

IMAGE OF THE BRAID GROUPS INSIDE THE FINITE IWAHORI-HECKE ALGEBRAS

OLIVIER BRUNAT, KAY MAGAARD, AND IVAN MARIN

ABSTRACT. We determine the image of the braid groups inside the Iwahori-Hecke algebras of type A, when defined over a finite field, in the semisimple case, and for suitably large (but controllable) order of the defining (quantum) parameter.

1. INTRODUCTION

The point of this paper is to enhance our understanding of the connection between braid groups and Hecke algebras of type A. This interplay has been at the core of the definition of the Jones and subsequently HOMFLYPT polynomial of knots and links, and is the source of the most classical linear representations of the braid groups. Because of that, it has also been used for the purpose of inverse Galois theory – in that case, with coefficients a finite field. Our aim here is to understand better the image of the braid group inside the (group of invertible elements of) the Hecke algebra, and especially to describe the finite group which is the image of the braid group inside the Hecke algebra over a finite field. We first review briefly what is known.

The closed image of the braid group inside the Hecke algebra over the complex numbers has been essentially determined in the first decade of the century. In this setting, it had been proved earlier by Jones and Wenzl that the Hecke algebra representations provided unitary representations of the braid group for suitable parameters. Using this, the closed image in these unitary cases was determined in [FLW]. Simultaneously and independently, the third author in his 2001 doctoral thesis (see [M0]), introduced a Lie algebra subsequently identified (see [M2]) with the Lie algebra of the algebraic closure of B_n in the generic (but not necessarily unitary) case. When the representation is known to be unitary, the algebraic closure determines the topological closure. On the other hand, the approach of [FLW] provides more precise information on specific values of the parameters, specifically when the parameter is a root of 1. Finally, other proofs and sources of justification, sometimes in a broader context, for the unitary structures have been provided in [M1] and [M3], part IV.

Back to the finite field situation, the classical “strong approximation” results suggest that, “most of the time”, we should get for images groups of \mathbb{F}_q -points of the algebraic groups defined above. This assertion is very vague because the algebraic groups are not a priori defined over \mathbb{Z} and because there is a parameter involved in the definition of the Hecke algebra that prevents the direct use of these classical results. Also, there is the question of unitarity which needs some work to be translated into the finite fields case. Nevertheless, the first and third author proved in [BM] that we can get the expected result for the quotient of the Hecke algebra known as the Temperley-Lieb algebra, under only a few conditions, the most restrictive of these being that the corresponding Hecke algebra is semisimple. By

classical results from representation theory this last condition can be made precise in terms of the order of the parameter inside \mathbb{F}_q^\times and in terms of the number n of strands.

In this paper we extend this to the full Hecke algebra, under the same conditions. For technical reasons we found it more handy to deal with the commutator subgroup \mathcal{B}_n of B_n instead of B_n itself. Since $B_n^{ab} \simeq \mathbb{Z}$ this does not diminish the strength of the results, and at the same time makes many proofs and statements more readable.

We now state the main result. We let \mathcal{E}_n denote the set of partitions on n which are not hooks. We choose some total ordering $<$ on \mathcal{E}_n . Let $b(\lambda) = \max\{i; \lambda_i \geq i\}$ denote the length of the diagonal of the Young diagram associated to $\lambda \vdash n$, and $\nu(\lambda) = 1$ if $(n - b(\lambda))/2$ is even, $\nu(\lambda) = -1$ otherwise. Without loss of generality we assume that $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ and denote $\mathrm{GL}(\lambda)$ the group of linear automorphisms of the \mathbb{F}_q -vector space associated to the representation of $H_n(\alpha)$ indexed by λ . Because of the existence of explicit matrix models recalled below, we know that these representations are indeed defined over $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. In §3 we attach to each $\lambda \in \mathcal{E}_n$ a classical subgroup $G(\lambda)$ of $\mathrm{GL}(\lambda)$ which contains the image of \mathcal{B}_n . Letting N denote the dimension of the representation attached to λ , we have the following, where we use the classical notations of e.g. [W]. In particular $\Omega_N^+(q)$ is the commutator subgroup of the orthogonal group for a form of ‘+’ type, meaning that it has Witt index 0.

- If $p = 2$, then
 - if $\mathbb{F}_2(\alpha + \alpha^{-1}) = \mathbb{F}_q$,
 - * if $\lambda \neq \lambda'$, $G(\lambda) = \mathrm{SL}_N(q)$
 - * if $\lambda = \lambda'$, then $G(\lambda) = \mathrm{SP}_N(q)$
 - if $\mathbb{F}_2(\alpha + \alpha^{-1}) \neq \mathbb{F}_q$, then $\mathbb{F}_2(\alpha + \alpha^{-1}) = \mathbb{F}_{\sqrt{q}}$ and
 - * if $\lambda \neq \lambda'$, $G(\lambda) = \mathrm{SU}_N(q)$
 - * if $\lambda = \lambda'$, then $G(\lambda) = \mathrm{SP}_N(\sqrt{q})$
- If p is odd, then
 - if $\mathbb{F}_p(\alpha + \alpha^{-1}) = \mathbb{F}_q$,
 - * if $\lambda \neq \lambda'$, $G(\lambda) = \mathrm{SL}_N(q)$
 - * if $\lambda = \lambda'$ and $\nu(\lambda) = -1$, then $G(\lambda) = \mathrm{SP}_N(q)$
 - * if $\lambda = \lambda'$ and $\nu(\lambda) = 1$, then $G(\lambda) = \Omega_N^+(q)$
 - if $\mathbb{F}_p(\alpha + \alpha^{-1}) \neq \mathbb{F}_q$, then $\mathbb{F}_p(\alpha + \alpha^{-1}) = \mathbb{F}_{\sqrt{q}}$ and
 - * if $\lambda \neq \lambda'$, $G(\lambda) = \mathrm{SU}_N(q)$
 - * if $\lambda = \lambda'$ and $\nu(\lambda) = -1$, then $G(\lambda) = \mathrm{SP}_N(\sqrt{q})$
 - * if $\lambda = \lambda'$ and $\nu(\lambda) = 1$, then $G(\lambda) = \Omega_N^+(\sqrt{q})$

We recall that the Hecke algebra $H_n(\alpha)$ for $\alpha \in \mathbb{F}_q^\times$ can be defined as the quotient of the group algebra $\mathbb{F}_q B_n$ of the braid group B_n by the relations $(\sigma_i + 1)(\sigma_i - \alpha) = 0$, where the σ_i are the usual Artin generators of B_n . The algebra $H_n(\alpha)$ is semisimple when the order of α is greater than n , and this provides an isomorphism $H_n(\alpha)^\times \simeq \prod_{\lambda \vdash n} \mathrm{GL}(\lambda)$.

Then, our main theorem states the following.

Theorem 1.1. *Assume $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ and that the order of α is $> n$ and not 2, 3, 4, 5, 6, 10. The morphism $\mathcal{B}_n \rightarrow H_n(\alpha)^\times \simeq \prod_{\lambda \vdash n} \mathrm{GL}(\lambda)$ factorizes through the morphism*

$$\Phi_n : \mathcal{B}_n \rightarrow G(\lambda^0) \times \prod_{\substack{\lambda \in \mathcal{E}_n \\ \lambda < \lambda'}} G(\lambda) \times \prod_{\substack{\lambda \in \mathcal{E}_n \\ \lambda = \lambda'}} G(\lambda)$$

where $\lambda^0 = [n - 1, 1]$.

The additional condition, that the order of α is not 2, 3, 4, 5, 6, 10, was expected, for the image of B_3 in these cases may in general factorize through the quotients of B_3 by the relations $\sigma_i^r = 1$ for $r \in \{2, 3, 4, 5\}$, which are imprimitive reflection groups of rank 2 (see [C]).

We explain the plan of the proof. The price for using the commutator subgroup instead of the full braid group is that we need a few additional technicalities that we gather in §2. The first step of the actual proof is then to get a description of the algebraic groups involved here in very explicit terms. For this we use Hoefsmit's combinatorial matrix models in order to define the expected orthogonal and symplectic forms as well as the expected diagonal embeddings (see §3). Using the vanishing of the Brauer group of the finite fields we show how to convert the unitarity property into a well-defined algebraic group over a smaller field (§4). Then we proceed by an induction argument (§5) in order to prove that the image of \mathcal{B}_n is what we expect it is. By [BM] we know it for $n \leq 5$. We first show that, assuming the result for some $n \geq 5$, we can determine the image of \mathcal{B}_{n+1} inside every single irreducible representation of the Hecke algebra. For this, our main tool is a theorem of Guralnik and Saxl on subgroups of finite classical groups acting irreducibly on the underlying vector space (notice that this theorem depends on the classification theorem of finite simple groups). Then, as in [BM], we glue the pieces together in order to get the result for $n + 1$ using Goursat's lemma. Finally, we indicate how the proof needs to be modified in case the order of the parameter implies that a unitary structure is involved.

Generalizations of this work can be expected in two directions. One of them is to look at what happens for the generalized braid groups associated to other (real or complex) reflection groups. The “generic image”, that is the Zariski closure over a field of characteristic 0 and for the generic values of the parameters, has been computed in [M3]. Moreover, the unitarity property has been proved for all Coxeter groups and most of the complex reflection groups, and is conjectured to hold in general (see [M3], part III, §6). However the interplay between the unitarity property and the algebraic structure, when looked at carefully, presents some additional difficulties for complex reflection groups, see [M3], part IV, §5 and remark 5.9 there. When the reflection group is not rational, there is moreover a specialization issue, because the base ring $\mathbb{Z}[q, q^{-1}]$ needs to be replaced by a ring of Laurent polynomials over a larger ring of algebraic integers. Finally, for exceptional complex reflection groups, even the basic structure theorems for the Hecke algebra are still conjectural (see [M4] for an overview and recent results). Even in the Coxeter case, quite a few tools we used here however cannot be applied directly in the more general context. Moreover, the Hecke algebras may involve several parameters, and also because of that the unitarity property may be more tricky to handle. As an example of what may happen, let us mention that the image of the generalized braid group of Coxeter type H_4 should be quite interesting, because the representations of the reflection groups can be defined only over $\mathbb{Q}(\sqrt{5})$, and because there is a Spin_8 group appearing in the description of the generic image.

A second natural direction is to try to understand what happens in the non-semisimple case, that is when the order of α is lower or equal to n . As far as we know, this is yet a completely unexplored territory, also over the complex numbers when α is a root of 1.

2. PRELIMINARIES ON BRAID GROUPS

We let \mathcal{B}_n denote the commutator subgroup of the braid group B_n on n strands, and always identify B_{n-1} with the subgroup of B_n fixing the last strand.

Lemma 2.1. *If $n \geq 4$ then \mathcal{B}_n is the normal closure of \mathcal{B}_{n-1} .*

Proof. Recall that the abelianization morphism $\ell : B_n \rightarrow \mathbb{Z}$ is given by $s_i \mapsto 1$. From the Reidemeister-Schreier method or even elementary group theory we know that \mathcal{B}_n is generated by the $s_1^k s_j s_1^{-k-1}$ for $j \geq 1$, $k \in \mathbb{Z}$. When $j > 2$ we have $s_1^k s_j s_1^{-k-1} = s_j$, which proves that \mathcal{B}_n is generated by \mathcal{B}_{n-1} and $s_n s_1^{-1}$. Now the braid relation $s_{n-1} s_n s_{n-1} = s_n s_{n-1} s_n$ implies $s_n = s_{n-1} s_n s_{n-1} (s_{n-1} s_n)^{-1}$ hence

$$s_n s_1^{-1} = (s_{n-1} s_n) s_{n-1} s_1^{-1} (s_{n-1} s_n)^{-1} = (s_{n-1} s_1^{-1} s_n s_1^{-1}) s_{n-1} s_1^{-1} (s_{n-1} s_1^{-1} s_n s_1^{-1})^{-1}$$

belongs to the normal closure of \mathcal{B}_{n-1} and this proves the claim. \square

In order to use known representation-theoretic results for the braid group, we shall need to lift isomorphisms between the restrictions of these representations to \mathcal{B}_n . This will be done by applying the following general lemma.

Lemma 2.2. *Let G be a group, \mathbb{k} a field and $R_1, R_2 : G \rightarrow \mathrm{GL}_N(\mathbb{k})$ with $N \geq 2$ two representations, such that $(R_1)_{|G'} = (R_2)_{|G'}$, where G' denotes the commutator subgroup of G , and such that the restriction of R_2 to G' is absolutely irreducible. Then there exists a character $\eta : G \rightarrow \mathbb{k}^\times$ such that $R_2 = R_1 \otimes \eta$.*

Proof. Let $\eta : G \rightarrow \mathrm{GL}_N(\mathbb{k})$ the map defined by $\eta(g) = R_2(g)R_1(g)^{-1}$. For $g \in G$ and $h \in G'$, we have $\eta(gh) = R_2(g)(R_2(h)R_1(h)^{-1})R_1(g)^{-1} = R_2(g)R_1(g)^{-1} = \eta(g)$, and also $\eta(gh) = \eta(ghg^{-1}.g) = R_2(ghg^{-1})R_2(g)R_1(g)^{-1}R_1(ghg^{-1}) = R_2(ghg^{-1})\eta(g)R_2(ghg^{-1})$. It follows that $\eta(g)$ centralizes $R_2(gG'g^{-1}) = R_2(G')$. By the absolute irreducibility assumption and Schur's lemma we get that $\eta(g) \in \mathbb{k}^\times$. Then $\eta(g_1 g_2) = R_2(g_1)(R_2(g_2)R_1(g_2)^{-1})R_1(g_1)^{-1} = R_2(g_1)\eta(g_2)R_1(g_1)^{-1} = R_2(g_1)R_1(g_1)^{-1}\eta(g_2) = \eta(g_1)\eta(g_2)$ for all $g_1, g_2 \in G$, which proves the claim. \square

We shall also use the following result.

Proposition 2.3. *Let K be a field, $\varphi : B_n \rightarrow \mathrm{PSL}_2(K)$ an homomorphism with $n \geq 5$. Then $\varphi(B_n)$ is abelian (and therefore cyclic).*

Proof. Without loss of generality we can assume that K is algebraically closed. Let $S_i = \varphi(s_i)$. If one of the S_i is 1, the same holds for the others since they are all conjugated one to the other, hence $\varphi = 1$. Also note that if two consecutive S_i commute, then the braid relation implies $S_i = S_{i+1}$, and this implies that all the S_i are equal, and therefore that $\varphi(B_n)$ is abelian. This is because every pair (s_i, s_{i+1}) is easily seen to be conjugated to any other pair (s_j, s_{j+1}) by an element of B_n .

Let i denote a primitive 4-root of 1, and E the image of $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \in \mathrm{SL}_2(K)$ inside $\mathrm{PSL}_2(K)$.

We let T denote the images of the diagonal matrices of determinant 1 inside $\mathrm{PSL}_2(K)$, and T' the images of the antidiagonal matrices. We first assume that S_1 is semisimple. Then all the S_i are semisimple. Up to conjugation, we can assume that $S_1 \in T$. Then the centralizer of S_1 is T , unless $S_1 = E$ in which case it is $T \cup T'$. If the centralizer is T , then $S_3, S_4 \in T$ and we get $S_3 S_4 = S_4 S_3$ and this implies that $\varphi(B_n)$ is abelian. If not, we have $S_1 = E$ hence $S_1^2 = 1$ and therefore $S_i^2 = 1$ for all i . It follows that φ factorizes through a morphism $\mathfrak{S}_n \rightarrow \mathrm{PSL}_2(K)$. If $\varphi(B_n)$ is not abelian the morphism $\mathfrak{S}_n \rightarrow \mathrm{PSL}_2(K)$ is into. But for $n \geq 5$ this contradicts Dickson's theorem (see e.g. [S] ch. 3 theorem 6.17). This proves the statement under the assumption that S_1 is semisimple.

If not, S_1 is unipotent and we can assume that S_1 is upper triangular. Then its centralizer is made of the image inside $\mathrm{PGL}_2(K)$ of upper-triangular matrices. It follows that S_3 and S_4 commute, and we conclude as before. \square

The statement we are mostly interested in is the following one.

Proposition 2.4. *Let K be a field. If $n \geq 7$ and $\varphi : \mathcal{B}_n \rightarrow \mathrm{PSL}_2(K)$ is an homomorphism, $\varphi = 1$.*

Proof. A presentation of \mathcal{B}_n has been obtained by Gorin-Lin in [GL], Theorem 2.1. We use it here. The group \mathcal{B}_n is generated by elements $p_0(= s_2 s_1^{-1})$, $p_1(= s_1 s_2 s_1^{-2})$, $b(= s_2 s_1^{-1} s_3 s_2^{-1})$, $q_\ell(= s_\ell s_1^{-1})$ for $3 \leq \ell \leq n-1$; and relations

$$\begin{aligned} (1) \quad & b = p_0 q_3 p_0^{-1} & (2) \quad & p_0 b p_0^{-1} = b^2 q_3^{-1} b & (3) \quad & p_1 q_3 p_1^{-1} = q_3^{-1} b \\ (4) \quad & p_1 b p_1^{-1} = (q_3^{-1} b)^3 q_3^{-2} b & (5) \quad & p_0 q_i = q_i p_1 \ (i \geq 4) & (6) \quad & p_1 q_i = q_i p_0^{-1} p_1 \ (i \geq 4) \\ (7) \quad & q_i q_{i+1} q_i = q_{i+1} q_i q_{i+1} \ (i \geq 3) & (8) \quad & q_i q_j = q_j q_i \ (i \geq 3, j > i+1) \end{aligned}$$

By abuse of notation, we identify these generators with their images under φ , and we show that they all become trivial. First note that, if one of the q_i is 1, then all the others are equal to 1 by relation (7), and then $b = 1$ by (3), $p_0 = p_1$ by (5) and $p_0 = 1$ by (6). Conversely, $p_0 = 1 \Leftrightarrow p_1 = 1$ by (5), and in this case $b = q_3$ by (1), and (2) implies $b^2 = b$ hence $b = q_3 = 1$. Finally, if $b = 1$, then $q_3 = 1$ by (1).

Now note that we have a morphism $B_{n-2} \rightarrow \mathcal{B}_n$ defined by $s_i \mapsto q_{i+2}$. By the above proposition we get that the $q_i, i \geq 3$ commute one to the other, and therefore are all equal to some element q .

$$p_1 q p_1^{-1} \stackrel{(3)}{=} q^{-1} b \stackrel{(1)}{=} q^{-1} p_0 q p_0^{-1} \stackrel{(5)}{=} q^{-1} q p_1 p_0^{-1}$$

hence $p_1 q p_1^{-1} = p_1 p_0^{-1}$ hence $p_1 q^{-1} = p_0$ and $p_1 = p_0 q \stackrel{(5)}{=} q p_1$ hence $q = 1$, a contradiction which proves the claim. \square

3. THE MAIN FACTORISATION

We recall that $H_n(\alpha)$ is semisimple as soon as the order of $\alpha \in \mathbb{F}_q^\times$ is greater than n . Moreover, in this case its simple modules are absolutely semisimple (see e.g. [Mat], cor. 3.44), and they are in 1-1 correspondence with the partitions of n . We now recall from [GP] explicit matrix models for these irreducible representations.

A combinatorial Gelfand model of $H_n(\alpha)$ is given by a \mathbb{F}_q -vector space \mathcal{V} with basis all the standard tableaux of size n . For each partition $\lambda \vdash n$, we denote V_λ the linear span of the standard tableaux of shape λ .

The action of the r -th generator on a standard tableau \mathbb{T} is given by the following rules

- (i) If r and $r+1$ lie in the same row of \mathbb{T} , then $s_r \cdot \mathbb{T} = \alpha \mathbb{T}$;
- (ii) if r and $r+1$ lie in the same column of \mathbb{T} , then $s_r \cdot \mathbb{T} = -\mathbb{T}$;
- (iii) otherwise, $s_r \cdot \mathbb{T} = m_r(\mathbb{T}) \mathbb{T} + (1 + m_r(\mathbb{T})) \mathbb{T}_{r \leftrightarrow r+1}$, where

$$m_r(\mathbb{T}) = \frac{(\alpha - 1)ct(\mathbb{T} : r+1)}{ct(\mathbb{T} : r+1) - ct(\mathbb{T} : r)},$$

$ct(\mathbb{T} : m) = -\alpha^{j-i}$ if m is in line i and column j , and $\mathbb{T}_{r \leftrightarrow r+1}$ is the tableau obtained from \mathbb{T} by interchanging r and $r+1$.

Notice that $(\mathbb{T}_{r \leftrightarrow r+1})' = (\mathbb{T}')_{r \leftrightarrow r+1}$. Moreover, if we let i denote the row, j denote the column where r lies, and similarly u, v for $r+1$, one checks easily that

$$m_r(\mathbb{T}') = m_r(\mathbb{T}_{r \leftrightarrow r+1}) = -\alpha^{j-i+u-v} m_r(\mathbb{T})$$

where \mathbb{T}' denotes the transposed of \mathbb{T} . We define a bilinear form on \mathcal{V} by the formula $(\mathbb{T}_1 | \mathbb{T}_2) = w(\mathbb{T}_1) \delta_{\mathbb{T}_2, \mathbb{T}_1'}$ where

$$w(\mathbb{T}) = \prod_{\substack{i < j \\ r_i(\mathbb{T}) > r_j(\mathbb{T})}} (-1) = (-1)^{\#\{i < j \mid r_i(\mathbb{T}) > r_j(\mathbb{T})\}}$$

and $r_k(\mathbb{T})$ denotes the row of \mathbb{T} in which lies k .

Proposition 3.1. *Let $b(\lambda) = \max\{i; \lambda_i \geq i\}$ denote the length of the diagonal of the Young diagram associated to $\lambda \vdash n$, and $\nu(\lambda) = 1$ if $(n - b(\lambda))/2$ is even, $\nu(\lambda) = -1$ otherwise.*

- (i) *For all $b \in B_n$, we have $(b.\mathbb{T}_1 | b.\mathbb{T}_2) = (-\alpha)^{\ell(b)} (\mathbb{T}_1 | \mathbb{T}_2)$ for any standard tableaux $\mathbb{T}_1, \mathbb{T}_2$.*
- (ii) *For all $b \in \mathcal{B}_n$, we have $(b.\mathbb{T}_1 | b.\mathbb{T}_2) = (\mathbb{T}_1 | \mathbb{T}_2)$ for any standard tableaux $\mathbb{T}_1, \mathbb{T}_2$.*
- (iii) *The restriction of the bilinear form (\mid) to subspaces V_λ if $\lambda = \lambda'$ and $V_\lambda \oplus V_{\lambda'}$ if $\lambda \neq \lambda'$ is nondegenerate. Its restriction to V_λ is symmetric if $\nu(\lambda) = 1$, and skew-symmetric otherwise. When it is symmetric, it has Witt index 0.*

Proof. In order to prove (i) and (ii), we check that $(s_r.\mathbb{T}_1 | s_r.\mathbb{T}_2) = (-\alpha)(\mathbb{T}_1 | \mathbb{T}_2)$ for all r . If r and $r+1$ lie in the same row or the same column of \mathbb{T}_1 , the LHS and RHS are both 0 unless $\mathbb{T}_2 = \mathbb{T}_1'$, and in that case the verification of the formula is immediate. If not, the LHS and RHS are again both 0, except in two cases that we consider separately. In the first one, we have $\mathbb{T}_1 = \mathbb{T}$, $\mathbb{T}_2 = \mathbb{T}'$. In that case we have $(s_r.\mathbb{T}_1 | s_r.\mathbb{T}_2) = (s_r.\mathbb{T} | s_r.\mathbb{T}')$ and, since $s_r.\mathbb{T}' = m_r(\mathbb{T}')\mathbb{T}' + (1 + m_r(\mathbb{T}'))\mathbb{T}'_{r \leftrightarrow r+1}$, we get

$$(s_r.\mathbb{T} | s_r.\mathbb{T}') = m_r(\mathbb{T})m_r(\mathbb{T}')w(\mathbb{T}) + (1 + m_r(\mathbb{T}))(1 + m_r(\mathbb{T}'))w(\mathbb{T}_{r \leftrightarrow r+1})$$

and $(s_r.\mathbb{T} | s_r.\mathbb{T}') = -\alpha(\mathbb{T} | \mathbb{T}')$ iff

$$(-\alpha - m_r(\mathbb{T})m_r(\mathbb{T}'))w(\mathbb{T}) = (1 + m_r(\mathbb{T}))(1 + m_r(\mathbb{T}'))w(\mathbb{T}_{r \leftrightarrow r+1})$$

In the other case we have $\mathbb{T}_1 = \mathbb{T}$, $\mathbb{T}_2 = \mathbb{T}'_{r \leftrightarrow r+1}$. In this case $(s_r.\mathbb{T}_1 | s_r.\mathbb{T}_2) = (s_r.\mathbb{T} | s_r.\mathbb{T}'_{r \leftrightarrow r+1})$ and, since $s_r.\mathbb{T}'_{r \leftrightarrow r+1} = m_r(\mathbb{T}'_{r \leftrightarrow r+1})\mathbb{T}'_{r \leftrightarrow r+1} + (1 + m_r(\mathbb{T}'_{r \leftrightarrow r+1}))\mathbb{T}'$ we get that $(s_r.\mathbb{T}_1 | s_r.\mathbb{T}_2)$ is

$$m_r(\mathbb{T})(1 + m_r(\mathbb{T}'_{r \leftrightarrow r+1}))w(\mathbb{T}) + (1 + m_r(\mathbb{T}))m_r(\mathbb{T}'_{r \leftrightarrow r+1})w(\mathbb{T}_{r \leftrightarrow r+1})$$

and $(s_r.\mathbb{T}_1 | s_r.\mathbb{T}_2) = -\alpha(\mathbb{T}_1 | \mathbb{T}_2) = 0$ iff

$$-m_r(\mathbb{T})(1 + m_r(\mathbb{T}'_{r \leftrightarrow r+1}))w(\mathbb{T}) = (1 + m_r(\mathbb{T}))m_r(\mathbb{T}'_{r \leftrightarrow r+1})w(\mathbb{T}_{r \leftrightarrow r+1})$$

By a direct computation we check that

$$\frac{-m_r(\mathbb{T})(1 + m_r(\mathbb{T}'_{r \leftrightarrow r+1}))}{(1 + m_r(\mathbb{T}))m_r(\mathbb{T}'_{r \leftrightarrow r+1})} = \frac{(-\alpha - m_r(\mathbb{T})m_r(\mathbb{T}'))}{(1 + m_r(\mathbb{T}))(1 + m_r(\mathbb{T}'))} = -1$$

hence the equations hold in both cases because of the elementary properties of w , namely $w(\mathbb{T}_{r \leftrightarrow r+1}) = -w(\mathbb{T})$.

We now prove (iii). The non-degeneracy of (\mid) follows from the decomposition of V_λ as an orthogonal direct sum of planes spanned by pairs \mathbb{T}, \mathbb{T}' , on which (\mid) is clearly non-degenerate. We consider now the possible symmetry of the restriction of (\mid) to some V_λ with

$\lambda = \lambda'$. We proved in [M2], Lemme 6, that $w(\mathbb{T})w(\mathbb{T}')$ only depends on the shape λ of \mathbb{T} , and is equal to $\nu(\lambda)$. Since

$$(\mathbb{T}_2|\mathbb{T}_1) = w(\mathbb{T}_2)\delta_{\mathbb{T}_1, \mathbb{T}'_2} = w(\mathbb{T}_2)\delta_{\mathbb{T}_2, \mathbb{T}'_1} = \frac{1}{\nu(\lambda)}w(\mathbb{T}'_2)\delta_{\mathbb{T}_2, \mathbb{T}'_1} = \nu(\lambda)w(\mathbb{T}_1)\delta_{\mathbb{T}_2, \mathbb{T}'_1} = \nu(\lambda)(\mathbb{T}_1|\mathbb{T}_2)$$

we get the conclusion. Finally, the computation of the Witt index in the symmetric case is an immediate consequence of the direct sum decomposition in hyperbolic planes already mentioned. \square

We define $\mathcal{L} \in \text{End}(\mathcal{V})$ by $\mathbb{T} \mapsto w(\mathbb{T})\mathbb{T}'$. We have

Lemma 3.2. *Let $\lambda \vdash n$ such that $\lambda \neq \lambda'$. Then \mathcal{L} induces an endomorphism of $V_\lambda \oplus V_{\lambda'}$ exchanging V_λ and $V_{\lambda'}$ such that the action of s_r satisfies*

$$\frac{\mathcal{L}s_r\mathcal{L}^{-1}}{(-\alpha)\nu(\lambda)} = {}^t s_r^{-1}$$

Proof. We check that the actions of the LHS and RHS coincide on every standard tableau \mathbb{T} of shape λ . When $s_r.\mathbb{T}$ is proportional to \mathbb{T} , this directly follows from the formula $w(\mathbb{T})w(\mathbb{T}') = \nu(\lambda)$. Otherwise, we restrict the action of s_r to the linear span of $\mathbb{T}, \mathbb{T}_{r \leftrightarrow r+1}$ and consider its matrix w.r.t. the basis $(\mathbb{T}, \mathbb{T}_{r \leftrightarrow r+1})$. It is

$$s_r = \begin{pmatrix} m_r(\mathbb{T}) & 1 + m_r(\mathbb{T}_{r \leftrightarrow r+1}) \\ 1 + m_r(\mathbb{T}) & m_r(\mathbb{T}_{r \leftrightarrow r+1}) \end{pmatrix}$$

and $\det(s_r) = -\alpha$ hence

$${}^t s_r^{-1} = \frac{-1}{\alpha} \begin{pmatrix} m_r(\mathbb{T}_{r \leftrightarrow r+1}) & -(1 + m_r(\mathbb{T})) \\ -(1 + m_r(\mathbb{T}_{r \leftrightarrow r+1})) & m_r(\mathbb{T}) \end{pmatrix}$$

On the other hand, we have $\mathcal{L}^2 = \nu(\lambda)\text{Id}$ hence $\mathcal{L}^{-1} : \mathbb{T} \mapsto w(\mathbb{T}')\mathbb{T}'$ and, since $w(\mathbb{T}'_{r \leftrightarrow r+1}) = -w(\mathbb{T}')$, we get $\mathcal{L}s_r\mathcal{L}^{-1}.\mathbb{T} = \nu(\lambda)m_r(\mathbb{T}')\mathbb{T} - \nu(\lambda)(1 + m_r(\mathbb{T}'))\mathbb{T}_{r \leftrightarrow r+1}$. It follows that

$$\frac{\mathcal{L}s_r\mathcal{L}^{-1}}{\nu(\lambda)} : \mathbb{T} \mapsto m_r(\mathbb{T}')\mathbb{T} - (1 + m_r(\mathbb{T}'))\mathbb{T}_{r \leftrightarrow r+1} = m_r(\mathbb{T}_{r \leftrightarrow r+1})\mathbb{T} - (1 + m_r(\mathbb{T}_{r \leftrightarrow r+1}))\mathbb{T}_{r \leftrightarrow r+1}$$

which proves the formula. \square

As a consequence, we get

Proposition 3.3. *If $\lambda \neq \lambda'$, the restriction to \mathcal{B}_n of $R_\lambda \times R_{\lambda'} : B_n \rightarrow \text{GL}(V_\lambda) \times \text{GL}(V_{\lambda'})$ factors through the restriction of R_λ and $(Q \mapsto (Q, \mathcal{L}^{-1} {}^t Q^{-1} \mathcal{L}))$*

Lemma 3.4. *If the order of α is $> n$, and $n \geq 2$, then the following are true.*

- (i) *For all $\lambda \vdash n$, the restriction of R_λ to \mathcal{B}_n is absolutely irreducible.*
- (ii) *Let $\lambda, \mu \vdash n$ such that $\dim V_\lambda, \dim V_\mu > 1$. If the restrictions of R_λ and R_μ to \mathcal{B}_n are isomorphic, then $\lambda = \mu$.*
- (iii) *Let $\lambda, \mu \vdash n$ such that $\dim V_\lambda, \dim V_\mu > 1$. If the restrictions of R_λ and of the dual representation of R_μ to \mathcal{B}_n are isomorphic, then $\lambda = \mu'$.*

Proof. We prove (i) by induction on n , the cases $n \leq 5$ being a consequence of [BM]. Let U be a \mathcal{B}_n -stable subspace of $V_\lambda \otimes_{\mathbb{F}_q} k$, for some extension k of \mathbb{F}_q . By the branching rule and the induction assumption, the action of B_{n-1} on V_λ is semisimple, and the decomposition of V_λ as a direct sum of simple modules for B_{n-1} is also a decomposition in a sum of simple modules

for \mathcal{B}_{n-1} . From this it follows that every simple submodule of U for the action of \mathcal{B}_{n-1} is also B_{n-1} -stable, hence U , being semisimple, is also B_{n-1} -stable. Since B_n is generated by B_{n-1} and \mathcal{B}_n it follows that U is B_n -stable hence $U = V_\lambda$ and this concludes the proof of (i).

We now prove (ii). By lemma 2.2 and because the abelianization of B_n is given by $\ell : B_n \rightarrow \mathbb{Z}$, $\sigma_i \mapsto 1$, this means that $R_\mu(b) = R_\lambda(b)u^{\ell(b)}$ for some $u \in \mathbb{F}_q^\times$, and this for all $b \in B_{n-1}$. This implies that the spectrum of $R_\mu(s_1)$, which is $\{-1, \alpha\}$, is also equal to $\{-u, u\alpha\}$. Since we assumed $\alpha^2 \neq 1$ this is possible only if $u = 1$ hence $R_\mu = R_\lambda$, which is excluded because these two representations of the Hecke algebras are non-isomorphic by assumption.

The proof of (iii) is similar, once we notice that the restriction to \mathcal{B}_n of the dual representation of R_μ is isomorphic to the restriction of $R_{\lambda'}$, by the above results. \square

We now let $\lambda = \lambda_r = [n - r, 1^r]$ and we want to compare R_{λ_r} with $\Lambda^r R_{\lambda_1}$. Any standard tableau of shape λ_r can be indexed by the set of indices $I = \{i_1, \dots, i_r\} \subset \{2, \dots, n\}$, assuming $i_1 < \dots < i_r$, where each i_k is the content of the unique box of the diagram in line $k + 1$. We let v_I denote the corresponding standard tableau, and we let $v_i = v_{\{i\}}$. Note that, when $\{k, k + 1\} \not\subset I$, then $ct(v_I : k)/ct(v_I : k + 1)$ only depends on the number of boxes lying between k and $k + 1$ inside the hook-shaped tableau v_I , and therefore only on k . From this we get by explicit computation that, if $k \in I$ but $k + 1 \notin I$, then

$$m_k(v_I) = \frac{\alpha - 1}{1 - \alpha^{-k}}, 1 + m_k(v_I) = \frac{\alpha - \alpha^{-k}}{1 - \alpha^{-k}},$$

and, if $k \notin I$ but $k + 1 \in I$, then

$$m_k(v_I) = \frac{\alpha - 1}{1 - \alpha^k}, 1 + m_k(v_I) = \frac{\alpha - \alpha^k}{1 - \alpha^k}.$$

It follows that

- if $k, k + 1 \notin I$, $s_k \cdot v_I = \alpha v_I$,
- if $k, k + 1 \in I$, $s_k \cdot v_I = -v_I$,
- if $k \in I$, $k + 1 \notin I$, $s_k \cdot v_I = \frac{\alpha - 1}{1 - \alpha^{-k}} v_I + \frac{\alpha - \alpha^{-k}}{1 - \alpha^{-k}} v_{I \Delta \{k, k + 1\}}$
- if $k \notin I$, $k + 1 \in I$, $s_k \cdot v_I = \frac{\alpha - 1}{1 - \alpha^k} v_I + \frac{\alpha - \alpha^k}{1 - \alpha^k} v_{I \Delta \{k, k + 1\}}$

where Δ denotes the symmetric difference : $A \Delta B = (A \cup B) \setminus (A \cap B)$.

On the other hand, to such an $I = \{i_1 < \dots < i_r\}$ we can associate $u_I = v_{i_1} \wedge \dots \wedge v_{i_r} \in \Lambda^r V_{\lambda_1}$. By direct computation we get

- if $k, k + 1 \notin I$, $s_k \cdot u_I = \alpha^r u_I$,
- if $k, k + 1 \in I$, $s_k \cdot u_I = -\alpha^{r-1} u_I$,
- if $k \in I$, $k + 1 \notin I$, $s_k \cdot u_I = \frac{\alpha - 1}{1 - \alpha^{-k}} \alpha^{r-1} u_I + \frac{\alpha - \alpha^{-k}}{1 - \alpha^{-k}} \alpha^{r-1} u_{I \Delta \{k, k + 1\}}$
- if $k \notin I$, $k + 1 \in I$, $s_k \cdot u_I = \frac{\alpha - 1}{1 - \alpha^k} \alpha^{r-1} u_I + \frac{\alpha - \alpha^k}{1 - \alpha^k} \alpha^{r-1} u_{I \Delta \{k, k + 1\}}$

meaning that, if we identify these two vector spaces via $v_I \leftrightarrow u_I$, we have $(\Lambda^r R_{\lambda_1})(s_r) = \alpha^{r-1} R_{\lambda_r}(s_r)$. Therefore, we get $(\Lambda^r R_{\lambda_1})(g) = \alpha^{(r-1)\ell(g)} R_{\lambda_r}(g)$ for all $g \in B_n$, and the following

Proposition 3.5. *For every $r \in \{1, n - 1\}$, the restriction to \mathcal{B}_n of the morphism $R_{[n-r, 1^r]} : B_n \rightarrow \text{GL}(V_{[n-r, 1^r]})$ factors through the restriction of $R_{[n-1, 1]} : B_n \rightarrow \text{GL}(V_{[n-1, 1]})$ to \mathcal{B}_n .*

Now assume that $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ but $\mathbb{F}_p(\alpha + \alpha^{-1}) \neq \mathbb{F}_q$. In that case there exists an involutive field automorphism $\varepsilon : x \mapsto \bar{x}$ of \mathbb{F}_q defined by $\bar{\alpha} = \alpha^{-1}$. We define a hermitian form on \mathcal{V} by

the formula $\langle \mathbb{T}_1, \mathbb{T}_2 \rangle = d(\mathbb{T}_1) \delta_{\mathbb{T}_1, \mathbb{T}_2}$ where

$$d(\mathbb{T}) = \prod_{\substack{i < j \\ \mathfrak{r}(i) > \mathfrak{r}(j)}} \frac{\alpha^{\mathfrak{c}(j) - \mathfrak{r}(j)} - \alpha^{\mathfrak{c}(i) - \mathfrak{r}(i) + 1}}{\alpha^{\mathfrak{c}(j) - \mathfrak{r}(j) + 1} - \alpha^{\mathfrak{c}(i) - \mathfrak{r}(i)}}$$

where $\mathfrak{c}(k)$, respectively $\mathfrak{r}(k)$, denote the column, respectively row, of \mathbb{T} where k lies.

Proposition 3.6. *The action of B_n on \mathcal{V} is unitary with respect to the above hermitian form. The restriction of this hermitian form on every subspace V_λ is nondegenerate.*

Proof. We need to check that $\langle s_r \mathbb{T}_1, s_r \mathbb{T}_2 \rangle = \langle \mathbb{T}_1, \mathbb{T}_2 \rangle$ for all standard tableaux $\mathbb{T}_1, \mathbb{T}_2$. If r lies in the same row or the same column of \mathbb{T}_1 or \mathbb{T}_2 then the equality simply follows from $\alpha \bar{\alpha} = (-1)^2 = 1$. If not, then we can assume that \mathbb{T}_2 is either $\mathbb{T} = \mathbb{T}_1$ or $\mathbb{T}_{r \leftrightarrow r+1}$, and thus we only need to check that the action of s_r on the plane spanned by $\mathbb{T}, \mathbb{T}_{r \leftrightarrow r+1}$ is unitary with respect to the induced hermitian form. We express s_r in the basis $(\mathbb{T}, \mathbb{T}_{r \leftrightarrow r+1})$. In order to check the unitarity, up to a harmless exchange of \mathbb{T} and $\mathbb{T}_{r \leftrightarrow r+1}$, we can assume that $\mathfrak{r}_{\mathbb{T}}(r) < \mathfrak{r}_{\mathbb{T}}(r+1)$. Then we get

$$d(\mathbb{T}_{r \leftrightarrow r+1}) = d(\mathbb{T}) \frac{\alpha^{\mathfrak{c}(r+1) - \mathfrak{r}(r+1)} - \alpha^{\mathfrak{c}(r) - \mathfrak{r}(r) + 1}}{\alpha^{\mathfrak{c}(r+1) - \mathfrak{r}(r+1) + 1} - \alpha^{\mathfrak{c}(r) - \mathfrak{r}(r)}} = d(\mathbb{T}) \frac{\alpha^{v-u} - \alpha^{j-i+1}}{\alpha^{v-u+1} - \alpha^{j-i}}$$

where (i, j) and (u, v) are the coordinates of r and $r+1$ inside \mathbb{T} , respectively. It remains to check that, if $D = \text{diag}(1, \frac{\alpha^{v-u} - \alpha^{j-i+1}}{\alpha^{v-u+1} - \alpha^{j-i}})$ and S_r is the 2×2 matrix representing the action of s_r , then we have $DS_r = {}^t S_r^{-1} D$, and this is straightforward. The nondegeneracy statement is obvious. \square

In these circumstances, we have that

Lemma 3.7. *We assume that the order of α is $> n$, $\mathbb{F}_p(\alpha + \alpha^{-1}) \neq \mathbb{F}_q$ and $\lambda, \mu \vdash n$ with $\dim V_\lambda > 1$. If $n \geq 3$, then the restrictions to \mathcal{B}_n of R_λ and $\overline{R_\mu}^*$ are isomorphic iff $\lambda = \mu$.*

Proof. Because of the unitary structure we get that the restrictions to \mathcal{B}_n of R_λ and of its conjugate-dual $\overline{R_\lambda}^*$ are isomorphic. Under the assumptions of the lemma this means that the restrictions of R_λ and R_μ are isomorphic, and this implies $\lambda = \mu$ by lemma 3.4. \square

4. REPRESENTATION-THEORETIC TECHNICALITIES

We also need to consider the set of elements that preserve both a unitary and an orthogonal/symplectic form. If φ denotes a nondegenerate bilinear form over \mathbb{F}_q^N we let $OSP_N(\varphi)$ denotes the group of isometries of this form ; if ψ is an hermitian form, we let $U_N(\psi)$ denote its group of isometries. We will use the following property, which is probably folklore.

Proposition 4.1. *Let $q = u^2$, φ a nondegenerate bilinear form over \mathbb{F}_q^N , ψ a nondegenerate hermitian form over \mathbb{F}_q^N . If $G \subset OSP_N(\varphi) \cap U_N(\psi)$ is absolutely irreducible, then there exists $x \in GL_N(q)$ and a nondegenerate bilinear form φ' over \mathbb{F}_u^N such that ${}^x G \subset OSP(\varphi')$. Moreover, φ' is (skew-)symmetric if and only if φ is so.*

Proof. We let $R : G \rightarrow \mathrm{GL}_N(q)$ denote the natural inclusion, and we consider it as a linear representation of G . We set $\Gamma = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_u) = \{\mathrm{Id}, \varepsilon\}$ and use both notations $\varepsilon(x) = \bar{x}$. We have $R^* \simeq R$ and $\bar{R}^* \simeq R$ hence $R \simeq \bar{R}$. As a consequence there exists $P \in \mathrm{GL}_N(q)$ such that $\bar{R}(g) = PR(g)P^{-1}$ for all $g \in G$. It follows that $\bar{P}P$ commutes to every $\bar{R}(g)$. By Schur's lemma and the absolute irreducibility of G we get $\bar{P}P \in (\mathbb{F}_q^\times)^\Gamma = \mathbb{F}_u^\times$. Since the norm map $\mathbb{F}_q^\times \rightarrow \mathbb{F}_u^\times$ is surjective, we have $\bar{P}P = \bar{\lambda}\lambda$ for some $\lambda \in \mathbb{F}_q^\times$ and thus, replacing if needed P with $P\lambda^{-1}$, we may assume $\bar{P}P = \mathrm{Id}$. Then $\mathrm{Id} \mapsto \mathrm{Id}, \varepsilon \mapsto P$ defines an element in $Z^1(\Gamma, \mathrm{GL}_N(q))$. By Hilbert's theorem 90 it follows that there exists $S \in \mathrm{GL}_N(q)$ such that $P = \bar{S}S^{-1}$. Then, setting $R'(g) = S^{-1}R(g)S$, we have $\bar{R}'(g) \in \mathrm{GL}_N(\mathbb{F}_u)$. Moreover, $R'(g)$ preserves the bilinear form deduced from φ : in matrix form, if W denotes the matrix of φ in the canonical basis of \mathbb{F}_q^N , we have ${}^tR(g)WR(g) = W$ for all $g \in G$, hence $R'(g)$ preserves the bilinear form φ^S given by the matrix $W^S = {}^tSW S \in \mathrm{GL}_N(q)$. Since $R'(g) \in \mathrm{GL}_N(u)$ it also preserves all the $\tilde{W}_\lambda = \lambda W^S + \bar{\lambda} \bar{W}^S$ for all $\lambda \in \mathbb{F}_q^\times$. Since $W^S \neq 0$, there exists $\lambda \in \mathbb{F}_q^\times$ such that $\tilde{W}_\lambda \neq 0$, for otherwise $\lambda/\bar{\lambda} = \mu/\bar{\mu}$ for all $\lambda, \mu \in \mathbb{F}_q^\times$, and this would imply $u = q$. Then \tilde{W}_λ for such a λ defines a bilinear form φ' over \mathbb{F}_u^N , and we have $R'(g) \in \mathrm{OSP}(\varphi')$ for all $g \in G$, hence ${}^xG \subset \mathrm{OSP}(\varphi')$ for $x = S^{-1}$. The last part of the statement is a consequence of our construction of φ' . \square

5. PROOF OF THE MAIN THEOREM

We let \mathcal{E}_n denote the set of partitions on n which are not hooks. From section 3 we know that the morphism $\mathcal{B}_n \rightarrow H_n(\alpha)^\times \simeq \prod_{\lambda \vdash n} \mathrm{GL}(\lambda)$ factorizes through the morphism

$$\Phi_n : \mathcal{B}_n \rightarrow \mathrm{SL}_{n-1}(q) \times \prod_{\substack{\lambda \in \mathcal{E}_n \\ \lambda < \lambda'}} \mathrm{SL}(\lambda) \times \prod_{\substack{\lambda \in \mathcal{E}_n \\ \lambda = \lambda'}} \mathrm{OSP}'(\lambda)$$

where $\mathrm{OSP}'(\lambda) = G(\lambda)$ denotes the commutator subgroup of the group of isometries of the bilinear form defined in section 3. In particular, when $\lambda = \lambda', p \neq 2$ and when the action of the braid group on V_λ preserves an orthogonal form, then $\mathrm{OSP}'(\lambda)$ denotes the group classically denoted $\Omega_N^+(q)$ (see [W]), where $N = \dim V_\lambda$. We assume that $\mathbb{F}_p(\alpha + \alpha^{-1}) = \mathbb{F}_q = \mathbb{F}_p(\alpha)$ and, as in [BM], that the order of $\alpha \in \mathbb{F}_q^\times$ is not 2, 3, 4, 5, 6, 10. Theorem 1.1 in that case states that Φ_n is surjective when the order of α is in addition greater than n . For $n \leq 5$ this is a consequence of [BM]. We then proceed by induction on n , assuming that Φ_{n-1} is surjective and $n \geq 6$. We first prove that each of the composites R_λ of Φ_n with the projection on the quasi-simple factor attached to λ is surjective. For this, let $\lambda \in \mathcal{E}_n$. If λ has at most two rows or at most two columns this is a consequence of [BM], so we can assume that λ contains $[3, 2, 1]$, hence $\dim V_\lambda \geq 16$. Moreover, for $n = 6$ the only case to be taken care of is $\lambda = [3, 2, 1]$. Finally note that, since $n \geq 6$, our assumptions imply that α has order at least 7, hence $q \geq 8$.

We use the notation $\mu \subset \lambda$ to indicate the inclusion of the corresponding Young diagrams, namely that $\mu_i \leq \lambda_i$ for all i 's. By the induction assumption, we know that

- if $\lambda \neq \lambda'$, there exists $\mu \subset \lambda$ of size $n-1$ such that $\mu' \not\subset \lambda$ and such that $\mu \supset [3, 2]$ or $\mu \supset [2, 2, 1]$ (this is because λ is equal to the union of the μ 's of size $n-1$ contained in it such that $\mu \supset [3, 2]$ or $\mu \supset [2, 2, 1]$). In particular $\mu \neq \mu'$. Since μ is not a hook, by the induction assumption it follows that the image of \mathcal{B}_{n-1} contains a direct factor

- $SL(\mu)$ and in particular some $SL_2(q)$ acting naturally on some 2-dimensional subspace and some $SL_3(q)$ acting naturally on some 3-dimensional subspace.
- if $\lambda = \lambda'$ and there exists $[3, 2] \subset \mu \subset \lambda$ of size $n - 1$ with $\mu \neq \mu'$, then $\mu' \subset \lambda$. By the induction assumption the image of \mathcal{B}_{n-1} contains a subgroup acting on a subspace of dimension $2 \dim V_\mu$ as $\{x \oplus^t x^{-1} \mid x \in SL_{\dim V_\mu}(q)\}$. Since $\dim V_\mu \geq 3$ it contains in particular a subgroup acting on a subspace of dimension 4 as $\{x \oplus^t x^{-1} \mid x \in SL_2(q)\}$, and a subgroup acting on some 6-dimensional subspace as $\{x \oplus^t x^{-1} \mid x \in SL_3(q)\}$.
 - if $\lambda = \lambda'$ and there does *not* exist $[3, 2] \subset \mu \subset \lambda$ of size $n - 1$ with $\mu \neq \mu'$. In this case it is easily checked that λ is a square diagram, hence the restriction of λ to \mathfrak{S}_{n-1} is irreducible, and that the corresponding diagram μ satisfies $\mu = \mu'$, $\mu \supset [3, 2, 1]$. Since the restriction to \mathfrak{S}_{n-1} is irreducible one can check that $OSP(\mu) = OSP(\lambda)$ hence, since $G \subset OSP'(\lambda)$, we get $G = OSP'(\lambda)$ and this case does not need to be considered further.

We notice that $\{x \oplus^t x^{-1} \mid x \in SL_2(q)\}$ contains the element

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix}$$

hence $R_\lambda(\mathcal{B}_n)$ contains in all cases an element x such that $[x, V_\lambda] = (x - 1)V_\lambda$ has dimension 2, this being obvious when it contains a natural $SL_2(q)$. We then use the following result of [GS], for $V = V_\lambda$, $G = R_\lambda(\mathcal{B}_n)$.

Theorem 5.1. ([GS], theorem 7.A) *Let V be a finite dimensional vector space of dimension $d > 8$ over an algebraically closed field \mathbb{F} of characteristic $p > 0$. Let G be a finite irreducible subgroup of $GL(V)$ which is primitive and tensor-indecomposable on V . Define $\nu_G(V)$ to be the minimum dimension of $[\beta g, V] = (\beta g - 1)V$ for $g \in G$, β a scalar with $\beta g \neq 1$. Then either $\nu_G(V) > \max(2, \sqrt{d}/2)$ or one of the following holds:*

- (i) G is classical in a natural representation
- (ii) G is alternating or symmetric of degree c and V is the deleted permutation module of dimension $c - 1$ or $c - 2$.
- (iii) $F^*(G) = U_5(2)$ with $p \neq 2, d = 10$.

Note that (iii) does not occur because $d \geq 16$. If G contains a natural $SL_2(q)$, then G is tensor-indecomposable by the following lemma.

Lemma 5.2. *If $d \geq 6$ and $G \subset GL_d(\mathbb{F})$ contains an element conjugated to $\text{diag}(\zeta, \zeta^{-1}, 1, 1, \dots)$ for $\zeta^2 \neq 1$, then G is tensor-indecomposable.*

Proof. Let r denote the order of g . Since \mathbb{F} has characteristic p , we know that r is coprime to p . Assume by contradiction that G is tensor-decomposable. Then, g could be written $g_1 \otimes g_2$, hence $g^r = 1$ implies that $g_1^r = t$ and $g_2^r = t^{-1}$ for some $t \in \mathbb{F}^\times$. Since r is prime to p , $X^r - t^{\pm 1}$ has no multiple root and thus g_1, g_2 are semisimple.

Assume $d = ab$ with $g_1 \in GL_a(\mathbb{F})$ and $g_2 \in GL_b(\mathbb{F})$ and let $\lambda_1, \dots, \lambda_a$ and μ_1, \dots, μ_b their eigenvalues. We can assume $a \geq 3, b \geq 2$, and $\lambda_1 \mu_1 = \zeta$. We let $\lambda_1 = \beta$, hence $\mu_1 = \beta^{-1} \zeta$. Up to reordering, there are only three cases :

- either $\lambda_2 \mu_2 = \zeta^{-1}$, and then $\lambda_1 \mu_2 = 1$ hence $\mu_2 = \beta^{-1}$;
- or $\lambda_1 \mu_2 = \zeta^{-1}$, and then $\mu_2 = \beta^{-1} \zeta^{-1}$;

- or $\lambda_2\mu_1 = \zeta^{-1}$, that is $\lambda_2 = \beta^{-1}$, and then $\lambda_1\mu_2 = \lambda_2\mu_2 = 1$ implying $\lambda_2 = \beta$ and $\beta^2 = 1$, hence also $\mu_2 = \beta^{-1} = \beta$, $\mu_1 = \beta\zeta$.

In these three cases, the fact that $1 = \lambda_3\mu_1 = \lambda_3\mu_2 \Rightarrow \mu_1 = \mu_2$ yields a contradiction. \square

If G does not contain a natural $\mathrm{SL}_2(q)$, then it contains a twisted-diagonal embedding of $\mathrm{SL}_2(q)$ and therefore an element which is conjugated to $\mathrm{diag}(\zeta, \zeta, \zeta^{-1}, \zeta^{-1}, 1, \dots, 1)$ with ζ of order $q - 1$. It is therefore tensor-indecomposable by the following lemma.

Lemma 5.3. *If $d \geq 16$ and $G \subset \mathrm{GL}_d(\mathbb{F})$ contains an element of order prime to p and conjugated to $\mathrm{diag}(\zeta, \zeta, \zeta^{-1}, \zeta^{-1}, 1, \dots, 1)$ with $\zeta^2 \neq 1$, then G is tensor indecomposable, except possibly if $G = G_1 \otimes G_2$ with $G_1 \subset \mathrm{GL}_2(\mathbb{F})$.*

Proof. We let g denote the element of the statement, and assume by contradiction that $g = g_1 \otimes g_2$ with $g_1 \in \mathrm{GL}_a(\mathbb{F})$, $g_2 \in \mathrm{GL}_b(\mathbb{F})$, $ab = d$ and $a, b \geq 3$. Since $d \geq 16$ we can assume $a \geq 3$, $b \geq \sqrt{d} \geq 4$. As in the proof of the previous lemma, the order condition imply that g_1 and g_2 are semisimple. Let $\lambda_1, \lambda_2, \dots$ and μ_1, μ_2, \dots denote the eigenvalues of g_1 and g_2 , respectively. Up to reordering we can assume $\lambda_1\mu_1 = \zeta$.

Let us first assume there exists $i \neq 1$ such that $\lambda_1\mu_i = \zeta$. Up to reordering we can assume $i = 2$, hence $\lambda_1\mu_2 = \lambda_1\mu_1 = \zeta$, hence $\mu_1 = \mu_2$. Hence $\lambda_2\mu_1 = \lambda_2\mu_2 \in \{\zeta^{-1}, 1\}$. If $\lambda_2\mu_1 = \lambda_2\mu_2 = \zeta^{-1}$, we then have $\lambda_1\mu_3 = \lambda_2\mu_3 = 1$, and therefore $\lambda_1 = \lambda_2$. But then $\zeta = \lambda_1\mu_1 = \lambda_2\mu_1 = \zeta^{-1}$, contradicting $\zeta^2 \neq 1$.

On the other hand, if $\lambda_2\mu_1 = \lambda_2\mu_2 = 1$, when $b \geq 5$ there exists $i > 2$ such that $\lambda_2\mu_i = 1$. But then $\mu_i = \mu_2$, hence $\lambda_1\mu_i = \lambda_1\mu_2 = \zeta$ and ζ would appear with multiplicity 3, a contradiction. If $b = 4$ and there is no $i > 2$ such that $\lambda_2\mu_i = 1$, then $\lambda_2\mu_3 = \lambda_2\mu_4 = \zeta^{-1}$. Since $a \geq 3$ this implies $\lambda_3\mu_2 = 1 = \lambda_3\mu_3$ hence $\mu_2 = \mu_3$, contradicting $\zeta = \lambda_1\mu_2 = \lambda_1\mu_3 = 1$.

We can thus assume without loss of generality that, for all $i \neq 1$, we have $\lambda_1\mu_i \neq \zeta$.

Let us assume now that $\lambda_2\mu_1 = \zeta$. Since $\lambda_1\mu_1 = \zeta$ we have $\lambda_2 = \lambda_1$. Since $a \geq 3$ we get $\lambda_3\mu_i = 1$ for all i , hence $\mu_1 = \mu_2 = \mu_3$ and $\zeta = \lambda_1\mu_1 = \lambda_1\mu_2$, contradicting $\lambda_1\mu_2 \neq \zeta$.

We can thus now assume without loss of generality that, for all $i \neq 1$, we have $\lambda_1\mu_i \neq \zeta$ and $\lambda_2\mu_1 \neq \zeta$. Up to reordering we can thus moreover assume $\lambda_2\mu_2 = \zeta$. If there existed $i > 2$ such that $\lambda_1\mu_i = \lambda_2\mu_i$, then the consequence $\lambda_1 = \lambda_2$ would contradict $\lambda_1\mu_2 \neq \lambda_2\mu_2$. We can thus assume that

- either $\lambda_1\mu_3 = \lambda_1\mu_4 = 1$, $\lambda_2\mu_3 = \lambda_2\mu_4 = \zeta^{-1}$, but then $\lambda_1\mu_2 = 1 = \lambda_1\mu_3$ hence $\mu_2 = \mu_3$ and $\lambda_2\mu_3 = \zeta^{-1} = \lambda_2\mu_2 = \zeta$, a contradiction;
- or $\lambda_1\mu_4 = \zeta^{-1} = \lambda_2\mu_3$, but then $\lambda_1\mu_2 = \lambda_1\mu_3 = 1$ hence $\mu_2 = \mu_3$ and $\zeta = \lambda_2\mu_2 = \lambda_2\mu_3 = \zeta^{-1}$, a contradiction;
- or $\lambda_1\mu_2 = \zeta^{-1}$ or $\lambda_2\mu_1 = \zeta^{-1}$, in which case there would exist $i \in \{3, 4\}$ such that $\lambda_1\mu_i = \lambda_2\mu_i$, hence $\lambda_1 = \lambda_2$, contradicting $\lambda_1\mu_2 \neq \lambda_2\mu_2$.

This concludes the proof. \square

We now want to rule out case (ii) of theorem 5.1. For this, we first consider the case where G contains a natural $\mathrm{SL}_2(q)$. In particular, it contains an element g of order $q - 1$ such that $\dim[g, V] = 2$. In case $G \subset \mathfrak{S}_m$ and V is the deleted representation of \mathfrak{S}_m of dimension $N = m - 1$ or $N = m - 2$ we notice that, the order of g being coprime to p , it acts as a semisimple endomorphism on the permutation representation \tilde{V} of \mathfrak{S}_m ; since the composition factors of \tilde{V} are V together with one or two copies of the trivial module, we get that $\dim[g, \tilde{V}] = \dim[g, V]$. But the condition $\dim[g, V] \leq 2$ implies that $g \in \mathfrak{S}_m$ has order at most 3, a contradiction since $q \geq 8$. The other case is when G contains a

twisted-diagonal embedding of $\mathrm{SL}_2(q)$. In this case it contains an element g conjugated to $\mathrm{diag}(\zeta, \zeta, \zeta^{-1}, \zeta^{-1}, 1, \dots, 1)$ of order $q-1 \geq 7$. We similarly get that, since $\dim[g, V] \leq 4$, the order of g can be at most 6, a contradiction.

Next we want to show that the action of G on V is primitive. We start by ruling out the monomial case. If $G \subset \mathbb{F}_q^\times \wr \mathfrak{S}_N$ then we use the fact $\mathrm{SL}_2(q)$ has a p -Sylow of order q , all of whose elements h satisfy $\dim[h, \mathbb{F}_{q^2}] \leq 1$, and therefore G contains an elementary abelian p -subgroup of order q , whose elements h satisfy $\dim[h, V] \leq 2$. By the Sylow theory these p -subgroups are conjugated inside $\mathbb{F}_q^\times \wr \mathfrak{S}_N \subset \mathrm{GL}(V)$ to a p -subgroup of \mathfrak{S}_N , since the order of $(\mathbb{F}_q^\times)^N$ is coprime to p . This means that \mathfrak{S}_N contains an elementary abelian p -subgroup H of order q such that, for all $h \in H$ $\dim[h, V] \leq 2$.

We then use the following lemma.

Lemma 5.4. *Let G be an elementary abelian p -subgroup of \mathfrak{S}_N of order p^r . Then G contains an element which is a product of at least r disjoint p -cycles.*

Proof. By the permutation action we can identify \mathfrak{S}_N and thus G with a subgroup of $\mathrm{GL}_N(\mathbb{C})$. Since G is commutative, it is conjugated to a group of diagonal matrices, and therefore can be identified with a subgroup of μ_p^N , where μ_p denotes the group of p -th roots of 1 in \mathbb{C} . Let $\zeta \in \mu_p$ be a primitive p -th root of 1. Every $g \in G$ is a product of m cycles, with m equal to the multiplicity of ζ in the spectrum of g . We thus need to prove that there exists $g \in G \subset \mu_p^N$ having at least r components equal to ζ .

Identifying μ_p with \mathbb{F}_p such that $\zeta \mapsto 1$, we get a structure of \mathbb{F}_p -vector space on μ_p^N , and the lemma follows from the following one.

Lemma 5.5. *Let K be a field, V a r -dimensional subspace of K^N . There exists $v \in V$ having at least r entries equal to 1.*

Proof. Let e_1^*, \dots, e_N^* denote the dual canonical basis of K^N , and $J \subset \{1, \dots, N\}$ of maximal cardinality containing an element v with $e_i^*(v) = 1$ for all $i \in J$. If $|J| < r$, the intersection of the hyperplanes $\mathrm{Ker}(e_i^*)$ for $i \in J$ and V would contain a non-zero element w . Moreover, we have an element $v \in J$ such that $e_i^*(v) = 1$ for all $i \in J$. Then $e_i^*(v + \beta w) = 1$ for all $\beta \in K$ and $i \in J$. Since $w \neq 0$ there exists $i_0 \notin J$ such that $e_{i_0}^*(w) \neq 0$. Therefore, we can find β such that $e_{i_0}(v + \beta w) = 1$, and this contradicts the maximality of J . \square

\square

By lemma 5.4 the group H contains a product h of r disjoint p -cycles. Since $\dim[h, V] = (p-1)r$ we get $(p-1)r \leq 2$, contradicting assumption $q > 4$.

We now want to rule out the non-monomial imprimitive case. Assume by contradiction that $G \subset H \wr \mathfrak{S}_m = (H_1 \times \dots \times H_m) \rtimes \mathfrak{S}_m$, where H_1, \dots, H_m denote the m copies of $H \simeq \mathrm{SL}_{N/m}(q)$ which are permuted by the action of \mathfrak{S}_m . Let us consider an element t of order p which is either a transvection or an element of Jordan form $M \oplus \mathrm{Id}_{N-4}$ with

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Notice that in both cases G contains such an element. The rank of $t - 1$ is at most 2. Assume also that $t \notin H_1 \times \dots \times H_m$. Up to reordering we can assume $H_1^t \neq H_1$. Since t has order p we can thus assume $H_i^t = H_{i+1}$ for $1 \leq i \leq p-1$, $H_{p-1}^t = H_p$. We let $U_1 \oplus \dots \oplus U_m$ be

the direct sum decomposition corresponding to the wreath product. Let $v_1 \in U_1 \setminus \{0\}$. By completing the family $(v_1, tv_1, \dots, t^{p-1}v_1)$ we get a basis on which t acts by a matrix of the form $M_p \oplus X$ where M_p is the circulating matrix of order p and X is some matrix of size $N - p$. We have $(M - 1)^2 = 0$ but $(M_p - 1)^2 \neq 0$ whenever $p \geq 3$. Assuming this, we get $t \in H_1 \times \dots \times H_m$. Notice that the induction assumption implies that $R_\lambda(\mathcal{B}_{n-1})$ is a direct product of quasi-simple groups containing elements of that type. Because these elements are not semisimple, they moreover do not belong to the centers of these groups. It follows that $R_\lambda(\mathcal{B}_{n-1})$ is normally generated by these elements hence is included in $H_1 \times \dots \times H_m$, which is normal in $H \wr \mathfrak{S}_m$. Since \mathcal{B}_n is normally generated by \mathcal{B}_{n-1} (see lemma 2.1) this proves that $R_\lambda(\mathcal{B}_n) \subset H_1 \times \dots \times H_m$, contradicting the irreducibility of R_λ .

It then remains to examine separately the case $p = 2$. If $\dim U_1 \geq 3$, we can pick a linearly independent family $v_1, v'_1, v''_1 \in U_1$ and, by completing the family $(v_1, tv_1, v'_1, tv'_1, v''_1, tv''_1)$ we get a basis on which t acts by a matrix of the form $M_p \oplus M_p \oplus M_p \oplus X$ for some X and we get that the rank of $t - 1$ is at least 3, a contradiction that proves $\dim U_1 \leq 2$. In case t is a transvection, the same contradiction proves $\dim U_1 = 1$, and we are reduced to the monomial case that we already did. If we cannot choose t to be a transvection, we have $p = 2$, $\dim U_1 = 2$. Under our assumption we know $q \neq 2$. Let us consider two \mathbb{F}_2 -linearly independent elements $a_1, a_2 \in \mathbb{F}_q$, and elements $t_1, t_2 \in G$ whose Jordan form in some common basis is

$$t_i = \begin{pmatrix} 1 & a_i & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & a_i \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Let us assume $t_1, t_2 \notin H_1 \times \dots \times H_m$. By the same argument as above with $t = t_1$, we can assume that $U = U_1 \oplus U_2$ is t_1 -stable, with $t_1(U_1) = U_2$ and therefore $t_1(U_2) = t_1^2(U_1) = U_1$, and $t_1(U_i) = U_i$ for $i \geq 3$. Using the same argument for t_2 we can also assume that $U' = U_a \oplus U_b$ is t_2 -stable with t_2 exchanging U_a and U_b for some $a \neq b$. Since $I = \text{Im}(t_i - 1)$ is independent of i , we have $I \subset U \cap U'$. We prove that $U_r \not\subset I$ for every r . When $r \notin \{1, 2, a, b\}$ this is clear because t_i acts as 1 on such a U_r . But $U_r \subset I = \text{Im}(t_i - 1) \subset \text{Ker}(t_i - 1)$ for all i implies $r \notin \{1, 2, a, b\}$ since each of the U_r for $r \in \{1, 2, a, b\}$ is not stable by at least one of the two t_i 's.

Then, $U \cap U'$ containing the 2-dimensional subspace I but no U_r , we have $U = U'$. It follows that $t_1 t_2(U_r) = U_r$ for all r , hence $t = t_1 t_2 \in H_1 \times \dots \times H_m$. We can thus resume the previous argument : since $R_\lambda(\mathcal{B}_{n-1})$ is normally generated by such elements, and because \mathcal{B}_n is normally generated by \mathcal{B}_{n-1} , we would get $R_\lambda(\mathcal{B}_n) \subset H_1 \times \dots \times H_m$, contradicting the irreducibility of R_λ .

This proves that G is primitive, tensor-indecomposable, and we ruled out cases (ii) and (iii) of the theorem.

Theorem 5.1 implies that G is a classical group over a finite subfield $\mathbb{F}_{q'}$ of \mathbb{F}_q . We first show that $q' = q$. We use the following lemmas, where $\text{SU}_m(q)$ denotes, in case q is a square, the unitary subgroup of $\text{SL}_m(q)$.

Lemma 5.6. *For all $m \geq 2$, the field generated over \mathbb{F}_p by $\{\text{tr}(g); g \in \text{SL}_m(q)\}$ is \mathbb{F}_q . For all $m \geq 3$, the field generated over \mathbb{F}_p by $\{\text{tr}(g); g \in \text{SU}_m(q)\}$ is \mathbb{F}_q .*

Proof. We start with the case $\text{SL}_m(q)$ and argue by contradiction. Suppose that $\{\text{tr}(g); g \in \text{SL}_m(q)\}$ generates a proper subfield $\mathbb{F}_{q'}$ with $q' \leq \sqrt{q}$. Since the action of $\text{SL}_m(q)$ on its natural representation is absolutely irreducible, it would be conjugate inside $\text{GL}_m(q)$ to some

subgroup of $\mathrm{GL}_m(q')$ (see e.g. [I], theorem 9.14), and therefore to some subgroup of $\mathrm{SL}_m(q')$ since $\mathrm{SL}_m(q)$ is perfect. But $|\mathrm{SL}_m(q)| > |\mathrm{SL}_m(q')|$ for $m \geq 2$, a contradiction. In the $\mathrm{SU}_m(q)$ case, $\{\mathrm{tr}(g); g \in \mathrm{SU}_m(q)\}$ would generate a proper subfield $\mathbb{F}_{q'}$ with $q' \leq \sqrt{q}$. Since the action of $\mathrm{SU}_m(q)$ on its natural representation is again absolutely irreducible, it would be conjugated inside $\mathrm{GL}_m(q)$ to some subgroup of $\mathrm{GL}_m(q')$ by the same argument, and therefore to some subgroup of $\mathrm{SL}_m(q')$ since $\mathrm{SL}_m(q)$ is perfect. Then the order of $\mathrm{SU}_m(q)$ is at most

$$|\mathrm{SL}_m(q')| = (q')^{\frac{n(n-1)}{2}} ((q')^2 - 1) \dots ((q')^n - 1) \leq \sqrt{q}^{\frac{n(n-1)}{2}} (\sqrt{q}^2 - 1) \dots (\sqrt{q}^n - 1) = |\mathrm{SL}_n(\sqrt{q})|$$

but $|\mathrm{SU}_m(q)| = \sqrt{q}^{\frac{m(m-1)}{2}} (\sqrt{q}^2 - 1)(\sqrt{q}^3 + 1) \dots (\sqrt{q}^m - (-1)^m)$ and thus $|\mathrm{SU}_m(q)| > |\mathrm{SL}_m(\sqrt{q})|$ as soon as $m \geq 3$, a contradiction. \square

Note that a similar statement does not hold for $\mathrm{SU}_2(q)$, for in that case every element of the group has a trace of the form $\zeta + \bar{\zeta} \in \mathbb{F}_{\sqrt{q}}$.

If G contains a natural $\mathrm{SL}_2(q)$, this proves $q' = q$. Otherwise, we can consider a twisted-diagonal embedding of $\mathrm{SL}_3(q)$ as a representation $\rho : \mathrm{SL}_3(q) \rightarrow G \subset \mathrm{GL}_N(\mathbb{F}_{q'}) \subset \mathrm{GL}_N(\overline{\mathbb{F}_p})$, and assume by contradiction that $\mathbb{F}_{q'}$ is a proper subfield of \mathbb{F}_q . Let $\varphi : \mathrm{SL}_3(\mathbb{F}_q) \rightarrow \mathrm{GL}_3(\overline{\mathbb{F}_p})$ denote the (absolutely irreducible) natural representation, and $\mathbb{1}$ the trivial one. We have $\rho \simeq \varphi \oplus \varphi^* \oplus \mathbb{1}^{N-6}$. Let σ be a generator of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_{q'})$. We have $\rho \simeq \rho^\sigma$ and therefore either $\varphi \simeq \varphi^\sigma$ or $\varphi^* \simeq \varphi^\sigma$. In the first case, Lemma 5.6 would imply $\mathbb{F}_q = (\mathbb{F}_q)^{\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_{q'})} = \mathbb{F}_{q'}$, a contradiction. In the second case, we could have $\varphi^{\sigma^2} \simeq (\varphi^*)^\sigma \simeq (\varphi^\sigma)^\sigma \simeq \varphi^{**} \simeq \varphi$ hence $\mathbb{F}_q = (\mathbb{F}_q)^{\langle \sigma^2 \rangle}$ by the same argument. Thus $\sigma : x \mapsto \bar{x}$ has order 2, q is a square, and we have $\varphi^* \simeq \bar{\varphi}$. But this implies that φ preserves some hermitian nondegenerate form on \mathbb{F}_q^3 , and therefore φ would embed $\mathrm{SL}_3(q)$ into some conjugate of $\mathrm{SU}_3(q)$, contradicting $|\mathrm{SL}_3(q)| > |\mathrm{SU}_3(q)|$ (see the proof of Lemma 5.6). Altogether this proves $q' = q$.

If $\lambda = \lambda'$ then we know $G \subset \mathrm{OSP}(\lambda)$, hence the only possibility left by Theorem 5.1 is that $G = \mathrm{OSP}'(\lambda)$. If $\lambda \neq \lambda'$, then G cannot preserve any nontrivial bilinear form, since R_λ , viewed as a representation of \mathcal{B}_n , is not isomorphic to its dual by Lemma 3.4, and neither can it preserve an hermitian form, because it is also not isomorphic to its conjugate-dual. This last property is because the restriction to \mathcal{B}_3 does not have this property when $\mathbb{F}_p(\alpha + \alpha^{-1}) = \mathbb{F}_p(\alpha)$, as is shown in [BM]. Theorem 5.1 thus implies $G = \mathrm{SL}(\lambda)$.

Now, we now recall Goursat's lemma, which describes the subgroups of a direct product, and that we need in the sequel.

Lemma 5.7. (*Goursat's lemma*) *Let G_1 and G_2 be two groups, $H \leq G_1 \times G_2$, and denote by $\pi_i : H \rightarrow G_i$. Write $H_i = \pi_i(H)$ and $H^i = \ker(\pi_{i'})$, where $\{i, i'\} = \{1, 2\}$. Then there is an isomorphism $\varphi : H_1/H^1 \rightarrow H_2/H^2$ such that*

$$(1) \quad H = \{(h_1, h_2) \in H_1 \times H_2 \mid \varphi(h_1 H^1) = h_2 H^2\}.$$

We now can prove that Φ_n is surjective. We choose a good ordering on the elements of \mathcal{E}_n such that $\lambda \leq \lambda'$, with the additional condition that the 2-rows diagram are smaller than the others. By numbering the partitions $\lambda \in \mathcal{E}_n$ such that $\lambda \leq \lambda'$ we can prove by induction on n that, for a given λ_0 , the composite of Φ_n with the projection of its target domain onto

$$G_{\lambda_0} = \mathrm{SL}_{n-1}(q) \times \prod_{\substack{\lambda \in \mathcal{E}_n \\ \lambda < \lambda', \lambda < \lambda_0}} \mathrm{SL}(\lambda) \times \prod_{\substack{\lambda \in \mathcal{E}_n \\ \lambda = \lambda', \lambda < \lambda_0}} \mathrm{OSP}'(\lambda)$$

is surjective. For λ_0 the minimal element of \mathcal{E}_n , $G_{\lambda_0} = \mathrm{SL}_{n-1}(q)$. By the results of [BM] this composite is surjective whenever λ_0 is a 2-rows diagram. We use Goursat's lemma with $G_1 = G_{\lambda_0}$ and $G_2 = G(\lambda_0 + 1)$, where we let as in the introduction $G(\mu) = \mathrm{SL}(\mu)$ if $\mu \neq \mu'$, and $G(\mu) = \mathrm{OSP}'(\mu)$ otherwise. We let $PG(\mu)$ denote its image in the projective linear group. We know that $H_1 = G_1$ and $H_2 = G_2$, and we get an isomorphism $\varphi : H_1/H^1 \rightarrow H_2/H^2$, which induces a surjective morphism $\tilde{\varphi} : H_1 \rightarrow H_2/H^2$.

Assume that $H_1/H^1 \simeq H_2/H^2$ is not abelian. Then H_2/H^2 has for quotient $PG(\mu)$ and we get a surjective morphism $\hat{\varphi} : H_1 \twoheadrightarrow PG(\lambda_0 + 1)$. Let now $\mu \leq \lambda_0$, and consider the restriction $\hat{\varphi}_\mu$ of $\hat{\varphi}$ to $G(\mu)$. Assume it is non-trivial. Since the image of the center is mapped to 1, it factorizes through an isomorphism $\tilde{\varphi}_\mu : PG(\mu) \rightarrow PG(\lambda_0 + 1)$. But this implies that the image of \mathcal{B}_n inside $G(\mu) \times G(\lambda_0 + 1)$ is included inside $H = \{(x, y) \mid \bar{y} = \tilde{\varphi}_r(\bar{x})\}$, where \bar{x}, \bar{y} denote the canonical images of x, y .

Let then $\overline{R_\lambda} : B_n \rightarrow \mathrm{PGL}(\lambda)$ denote the projective representation deduced from R_λ . By the very description of H we have $\overline{R_{\lambda_0+1}}(b) = \hat{\varphi}(R_\mu(b))$ for all $b \in \mathcal{B}_n$, where $\hat{\varphi}$ is the composite $H_1 \twoheadrightarrow H_1/H^1 \xrightarrow{\sim} H_2/H^2 \rightarrow \mathrm{PGL}(\lambda_0 + 1)$. Since $\varphi : H_1/H^1 \xrightarrow{\sim} H_2/H^2$ is an isomorphism and $Z(H_i/H^i)$ is the image of $\mathbb{F}_q^\times \cap H_i$ inside H_i/H^i , we have $\hat{\varphi}(\mathbb{F}_q^\times \cap H_1) = 1$, hence $\overline{R_{\lambda_0+1}}(b) = \tilde{\varphi}(\overline{R_\mu}(b))$ for all $b \in \mathcal{B}_n$, where $\tilde{\varphi} : H_1/(\mathbb{F}_q^\times \cap H_1) \rightarrow \mathrm{PGL}(\lambda_0 + 1)$ is the induced morphism.

Note that $H_1/(\mathbb{F}_q^\times \cap H_1) \subset \mathrm{PGL}(\mu)$, and clearly $\mathrm{Im} \tilde{\varphi} \supset PG(\lambda_0 + 1)$. From this one deduces that the restriction of $\tilde{\varphi}$ to $PG(\mu)$ is non-trivial, hence induces an isomorphism ψ between the simple groups $\psi : PG(\mu) \rightarrow PG(\lambda_0 + 1)$. Since $\dim \mu \geq 16$ no triality phenomenon can be involved and thus, up to a possible linear conjugation of the representations R_μ, R_{λ_0+1} , we get (see [W] §3.7.5 and §3.8) that ψ is either induced by a field automorphism $\Phi \in \mathrm{Aut}(\mathbb{F}_q)$, or, in case $\lambda \neq \lambda'$, by the composition of such an automorphism with $X \mapsto {}^t X^{-1}$. In the first case we let $S = R_\mu$, in the second case we let $S : g \mapsto {}^t R_\mu(g^{-1})$.

In both cases, we have $\overline{R_{\lambda_0+1}}(b) = \Phi(\overline{S}(b)) = \overline{S^\Phi}(b)$ for all $b \in \mathcal{B}_n$, with $S^\Phi : g \mapsto \Phi(S(g))$, meaning that the two representations of \mathcal{B}_n afforded by R_{λ_0+1} and S^Φ are projectively equivalent, that is there is $z : \mathcal{B}_n \rightarrow \mathbb{F}_q^\times$ such that $R_{\lambda_0+1}(b) = S^\Phi(b)z(b)$ for all $b \in \mathcal{B}_n$. Since \mathcal{B}_n is perfect for $n \geq 5$ (see [GL]) we get $z = 1$; this proves that the restrictions of R_{λ_0+1} and S^Φ to \mathcal{B}_n are isomorphic. In particular, their restrictions to \mathcal{B}_3 are isomorphic. The restrictions of R_{λ_0+1} and S to \mathcal{B}_3 are direct sums of the irreducible representations of the Hecke algebra for $n = 3$, restricted to the derived subgroups. There are three such irreducible representations, of dimensions 1 and 2, corresponding to the partitions $[3], [2, 1], [1, 1, 1]$. Note that these restrictions have to contain a constituent of dimension 2, for otherwise the image of \mathcal{B}_3 would be trivial, hence s_1 and s_2 would have the same image (as $s_1 s_2^{-1} \in \mathcal{B}_3$), which easily implies that the image of B_n is abelian, contradicting the irreducibility.

But this implies that the representation of \mathcal{B}_3 associated to $[2, 1]$ has to be isomorphic to its twisted by Φ . By explicit computation we get that the trace of $s_1 s_2 s_1^{-1} s_2^{-1}$ is $1 - (\alpha + \alpha^{-1})$. Since $\mathbb{F}_q = \mathbb{F}_p(\alpha) = \mathbb{F}_p(\alpha + \alpha^{-1})$ this implies $\Phi = 1$.

We thus have $R_\mu(b) = S(b)$ for all $b \in \mathcal{B}_{n-1}$. Note that S , viewed as a representation of B_n , is isomorphic to R_λ for λ equal to either $\lambda_0 + 1$ or possibly to its transpose. By Lemma 3.4 we get that the only possibility is $\mu = \lambda_0 + 1$, since \mathcal{E}_n contains $\lambda_0 + 1$ hence not its transposed if different. But this is a contradiction which proves that each $\hat{\varphi}_\mu$ is trivial, hence so is $\hat{\varphi}$, and this contradicts its surjectivity. Therefore, $H_1/H^1 \simeq H_2/H^2$ is abelian. It follows that each H^i contains the commutator subgroup of H_i . Since both of the H_i are perfect we get the conclusion by induction on λ_0 .

We now explain how to adapt the proof to the ‘unitary’ case, that is when $\mathbb{F}_p(\alpha + \alpha^{-1}) = \mathbb{F}_{\sqrt{q}} \subsetneq \mathbb{F}_q = \mathbb{F}_p(\alpha)$. We denote $\mathrm{SU}_m(q) \subset \mathrm{GL}_m(q)$ the unitary group associated to the involutive automorphism of \mathbb{F}_q and recall that $\mathrm{SU}_2(q) \simeq \mathrm{SL}_2(\sqrt{q})$. We also recall that $\mathrm{SU}_2(q)$ contains a semisimple element of order $1 + \sqrt{q}$, namely $\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$ with ζ of order $1 + \sqrt{q}$, so that $\bar{\zeta} = \zeta^{-1}$, and we note that $|\mathrm{SU}_2(q)| = \sqrt{q}(q-1)$. We note that the assumption $o(\alpha) > n$ remains in force. But here we have $\varepsilon(\alpha) = \alpha^{-1}$. Since $\varepsilon(\alpha) = \alpha^{\sqrt{q}}$ this implies $\alpha^{1+\sqrt{q}} = 1$ and therefore $1 + \sqrt{q} > n \geq 6$ hence $\sqrt{q} \geq 6$.

First of all, the preliminary analysis of the partitions imply that we can assume that the image of \mathcal{B}_{n-1} contains a copy of $\mathrm{SU}_2(q)$ acting either on a 2-dimensional subspace, or on a 4-dimensional subspace via the twisted action $x \oplus x^{-1}$. Therefore, there is an $x \in G$ originating either from a toric element or from a unitary transvection of $\mathrm{SU}_2(q)$ such that $\dim(x-1)V = 2$. Moreover, G is tensor-indecomposable by Lemmas 5.2 and 5.3, provided we know that $\mathrm{SU}_2(q)$ contains a semisimple element of order > 2 and this holds because $1 + \sqrt{q} > 2$.

Case (ii) is ruled out in a similar way. If G contains a natural $\mathrm{SU}_2(q)$ and therefore some g with $\dim[g, V] \leq 2$ of order $1 + \sqrt{q}$ we conclude as in the non-unitary case. If G contains instead a twisted-diagonal $\mathrm{SU}_2(q)$, we similarly get an element g of order $1 + \sqrt{q}$ with $\dim[g, V] \leq 4$ providing the same contradiction as in the non-unitary case, as soon as $1 + \sqrt{q} \geq 7$, which is our assumption here.

For ruling out the monomial case, we assume again $G \subset \mathbb{F}_q^\times \rtimes \mathfrak{S}_N$, and we notice again that G contains some natural or twisted-diagonal $\mathrm{SU}_2(q)$, and one of its p -Sylow subgroups induces as in the classical case an elementary abelian p -subgroup H of \mathfrak{S}_N with $\dim[g, V] \leq 2$ for all $g \in H$, but this time of order $\sqrt{q} \geq 6$. This again provides a contradiction by the same argument.

The argument for the non-monomial imprimitive case applies here verbatim when $p \geq 3$ and, when $p = 2$ we can similarly pick two \mathbb{F}_2 -linearly independent elements $t_1, t_2 \in G$ originating from some p -Sylow subgroup of $\mathrm{SU}_2(q)$, because we have $\sqrt{q} > 2$.

This proves again that G is primitive, tensor-indecomposable, and we rule out cases (ii) and (iii) of Theorem 5.1.

Applying theorem 5.1, we get again that G is a classical group over a subfield $\mathbb{F}_{q'}$ of \mathbb{F}_q .

A consequence of lemma 5.6 is that, whenever λ contains a partition μ of size $n-1$ but not its transpose μ' , then G contains a natural $\mathrm{SU}_3(q)$ and thus $q' = q$. Otherwise, we have $\lambda = \lambda'$, and therefore G is a subgroup of some $\mathrm{OSP}(\sqrt{q})$. Moreover, it contains a twisted-diagonal $\mathrm{SU}_3(q)$, and therefore $\mathbb{F}_{q'}$ has to contain all the $\mathrm{tr}(g) + \overline{\mathrm{tr}(g)}$ for $g \in \mathrm{SU}_3(q)$, hence all the $\beta + \bar{\beta}$ for $\beta \in \mathbb{F}_q$, that is $\mathbb{F}_{\sqrt{q}}$.

The remaining part of the argument is then completely similar to the first case (and actually easier).

REFERENCES

- [BM] O. Brunat, I. Marin, *The image of the braid groups inside the finite Temperley-Lieb algebras*, to appear in Math. Zeit.
- [C] H.S.M. Coxeter, *Factor groups of the braid groups*, Proc. Fourth Canad. Math. Congress, 95–122 (1957).
- [FLW] M. Freedman, M. Larsen, Z. Wang, *The two-eigenvalue problem and density of Jones representation of braid groups*, Comm. Math. Phys. **228** (2002), 177–199.

- [GP] M. Geck, G. Pfeiffer, *Characters of finite Coxeter groups and Iwahori-Hecke algebras*. London Mathematical Society Monographs. New Series, 21. The Clarendon Press, Oxford University Press, New York, 2000.
- [GL] E.A. Gorin, V. Ja. Lin, *Algebraic equations with continuous coefficients and some problems of the algebraic theory of braids*, Mat. Sbornik. **78 (120)** (1969), 569-596.
- [GS] R.M. Guralnik, J. Saxl, *Generation of finite almost simple groups by conjugates*, J. Algebra **268** (2003), 519–571.
- [I] I.M. Isaacs, *Character Theory of Finite Groups*, Academic Press, New York, 1976.
- [M0] I. Marin, *Représentations linéaires des tresses infinitésimales*, Thèse de l'université d'Orsay, 2001.
- [M1] I. Marin, *Caractères de rigidité du groupe de Grothendieck-Teichmüller*, Compositio Mathematica **142** (2006) 657-678.
- [M2] I. Marin, *L'algèbre de Lie des transpositions*, J. Algebra **310** (2007) 742-774.
- [M3] I. Marin, *Infinitesimal Hecke Algebras II, III, IV*, preprint arXiv:0911.1879 v1 (II) arXiv:1012.4424 v1 (III), arXiv:1212.1279 v1 (IV).
- [M4] I. Marin, *The freeness conjecture for Hecke algebras of complex reflection groups, and the case of the Hessian group G_{26}* , J. Pure Applied Algebra **218** (2014), 704-720.
- [Mat] A. Mathas, *Iwahori-Hecke algebras and Schur algebras of the symmetric groups*, University Lecture Series, 15, American Mathematical Society, Providence, 1999.
- [S] M. Suzuki, *Group Theory I*, Springer-Verlag, 1982.
- [W] R.A. Wilson, *The Finite Simple Groups*, GTM 251, Springer, London-Dordrecht-Heidelberg-New York, 2009.

INSTITUT DE MATHÉMATIQUES DE JUSSIEU, UNIVERSITÉ PARIS 7, 175 RUE DU CHEVALERET, 75013 PARIS, FRANCE

E-mail address: `brunat@math.jussieu.fr`

SCHOOL OF MATHEMATICS, UNIVERSITY OF BIRMINGHAM, EDGBASTON, BIRMINGHAM B15 2TT, UNITED KINGDOM

E-mail address: `k.magaard@bham.ac.uk`

LAMFA, UNIVERSITÉ DE PICARDIE-JULES VERNE, 33 RUE SAINT-LEU, 80039 AMIENS CEDEX 1, FRANCE

E-mail address: `ivan.marin@u-picardie.fr`