

IMAGE OF THE BRAID GROUPS INSIDE THE FINITE TEMPERLEY-LIEB ALGEBRAS

OLIVIER BRUNAT AND IVAN MARIN

ABSTRACT. We determine the image of the braid groups inside the Temperley-Lieb algebras, defined over finite field, in the semisimple case, and for suitably large (but controllable) order of the defining (quantum) parameter. We also prove that, under natural conditions on this parameter, the representations of the Hecke algebras over a finite field are unitary for the action of the braid groups.

1. INTRODUCTION

Let B_n denote the braid group on n strands. A natural question concerns the image of B_n inside its classical linear representations, the most classical ones being the ones which factor through the Hecke algebra $H_n(\alpha)$ of type A_{n-1} , such as the Burau or the Jones representation. Inside an infinite field, the determination of the Zariski closure of such representations in the generic case is completely known by [FLW] and [Mar1] ; actually the more general cases of the representations of the Birman-Wenzl-Murakami algebra and of the Hecke algebras for other reflection groups is also known by [Mar4, Mar2], and more precise information on the Jones representation can be found in [FLW] and [Ku] in the non-generic case.

In vague terms, the theory of ‘strong approximation’ should imply that, for ‘almost all’ maximal ideals \mathfrak{m} of the ring of definition $\mathbb{Z}[\alpha, \alpha^{-1}]$ of the representation, the image of B_n should be the set of points over $\mathbb{F}_q = \mathbb{Z}[\alpha, \alpha^{-1}]/\mathfrak{m}$ of the corresponding algebraic group. However, it is unclear to us, partly because $\mathbb{Z}[\alpha, \alpha^{-1}]$ has Krull dimension 2, whether strong approximation techniques can lead to reasonably precise results in this case.

In the case of the Jones representation, the problem is equivalent to determining the image of the braid group inside the Temperley-Lieb algebra, defined over a finite field. It is a natural generalization of a problem which has already been studied, in the case of the Burau representation, in the realm of inverse Galois theory.

Indeed, by [SZ2] and [W] (see also [MM] II §2, Theorem 2.3), we have the following result.

Theorem 1.1. (*Serežkin-Zalesskiĭ, Wagner*) *Let $n \geq 3$, $q = p^m$ and H a primitive subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ generated by semisimple pseudo-reflections of order at least 3, then one of the following holds.*

- (i) $\mathrm{SL}_n(\mathbb{F}_{\tilde{q}}) \leq H \leq \mathrm{GL}_n(\mathbb{F}_{\tilde{q}})$ for $\tilde{q}|q$ or
- (ii) $\mathrm{SU}_n(\tilde{q}) \leq H \leq \mathrm{GU}_n(\tilde{q})$ for $\tilde{q}^2|q$

or $n \leq 4$ and $H \simeq \mathrm{GU}_n(2)$. In the latter case the pseudo-reflections have order 3.

As noticed in [SV], this theorem determines the image of the braid group inside the Burau representation. A natural question, raised by Strambach and Völklein in [SV], is to determine the image of the braid group, and of other generalized braid groups, inside the representations

of the Hecke algebra representations over a finite field. This is relevant to the question of determining rigid geometric Galois actions. The special case of the Temperley-Lieb algebra can thus also be seen as a first step towards answering this question.

We thus consider the Hecke algebra $H_n(\alpha)$ as defined over a finite field \mathbb{F}_q , meaning that we choose $\alpha \in \mathbb{F}_q^\times$ and consider the quotient of the group algebra $\mathbb{F}_q B_n$ by the relations $(\sigma_i + 1)(\sigma_i - \alpha) = 0$, where the σ_i are the usual Artin generators of B_n . In studying the representation theory of $H_n(\alpha)$, an important integer e is the smallest positive one such that $[e]_\alpha = 1 + \alpha + \dots + \alpha^{e-1} = 0$. If $\alpha = 1$, then $e = p = \text{char.}\mathbb{F}_q$, otherwise $[e]_\alpha = (\alpha^e - 1)/(\alpha - 1) = 0$ means $\alpha^e = 1$.

The irreducible representations of $H_n(\alpha)$ are in 1-1 correspondence with the partitions $\lambda = (\lambda_1 \geq \lambda_2 \geq \dots)$ of n which are e -restricted, meaning that $\lambda_i - \lambda_{i+1} < e$ for all i , and $H_n(\alpha)$ is (split) semisimple if and only if all partitions of n are e -restricted, meaning $e > n$ (see [Mat], cor. 3.44). In that case, all the irreducible representations are afforded by the classical Specht modules, and are thus reductions modulo \mathfrak{m} of the representations in characteristic 0.

We focus on the partitions of at most two rows, and denote $c(n, r)$ the dimension of the representation associated to $[n - r, r]$. These representations are exactly the irreducible representations which factors through the Temperley-Lieb algebra. This algebra $TL_n(\alpha)$ can be defined as the quotient of the Hecke algebra $H_n(\alpha)$ by the relation $\sigma_2 \sigma_1 \sigma_2 + \sigma_1 \sigma_2 + \sigma_2 \sigma_1 + \sigma_1 + \sigma_2 + 1 = 0$.

We now can state the main result of this paper.

Theorem 1.2. *Let n be a positive integer and let p be a prime number. Let $\alpha \in \overline{\mathbb{F}_p}^\times$ of order $e > n$ and $e \notin \{2, 3, 6, 10\}$, and let $\mathbb{F}_q = \mathbb{F}_p(\alpha)$.*

- (i) *Let $\lambda \vdash n$ be a partition with at most two rows. If $R : B_n \rightarrow \text{GL}_N(\mathbb{F}_q)$ denotes the representation of $H_n(\alpha)$ associated to λ , then*
 - *either $\mathbb{F}_p(\alpha + \alpha^{-1}) = \mathbb{F}_p(\alpha) = \mathbb{F}_q$ and $R(B_n)$ contains $\text{SL}_N(\mathbb{F}_q)$,*
 - *or $\mathbb{F}_p(\alpha + \alpha^{-1}) = \mathbb{F}_{q^{1/2}}$ and, up to conjugacy, $\text{SU}_N(q^{1/2}) \subset R(B_n) \subset \text{GU}_N(q^{1/2})$.*
- (ii) *Let G be the image of B_n in $TL_n(\alpha)^\times = \prod_{r=0}^n \text{GL}_{c(n,r)}(\mathbb{F}_p)$. Then*
 - *either $\mathbb{F}_p(\alpha + \alpha^{-1}) = \mathbb{F}_p(\alpha) = \mathbb{F}_q$ and G contains $\prod_{r=0}^n \text{SL}_{c(n,r)}(\mathbb{F}_q)$,*
 - *or $\mathbb{F}_p(\alpha + \alpha^{-1}) = \mathbb{F}_{q^{1/2}}$ and*

$$\prod_{r=0}^n \text{SU}_{c(n,r)}(q^{1/2}) \subset PR(B_n)P^{-1} \subset \prod_{r=0}^n \text{GU}_{c(n,r)}(q^{1/2})$$

for some $P \in \prod_{r=0}^n \text{GL}_{c(n,r)}(\mathbb{F}_q)$.

The article is organized as follows. In Section 2, we give some results that we need in the sequel. Then in Section 3, we reduce the proof of Theorem 1.2 to the following statements.

Theorem 1.3. *Let p be a prime and q a p -power. Let $\Gamma < \text{GL}_N(\mathbb{F}_q)$ with $N \geq 5$ and $q > 3$, such that*

- (i) *Γ is absolutely irreducible.*
- (ii) *Γ contains $\text{SL}_a(\mathbb{F}_q)$ with $a \geq N/2$.*

If $N \neq 2a$, then Γ contains $\text{SL}_N(\mathbb{F}_q)$. Otherwise, either Γ contains $\text{SL}_N(\mathbb{F}_q)$, or Γ is a subgroup of $\text{GL}_{N/2}(\mathbb{F}_q) \wr \mathfrak{S}_2$.

We also need the unitary version of this result.

Theorem 1.4. *Let p be a prime and q a p -power. Let $\Gamma < \mathrm{GU}_N(\mathbb{F}_q)$ with $N \geq 5$ and $q > 3$, such that*

- (i) Γ is absolutely irreducible.
- (ii) Γ contains $\mathrm{SU}_a(q)$ with $a \geq N/2$.

If $N \neq 2a$, then Γ contains $\mathrm{SU}_N(q)$. Otherwise, either Γ contains $\mathrm{SU}_N(q)$, or Γ is a subgroup of $\mathrm{GU}_{N/2}(q) \wr \mathfrak{S}_2$.

Remark 1.5.

The assumptions used in Theorem 1.3 are clearly too strong. However, this result does not hold in general (that is : arbitrary field and arbitrary N), as exemplified by $N = 4$, $q = 2$. In that case, $\mathrm{Sp}_4(\mathbb{F}_2)$ is an absolutely irreducible subgroup of order 720 of $\mathrm{GL}_4(\mathbb{F}_2)$ containing $\mathrm{SL}_2(\mathbb{F}_2) \times \mathrm{SL}_2(\mathbb{F}_2)$. It is clearly not contained in $\mathrm{GL}_2(\mathbb{F}_2) \wr \mathfrak{S}_2$, which has order 72.

Acknowledgements. I.M. thanks R. Rouquier for pointing out the paper [SV] to him. We thank M. Cabanes for fruitful discussions, and K. Magaard for indicating the reference [Ka] to us, which led to a dramatic improvement of a previous version of this paper.

2. PRELIMINARY RESULTS

For the convenience of the reader, we give a proof of the following well-known result.

Lemma 2.1. *Let \mathbb{k} be a field and a positive integer n . Write $\mathfrak{q} : \mathrm{GL}_n(\mathbb{k}) \rightarrow \mathrm{PGL}_n(\mathbb{k})$ for the natural projection. If $G \leq \mathrm{GL}_n(\mathbb{k})$ is such that $\mathrm{PSL}_n(\mathbb{k}) \leq \mathfrak{q}(G)$, then $\mathrm{SL}_n(\mathbb{k}) \leq G$.*

Proof. First, assume that $\mathrm{SL}_n(\mathbb{k})$ is perfect, i.e. $\mathrm{SL}_n(\mathbb{k}) \notin \{\mathrm{SL}_2(\mathbb{F}_2), \mathrm{SL}_2(\mathbb{F}_3)\}$. Set $G' = [G, G]$. In particular, $G' \leq \mathrm{SL}_n(\mathbb{k})$, and $\mathfrak{q}(G') = \mathrm{PSL}_n(\mathbb{k})$. Thus, $\mathrm{SL}_n(\mathbb{k}) = \mu_n(\mathbb{k})G'$, where $\mu_n(\mathbb{k})$ is the group of the n -th roots of 1 in \mathbb{k} . Now, we have

$$\mathrm{SL}_n(\mathbb{k}) = [\mathrm{SL}_n(\mathbb{k}), \mathrm{SL}_n(\mathbb{k})] = [\mu_n(\mathbb{k})G', \mu_n(\mathbb{k})G'] = [G', G'] \leq G,$$

as required. Moreover, we easily check that the statement holds for $\mathrm{SL}_2(\mathbb{F}_2)$ and $\mathrm{SL}_2(\mathbb{F}_3)$. \square

Now, we recall Goursat's lemma (sometimes also attributed to P. Hall), which describes the subgroups of a direct product, and that we need in the following.

Lemma 2.2. (*Goursat's lemma*) *Let G_1 and G_2 be two groups, $H \leq G_1 \times G_2$, and denote by $\pi_i : H \rightarrow G_i$ the natural projections. 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*

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

Lemma 2.3. *Let p be a prime and $q > 3$ be a p -power. Let a_1, \dots, a_n be distinct positive integers, and $H \leq \mathrm{GL}_{a_1}(\mathbb{F}_q) \times \dots \times \mathrm{GL}_{a_n}(\mathbb{F}_q)$. For $1 \leq i \leq n$, write $p_i : H \rightarrow \mathrm{GL}_{a_i}(\mathbb{F}_q)$ for the natural projection. If $\mathrm{SL}_{a_i}(\mathbb{F}_q) \leq p_i(H)$, then H contains $\mathrm{SL}_{a_1}(\mathbb{F}_q) \times \dots \times \mathrm{SL}_{a_n}(\mathbb{F}_q)$.*

Proof. We prove the statement by induction on n . The case $n = 1$ is trivial so we can assume $n \geq 2$. Set $G_1 = \mathrm{GL}_{a_1}(\mathbb{F}_q) \times \dots \times \mathrm{GL}_{a_{n-1}}(\mathbb{F}_q)$ and $G_2 = \mathrm{GL}_{a_n}(\mathbb{F}_q)$. As in Lemma 2.2, for $1 \leq i \leq 2$, write $\pi_i : H \rightarrow G_i$ for the natural projections, $H_i = \pi_i(H)$ and $H^i = \ker(\pi_{i'})$. Hence, by Lemma 2.2, there is an isomorphism $\varphi : H_1/H^1 \rightarrow H_2/H^2$ such that Equation (1) holds. We have $\mathrm{SL}_{a_n}(\mathbb{F}_q) \leq H_2$ by assumption. Moreover, by the induction assumption, H_1 contains $\mathrm{SL}_{a_1}(\mathbb{F}_q) \times \dots \times \mathrm{SL}_{a_{n-1}}(\mathbb{F}_q)$. Since $[H_1, H_1] = \mathrm{SL}_{a_1}(\mathbb{F}_q) \times \dots \times \mathrm{SL}_{a_{n-1}}(\mathbb{F}_q)$, it follows

that the non-cyclic decomposition factors of H_1 are $\mathrm{PSL}_{a_1}(\mathbb{F}_q), \dots, \mathrm{PSL}_{a_{n-1}}(\mathbb{F}_q)$. Similarly, we get that the non-cyclic decomposition factor of H_2 is $\mathrm{PSL}_{a_n}(\mathbb{F}_q)$. Therefore, using φ , we deduce that H_2/H^2 is solvable. Its commutator subgroup is a quotient of $[H_2, H_2] = \mathrm{SL}_{a_n}(\mathbb{F}_q)$. Since it is solvable, it has to be trivial. In particular, H_2/H^2 is abelian, implying that H_1/H^1 is abelian. Thus, $[H_1, H_1] \leq H^1$ and $[H_2, H_2] \leq H^2$. The result follows. \square

We recall the following classical fact.

Lemma 2.4. *Let G be a group, and $\rho : G \rightarrow \mathrm{GL}_N(\mathbb{F}_{q^2})$ be an absolutely irreducible representation such that $\varepsilon \circ \rho^*$ is isomorphic to ρ , where $\varepsilon \in \mathrm{Aut}(\mathbb{F}_{q^2})$ has order 2. Then there exists $P \in \mathrm{GL}_N(\mathbb{k})$ such that $P\rho(g)P^{-1} \in \mathrm{GU}_N(q)$ for all $g \in G$.*

Proof. By assumption there exists $P \in \mathrm{GL}_N(\mathbb{F}_{q^2})$ such that $\varepsilon({}^t\rho(g^{-1})) = P\rho(g)P^{-1}$ for all $g \in G$, that is $\varepsilon({}^t\rho(g^{-1}))P = P\rho(g)$. It follows that $\rho(g) = \varepsilon({}^t(\varepsilon({}^t\rho(g)^{-1}))^{-1}) = \varepsilon({}^tP^{-1})\varepsilon({}^t\rho(g)^{-1})\varepsilon({}^tP) = \varepsilon({}^tP^{-1})P\rho(g)P^{-1}\varepsilon({}^tP)$ hence ${}^t\varepsilon(P)^{-1}P$ intertwines ρ with itself. Since ρ is absolutely irreducible, this implies ${}^t\varepsilon(P)^{-1}P = \mu \in \mathbb{F}_{q^2}^\times$. Moreover $\mu = {}^t\mu = {}^tP\varepsilon(P)^{-1}$, hence $\mu = \varepsilon(P)^{-1}{}^tP$ and $\mu\varepsilon(\mu) = \varepsilon(P)^{-1}{}^tP{}^tP^{-1}\varepsilon(P) = 1$. It follows that $1 \mapsto 1$, $\varepsilon \mapsto \mu$ defines a 1-cocycle of $\mathrm{Gal}(\mathbb{F}_{q^2}|\mathbb{F}_q) \simeq \mathbb{Z}/2\mathbb{Z}$ with values in $\mathbb{F}_{q^2}^\times$. By Hilbert's Theorem 90 such a 1-cocycle is a coboundary, that is there exists $\lambda \in \mathbb{F}_{q^2}^\times$ such that $\mu = \varepsilon(\lambda)\lambda^{-1}$. Hence ${}^t\varepsilon(P)^{-1}P = \varepsilon(\lambda)\lambda^{-1}$, and ${}^t\varepsilon(\lambda P) = \lambda P$. Up to replacing P by λP , we can thus assume that ${}^t\varepsilon(P) = P$. Then ${}^t(\varepsilon(\rho(g)X))P(\rho(g)Y){}^t\varepsilon(X)PY$ for all $X, Y \in \mathbb{F}_{q^2}^\times$, that is to say that all $\rho(g)$ preserves a non-degenerate hermitian form over $\mathbb{F}_{q^2}^N$, with respect to ε . Since all such form are equivalent (see e.g. [GR], Theorem 10.3) this implies the conclusion. \square

3. PROOF OF THEOREM 1.2

We use the notations of Theorem 1.2. In all what follows, we assume that Theorems 1.3 and 1.4 hold. In §3.1, §3.2 and §3.3, we assume $\mathbb{F}_p(\alpha + \alpha^{-1}) = \mathbb{F}_p(\alpha) = \mathbb{F}_q$. Then we will indicate in §3.4 the modifications that are needed for the unitary case.

3.1. Technical preliminaries. We first prove the following proposition.

Proposition 3.1. *Assume $n \geq 5$, $r_1, r_2 \leq n/2$ with $r_1 \neq r_2$, and let $N_i = c(n, r_i)$, $R_i : B_n \rightarrow \mathrm{GL}_{N_i}(\mathbb{F}_q)$ denote the representation associated to $[n - r_i, r_i]$. Assume that $\mathbb{F}_p(\alpha) = \mathbb{F}_p(\alpha + \alpha^{-1})$, and let $R = R_1 \oplus R_2$. If $R_i(B_n) \supset \mathrm{SL}_{N_i}(\mathbb{F}_q)$ for $i \in \{1, 2\}$, then $R(B_n) \supset \mathrm{SL}_{N_1}(\mathbb{F}_q) \times \mathrm{SL}_{N_2}(\mathbb{F}_q)$.*

Corollary 3.2. *Assume $n \geq 6$, $r \leq n/2$, $N = c(n, r)$, and $R : B_n \rightarrow \mathrm{GL}_N(\mathbb{F}_q)$ the representation associated to $[n - r, r]$. Assume that $\mathbb{F}_p(\alpha) = \mathbb{F}_p(\alpha + \alpha^{-1})$. Assume that $[n - r - 1, r]$ and $[n - r, r - 1]$ are partitions of $n - 1$, with associated representations $R_i : B_{n-1} \rightarrow \mathrm{GL}_{N_i}(\mathbb{F}_q)$ and that the restriction of R to B_{n-1} is $R_1 \oplus R_2$. Finally, assume that $R_i(B_{n-1}) \supset \mathrm{SL}_{N_i}(\mathbb{F}_q)$ for $i = 1, 2$. Then $R(B_{n-1}) \supset \mathrm{SL}_{N_1}(\mathbb{F}_q) \times \mathrm{SL}_{N_2}(\mathbb{F}_q)$.*

We will need the following lemmas.

When $[n - r, r]$ is a partition of n with associated representation $R : B_n \rightarrow \mathrm{GL}_{c(n, r)}(\mathbb{F}_q)$, we let $a(n, r) = \dim \mathrm{Ker}(R(\sigma_1) + 1)$ and $b(n, r) = \dim \mathrm{Ker}(R(\sigma_1) - \alpha)$. Clearly $a(n, r) + b(n, r) = c(n, r)$. When $[n - r, r]$ is not a partition of n we let $a(n, r) = b(n, r) = c(n, r) = 0$.

Lemma 3.3. *If $[n - r, r]$ is a partition of n and $n \geq 5$, then $a(n, r) > b(n, r)$.*

Proof. The statement holds true for $n = 5$ by a direct computation : $a(5, 0) = 1, b(5, 0) = 0, a(5, 1) = 3, b(5, 1) = 1, a(5, 2) = 3, b(5, 2) = 2$ (note that it is not true for $n = 4$, as $a(4, 2) = b(4, 2) = 1$).

We prove it by induction on n , now assuming $n \geq 6$. By the branching rule we have $a(n, r) = a(n-1, r) + a(n-1, r-1)$ and $b(n, r) = b(n-1, r) + b(n-1, r-1)$. Since at least one of the two couples $[n-1-r, r]$ and $[n-r, r-1]$ is a partition of r , the induction assumption immediately implies the conclusion. \square

Lemma 3.4. *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 $R_1(G') = R_2(G') \supset \mathrm{SL}_N(\mathbb{k})$. 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 $R_2(gG'g^{-1}) = R_2(G') \supset \mathrm{SL}_N(\mathbb{k})$ hence $\eta(g) \in \mathbb{k}^\times$. Then $\eta(g_1g_2) = R_2(g_1)(R_2(g_2)R_1(g_2)^{-1})R_1(g_1)^{-1} = R_2(g_1)\eta(g_2)R_1(g_1)^{-1} = R_2(g_1)R_1(g_1)^{-1}\eta(g_2) = \eta(g_1)\eta(g_2)$ for all $g_1, g_2 \in G$, which proves the claim. \square

We can now prove Proposition 3.1.

Proof. First note that the assumption $R_i(B_n) \supset \mathrm{SL}_{N_i}(\mathbb{F}_q)$ imply $\mathbb{F}_q = \mathbb{F}_p(\alpha) = \mathbb{F}_p(\alpha + \alpha^{-1})$. We use the notations of Goursat's lemma : $H = R(B_n)$ is the subgroup of $\mathrm{GL}_{N_1}(\mathbb{F}_q) \times \mathrm{GL}_{N_2}(\mathbb{F}_q)$ defined by $H = \{(x, y) \in H_1 \times H_2 \mid \varphi(xH^1) = yH^2\}$, where $R_i(B_n) = H_i \subset \mathrm{GL}_{N_i}(\mathbb{F}_q)$ with by assumption $H_i \supset \mathrm{SL}_{N_i}(\mathbb{F}_q)$, and $H^i \triangleleft H_i$. If the H_i/H^i are both abelian, then we can conclude by the argument used in Lemma 2.3. Otherwise, they are both non-abelian, hence $H^i \subset \mathbb{F}_q^\times$. The only non-abelian simple composition factor of H_i/H^i being $\mathrm{PSL}_{N_i}(\mathbb{F}_q)$, this is possible only if $N_1 = N_2 = N/2$. Let then $\overline{R}_i : B_n \rightarrow \mathrm{PGL}_{N_i}(\mathbb{F}_q)$ the projective representation of B_n deduced from R_i . By the very description of H we have $\overline{R}_2(b) = \hat{\varphi}(R_1(b))$ for all $b \in B_n$, where $\hat{\varphi}$ is the composite $H_1 \twoheadrightarrow H_1/H^1 \xrightarrow{\sim} H_2/H^2 \rightarrow \mathrm{PGL}_{N_2}(\mathbb{F}_q)$. Since φ 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 $\overline{R}_2(b) = \check{\varphi}(\overline{R}_1(b))$ for all $b \in B_n$, where $\check{\varphi} : H_1/(\mathbb{F}_q^\times \cap H_1) \rightarrow \mathrm{PGL}_{N_2}(\mathbb{F}_q)$ is the induced morphism. Note that $H_1/(\mathbb{F}_q^\times \cap H_1) \subset \mathrm{PGL}_{N_1}(\mathbb{F}_q)$, and clearly $\mathrm{Im} \check{\varphi} \supset \mathrm{PSL}_{N_2}(\mathbb{F}_q)$. From this one deduce that the restriction of $\check{\varphi}$ to $\mathrm{PSL}_{N_1}(\mathbb{F}_q)$ is non-trivial, hence induces an isomorphism ψ between the simple groups $\psi : \mathrm{PSL}_{N_1}(\mathbb{F}_q) \rightarrow \mathrm{PSL}_{N_2}(\mathbb{F}_q)$. Up to a possible conjugation of the representations R_1, R_2 , we get (see [GLS] Theorem 2.5.12) that ψ is either induced by a field automorphism $\Phi \in \mathrm{Aut}(\mathbb{F}_q)$, or by the composition of such an automorphism with $X \mapsto {}^tX^{-1}$. In the first case we let $S = R_1$, in the second case we let $S : g \mapsto {}^tR_1(g^{-1})$. In both cases, we have $\overline{R}_2(b) = \Phi(\overline{S}(b)) = \overline{S^\Phi}(b)$ for all $b \in B'_n$, with $S^\Phi : g \mapsto \Phi(S(g))$, meaning that the two representations of B'_n afforded by R_2 and S^Φ are projectively equivalent, that is there is $z : B'_n \rightarrow \mathbb{F}_q^\times$ such that $R_2(b) = S^\Phi(b)z(b)$ for all $b \in B'_n$. Since B'_n is perfect for $n \geq 5$ (see [GL]) we get $z = 1$; this proves that the restrictions of R_2 and S^Φ to B'_n are isomorphic. In particular, their restrictions to B'_3 are isomorphic. The restrictions of R_2 and S to B'_3 are direct sums of the irreducible representations of TL_3 , restricted to the derived subgroups. There are two such irreducible representations, of

dimensions 1 and 2, corresponding to the partitions [3] and [2, 1], respectively. Note that these restrictions have to contain a component of dimension 2, for otherwise the image of B'_3 would be trivial, hence σ_1 and σ_2 would have the same image (as $\sigma_1\sigma_2^{-1} \in B'_3$), which easily implies that the image of B_n is abelian, contradicting either $R_2(B_n) \supset \mathrm{SL}_{N_2}(\mathbb{F}_q)$ or $R_1(B_n) \supset \mathrm{SL}_{N_1}(\mathbb{F}_q)$. But this implies that the representation of B'_3 associated to [2, 1] has to be isomorphic to its twisted by Φ . By explicit computation we get that the trace of $\sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}$ 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 $R_2(b) = S(b)$ for all $b \in B'_{n-1}$. By Lemma 3.4 and because the abelianization of B_n is given by $\ell : B_n \rightarrow \mathbb{Z}$, $\sigma_i \mapsto 1$, this means that $R_2(b) = S(b)u^{\ell(b)}$ for some $u \in \mathbb{F}_q^\times$, and this for all $b \in B_{n-1}$.

If $S = R_1$, this implies that the spectrum of $R_2(\sigma_1)$, which is made of -1 with multiplicity $a(n, r_2)$ and α with multiplicity $b(n, r_2)$, is also made of $-u$ with multiplicity $a(n, r_1)$ and $u\alpha$ with multiplicity $b(n, r_1)$. Since $a(n, r_1) > b(n, r_1)$ and $a(n, r_2) > b(n, r_2)$ by Lemma 3.3, this implies $u = 1$, hence $R_2 = R_1$, which is excluded because these two representations of the Temperley-Lieb algebras are non-isomorphic by assumption.

Finally, if $S(b) = {}^t R_1(b^{-1})$ for all $b \in B_n$, the spectrum of $R_2(\sigma_1)$, made of -1 with multiplicity $a(n, r_2)$ and α with multiplicity $b(n, r_2)$, is also made of $-u$ with multiplicity $a(n, r_1)$ and $u\alpha^{-1}$ with multiplicity $b(n, r_1)$. Again by Lemma 3.3, this implies $u = 1$, and $\alpha = \alpha^{-1}$ hence $\alpha^2 = 1$, contradicting the assumption on the order of α . This concludes the proof. \square

Corollary 3.2 is an immediate consequence of Proposition 3.1.

3.2. The case of $[n - 1, 1]$. We first prove part (i) of Theorem 1.2 (under the assumption that Theorem 1.3 holds) when $\lambda = [n - 1, 1]$. This case is essentially dealt by Theorem 1.1, as we show now.

Indeed, $R(B_n)$ is generated by the $R(\sigma_i)$, which in our case $\lambda = [n - 1, 1]$ have eigenvalues α with multiplicity 1 and -1 with multiplicity $n - 2$, and thus the $(-1)R(\sigma_i)$ are semisimple pseudo-reflections of order at least 4 as α has order not dividing 6.

When $R(B_n)$ is primitive and $n \geq 4$, Theorem 1.1 states that $\mathrm{SL}_N(\mathbb{F}_{\tilde{q}}) \leq R(B) \leq \mathrm{GL}_N(\mathbb{F}_{\tilde{q}})$ for some \tilde{q} dividing q , or $R(B) \leq \mathrm{GU}_N(\tilde{q})$ for some $\tilde{q}^2 | q$. Notice now that $\det \sigma_1 = \alpha$. If $R(B) \subset \mathrm{GU}_N(\tilde{q})$, α would be fixed by $\mathrm{Gal}(\mathbb{F}_{\tilde{q}^2} | \mathbb{F}_{\tilde{q}})$ which embeds in $\mathrm{Gal}(\mathbb{F}_{\tilde{q}} | \mathbb{F}_p)$, and this would contradict $\mathbb{F}_p(\alpha) = \mathbb{F}_q$. Then $\mathrm{SL}_N(\mathbb{F}_{\tilde{q}}) \leq R(B) \leq \mathrm{GL}_N(\mathbb{F}_{\tilde{q}})$, and $\mathbb{F}_q = \mathbb{F}_p(\alpha) \subset \mathbb{F}_{\tilde{q}}$ implies $\tilde{q} = q$ and the conclusion. We thus only need to prove the primitiveness, and to take separate care for the case $n = 3$. In this case, one matrix model is given by :

$$\sigma_1 \mapsto s_1 = \begin{pmatrix} -1 & -1 \\ 0 & \alpha \end{pmatrix} \quad \sigma_2 \mapsto s_2 = \begin{pmatrix} -1 & 0 \\ 1 + \alpha + \alpha^2 & \alpha \end{pmatrix}.$$

We let \bar{s}_1 and \bar{s}_2 their image in $\mathrm{PGL}_2(\mathbb{F}_q)$. We prove the following lemma

Lemma 3.5. *If the order of α is not in $\{1, 2, 3, 6, 10\}$, then $\langle s_1, s_2 \rangle$ contains $\mathrm{SL}_2(\mathbb{F}_q)$.*

Proof. Let $G = \langle s_1, s_2 \rangle \subset \mathrm{GL}_2(\mathbb{F}_q)$, and choose $u \in \overline{\mathbb{F}_p}$ such that $u^2 = -\alpha^{-1}$. We let $\mathbb{F}_{q'} = \mathbb{F}_q(u)$ and \overline{G} the image of G in $\mathrm{PGL}_2(\mathbb{F}_q) \subset \mathrm{PGL}_2(\mathbb{F}_{q'})$. Then $\overline{G} = \langle \bar{s}_1, \bar{s}_2 \rangle = \langle \bar{u}s_1, \bar{u}s_2 \rangle \subset \mathrm{PSL}_2(\mathbb{F}_{q'})$. By Dickson's theorem (see [H] Theorem 8.27), we know that \overline{G} is either abelian by abelian, or isomorphic to one of the groups \mathfrak{A}_5 , \mathfrak{S}_4 , $\mathrm{PSL}_2(\mathbb{F}_{q'})$ or $\mathrm{PGL}_2(\mathbb{F}_{q'})$ for $\tilde{q}' | q'$ and $\tilde{q}' \geq 4$.

We first prove that $\overline{G} \subset \mathrm{PSL}_2(\mathbb{F}_{q'})$ cannot be abelian by abelian. For this we note that $s_1 s_2^{-1}$ and $s_1^{-1} s_2$ belong to the image of (B_3, B_3) , hence the commutator subgroup of $[\overline{G}, \overline{G}]$ contains the commutator of $\overline{s}_1 \overline{s}_2^{-1}$ and $\overline{s}_1^{-1} \overline{s}_2$, which is non trivial because

$$(s_1 s_2^{-1})(s_1^{-1} s_2) - (s_1^{-1} s_2)(s_1 s_2^{-1}) = \begin{pmatrix} \frac{-\alpha^2 + \alpha^3 - 1}{\alpha^2} & -\frac{(\alpha-1)(1+\alpha^2)}{\alpha^2} \\ \frac{(\alpha-1)(\alpha^2 + \alpha + 1)}{\alpha} & \frac{\alpha^3 + \alpha - 1}{\alpha} \end{pmatrix}$$

is non-scalar when α has order at least 4.

Now note that $\overline{s}_1^r = 1$ means that $u^r = u^{-r}$, that is $\alpha^r = (-1)^r$. Our conditions thus imply that $r \notin \{1, 2, 3, 4, 5, 6\}$, which rules out the cases $\overline{G} \simeq \mathfrak{S}_4$ and $\overline{G} \simeq \mathfrak{A}_5$. This proves that $[\overline{G}, \overline{G}] \simeq \mathrm{PSL}_2(\mathbb{F}_{q'})$ for some $q'|q$. Since $[\overline{G}, \overline{G}] = [\overline{G}, \overline{G}] \subset \mathrm{PSL}_2(\mathbb{F}_q)$ this implies $q'|q$, so we denote $q' = \tilde{q}|q$.

The natural embedding $\overline{G} \subset \mathrm{PSL}_2(\mathbb{F}_{q'})$ can be considered as a projective representation $\bar{\rho}$ of $[\overline{G}, \overline{G}] \simeq \mathrm{PSL}_2(\mathbb{F}_{\tilde{q}})$ with associated cocycle $c \in Z^2(\mathrm{PSL}_2(\mathbb{F}_{\tilde{q}}), \mathbb{F}_{q'}^\times)$. When $\mathrm{SL}_2(\mathbb{F}_{\tilde{q}})$ is the Schur cover of $\mathrm{PSL}_2(\mathbb{F}_{\tilde{q}})$, then c becomes cohomologous to 0 inside $Z^2(\mathrm{SL}_2(\mathbb{F}_{\tilde{q}}), \mathbb{F}_{q'}^\times)$ by the universal coefficient theorem and because $\mathrm{PSL}_2(\mathbb{F}_{\tilde{q}})$ and $\mathrm{SL}_2(\mathbb{F}_{\tilde{q}})$ are perfect. In the two cases where this does not hold, that is $\mathrm{PSL}_2(\mathbb{F}_4)$ and $\mathrm{PSL}_2(\mathbb{F}_9)$, we check on the Brauer character tables that every 2-dimentional irreducible projective representations in natural characteristic of these groups can be linearized when lifted to $\mathrm{SL}_2(\mathbb{F}_4)$ and $\mathrm{SL}_2(\mathbb{F}_9)$, respectively. Moreover, $\mathrm{SL}_2(\mathbb{F}_{\tilde{q}})$ admits a unique non-trivial representation in natural characteristic, up to twisting by a field automorphism. This implies that $[\overline{G}, \overline{G}]$ is *conjugated* to $\Phi(\mathrm{PSL}_2(\mathbb{F}_{\tilde{q}}))$ for some $\Phi \in \mathrm{Aut}(\mathbb{F}_q)$ over $\overline{\mathbb{F}_p}$. Now, the trace of $s_1 s_2^{-1} \in \mathrm{SL}_2(\mathbb{F}_q)$ belongs to $\Phi(\mathbb{F}_{\tilde{q}})$, hence $\mathbb{F}_q = \mathbb{F}_p(\alpha + \alpha^{-1}) \subset \Phi(\mathbb{F}_{\tilde{q}})$ since

$$s_1 s_2^{-1} = \begin{pmatrix} -(\alpha + \alpha^{-1}) & -\alpha^{-1} \\ \alpha^2 + \alpha + 1 & 1 \end{pmatrix}.$$

This proves $\tilde{q} = q$ and the conclusion by Lemma 2.1. □

Now we can get the conclusion for $[n-1, 1]$ by induction on n , provided $n \geq 4$: since $R(B_{n-1}) \subset \mathrm{GL}_{n-1}(\mathbb{F}_q)$ has been shown to contain $\mathrm{SL}_{n-2}(\mathbb{F}_q)$ by the branching rule and the induction assumption, R is primitive, hence contains $\mathrm{SL}_{n-1}(\mathbb{F}_q)$ by the previous argument. This concludes the case $[n-1, 1]$, and in particular the cases $n \leq 3$.

3.3. Induction step for Theorem 1.2. We now can prove part (i) of Theorem 1.2 (under the assumption that Theorem 1.3 holds) by induction on n , and restrict to the partitions λ which are not of the form $[n]$ or $[n-1, 1]$, as the former case is trivial and the latter has been dealt with in §3.2 (in particular this settles the initial cases $n \leq 3$).

When $n = 4$, the additional λ is $[2, 2]$, which is an immediate consequence of the case $\lambda = [2, 1]$; indeed, one is deduced from the other through the ‘special morphism’ $B_4 \rightarrow B_3$ which maps $s_3, s_1 \mapsto s_1$ and $s_2 \mapsto s_2$. When $n = 5$, the only case to consider is the 5-dimensional representation $\lambda = [3, 2]$, for which the restriction to B_{n-1} is the direct sum of $[4, 1]$ (3-dimensional) and $[2, 2]$ (2-dimensional). By Lemma 2.3 and the case $n = 4$ we get that $R(B_4) \supset \mathrm{SL}_3(\mathbb{F}_q) \times \mathrm{SL}_2(\mathbb{F}_q)$ and we get $R(B_5) \supset \mathrm{SL}_5(\mathbb{F}_q)$ by Theorem 1.3. Finally, when $n \geq 6$, we can use Corollary 3.2 to get the result by Theorem 1.3, except for the case $n = 2m$, $\lambda = [m, m]$, in which case $c(2m, m) = c(2m-1, m-1)$ and one immediately gets $R(B_n) \supset R(B_{n-1}) \supset \mathrm{SL}_{c(2m, m)}(\mathbb{F}_q)$ from the induction assumption, and when $\lambda = [n-r, r]$

with $c(n-1, r) = c(n-1, r-1)$. Letting $N = \dim \lambda$ we get in this case $R(B_n) \supset \mathrm{SL}_{N/2}(\mathbb{F}_q) \times \mathrm{SL}_{N/2}(\mathbb{F}_q)$, and Theorem 1.3 implies $R(B_n) \supset \mathrm{SL}_N(\mathbb{F}_q)$ or $R(B_n) \subset \mathrm{GL}_{N/2}(\mathbb{F}_q) \wr \mathfrak{S}_2$. We need to exclude the latter case. For this, note that the composite $B_n \rightarrow \mathrm{GL}_{N/2}(\mathbb{F}_q) \wr \mathfrak{S}_2 \rightarrow \mathfrak{S}_2$ factorizes through B_n^{ab} , hence $R(B'_n) \subset \mathrm{GL}_{N/2}(\mathbb{F}_q) \times \mathrm{GL}_{N/2}(\mathbb{F}_q)$. Since $R(B_{n-1}) \subset \mathrm{GL}_{N/2}(\mathbb{F}_q) \times \mathrm{GL}_{N/2}(\mathbb{F}_q)$ and because B_n is generated by B_{n-1} and B'_n , this implies $R(B_n) \subset \mathrm{GL}_{N/2}(\mathbb{F}_q) \times \mathrm{GL}_{N/2}(\mathbb{F}_q)$, contradicting the irreducibility of R . This concludes the proof of (i).

We now prove (ii). By (i), the image of B_n inside each of the $\mathrm{GL}_{c(n,r)}(\mathbb{F}_q)$ contains $\mathrm{SL}_{c(n,r)}(\mathbb{F}_q)$, hence the image of B'_n also contains $\mathrm{SL}_{c(n,r)}(\mathbb{F}_q)$. We prove that the image of B_n inside $\prod_{1 \leq r \leq k} \mathrm{GL}_{c(n,r)}(\mathbb{F}_q)$ contains $\prod_{1 \leq r \leq k} \mathrm{SL}_{c(n,r)}(\mathbb{F}_q)$ for $1 \leq k \leq n/2$ by induction on k . This amounts to saying that the image H of B'_n is $\prod_{1 \leq r \leq k} \mathrm{SL}_{c(n,r)}(\mathbb{F}_q)$. The cases $k = 1$ and $k = 2$ are trivial, so we assume $k \geq 3$. We use Goursat's lemma with $G_1 = \prod_{1 \leq r \leq k-1} \mathrm{SL}_{c(n,r)}(\mathbb{F}_q)$ and $G_2 = \mathrm{SL}_{c(n,k)}(\mathbb{F}_q)$. By assumption and (i) we have $H_1 = G_1$ 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 $\mathrm{PSL}_{c(n,k)}(\mathbb{F}_q)$ and we get a surjective morphism $\hat{\varphi} : H_1 \twoheadrightarrow \mathrm{PSL}_{c(n,k)}(\mathbb{F}_q)$. Let now $r < k$, and consider the restriction $\hat{\varphi}_r$ of $\hat{\varphi}$ to $\mathrm{SL}_{c(n,r)}(\mathbb{F}_q)$. Assume it is non-trivial. Since the image of the center is mapped to 1, it factorizes through an isomorphism $\check{\varphi}_r : \mathrm{PSL}_{c(n,r)}(\mathbb{F}_q) \rightarrow \mathrm{PSL}_{c(n,k)}(\mathbb{F}_q)$. But this implies that the image of B'_n inside $\mathrm{SL}_{c(n,r)}(\mathbb{F}_q) \times \mathrm{SL}_{c(n,k)}(\mathbb{F}_q)$ is included inside $\{(x, y) \mid \bar{y} = \check{\varphi}_r(\bar{x})\}$, where \bar{x}, \bar{y} denote the canonical images of x, y . On the other hand, we know by Proposition 3.1 that the image is all $\mathrm{SL}_{c(n,r)}(\mathbb{F}_q) \times \mathrm{SL}_{c(n,k)}(\mathbb{F}_q)$, a contradiction that proves that each $\hat{\varphi}_r$ is trivial, hence so is $\hat{\varphi}$. Since it is surjective, this provides a contradiction which excludes this case. Thus $H_1/H^1 \simeq H_2/H^2$ is abelian, and we can conclude as in the proof of Lemma 2.3.

Remark 3.6. *Note that we cannot immediately apply Lemma 2.3, in order to prove part (ii) of theorem 1.2, because it may happen that $c(n, r+1) = c(n, r)$, for instance $c(7, 3) = c(7, 4) = 14$.*

3.4. Unitary case. We now assume $\mathbb{F}_p(\alpha + \alpha^{-1}) \neq \mathbb{F}_p(\alpha) = \mathbb{F}_q$, and denote $\varepsilon \in \mathrm{Aut}(\mathbb{F}_q)$ the generator of $\mathrm{Gal}(\mathbb{F}_q | \mathbb{F}_{q^{1/2}})$. We first prove that, in the semisimple case and over a finite field, all representations of the Hecke algebra are unitary.

Proposition 3.7. *If $\mathbb{F}_p(\alpha + \alpha^{-1}) \neq \mathbb{F}_p(\alpha) = \mathbb{F}_q$, and $R : B_n \rightarrow \mathrm{GL}_N(\mathbb{F}_q)$ is an absolutely irreducible representation associated to a partition $\lambda \vdash n$, then there exists $P \in \mathrm{GL}_N(\mathbb{F}_q)$ such that $PR(B_n)P^{-1} \subset \mathrm{GU}_N(q^{1/2})$.*

Proof. First note that, in that case, $\mathbb{F}_p(\alpha + \alpha^{-1}) = \mathbb{F}_{q^{1/2}}$, and let ε be the generator (of order 2) of $\mathrm{Gal}(\mathbb{F}_q | \mathbb{F}_{q^{1/2}})$. Then ε exchanges the roots α and α^{-1} of the polynomial $X^2 - (\alpha + \alpha^{-1})X + 1$. According to Lemma 2.4 we only need to prove that $\varepsilon \circ \rho^* \simeq \rho$. Recall that two irreducible representations of the Hecke algebra $H_n(\alpha)$ for $n \geq 4$ are isomorphic if and only if their restriction to the Hecke algebra of type $H_{n-1}(\alpha)$ are isomorphic : this means that two Young diagrams of size $n \geq 3$ are the same if and only if the set of all their subdiagrams of size $n-1$ are the same, and this is a simple exercise in the combinatorics of Young diagrams. Since the restriction of representations commutes with twisting by ε and taking the dual, this readily proves the statement $\varepsilon \circ \rho^* \simeq \rho$ by induction on n , provided we know how to prove it for $n = 2$. In that case however, it is trivial because all irreducible representations are 1-dimensional,

and given by $\sigma_1 \mapsto -1$, $\sigma_1 \mapsto \alpha$. Unitarity in that case simply means $\alpha^{-1} = \varepsilon(\alpha)$, and this concludes the proof. \square

Up to conjugating the representations, we can thus assume $R(B_n) \subset \mathrm{GU}_N(q^{1/2})$. One can then mimic the proof of the part (i) of the theorem for the case $\mathbb{F}_p(\alpha) = \mathbb{F}_p(\alpha + \alpha^{-1})$. Indeed,

- we have a similar statement as Lemma 3.4 for representations $R_1, R_2 : G \rightarrow \mathrm{GU}_N(q^{1/2})$ for $N \geq 2$ with $(R_1)_{|G'} = (R_2)_{|G'}$ for $N \geq 2$ and $R_1(G') = R_2(G') \supset \mathrm{SU}_N(q^{1/2})$: then there exists $\eta : G \rightarrow \mathbb{F}_q^\times$ such that $R_2 = R_1 \otimes \eta$. Indeed, the same proof applies, because the centralizer of $\mathrm{SU}_N(q^{1/2})$ in $\mathrm{GL}_N(\mathbb{F}_q)$ is $(\mathbb{F}_q)^\times$.
- when $n = 3$, the same argument and Dickson's theorem imply (with the same notations as in the proof of Lemma 3.5) that $[\overline{G}, \overline{G}] = \mathrm{PSL}_2(\mathbb{F}_{q^{1/2}}) = \mathrm{PSU}_2(q^{1/2})$ hence $[G, G] \supset \mathrm{SU}_2(q^{1/2})$.
- we have a statement similar to Proposition 3.1 for the unitary case namely that, with the notations of this proposition, if $\mathbb{F}_p(\alpha + \alpha^{-1}) \neq \mathbb{F}_p(\alpha) = \mathbb{F}_q$, and $R_i(B_n) \supset \mathrm{SU}_{N_i}(q^{1/2})$, then $R(B_n) \supset \mathrm{SU}_{N_1}(q^{1/2}) \times \mathrm{SU}_{N_2}(q^{1/2})$. The proof is similar, additional care being needed only when considering the possible automorphisms ψ of $\mathrm{PSU}_{N/2}(q^{1/2})$. Up to possible (unitary) conjugation of R_1 and R_2 , ψ is again either induced by $\Phi \in \mathrm{Aut}(\mathbb{F}_q)$ or by the composition by such a field automorphism with $\mathfrak{s} : X \mapsto {}^t \varepsilon(X)^{-1}$ (see [GLS] Theorem 2.5.12). Here $q = p^{2f}$, and $\Phi = F^r$ for $F : x \mapsto x^p$ the Frobenius automorphism and some $0 \leq r < 2f$, and we can assume $r < f$ because the actions of F^f and \mathfrak{s} coincide on $\mathrm{PSU}_{N/2}(q^{1/2})$. We need to prove $\Phi = 1$, and for this we are similarly reduced to considering the case [2, 1]. Then the final condition that $1 - (\alpha + \alpha^{-1})$ is fixed implies that $\Phi \in \mathrm{Gal}(\mathbb{F}_q | \mathbb{F}_{q^{1/2}}) = \{1, F^f\}$ hence $\Phi = 1$ since $r < f$. The conclusion is then similar, using the analogue of Lemma 3.4.
- One uses Theorem 1.4 instead of Theorem 1.3.

4. PROOFS OF THEOREM 1.3 AND OF THEOREM 1.4

For any finite group H and any prime p , we denote by $O_p(H)$ the unique maximal normal p -subgroup of H . We will need the following result, that we derive from Kantor [Ka], Theorem II (see also [SZ1]).

Theorem 4.1. *Let p be a prime and q be a p -power. Suppose that H is an irreducible subgroup of $\mathrm{SL}_N(\mathbb{F}_q)$ generated by a conjugacy class of transvections, such that $O_p(H) \leq [H, H] \cap Z(H)$. Then H is one of the following groups.*

- (i) $H = \mathrm{SL}_N(\mathbb{F}_{q'})$ or $H = \mathrm{Sp}_N(\mathbb{F}_{q'})$ in $\mathrm{SL}_N(\mathbb{F}_{q'})$, or $H = \mathrm{SU}_N(q^{1/2})$ in $\mathrm{SL}_N(q')$
- (ii) $H = \mathrm{O}_N^\pm(\mathbb{F}_{q'}) < \mathrm{SL}_N(\mathbb{F}_{q'})$, q' even.
- (iii) $H = \mathfrak{S}_n < \mathrm{SL}_N(\mathbb{F}_2)$, where $N = n - d$ with $d = \gcd(n, 2)$.
- (iv) $H = \mathfrak{S}_{2n}$ in $\mathrm{SL}_{2n-1}(\mathbb{F}_2)$ or in $\mathrm{SL}_{2n}(\mathbb{F}_2)$.
- (v) $H = 3 \cdot \mathfrak{A}_6 < \mathrm{SL}_3(\mathbb{F}_4)$.
- (vi) $H = \mathrm{SL}_2(\mathbb{F}_5) < \mathrm{SL}_2(\mathbb{F}_9)$.
- (vii) $H = 3 \cdot \mathrm{P}\Omega_6^{-, \pi}(\mathbb{F}_3) < \mathrm{SL}_6(\mathbb{F}_4)$.
- (viii) $H = \mathrm{SU}_4(2) < \mathrm{SL}_5(\mathbb{F}_4)$.
- (ix) $H = A \rtimes \mathfrak{S}_N$ in $\mathrm{SL}_N(\mathbb{F}_{2^i})$ where A is a subgroup of diagonal matrices.

where $q' | q$.

Assume that $N \geq 5$ and $a \geq N - a$. In particular, $a \geq 3$. Let Γ be an absolutely irreducible subgroup of $\mathrm{GL}_N(\mathbb{F}_q)$ containing $\mathrm{SL}_a(\mathbb{F}_q)$. Write $G = [\Gamma, \Gamma]$. Note that $\mathrm{SL}_a(\mathbb{F}_q) \leq G$ (because $\mathrm{SL}_a(\mathbb{F}_q)$ is perfect since $a > 2$). Denote by $V = \mathbb{F}_q^N$ the natural representation of $\mathrm{SL}_N(\mathbb{F}_q)$. Let t be a transvection in $\mathrm{SL}_a(\mathbb{F}_q)$. Write $G_0 = G$ and for every $i \geq 1$, define G_i the subgroup of G_{i-1} generated by the conjugacy class of t in G_{i-1} . Note that G_i is a normal subgroup of G_{i-1} and that $\mathrm{SL}_a(\mathbb{F}_q) \leq G_i$ (because $\mathrm{SL}_a(\mathbb{F}_q) \leq G$ is generated by the conjugacy class of t in $\mathrm{SL}_a(\mathbb{F}_q)$).

First, assume that there is a positive integer i such that V is an irreducible $\mathbb{F}_q G_j$ -module for every $0 \leq j < i$ and as an $\mathbb{F}_q G_i$ -module, V is reducible. Note that if such an i exists, then $i > 0$ because V is an irreducible $\mathbb{F}_q G_0$ -module by assumption. Since G_i is normal in G_{i-1} and V is an irreducible $\mathbb{F}_q G_{i-1}$ -module, Clifford's theorem (see for example [CR], §11A) implies that

$$\mathrm{Res}_{G_i}^{G_{i-1}}(V) = \bigoplus_{k=1}^r W_k,$$

where W_k are irreducible $\mathbb{F}_q G_i$ -modules and the W_k are G_{i-1} -conjugate to W_1 . Moreover, we can choose W_1 to be an irreducible component of $\mathrm{Res}_{G_i}^{G_{i-1}}(V)$ such that the natural representation V_a of $\mathrm{SL}_a(\mathbb{F}_q)$ is a component of $\mathrm{Res}_{\mathrm{SL}_a(\mathbb{F}_q)}^{G_i}(W_1)$. Hence,

$$\dim(W_k) = \dim(W_1) \geq \dim(V_a) = a,$$

and we deduce that $r = 2$ and $a = N/2$. In particular, G_i is a subgroup of $\mathrm{GL}(W_1) \times \mathrm{GL}(W_2) \leq \mathrm{GL}_N(\mathbb{F}_q)$, and since W_1 and W_2 are G_{i-1} -conjugate, there is $g \in G_{i-1}$ such that ${}^g\mathrm{GL}(W_1) = \mathrm{GL}(W_2)$. Note that as vector space, we have $W_1 = V_a$. Thus, $\mathrm{SL}(W_1) \leq G_i$. However, ${}^g\mathrm{SL}(W_1)$ is a normal subgroup of $\mathrm{GL}(W_2)$ isomorphic to $\mathrm{SL}_a(\mathbb{F}_q)$, hence ${}^g\mathrm{SL}(W_1) = \mathrm{SL}(W_2)$. Since G_i is normal in G_{i-1} , we obtain

$$\mathrm{SL}(W_1) \times \mathrm{SL}(W_2) \leq G_i.$$

Now, using that $G_i \leq \mathrm{GL}(W_1) \times \mathrm{GL}(W_2)$, we deduce that $[G_i, G_i] = \mathrm{SL}(W_1) \times \mathrm{SL}(W_2)$. In particular, $\mathrm{SL}(W_1) \times \mathrm{SL}(W_2)$ is a characteristic subgroup of G_i . Thus, G_{i-1} normalizes $\mathrm{SL}(W_1) \times \mathrm{SL}(W_2)$. However, $N_{\mathrm{GL}_N(\mathbb{F}_q)}(\mathrm{SL}(W_1) \times \mathrm{SL}(W_2)) = \mathrm{GL}_{N/2}(\mathbb{F}_q) \wr \mathbb{Z}/2\mathbb{Z}$ and we get

$$G_{i-1} \leq \mathrm{GL}_{N/2}(\mathbb{F}_q) \wr \mathbb{Z}/2\mathbb{Z}.$$

Now, we prove by induction on $0 \leq j \leq i - 1$ that $G_j \leq \mathrm{GL}_{N/2}(\mathbb{F}_q) \wr \mathbb{Z}/2\mathbb{Z}$. We have shown that this is true for G_{i-1} . Assume it holds for G_j . Then we have $\mathrm{SL}(W_1) \times \mathrm{SL}(W_2) \leq G_j \leq \mathrm{GL}_{N/2}(\mathbb{F}_q) \wr \mathbb{Z}/2\mathbb{Z}$. Thus, $\mathrm{SL}(W_1) \times \mathrm{SL}(W_2)$ is characteristic in G_j (because the second derived subgroup of G_j is $\mathrm{SL}(W_1) \times \mathrm{SL}(W_2)$). Since G_j is normal in G_{j-1} , we deduce that G_{j-1} normalizes $\mathrm{SL}(W_1) \times \mathrm{SL}(W_2)$ and we conclude as above that $G_{j-1} \leq \mathrm{GL}_{N/2}(\mathbb{F}_q) \wr \mathbb{Z}/2\mathbb{Z}$. In particular, $G = G_0$ is a subgroup of $\mathrm{GL}_{N/2}(\mathbb{F}_q) \wr \mathbb{Z}/2\mathbb{Z}$. Now, since G is the derived subgroup of Γ , we deduce that the third derived subgroup of Γ is $\mathrm{SL}(W_1) \times \mathrm{SL}(W_2)$. Thus, $\mathrm{SL}(W_1) \times \mathrm{SL}(W_2)$ is a characteristic subgroup of Γ and we conclude with the same argument that $\Gamma \leq \mathrm{GL}_N(\mathbb{F}_q) \wr \mathbb{Z}/2\mathbb{Z}$.

Now, we assume that V is an irreducible $\mathbb{F}_q G_j$ -module for all non-negative integer j . Note that there is a positive integer r such that $G_r = G_{r+1}$ (because the groups G_i are finite). In particular, G_r is generated by the class of t in G_r and V is an irreducible $\mathbb{F}_q G_r$ -module. By Clifford theorem, $\mathrm{Res}_{O_p(G_r)}^{G_r}(V)$ is semisimple. However, as p -group, the only irreducible $\mathbb{F}_q O_p(G_r)$ -module of $O_p(G_r)$ is the trivial module. Thus, $\mathrm{Res}_{O_p(G_r)}^{G_r}(V)$ is trivial, which implies

that $O_p(G_r) = 1$. So, we can apply Theorem 4.1 to G_r . Note that $\mathrm{SL}_a(\mathbb{F}_q) \leq G_r$ implies that $q' = q$.

If $G_r = \mathrm{SU}_N(q^{1/2})$ or $G_r = \mathrm{Sp}_N(\mathbb{F}_q)$ or $G_r = \mathrm{O}_N^\pm(\mathbb{F}_q)$ (for q even), then the contragredient representation ρ^* of the natural representation $\rho : G_r \rightarrow \mathrm{GL}_N(\mathbb{F}_q)$ would satisfy either $\rho^* \simeq \rho$ or $\rho^* \simeq \varepsilon \circ \rho$, where $\varepsilon \in \mathrm{Aut}(\mathbb{F}_q)$ has order 2. Since its restriction to $\mathrm{SL}_a(\mathbb{F}_q) \subset G_r$ does not (because $a \geq 3$), this is a contradiction.

Note that G_r contains matrices whose coefficients are not in \mathbb{F}_2 (because $q > 3$). Hence, the cases (iii) and (iv) are excluded. The cases (v) and (vi) are excluded, because $N \geq 5$. Recall from [Ka] that case (vii) actually corresponds to an embedding of G_r into $\mathrm{SU}_6(2)$. This excludes the possibility that G_r contains $\mathrm{SL}_3(\mathbb{F}_4)$, because every 3-dimensional subspace of \mathbb{F}_4^6 contains a nonzero vector v of norm 0, and therefore G_r would contain all the transvections $x \mapsto x + \lambda \langle v | x \rangle v$ for $\lambda \in \mathbb{F}_4$. But such a transvection is an isometry only if $\lambda + \bar{\lambda} = 0$, and therefore any $\lambda \in \mathbb{F}_4 \setminus \mathbb{F}_2$ provides a contradiction and thus case (vii) is excluded.

Now, note that 7 does not divide the order of the group $\mathrm{SU}_4(\mathbb{F}_2)$. But 7 divides $|\mathrm{SL}_3(\mathbb{F}_4)|$, and a fortiori $|\mathrm{SL}_a(\mathbb{F}_4)|$ excluding the cases (vii) and (viii).

Now, suppose that $G_r = A \rtimes \mathfrak{S}_N$, where A is a subgroup of diagonal matrices and \mathfrak{S}_N is identified with the subgroup of permutation matrices of $\mathrm{SL}_N(\mathbb{F}_q)$. Let $g \in G_r$. Then g is a transvection of G_r if and only if g has order 2 and has only one Jordan block $J_2(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in its Jordan decomposition. Write $\theta : G_r \rightarrow \mathfrak{S}_N$ for the natural projection. Note that g is conjugate to a block-diagonal matrix, whose block-matrices A_1, \dots, A_k correspond to the decomposition of $\theta(g) = c_1 \cdots c_k$ into cycles with disjoint support. Furthermore, if c_i has length l , then A_i is a $l \times l$ -matrix of order greater than l . Then the c_i 's are transpositions and $A_i = \begin{pmatrix} 0 & a \\ a^{-1} & 0 \end{pmatrix}$ for some $a \in \mathbb{F}_q^\times$, because $A_i^2 = 1$. It follows that the characteristic polynomial of A_i is $(X - 1)^2$, and A_i is conjugate in $\mathrm{GL}_2(\mathbb{F}_q)$ to $J_2(1)$, because A_i is non-trivial. Hence, the Jordan decomposition of g consists in k Jordan blocks $J_2(1)$. Therefore, if g a transvection, then $k = 1$ and $\theta(g)$ is a transposition. Conversely, the matrix $t(a, i, j) = (t_{kl})_{1 \leq k, l \leq n}$, for $a \in \mathbb{F}_q^\times$ and $1 \leq i < j \leq N$, defined by $t_{ii} = t_{jj} = 0$, $t_{kk} = 1$ for $k \neq i, j$, $t_{ij} = a$, $t_{ji} = a^{-1}$ and $t_{kl} = 0$ otherwise, is a transvection of $\mathrm{SL}_N(\mathbb{F}_q)$. This proves that the number of transvections in G_r is at most

$$T = (q - 1) \frac{N(N - 1)}{2}.$$

Moreover, recall that the transvections of $\mathrm{SL}_k(\mathbb{F}_q)$ are the set of linear transformations

$$t_{\varphi, v} : \mathbb{F}_q^k \rightarrow \mathbb{F}_q^k, \quad x \mapsto x + \varphi(x)v,$$

where φ is a non-zero linear form and $v \in \ker(\varphi)$ is a non-zero vector. Moreover, $t_{\varphi, v} = t_{\varphi', v'}$ if and only if there is a scalar $\alpha \in \mathbb{F}_q^\times$ such that $\varphi' = \alpha\varphi$ and $v = \alpha v'$. The number of transvections in $\mathrm{SL}_k(\mathbb{F}_q)$ is then

$$T' = \frac{(q^k - 1)(q^{k-1} - 1)}{q - 1}.$$

Put $k = \lfloor N/2 \rfloor$ and define f by $f(x) = (1 + x + \cdots + x^{k-1})(1 + x + \cdots + x^{k-2}) - k(2k - 1)$. Note that if $f(q) > 0$, then $T' > T$. Suppose $N \geq 6$. Then $k \geq 3$. Moreover, we have $f(q) \geq f(4)$, because f is increasing. Using the fact that $4^i = (3 + 1)^i \geq 1 + 3i$ for $i \geq 1$, we obtain

$$f(4) \geq (1 + 3(k - 1))(1 + 3(k - 2)) - k(2k - 1) = 7k^2 - 20k + 10 > 0.$$

Assume now that $N = 5$. Then $k = 2$ and $f(q) = 1 + q - 4 > 0$ for $q \geq 4$. This proves that $T' > T$, excluding $G_r = A \rtimes \mathfrak{S}_N$. Finally, $G_r = \mathrm{SL}_N(\mathbb{F}_q)$, and $\mathrm{SL}_N(\mathbb{F}_q) \leq \Gamma$, as required.

We prove Theorem 1.4 in the same way. First, recall that if $(k, q) \notin \{(2, 2), (2, 3), (3, 3)\}$, then $\mathrm{SU}_k(q)$ is perfect and $\mathrm{PSU}_k(q)$ is simple. Note that in this case, if H is a subgroup of $\mathrm{SU}_k(q)$ generated by a non-central conjugacy class of $\mathrm{SU}_k(q)$, then $H = \mathrm{SU}_k(q)$. Indeed, write $\pi : \mathrm{SU}_k(q) \rightarrow \mathrm{PSU}_k(q)$ for the natural projection. Then $\pi(H)$ is a non-trivial normal subgroup of $\mathrm{PSU}_k(q)$. It follows that $\pi(H) = \mathrm{PSU}_k(q)$ (because $\mathrm{PSU}_k(q)$ is simple). Hence, $\mathrm{SU}_k(q) = HZ$, where $Z = \ker(\pi)$ is the center of $\mathrm{SU}_k(q)$. Moreover,

$$[H, H] = [HZ, HZ] = [\mathrm{SU}_k(q), \mathrm{SU}_k(q)] = \mathrm{SU}_k(q),$$

because $\mathrm{SU}_k(q)$ is perfect, and the result follows.

So, assume that $N \geq 5$, $a \geq N - a$ and $q > 3$. In particular, $\mathrm{SU}_a(q)$ is perfect. Let Γ be a subgroup of $\mathrm{SU}_N(q)$ containing $\mathrm{SU}_a(q)$, and write $G = [\Gamma, \Gamma]$. Then $\mathrm{SU}_a(q) \leq G$. Let t be a root element of $\mathrm{SU}_a(q)$, that is a generator of a root subgroup. Put $G_0 = G$ and for every $i \geq 1$, denote by G_i the subgroup of G_{i-1} generated by the conjugacy class of t in G_{i-1} . Since t is not central in $\mathrm{SU}_a(q)$, it follows from the above discussion that $\mathrm{SU}_a(q) \leq G_i$ for all $i \geq 0$.

Now, the same argument as the one for SL_N gives that if the natural representation V of $\mathrm{SU}_N(q)$ is not G_j -irreducible for some $j > 0$, then $\Gamma \leq \mathrm{GU}_{N/2}(q) \wr \mathbb{Z}/2\mathbb{Z}$, and otherwise, there is some positive integer r such that V is an irreducible $\mathbb{F}_{q^2} G_r$ -module and G_r is generated by the conjugacy class of t in G_r . Thanks to [Ka], §11, our assumptions, and the fact that G_r contains matrices with coefficients lying inside \mathbb{F}_{q^2} and in no proper subfield of \mathbb{F}_{q^2} , we conclude that G_r is either $\mathrm{SU}_N(q)$, or $\mathrm{Sp}_N(q^2)$, or $\mathrm{O}_N^\pm(q^2)$ (for N and q even), or $3 \cdot \mathrm{P}\Omega^{-,\pi}(6, 3)$ in $\mathrm{SU}_6(q)$, or $A \rtimes \mathfrak{S}_N$ in $\mathrm{SU}_N(q)$, q even, $A = a^{n-1}$ and $a|q+1$. The cases $G_r = \mathrm{Sp}_N(q^2)$ and $G_r = \mathrm{O}_N^\pm(q^2)$ are excluded, again because the natural representation of $\mathrm{SU}_a(\mathbb{F}_q)$ is not self-dual for $a \geq 3$.

Furthermore, the case $G_r = 3 \cdot \mathrm{P}\Omega^{-,\pi}(6, 3)$ is excluded, because 13 divides $|\mathrm{SU}_3(4)|$ and does not divide $|3 \cdot \mathrm{P}\Omega^{-,\pi}(6, 3)|$.

Assume now that $G_r = A \rtimes \mathfrak{S}_N$ with A a subgroup of the diagonal matrices of $\mathrm{SU}_N(q)$ of order a^{N-1} with $a|q+1$. Then the same argument as above shows that the number of transvections in G_r is at most

$$T = (q+1) \frac{N(N-1)}{2}.$$

Note that a transvection $t_{\varphi, v}$ of $\mathrm{SL}_k(\mathbb{F}_q)$ is unitary if its adjoint is equal to its inverse $t_{\varphi, v}^{-1} = t_{-\varphi, v}$. This means that v determines φ (up to a scalar) and that v is isotropic. The number of unitary transvections is then the number of non-zero isotropic vectors divided by $|\{\lambda \in \mathbb{F}_{q^2}^\times \mid \lambda^{q+1} = 1\}| = q+1$. By induction on k , we get that the number $a_{k-1} + ((q^2)^{k-1} - a_{k-1} - 1)(q+1)$. Hence, $a_k = q^{2k-1} + (-q)^k + (-q)^{k-1} - 1$, and the number of unitary transvections is

$$T' = \frac{((-q)^k - 1)((-q)^{k-1} - 1)}{(-q) - 1}.$$

(Note that conformally to the principle of Ennola's duality, this is the same formula as before by replacing q with $-q$.)

Now, for $k \geq 1$, let $h_k(x) = \frac{((-x)^k - 1)((-x)^{k-1} - 1)}{-(-x+1)^2}$. If $k = \lfloor N/2 \rfloor$ then $h_k(q) - k(2k-1) > 0$ implies that $T' > T$, and we get the conclusion. Since for $m \geq 1$, the functions $x \mapsto \frac{x^m - 1}{x+1}$ and

$x \mapsto \frac{x^m+1}{x+1}$ are increasing and positive for $x \geq 1$, the same holds for h_k when $k \geq 3$. Suppose that k is even and $k \geq 4$. Then

$$\begin{aligned} h_k(q) - k(2k-1) &= \frac{(q^k)(q^{k-1}+1)}{(q+1)^2} - k(2k-1) \\ &\geq \frac{(4^k-1)(4^{k-1}+1)}{25} - k(2k-1) \geq \frac{(4^{k-1}-1)(4^{k-1}+1)}{25} - k(2k-1) \end{aligned}$$

is positive as soon as $4^{2(k-1)} - 1 - 25k(2k-1) > 0$. This is easily checked to hold true. Suppose k is odd and $k \geq 3$. Once again, we have

$$h_k(q) - k(2k-1) = \frac{(q^k+1)(q^{k-1}-1)}{(q+1)^2} - k(2k-1) > 0$$

if $k \geq 5$. Moreover,

$$h_3(q) - 15 = \frac{(q^3+1)(q^3-1)}{(q+1)^2} - 15 > 0$$

when $q \geq 4$. It remains to consider when $\lfloor N/2 \rfloor = 2$, meaning in our case $N = 5$. Then $T = 10(q+1)$ and the number of unitary transvections in $\text{SU}_3(q)$ is

$$\frac{(q^3+1)(q^2-1)}{(q+1)^2} > T$$

when $q \geq 3$. This proves the result.

REFERENCES

- [CR] C. W. Curtis, I. Reiner, *Methods of representation theory. Vol. I. With applications to finite groups and orders*. Reprint of the 1981 original. Wiley Classics Library. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1990. xxiv+819 pp.
- [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.
- [GLS] D. Gorenstein, R. Lyons, R. Solomon. *The classification of the finite simple groups, Number 3*, volume 40 of *Mathematical Surveys and Monographs*. American Mathematical Society, Cambridge, 1991.
- [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.
- [GR] L.C. Grove, *Classical groups and geometric algebra*, Graduate Studies in Mathematics, 39, Providence, R.I. American Mathematical Society, 2002.
- [H] B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band **134**, Springer-Verlag, Berlin-New York 1967.
- [Ka] W. M. Kantor, *Subgroups of classical groups generated by long root elements*, Trans. Amer. Math. Soc. **248** (1979), no 2, 347–379.
- [Ku] G. Kuperberg, *Denseness and Zariski denseness of Jones braid representations*, Geom. Topol. **15** (2011), 11–39.
- [MM] G. Malle, B.H. Matzat, *Inverse Galois Theory*, Springer-Verlag, Berlin, 1999.
- [Mar1] I. Marin, *L’algèbre de Lie des transpositions*, J. Algebra **310** (2007) 742–774.
- [Mar2] I. Marin, *Infinitesimal Iwahori-Hecke algebras II*, preprint 2009, arxiv:0911.1879.
- [Mar3] I. Marin, *Caractères de rigidité du groupe de Grothendieck-Teichmüller*, Compositio Mathematica **142** (2006) 657–678.
- [Mar4] I. Marin, *Braids inside the Birman-Wenzl-Murakami algebra*, Algebraic Geometric Topology **10** (2010) 1865–1886.
- [Mat] A. Mathas, *Iwahori-Hecke algebras and Schur algebras of the symmetric groups*, University Lecture Series, 15, American Math. Soc., Providence, RI, 1999.
- [SZ1] V.N. Serežkin, A. E. Zalesskiĭ, *Linear groups generated by transvections*, Izv. Akad. Nauk SSSR Ser. Mat. **40** (1976), no. 1, 26–49, 221.

- [SZ2] V.N. Serežkin, A. E. Zalesskiĭ, *Finite linear groups generated by reflections*, Izv. Akad. Nauk SSSR Ser. Mat. 44 (1980), no. 6, 1279–1307, 38.
- [SV] K. Strambach, H. Völklein, *Generalized braid groups and rigidity*, J. Algebra **175** (1995), 604–615.
- [W] A. Wagner, *Collineation groups generated by homologies of order greater than 2*, Geom. Dedicata **7** (1978) 387–398.
- [We] H. Wenzl, *Hecke algebras of type A_n and subfactors*, Invent. Math. **92** (1988), 349–383.

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

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

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

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