TÜBİTAK

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2016) 40: 191 – 200
© TÜBİTAK
doi:10.3906/mat-1506-2

On the twisted modules for finite matrix groups

Kübra GÜL[1], **Nurullah ANKARALIOĞLU**[2,*]
[1]Department of Computer Engineering, Kafkas University, Kars, Turkey
[2]Department of Mathematics, Faculty of Science, Atatürk University, Erzurum, Turkey

Received: 01.06.2015 • **Accepted/Published Online:** 10.08.2015 • **Final Version:** 01.01.2016

Abstract: Suppose that W is an irreducible F_qG-module of dimension n $(d^2 < n < d^3)$ and that H is given as $G = \langle X \rangle$ acting irreducibly on W where X is a set of $n \times n$ matrices with entries in $F = F_q$. In this paper, we present a Las Vegas algorithm that constructs a representation of G of dimension d. We consider the twisted tensor products of the modules of high weights $\lambda_1, \lambda_2, \lambda_{d-2}, \lambda_{d-1}, 2\lambda_1, 2\lambda_{d-1}$.

Key words: Twisted module, irreducible F_qG-module, Las Vegas algorithm

1. Introduction

The majority of recent studies in computational group theory deal with the development of algorithms for the investigation of subgroups of $GL(d, q)$. O'Brien led this work [12]. A particular aim is to develop the algorithms constructing an isomorphism between an arbitrary representation of a classical group and its natural representation. Kantor and Serees [7] presented an algorithm that constructs an isomorphism between an arbitrary permutation or matrix representation and the natural projective representation of H, where H is an almost simple classical group. Magaard et al. [11] described algorithms to set up an isomorphism for a projective matrix representation of degree of at most d^2 of the general linear groups having natural module of dimension d. In this paper, they construct a "nice" generating set in the natural module by using algorithms presented by [3] or [9]. In addition, there is an effective algorithm constructing an isomorphism between an arbitrary permutation or matrix representation of A_n, S_n of large degree and the natural permutation representation [1], and in [2] a specialized algorithm does the same for the small degree case.

This study presents an algorithm that constructs an isomorphism such as in [11]. We consider the twisted tensor products of modules of the high weights $\lambda_1, \lambda_2, \lambda_{d-2}, \lambda_{d-1}, 2\lambda_1, 2\lambda_{d-1}$.

We now give some required information for our task. Let $q = p^f$ be a prime power and F_q be a finite field. Let $V = \langle v_1, v_2, \ldots, v_d \rangle$ be a natural module of H and V^* be its dual module. The symmetric square $Sym^2(V)$ of V is the subspace of $V \otimes V$ spanned by

$$\{e_i \otimes e_j + e_j \otimes e_i : 1 \leq i < j \leq d\} \cup \{e_i \otimes e_i : 1 \leq i \leq d\}.$$

The alternating square $\Lambda^2(V)$ of V is the subspace of $V \otimes V$ spanned by

$$\{e_i \otimes e_j - e_j \otimes e_i : 1 \leq i < j \leq d\}.$$

*Correspondence: ankarali@atauni.edu.tr
2010 *AMS Mathematics Subject Classification:* 20C20, 20C40.

The following theorem shows how all highest weight modules of G can be constructed with p-restricted highest weights.

Theorem 1.1 *Let τ be the Frobenius automorphism, raising elements to their pth power. Twisting the G-action on a G-module M with $\tau^{(i)}$, $i \in \mathbb{Z}_{\geq 0}$, we get another G-module, which we denote by $M^{(i)}$. If λ_i are p-restricted weight, then*

$$M\left(\lambda_0 + p\lambda_1 + \cdots + p^n\lambda_n\right) \cong M\left(\lambda_0\right) \otimes M(\lambda_1)^{(1)} \otimes \cdots \otimes M(\lambda_n)^{(n)}$$

by [10].

In this paper, τ is an operation taking p^eth powers of the entries in the matrices representing the group elements, for some $e < f$. By the above theorem, the tensor products of the modules of the high weights $\lambda_1, \lambda_2, \lambda_{d-2}, \lambda_{d-1}, 2\lambda_1, 2\lambda_{d-1}$ can be given as follows:

1. $V \otimes V^{\tau} \otimes V^{\tau^2}$, tensor products consisting of replaced by duals of one or more factors in $V \otimes V^{\tau} \otimes V^{\tau^2}$, and duals of these products,
2. $V \otimes \left(\Lambda^2(V)\right)^{\tau}$, $V^* \otimes \left(\Lambda^2(V)\right)^{\tau}$, and duals of these products,
3. $V \otimes \left(Sym^2(V)\right)^{\tau}$, $V^* \otimes \left(Sym^2(V)\right)^{\tau}$, and duals of these products.

Suppose that s has an irreducible action on V. Then the eigenvalues of s on $V \otimes F_{q^d}$ are $l_i = w^{q^{i-1}}$ for $1 \leq i \leq d$.

A prime r is a primitive prime divisor of $q^d - 1$ if $r | q^d - 1$ and $r \nmid q^e - 1$ for $1 \leq e < d$ and it is denoted by $\mathrm{ppd}(q;d)$. For more detail, see [8]. Suppose that H is given as $G \leq GL(W)$ where $W = F_q^n$. Assume that $s \in H$, r a $\mathrm{ppd}(q;d)$, and $r \,|\, |s|$. Hence, s is a power of a Singer cycle. Let $\sigma = \delta^f$ be the Frobenius map of $GL\left(d, q^d\right)$ whose fixed points contain H. There exist the eigenspaces $\langle e_i \rangle$ of s such that $e_i^{\sigma} = e_{i+1}$ for all $i \in \{1, 2, ..., d-1\}$ and $e_d^{\sigma} = e_1$. Thus, σ centralizes $\langle s \rangle$ and so σ transitively permutes the eigenspaces of s acting on $V \otimes F_{q^d}$.

We assume that random elements of a finite group G can be constructed with our algorithm. An algorithm outputs an ε-uniformly distributed random element x of G if $(1-\varepsilon)/|G| < \mathrm{Prob}(x = g) < (1+\varepsilon)/|G|$ for all $g \in G$ [13]. In our context, 'nearly uniform' means ε-uniform for some $\varepsilon < 1/2$.

Let ξ be the time required to choose a nearly uniformly random element of G and let ρ_q indicate the cost of a field operation in a finite field F_q.

Our main results are stated in the following theorem:

Theorem 1.2 *Let $q = p^f$ be a prime power and H have the natural module of dimension d. Suppose a set X of $n \times n$ matrices with entries in F_q, and suppose that H is given as $G = \langle X \rangle$ acting irreducibly on a twisted module of dimension $n (d^2 < n \leq d^3)$ of high weights $\lambda_1, \lambda_2, \lambda_{d-2}, \lambda_{d-1}, 2\lambda_1, 2\lambda_{d-1}$. For the inputs G and d, there is a polynomial-time Las Vegas algorithm that, with probability of at least $1-\varepsilon$, sets up a data structure for rewriting G as a d-dimensional projective representation in time $O(\xi d^2 \log q \log \varepsilon^{-1} + \rho_q d^{11} (\log q)^2 \log \varepsilon^{-1} + \rho_{q^d} d^{11} \log q + \rho_{q^d} d^6 \log^2 d \log(dq) \log q \log \varepsilon^{-1})$. The procedure that finds the image of g in a representation of degree d costs $O(\xi + \rho_{q^d} d^9 \log q)$.*

We prove this theorem by giving an algorithm with the stated complexity. Now we give a summary for the recognition algorithm, which constructs a matrix representation of dimension d.

Algorithm 1.

Input: G, which is isomorphic to a classical group H with natural module of dimension d, and W is an irreducible F_qG module of dimension n.

Output: The action of g on a d-dimensional vector space in F_q.

Procedure:

1. Find a random element $s \in G$ that satisfies the following:

   s has n one-dimensional eigenspaces and r divides $|s|$ where r is a $\mathrm{ppd}(q;d)$.

2. Label the eigenvalues of s and find a basis of s-eigenvectors on $W \otimes F_{q^d}$.

3. Compute the vector corresponding to $e_i \otimes e_j \otimes e_k$ from the eigenspace $\langle e_{i,j,k} \rangle$ labeled with (i,j,k).

4. Find the image of $g \in G$ on a d-dimensional vector space.

The output of all steps of the algorithm is the input of the following step. In order to prove this theorem, we consider each of the steps separately. In [11], common steps of the algorithm were given comprehensively. Therefore, we are not interested in these steps. In the last step of our algorithm, we find the image of g, which is a matrix in $GL(d, F_{q^d})$. However, the aim of the final step of our algorithm is to rewrite the output as a $d \times d$ matrix over F_q. In order to determine the base change matrix between the base of V and the base of $V \otimes F_{q^d}$, we use the algorithm of [5], a Las Vegas algorithm that finds the base change matrix.

2. Finding the random element

The first step of the recognition algorithm is common for all representations. We now discuss whether or not a random element $s \in G$ that satisfies Step 1 has order divisible by an r primitive prime divisor of $q^d - 1$. We require a test searching a suitable element $s \in G$ and its eigenvalues over F_{q^d}. The procedure of finding the random element was given in [4]. We will only point out a particular focus. If $(q,d) = (2,6)$, then $m = 21$. If $(q,d) = (p,2)$ with p a Mersenne prime, then $m = p - 1$. Otherwise,

$$m = \prod_{j|d,\ \ j \neq d} \frac{d}{j} \ (q^j - 1).$$

The order of s is the factor of a $\mathrm{ppd}(q;d)$ prime if and only if $s^m \neq 1$. Since the order of s is divisible by the order of an eigenvalue, we decide this by taking the mth power of the eigenvalues of s.

We will now give a lemma identifying a sufficient condition for a suitable random element of H.

Lemma 2.1 *Suppose that W are the tensor products of the modules of the high weights $\lambda_1, \lambda_2, \lambda_{d-2}, \lambda_{d-1}, 2\lambda_1, 2\lambda_{d-1}$ and that the order of $s \in H$ is a multiple of $(q^d - 1)/(q - 1)$. Then s has distinct eigenvalues in F_{q^d}.*

Proof Let $q = p^f$ be a prime power and λ be a primitive element of F_{q^d}. Since s has the order that is a factor of $(q^d - 1)/(q - 1)$, the eigenvalues of s in $V \otimes F_{q^d}$ are $\omega,\ \omega^q, \ldots,\ \omega^{q^{d-1}}$, where $\omega = \lambda^k$ for some divisor k of $q - 1$.

We first consider the case $W = V \otimes \left(Sym^2(V)\right)^{\tau}$. The eigenvalues of s on $W \otimes F_{q^d}$ are $\omega^{q^{i-1}+p^e(q^{j-1}+q^{k-1})}$ for $1 \leq i,j,k \leq d$ and $1 \leq j \leq k \leq d$. If $\omega^{q^{i_1-1}+p^e(q^{j_1-1}+q^{k_1-1})} = \omega^{q^{i_2-1}+p^e(q^{j_2-1}+q^{k_2-1})}$ for some $1 \leq i_1, j_1, k_1, i_2, j_2, k_2 \leq d$ and $1 \leq j_1 \leq k_1 \leq d$, $1 \leq j_2 \leq k_2 \leq d$, then

$$\lambda^{k(q^{i_1-1}+p^e(q^{j_1-1}+q^{k_1-1}))} = \lambda^{k(q^{i_2-1}+p^e(q^{j_2-1}+q^{k_2-1}))}. \tag{1}$$

If any two of $i_1 = i_2$, $j_1 = j_2$, and $k_1 = k_2$ hold, then the other equality holds.

If $i_1 = i_2$, then $\lambda^{kp^e(q^{j_1-1}+q^{k_1-1})} = \lambda^{kp^e(q^{j_2-1}+q^{k_2-1})}$ for $1 \leq j_1 \leq k_1 \leq d$, $1 \leq j_2 \leq k_2 \leq d$. The solution is $j_1 = j_2$, $k_1 = k_2$ [11].

If $k_1 = k_2$, then $\lambda^{k(q^{i_1-1}+p^e q^{j_1-1})} = \lambda^{k(q^{i_2-1}+p^e q^{j_2-1})}$ for $1 \leq i_1, j_1, i_2, j_2 \leq d$ and if $j_1 = j_2$, then $\lambda^{k(q^{i_1-1}+p^e q^{k_1-1})} = \lambda^{k(q^{i_2-1}+p^e q^{k_2-1})}$ for $1 \leq i_1, k_1, i_2, k_2 \leq d$. The only solution is $i_1 = i_2$, $j_1 = j_2$ or $i_1 = i_2$, $k_1 = k_2$ when $d \neq 3$, $q \neq 4$ [11].

If the exponents on both sides of equation (1) are equal, then

$$q^{i_1-1} - q^{i_2-1} = p^e\left(\left(q^{j_2-1} - q^{j_1-1}\right) + \left(q^{k_2-1} - q^{k_1-1}\right)\right).$$

If $k_1 \neq k_2$ and $j_1 \neq j_2$, then the right side of this equation is divisible by p^e and the left side of this equation is divisible by p^f. Thus, the exponents on both sides of the equation are equal to e, $0 \bmod f$, respectively. This is a contradiction. Therefore, $k_1 = k_2$, $j_1 = j_2$ and so $i_1 = i_2$. If the exponents on each side of (1) are less than $q^d - 1$, then both exponents in (1) are at most $k\left(q^{d-1} + p^e q^{d-3} + p^e q^{d-3}\right) < (q-1)(q^{d-1} + q^{d-2} + q^{d-3}) \leq q^d - 1$ for $j_1, j_2 \leq d-2$ and $k_1, k_2 \leq d-2$, so these exponents are equal. There is only one solution $k_1 = k_2$ and $j_1 = j_2$ and $i_1 = i_2$.

If $j_l + t - 1 \leq 2d-2$, $k_l + t - 1 \leq 2d-2$ for $l = 1, 2$, then by taking the q^tth powers of the exponents (1), we obtain q^{i_l+t-1}, q^{j_l+t-1}, q^{k_l+t-1} for $l = 1, 2$. When these exponents are greater than d, the solution of (1) is obtained with $j_l \leq k_l \leq d-2$ for $l = 1, 2$. We have $k_1 + t - 1 \equiv k_2 + t - 1 \pmod d$ and $j_1 + t - 1 \equiv j_2 + t - 1 \pmod d$. Then we get $k_1 = k_2$, $j_1 = j_2$ and so $i_1 = i_2$. If $j_1 \leq k_1 \leq d-1$, then $k(q^{i_1-1} + p^e(q^{j_1-1} + q^{k_1-1}))$ is greater than $q^d - 1$ in case of $k = q-1$, $i_1 = d$, $j_1 \leq k_1 = d-1$; that is to say, $k(q^{i_1-1} + p^e(q^{j_1-1} + q^{k_1-1})) > q^d - 1$ and also $k\left(q^{i_1-1} + p^e\left(q^{j_1-1} + q^{k_1-1}\right)\right) < 2(q^d - 1)$. From both inequalities, we deduce that the only case is

$$(q-1)\left(q^{d-1} + p^e\left(2q^{d-2}\right)\right) = (q-1)\left(q^{i_2-1} + p^e\left(q^{j_2-1} + q^{k_2-1}\right)\right) + q^d - 1.$$

While the left side of the last equation is divisible by p, the other side is divisible by p if and only if $i_2 = 1$ and $p = 2$. Hence, the equation is obtained as

$$2^e\left(2q^{d-2} - q^{j_2-1} - q^{k_2-1}\right) = \left(q^{d-1} + q - 2\right)/(q-1).$$

For $j_2 \leq k_2 \leq d-2$, the left side of the last equation is greater than the other side. This is a contradiction. When $d = 3$, suppose that $k_1 \neq k_2$, $j_1 \neq j_2$, and $i_1 \neq i_2$. Then

$$k\left(q^2 + p^e - 1 - p^e q^2\right) = k\left(q^2 - 1\right)\left(p^e - 1\right)$$

must be a multiple of $q^d - 1$, but it is not divisible by a $\mathrm{ppd}(q;d)$. Therefore, this is a contradiction. Similarly, for $d = 2$, suppose that $k_1 \neq k_2$, $j_1 \neq j_2$, and $i_1 \neq i_2$. Then this implies that

$$k\left(q + 2p^e - 1 - 2qp^e\right) = k\left(q-1\right)\left(1 - 2p^e\right)$$

is a multiple of q^d-1, but it is not divisible by a $\mathrm{ppd}(q;d)$. Therefore, this is a contradiction.

If W is $V\otimes\left(\Lambda^2(V)\right)^\tau$, then the eigenvalues of s on $W\otimes F_{q^d}$ are $\omega^{q^{i-1}+p^e(q^{j-1}+q^{k-1})}$ for $1\leq i,j,k\leq d$ and $1\leq j<k\leq d$. Since its eigenvalues consist of eigenvalues for $V\otimes\left(Sym^2(V)\right)^\tau$, it is applied as above.

When the case is $W=V\otimes V^\tau\otimes V^{\tau^2}$, then the eigenvalues of s on $W\otimes F_{q^d}$ are $\omega^{q^{i-1}+p^eq^{j-1}+p^{2e}q^{k-1}}$ for $1\leq i,j,k\leq d$. Since it is shown that its eigenvalues are distinct in a way similar to $V\otimes\left(Sym^2(V)\right)^\tau$, we will not give its proof.

If W is $V^*\otimes\left(Sym^2(V)\right)^\tau$, then the eigenvalues of s on $W\otimes F_{q^d}$ are $\omega^{-q^{i-1}+p^e(q^{j-1}+q^{k-1})}$ for $1\leq i,j,k\leq d$ and $1\leq j\leq k\leq d$. If $\omega^{-q^{i_1-1}+p^e(q^{j_1-1}+q^{k_1-1})}=\omega^{-q^{i_2-1}+p^e(q^{j_2-1}+q^{k_2-1})}$ for some $1\leq i_1,j_1,k_1,i_2,j_2,k_2\leq d$ and $1\leq j_1\leq k_1\leq d, 1\leq j_2\leq k_2\leq d$, then

$$\lambda^{k(q^{i_2-1}+p^e(q^{j_1-1}+q^{k_1-1}))}=\lambda^{k(q^{i_1-1}+p^e(q^{j_2-1}+q^{k_2-1}))}.$$

As before, the only solution is $i_1=i_2$, $j_1=j_2$, and $k_1=k_2$. Similarly, if W is $V^*\otimes\left(\Lambda^2(V)\right)^\tau$, then the eigenvalues of s on $W\otimes F_{q^d}$ are $\omega^{-q^{i-1}+p^e(q^{j-1}+q^{k-1})}$ for $1\leq i,j,k\leq d$ and $1\leq j<k\leq d$. If $\omega^{-q^{i_1-1}+p^e(q^{j_1-1}+q^{k_1-1})}=\omega^{-q^{i_2-1}+p^e(q^{j_2-1}+q^{k_2-1})}$ for some $1\leq i_1,j_1,k_1,i_2,j_2,k_2\leq d$ and $1\leq j_1<k_1\leq d, 1\leq j_2<k_2\leq d$, then $\lambda^{k(q^{i_2-1}+p^e(q^{j_1-1}+q^{k_1-1}))}=\lambda^{k(q^{i_1-1}+p^e(q^{j_2-1}+q^{k_2-1}))}$. As before, the only solution is $i_1=i_2$, $j_1=j_2$, and $k_1=k_2$. Besides, it is shown that their eigenvalues are distinct when the cases are tensor products consisting of replaced by duals of one or more factors of $W=V\otimes V^\tau\otimes V^{\tau^2}$. □

In [4, 11], the authors showed that there is an element $s\in G$ that satisfies the steps of the following Las Vegas algorithm.

Algorithm 2.

Input: G, which is isomorphic to a classical group H with natural module of dimension d.

Output: $s\in G$ and its eigenvalues over F_{q^d}.

Procedure:

1. Set $T:=\lceil 2/P\log\varepsilon^{-1}\rceil$, where P is given as the proportion of random elements in G with $\frac{1}{P}<3d^2\log q$ and T is the upper bound of random elements of G.
2. Compute the characteristic polynomial $c(x)$ of a random element $s\in G$, and find the square-free factorization of $c(x)$, the distinct-degree factorization of $c(x)$.
3. Compute the distinct linear factors of $c(x)$ over F_{q^d} and the eigenvalues of s over F_{q^d}. For a zero $\beta\in F_{q^d}$ of one of the irreducible divisors of $c(x)$ largest degree, compute β^m. If the value of β^m is 1 or if the computation of linear factors returns FAIL, then discard s and return 2.
4. Return s and its eigenvalues over F_{q^d}.

Our procedure determining a random element is the same as the procedures performed in recent papers [4, 11]. We obtain the required time for the procedure determining a random element in our representations by the following lemma.

Lemma 2.2 *Let W be an irreducible F_qG-module dimension of $n(d^2 < n \leq d^3)$. There is a Las Vegas algorithm that, with probability $1-\varepsilon$, finds $s \in G$ such that s is a $ppd(q;d)$ one-dimensional eigenspace of its eigenvalues. Algorithm 2 has complexity*

$$O((\xi + \rho_q d^9 + \rho_q d^3 \log q \ + \rho_{q^d} \ d^4 \log^2 d \ \log(dq) \ ) \ \frac{1}{P} \log \varepsilon^{-1}),$$

where P is the proportion of random elements in G. Then the complexity is $O((\xi + \rho_q d^9 + \rho_q d^3 \log q \ + \rho_{q^d} \ d^4 \log^2 d \ \log(dq) \ ) d^2 \log q \log \varepsilon^{-1})$ [6].

3. Labeling the eigenvalues l_{ijk}

Assume that $G \leq GL(W)$ where W is an irreducible F_qG-module W of dimension n. In the previous section, the element $s \in G$ providing conditions in the first step of the recognition algorithm was found. We now perform steps 2 and 3 of the recognition algorithm in this section. As before, the eigenvalues of s on $V \otimes F_{q^d}$ are $l_i = w^{q^{i-1}}$ for $1 \leq i \leq d$ and its eigenspaces on W are $\langle e_{i,j,k} \rangle$ for $1 \leq i,j,k \leq d$. Sets of eigenvalues of s on W such that $W = V \otimes V^{\tau} \otimes V^{\tau^2}$, $W = V \otimes \left(\Lambda^2(V)\right)^{\tau}$, and $W = V \otimes \left(Sym^2(V)\right)^{\tau}$ are denoted as follows, respectively,

$$\left\{ l_{i,j,k} := l_i \, (l_j)^{p^e} \, (l_k)^{p^{2e}} : 1 \leq i,j,k \leq d \right\},$$

$$\left\{ l_{i,j,k} := l_i \, (l_j)^{p^e} \, (l_k)^{p^e} : 1 \leq i,j,k \leq d, \ j < k \right\},$$

$$\left\{ l_{i,j,k} := l_i \, (l_j)^{p^e} \, (l_k)^{p^e} : 1 \leq i,j,k \leq d, \ j \leq k \right\}.$$

The remaining modules of dimension between d^2 and d^3 are the products that consist of replaced by duals of one or more factors of above products. We choose a basis of $F_W = \{f_{i,j,k}\}$, $f_{i,j,k} \in \langle e_{i,j,k} \rangle$ by using the following algorithm.

Algorithm 3.

Input: Random element s and eigenvalues of s on W.

Output: Labeling the eigenvalues l_{ijk} and the basis $F_W = \{f_{ijk}\}$.

Procedure:

1. Construct the orbits of eigenvalues under the Frobenius map σ and compute their qth powers.
2. Perform suitable labeling of the eigenvalues l_{1jk} and for $2 \leq i,j,k \leq d$, $l_{ijk} = l^q_{i-1,j-1,k-1}$.
3. Take $l_{1jk} \in \Omega$ for each orbit Ω of eigenvalues and choose the vector $f_{1,j,k} \in \langle e_{1,j,k} \rangle$ whose first nonzero coordinate is equal to 1.
4. Compute $f_{i+r,j+r,k+r} = f^{\sigma^r}_{i,j,k}$ for other $l^{\sigma^r}_{i,j,k} \in \Omega$.

Lemma 3.1 *Let $l_i = w^{q^{i-1}}$, for $1 \leq i \leq d$, be eigenvalues of s on $V \otimes F_{q^d}$ and let W be the irreducible FG-modules corresponding with tensor products of high weights $\lambda_1, \lambda_{d-1}, \lambda_2, \lambda_{d-2}, 2\lambda_1, 2\lambda_{d-1}$. There are suitable labelings $l_{i,j,k}$ of the eigenvalues of s on W with a basis $F_W = \{f_{i,j,k}\}$. The cost of this labeling procedure is $O\left(\rho_{q^d}\left(d^{11} + d^9 \log q\right)\right)$ where ρ_{q^d} is the cost of a field operation in F_{q^d}.*

Proof Let W be the irreducible FG-modules corresponding with high weights $\lambda_1, \lambda_{d-1}, \lambda_2, \lambda_{d-2}, 2\lambda_1, 2\lambda_{d-1}$. We perform suitable labelings $l_{i,j,k}$ of the eigenvalues of s on W as follows. Let $W = V \otimes V^{\tau} \otimes V^{\tau^2}$ and let $q = p^f$ be a prime power. We know the set for the eigenvalues of s in its action on W by

$$\left\{ l_{i,j,k} := l_i \left(l_j\right)^{p^e} \left(l_k\right)^{p^{2e}} : 1 \leq i,j,k \leq d \right\}.$$

Its eigenspaces on W are $\langle e_{i,j,k} = e_i \otimes e_j \otimes e_k \rangle$, for $1 \leq i,j,k \leq d$. First, we choose one of these orbits and take an entry α from this orbit as $l_1 l_1 l_1$. If there exists an eigenvalue w where $w^{1+p^e+p^{2e}} = \alpha^{1+qp^e+qp^{2e}}$ and if $\alpha^{q+1} w^{-1}$ is an eigenvalue, then we identify $l_{1,2,2}$ as w and $\alpha^{q+1} w^{-1}$ as $l_{2,1,1}$. Otherwise, we choose a new orbit.

We perform the labeling of the eigenvalues $l_{i,j,k}$ as follows:

For $k \in \{2,3,\ldots,d\}$, $l_{k,k,k} = l^q_{k-1,k-1,k-1}$, for $k \in \{2,3,\ldots,d-1\}$, $l_{k,k+1,k+1} = l^q_{k-1,k,k}$ and $l_{d,1,1} = l^q_{d-1,d,d}$.

For $k \in \{2,3,\ldots,d-1\}$, $l_{k+1,1,1} = l_{1,1,1} l_{k,k,k} l_{k+1,k+1,k+1} / l_{1,k,k} l_{k,k+1,k+1}$ and $l_{1,k+1,k+1} = l_{1,1,1} l_{k+1,k+1,k+1} / l_{k+1,1,1}$.

For $k \in \{1,2,\ldots,d-1\}$, $l_{k+1,k+1,1} = l_{1,1,1} l_{k,k,k} l_{k+1,k+1,k+1} / l_{1,1,k} l_{k,k,k+1}$ and $l_{1,1,k+1} = l_{1,1,1} l_{k+1,k+1,k+1} / l_{k+1,k+1,1}$.

We label $l_{1,2,1} = l_{1,1,1} l_{1,2,2} / l_{1,1,2}$, $l_{2,1,2} = l_{1,1,1} l_{2,2,2} / l_{1,2,1}$. For $k \in \{2,3,\ldots,d-1\}$,

$$l_{k,k+1,k} = l^q_{k-1,k,k-1}, l_{d,1,d} = l^q_{d-1,d,d-1},$$

$$l_{k+1,1,k+1} = l_{1,1,k+1} l_{k+1,k+1,k+1} / l_{1,k+1,k+1}$$

$$l_{1,k+1,1} = l_{1,1,1} l_{k+1,k+1,k+1} / l_{k+1,1,k+1}.$$

We label for $(i,j,k) \to (1,2,3)$, $l_{1,2,3} = {l_{1,2,2}}^{q+1} / {l_{1,2,1}}^{q}$. For $k \in \{2,3,\ldots,d-2\}$, we determine

$$l_{k,k+1,k+2} = l^q_{k-1,k,k+1}, l_{d-1,d,1} = l^q_{d-2,d-1,d},$$

and for $k \in \{2,3,\ldots,d-1\}$,

$$l_{k,k+1,1} = l_{1,1,1} l_{k+1,k+1,k+1} l_{k,k,k} / l_{1,k,k} l_{k+1,1,k+1},$$

$$l_{1,k,k+1} = l_{1,k+1,k+1} l_{k,k,k} / l_{k,k+1,k}.$$

Also, $(1,k+1,k)$, $(k,1,k+1)$, $(k+1,1,k)$, $(k+1,k,1)$ triples are determined by the same way.

For $r \in \{2,3,\ldots,d-k\}$, we label $l_{1,k,k+r} = l^{q+1}_{1,k,k+r-1} / l^q_{1,k,k+r-2}$ and other triples. Other values of $l_{k,l,m}$ are determined by taking qth powers of labeled elements of orbits.

Now we consider the case $W = V \otimes \left(\Lambda^2(V)\right)^{\tau}$. We know the set for the eigenvalues of s in its action on W by

$$\left\{ l_{i,j,k} := l_i \left(l_j\right)^{p^e} \left(l_k\right)^{p^e} : 1 \leq i,j,k \leq d,\ j < k \right\}.$$

Its eigenspaces on W are $\langle e_{i,j,k} = e_i \otimes e_j \otimes e_k \rangle$, for $1 \leq i,j,k \leq d$ and $j < k$. We choose one of these orbits and take an entry α from this orbit as $l_1 l_1 l_2$. If there exists an eigenvalue w where $w^{1+p^e+qp^e} = \alpha^{1+p^e+q^2p^e}$, then we identify $l_{1,1,3}$ as w. Otherwise, we choose a new orbit.

We perform the labeling of the eigenvalues $l_{i,j,k}$ as follows:

For $k \in \{4,5,\ldots,d\}$, $l_{1,1,k} = \frac{l^{q+1}_{1,1,k-1}}{l^{q}_{1,1,k-2}}$ and then $l^{q}_{1,1,d} = l_{2,1,2}$, $l_{123} = \frac{l^{q+1}_{112}}{l_{212}}$, $l_{124} = \frac{l_{123}l_{224}}{l_{223}}$ and $l_{313} = \frac{l_{113}l^{q}_{212}}{l_{123}}$.

For $k \in \{4,5,\ldots,d\}$, $l_{k,1,k} = \frac{l^{q+1}_{k-1,1,k-1}}{l^{q}_{k-2,1,k-2}}$.

For $k \in \{3,4,\ldots,d\}$ and $r \in \{1,2,\ldots,d-k\}$, $l_{k,1,k+r} = \frac{l^{q+1}_{k-1,1,k+r-1}}{l^{q}_{k-2,1,k+r-2}}$ and $l_{k+r,1,k} = \frac{l^{q+1}_{k+r-1,1,k-1}}{l^{q}_{k+r-2,1,k-2}}$.

For $k \in \{5,6,\ldots,d\}$, $l_{1,2,k} = \frac{l^{q+1}_{1,2,k-1}}{l^{q}_{1,2,k-2}}$.

For $k \in \{3,4,\ldots,d\}$, $l_{2,1,k} = \frac{l^{q+1}_{2,1,k-1}}{l^{q}_{2,1,k-2}}$ and $l_{k,1,2} = \frac{l^{q+1}_{k-1,1,2}}{l^{q}_{k-2,1,2}}$.

For $k \in \{3,4,\ldots,d\}$ and $r \in \{1,2,\ldots,d-k\}$, $l_{1,k,k+r} = \frac{l^{q+1}_{1,k-1,k+r-1}}{l^{q}_{1,k-2,k+r-2}}$.

Other values of $l_{k,l,m}$ are determined by taking qth powers of labeled elements of orbits.

Finally, we consider the case $W = V \otimes \left(Sym^2(V)\right)^{\tau}$. We know the set for the eigenvalues of s in its action on W by

$$\left\{ l_{i,j,k} := l_i \left(l_j\right)^{p^e} \left(l_k\right)^{p^e} : 1 \le i,j,k \le d,\ j \le k \right\}.$$

Its eigenspaces on W are $\langle e_{i,j,k} = e_i \otimes e_j \otimes e_k \rangle$, for $1 \le i,j,k \le d$ and $j \le k$.

We choose one of these orbits and take an entry α from this orbit as $l_1 l_1 l_1$. If there exists an eigenvalue w where $w^{1+2p^e} = \alpha^{1+p^e+qp^e}$, then we identify $l_{1,1,2}$ as w. Otherwise, we choose a new orbit. We perform the labeling of the eigenvalues $l_{i,j,k}$ as follows:

For $k \in \{3,4,\ldots,d\}$, $l_{1,1,k} = \frac{l^{q+1}_{1,1,k-1}}{l^{q}_{1,1,k-2}}$ then $l^{q}_{1,1,d} = l_{2,1,2}$, $l_{211} = \frac{l_{212}l_{111}}{l_{112}}$, $l_{122} = \frac{l^{q+1}_{111}}{l_{211}}$, $l_{123} = \frac{l^{q+1}_{112}}{l_{212}}$, $l_{124} = \frac{l_{123}l_{224}}{l_{223}}$ and $l_{313} = \frac{l_{113}l^{q}_{212}}{l_{123}}$, $l_{k,1,1} = \frac{l^{q+1}_{k-1,1,1}}{l^{q}_{k-2,1,1}}$.

For $k \in \{4,5,\ldots,d\}$, $l_{k,1,k} = \frac{l^{q+1}_{k-1,1,k-1}}{l^{q}_{k-2,1,k-2}}$.

For $k \in \{3,4,\ldots,d\}$ and $r \in \{1,2,\ldots,d-k\}$, $l_{k,1,k+r} = \frac{l^{q+1}_{k-1,1,k+r-1}}{l^{q}_{k-2,1,k+r-2}}$ and $l_{k+r,1,k} = \frac{l^{q+1}_{k+r-1,1,k-1}}{l^{q}_{k+r-2,1,k-2}}$.

For $k \in \{5,6,\ldots,d\}$, $l_{1,2,k} = \frac{l^{q+1}_{1,2,k-1}}{l^{q}_{1,2,k-2}}$.

For $k \in \{3,4,\ldots,d\}$, $l_{2,1,k} = \frac{l^{q+1}_{2,1,k-1}}{l^{q}_{2,1,k-2}}$ and $l_{k,1,2} = \frac{l^{q+1}_{k-1,1,2}}{l^{q}_{k-2,1,2}}$.

For $k \in \{3,4,\ldots,d\}$, $l_{1,k,k} = \frac{l^{q+1}_{1,k-1,k-1}}{l^{q}_{1,k-2,k-2}}$.

For $k \in \{3,4,\ldots,d\}$ and $r \in \{1,2,\ldots,d-k\}$, we determine $l_{1,k,k+r} = \frac{l^{q+1}_{1,k-1,k+r-1}}{l^{q}_{1,k-2,k+r-2}}$.

Other values of $l_{k,l,m}$ are determined by taking qth powers of labeled elements of orbits.

The labelings for probable modules consisting of their duals instead of one or more factors are identical with the cases given above. Therefore, we do not restate their proofs.

In Algorithm 3, step 1 costs $O(d^3)$ qth power, a cost of $O(\rho_{q^d} \log q\ )$ for each, and thus the set up of this data structure has complexity $O(\rho_{q^d} d^3 \log q\ )$. In step 3, we compute d^2 eigenvectors at a cost $O(\rho_{q^d} d^9)$ of

each, and then step 3 has complexity $O(\rho_{q^d} d^{11})$. Step 4 costs $O(\rho_{q^d} d^9 \log q\ )$. The total time of this procedure is $O\left(\rho_{q^d}(d^{11} + d^9 \log q\ )\right)$. □

Since we can assume that the first coordinate of each e_i is 1, the vector $f_{i,j,k}$ corresponds precisely to $e_i \otimes e_j \otimes e_k$, and so it does not need a scalar multiple [11].

We use the algorithm of [5] to perform the final base change. This algorithm is a Las Vegas algorithm that determines the base change matrix with complexity $O\left(\rho_{q^d} |X| d^3\right) + O^{\sim}(\rho_q d \log q)$. Its procedure is fast and hence it has no effect on the complexity of Algorithm 3.

4. Finding images

It only remains to determine the image of an arbitrary $g \in G$. We compute $K = (\kappa_{ijk,lmn})$, the matrix of g in the basis F_W. Let $A = (a_{ij})$ be the matrix of g in the basis $\{e_1, e_2, \ldots, e_d\}$. The a_{ij} is computed since we know $K = (\kappa_{ijk,lmn})$. Finally, g is rewritten in the basis ß $= \{b_1, b_2, \ldots, b_d\}$ for the natural module V.

Lemma 4.1 *Let $K = (\kappa_{ijk,lmn})$ be the matrix representation defined with the action of g on W with respect to the basis $F_W = \{f_{i,j,k}\}$. The matrix a_{ij} of g is determined with the cost $O\left(\xi + \rho_{q^d}\left(d^9 + d^2 \log q\ \right)\right)$ where ξ is the required cost to choose a random element of G, and ρ_{q^d} is the cost of a field operation in F_{q^d}.*

Proof If W is $V \otimes V^{\tau} \otimes V^{\tau^2}$, then the basic equation for $\kappa_{ijk,lmn}$ with all $1 \leq i,\ j,\ k,\ l,\ m,\ n \leq d$ is

$$\kappa_{ijk,lmn} = a_{il}(a_{jm})^{p^e}(a_{kn})^{p^{2e}}.$$

If W is $V \otimes \left(\Lambda^2(V)\right)^{\tau}$, then the basic equation for $\kappa_{ijk,lmn}$ with $j < k$ and $m < n$ is

$$\kappa_{ijk,lmn} = a_{il}(a_{jm})^{p^e}(a_{kn})^{p^e}.$$

If W is $V \otimes \left(Sym^2(V)\right)^{\tau}$, then the basic equation for $\kappa_{ijk,lmn}$ with $j \leq k$ and $m \leq n$ is

$$\kappa_{ijk,lmn} = a_{il}(a_{jm})^{p^e}(a_{kn})^{p^e}.$$

We choose an arbitrary nonzero entry $\kappa_{i_0 j_0 k_0, l_0 m_0 n_0}$ in F_{q^d}. The matrices with (i,l) entry

$$\kappa_{ij_0k_0,lm_0n_0} = a_{il}(a_{j_0m_0})^{p^e}(a_{k_0n_0})^{p^{2e}},\ \kappa_{ij_0k_0,lm_0n_0} = a_{il}(a_{j_0m_0})^{p^e}(a_{k_0n_0})^{p^e}$$

$\kappa_{ij_0k_0,lm_0n_0} = a_{il}(a_{j_0m_0})^{p^e}(a_{k_0n_0})^{p^e}$ are images of g. When one or more factors replace with their duals, finding the image of g is similar to the cases given above. Let $A^* = \left(a^*_{ij}\right)$ be the matrix of $\varphi(g)$ in the basis $\{e_1, e_2, \ldots, e_d\}$ for a graph automorphism φ. Here we give only one of these cases when $W = V^* \otimes V^{\tau} \otimes V^{\tau^2}$. The basic equation for $\kappa_{ijk,lmn}$ is

$$\kappa_{ijk,lmn} = a^*_{il}(a_{jm})^{p^e}(a_{kn})^{p^{2e}}.$$

We choose an arbitrary nonzero entry $\kappa_{i_0 j_0 k_0, l_0 m_0 n_0}$ in F_{q^d}. The matrix with (i,l) entry $\kappa_{ij_0k_0,lm_0n_0} = a^*_{il}(a_{j_0m_0})^{p^e}(a_{k_0n_0})^{p^{2e}}$ is an image of g. For computing $K = (\kappa_{ijk,lmn})$, the matrix representation, the cost requires $O(\rho_{q^d} n^3) = O(\rho_{q^d} d^9)$. Of the remaining part of the procedure, the most expensive is to take the qth power of a_{ij}. The time required for it is $O(\rho_{q^d} d^2 \log q\ )$. The procedure has complexity $O\left(\xi + \rho_{q^d}\left(d^9 + d^2 \log q\ \right)\right)$. □

References

[1] Beals R, Leedham-Green C, Niemeyer A, Praeger C, Seress A. A black-box group algorithm for recognizing finite symmetric and alternating groups I. T Am Math Soc 2003; 355: 2097–2113.

[2] Beals R, Leedham-Green C, Niemeyer A, Praeger C, Seress A. Constructive recognition of finite alternating and symmetric groups acting as matrix groups on their natural permutation modules. J Algebra 2005; 292: 4–46.

[3] Brooksbank PA. Constructive recognition of classical groups in their natural representation. J Symb Comput 2003; 35: 195–239.

[4] Corr BP. Estimation and computation with matrices over finite fields. PhD, University of Western Australia, Crawley, Australia, 2014.

[5] Glasby SP, Leedham-Green CR, O'Brien EA. Writing projective representations over subfields. J Algebra 2006; 295: 51–61.

[6] Gül K, Çağman A, Ankaralıoğlu N. An algorithm for projective representations of some matrix groups. Life Science Journal 2014; 11: 1005–1009.

[7] Kantor WM, Seress Á. Black box classical groups. Mem Am Math Soc 2001; 708: 149.

[8] Kleidman P, Liebeck M. The Subgroup Structure of the Finite Classical Groups. New York, NY, USA: Cambridge University Press, 1990.

[9] Leedham-Green CR, O'Brien EA. Constructive recognition of classical groups in odd characteristic. J Algebra 2009; 322: 833–881.

[10] Lübeck F. Small degree representations of finite Chevalley groups in defining characteristic. Lond Math S 2003; 4: 135–169.

[11] Magaard K, O'Brien EA, Seress Á. Recognition of small dimensional representations of general linear groups. J Aust Math Soc 2008; 85: 229–250.

[12] O'Brien EA. Towards effective algorithms for linear groups. In: Hulpke A, Penttila T, Liebler R, Seress Á, editors. Finite Geometries, Groups and Computation: Proceedings. Berlin, Germany: De Gruyter, pp. 163–190.

[13] Seress Á. Permutation Group Algorithms. Cambridge, MA, USA: Cambridge University Press, 2003.