp}(n-1,\mathbb{F}_5)$ with two irreducible subrepresentations of dimension $((\sqrt{5})^{n-1}\pm 1)/2$. It appears that this can be generalized: there is evidence that quantum groups of type B_k at $(4k+2)$–th roots of unity and D_k at $4k$–th roots of unity support braid group representations with finite symplectic groups as images.

References

[1] **B Bakalov**, **A Kirillov, Jr**, *Lectures on tensor categories and modular functors*, University Lecture Series 21, Amer. Math. Soc. (2001) MR1797619

[2] **J S Birman**, **B Wajnryb**, *Markov classes in certain finite quotients of Artin's braid group*, Israel J. Math. 56 (1986) 160–178 MR880289

[3] **A Borel**, **J Tits**, *Éléments unipotents et sous-groupes paraboliques de groupes réductifs. I*, Invent. Math. 12 (1971) 95–104 MR0294349

[4] **P Etingof**, **D Nikshych**, **V Ostrik**, *On fusion categories*, Ann. of Math. (2) 162 (2005) 581–642 MR2183279

[5] **P Etingof**, **E Rowell**, **S Witherspoon**, *Braid group representations from twisted quantum doubles of finite groups*, Pacific J. Math. 234 (2008) 33–41 MR2375313

[6] **E Formanek**, *Braid group representations of low degree*, Proc. London Math. Soc. (3) 73 (1996) 279–322 MR1397691

[7] **E Formanek**, **W Lee**, **I Sysoeva**, **M Vazirani**, *The irreducible complex representations of the braid group on n strings of degree $\le n$*, J. Algebra Appl. 2 (2003) 317–333 MR1997750

[8] **M H Freedman**, **M J Larsen**, **Z Wang**, *The two-eigenvalue problem and density of Jones representation of braid groups*, Comm. Math. Phys. 228 (2002) 177–199 MR1911253

[9] **D M Goldschmidt**, **V F R Jones**, *Metaplectic link invariants*, Geom. Dedicata 31 (1989) 165–191 MR1012438

[10] **V F R Jones**, *Braid groups, Hecke algebras and type* II_1 *factors*, from: "Geometric methods in operator algebras (Kyoto, 1983)", Pitman Res. Notes Math. Ser. 123, Longman Sci. Tech., Harlow (1986) 242–273 MR866500

[11] **V F R Jones**, *On a certain value of the Kauffman polynomial*, Comm. Math. Phys. 125 (1989) 459–467 MR1022523

[12] **V Landazuri**, **G M Seitz**, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra 32 (1974) 418–443 MR0360852

[13] **E C Rowell**, *From quantum groups to unitary modular tensor categories*, from: "Representations of algebraic groups, quantum groups, and Lie algebras", Contemp. Math. 413, Amer. Math. Soc. (2006) 215–230 MR2263097

[14] **G M Seitz**, *The maximal subgroups of classical algebraic groups*, Mem. Amer. Math. Soc. 67 (1987) no. 365 MR888704

[15] **G M Seitz**, *Maximal subgroups of exceptional algebraic groups*, Mem. Amer. Math. Soc. 90 (1991) no. 441 MR1048074

[16] **R Steinberg**, *Endomorphisms of linear algebraic groups*, Mem. Amer. Math. Soc. 80, Amer. Math. Soc. (1968) MR0230728

[17] **I Sysoeva**, *Dimension n representations of the braid group on n strings*, J. Algebra 243 (2001) 518–538 MR1850645

[18] **V G Turaev**, *Quantum invariants of knots and 3–manifolds*, de Gruyter Studies in Math. 18, Walter de Gruyter & Co., Berlin (1994) MR1292673

[19] **B Wajnryb**, *A braidlike presentation of* $\mathrm{Sp}(n, p)$, Israel J. Math. 76 (1991) 265–288 MR1177345

Department of Mathematics, Indiana University
Bloomington, IN 47405, USA

Department of Mathematics, Texas A&M University
College Station, TX 77843-3368, USA

mjlarsen@indiana.edu, rowell@math.tamu.edu

http://mlarsen.math.indiana.edu/~larsen/,
http://www.math.tamu.edu/~rowell/

Received: 31 May 2008 Revised: 25 September 2008