An Algorithm for Projective Representations of some Matrix Groups

Kübra GÜL[1], Abdullah ÇAĞMAN[2], Nurullah ANKARALIOĞLU[1]

[1]Mathematics Department, Faculty of Science, Ataturk University, 25240, Erzurum, Turkey
[2]Mathematics Department, Faculty of Science and Letters, Agri Ibrahim Cecen University, 04100, Ağrı, Turkey
kubra.gul@atauni.edu.tr, acagman@agri.edu.tr, ankarali@atauni.edu.tr

Abstract: We describe an algorithm which takes as an input W to construct a projective representation of G of dimension d, where G is isomorphic to a group H satisfying $SL(d,q) \leq H \leq GL(d,q)$ and W is irreducible F_qG-module of dimension between d^2 and d^3.
[Gül K, Çağman A, Ankaralıoğlu N. **An Algorithm for Projective Representations of some Matrix Groups.** *Life Sci J* 2014;11(10):1005-1009]. (ISSN:1097-8135). http://www.lifesciencesite.com. 154

Keywords: Matrix group, irreducible representation, FG-module, projective representation.

1. Introduction

One of the research topic in recent years is the development of the algorithms to construct an isomorphism between the natural representation and an arbitrary representation of a classical group.

In Kantor and Seress (2001), they present an algorithm that, given as input an arbitrary permutation or matrix representation G of an almost simple classical group H of Lie type of known characteristic, constructs an isomorphism between G and the natural projective representation of H.

Magaard et al. (2008) provide efficient algorithms to construct such an isomorphism for a projective matrix representation of degree at most d^2 of the general lineer groups having natural module of dimension d.

In this paper, we present an algorithm dealing with irreducible representations $\Gamma_{1,1,0,\dots}$, $\Gamma_{0,1,0,\dots,0,1}$ and $\Gamma_{2,0,\dots,0,1}$ dimension of n ($d^2 \leq n \leq d^3$).

An effective algorithm in Beals et al. (2003) is given for representations of A_n and S_n, and in Beals et al. (2005) a specialised algorithm does the same for the small degree case.

Babai, (1991) presents a black-box Monte Carlo algorithm that produces nearly uniformly distributed random elements of G. Also the product replacement algorithm produces random elements in a matrix group. For a general discussion of the product replacement algorithm you can see Pak (2000). We use the notation of Seress (2003) in our algorithm to construct random elements of a finite group G.

2. Background and Main Results

Let $SL(d,q) \leq H \leq GL(d,q)$ with $q = p^f$. Suppose that H has the natural module V. Let W be an irreducible F_qG-module of dimension between d^2 and d^3 and H acts on W.

We now briefly give some informations about irreducible representations of dimension between d^2 and d^3.

The irreducible representation appears as a subspace of

$Sym^{a_1}V \otimes Sym^{a_2}(\Lambda^2(V)) \otimes \dots \otimes Sym^{a_{d-1}}(\Lambda^{d-1}(V))$

or equivalently as a subspace of the d-th tensor power $V^{\otimes d}$ of V.

The general irreducible representation $\Gamma_{a_1,\dots,a_{d-1}}$ with highest weight

$$(a_1 + \dots + a_{d-1})L_1 + (a_2 + \dots + a_{d-1})L_2 + \dots + a_{d-1}L_{d-1}$$

occurs in the tensor product of symmetric powers

$$Sym^{a_1}V \otimes \dots \otimes Sym^{a_{d-1}}\Lambda^{d-1}(V) \to Sym^{a_1-1}V \otimes \dots \otimes Sym^{a_{d-1}-1}\Lambda^{d-1}(V).$$

Irreducible representations of dimension between d^2 and d^3 can be obtained as follows.

i. $\Gamma_{1,1,0,\dots}$ is the irreducible representation with highest weight $2L_1 + L_2$ and its dimension $d(d-1)(d+1)/3$,

ii. $\Gamma_{0,1,0,\dots,0,1}$ is the irreducible representation with highest weight $L_2 + L_{d-1}$ and its dimension $d(d-2)(d+1)/2$,

iii. $\Gamma_{2,0,\dots,0,1}$ is the irreducible representation with highest weight $2L_1 + L_{d-1}$ and its dimension $d(d+2)(d-1)/2$,

iv. $Sym^3V = \Gamma_{3,0,\dots,0}$ and $\Lambda^3V = \Gamma_{0,0,1,0,\dots,0}$ are the irreducible representations with highest weights $3L_1$ and $L_1 + L_2 + L_3$ and their dimensions $(d+2)(d+1)d/6$ and $d(d-1)(d-2)/6$ respectively.

For further details about such irreducible representations look Fulton and Harris (1999).

In this paper, we consider $\Gamma_{1,1,0,\dots}$, $\Gamma_{0,1,0,\dots,0,1}$ and $\Gamma_{2,0,\dots,0,1}$ irreducible representations.

We will use an algorithm to find random elements in black-box groups. The algorithm outputs an ε-uniformly distributed random element x of G if

$(1-\varepsilon)/|G| < \text{Prob}\ (x=g) < (1+\varepsilon)/|G|$ for all $g \in G$. 'Nearly uniform' means ε-uniform for some $\varepsilon < 1/2$ (Seress, 2003).

Let ξ_G be the cost of choosing a random element of G and let ρ_q be the cost of a field operation in a finite field F_q. In Magaard et al. (2008, Lemma 4.1), they set up a Las Vegas algorithm which constructs F_{q^d}, in $O(\rho_q d^3 \log^2 d \log q)$ time.

Let G is isomorphic to H. Assume that $s \in H$, r is a ppd$(q;d)$ and that $r \mid |s|$. Therefore, s is a power of a singer cycle and there are d one-dimensional eigenspaces in $V \otimes F_q^d$. Let $\sigma = \delta^f$ be the Frobenius map of $GL(d,q^d)$ whose fixed points contain H. Thus, σ centralizes $\langle s \rangle$ and σ transitively permutes the eigenspaces of s acting on $V \otimes F_{q^d}$.

As a result, we can list the eigenspaces $\langle e_i \rangle$ of s and choose the eigenvectors e_i within the eigenspaces in such a way that $e_i^\sigma = e_{i+1}$ where the index is computed modulo d.

Our main results are stated in the following theorem:

Theorem 2.1. Let $q = p^f$ be a prime power and V be the natural module of H. Suppose that H is given as $G = \langle X \rangle$ acting irreducibly on W. For the input G and d, there is a polynomial-time Las Vegas algorithm which, with probability at least $1-\epsilon$, sets up a data structure for rewriting G as a d-dimensional projective representation in time

$$O\big(\xi_G \log d^2 \log q \log \epsilon^{-1} + \rho_q d^9 \log d^2 \log^2 q \log \epsilon^{-1} + \rho_{q^d}\ d^4 \log^2 d \log(dq) \log d^2 \log q \log \epsilon^{-1} + \rho_{q^d} d^{11} \log q\big).$$

The procedure which finds the image of g in a representation of degree d costs $O((\xi_G + \rho_{q^d} d^9 \log q) \log \epsilon^{-1})$.

Algorithm 2.2. Here we give a summary for recognition algorithm which construct a matrix representation dimension of d.

i. Find a random element $s \in G$ which satisfies the following:

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

iii. Label the eigenvalues and produce F_W, a basis of s-eigenvectors on $W \otimes F_{q^d}$.

iv. Compute the vector corresponding to $e_i \otimes e_j \otimes e_k$ from the eigenspace labelled with (i,j,k).

v. The data structure described in Theorem 2.1 consists of steps 1 to 3 and the image of $g \in G$ is obtained with the following step.

vi. First write g in the basis F_w; then compute the action of g on $V \otimes F_{q^d}$ in the basis $\mathfrak{E} = \{e_1, e_2, \dots, e_d\}$; finally rewrite with respect to the basis $\beta = \{b_1, b_2, \dots, b_d\}$ for the natural module V.

3. Finding the special element

Step 1 is common for all representations, so we discuss it in this section.

We now consider whether or not a random element $s \in G$ with conditions given in Step 1 has order divisible by a r primitive prime divisor of $q^d - 1$. We know that if $(q,d) = (2,6)$, then define $m := 21$. If $(q,d) = (p,2)$ with p a Mersenne prime, then define $m := p-1$. Otherwise

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

Order of s is the factor of a ppd$(q;d)$ prime if and only if $s^m \neq 1$. Then, we say that we can decide this by taking mth powers of s-eigenvalues.

As given in Step 1 of Algorithm 2.2, with probability at least $1-\epsilon$, there is an element $g \in G$ which satisfies the following:

Set $T := \left\lceil \frac{2}{P} \log(\epsilon^{-1}) \right\rceil$, where P is given as the proportion of special elements in G. T is upper bound of random elements of G. Compute

i. the characteristic polynomial $c(x)$ of a random element $g \in G$,

ii. the square-free factorisation of $c(x)$,

iii. the distinct-degree factorisation of $c(x)$,

iv. the distinct linear factors of $c(x)$ over F_{q^d},

hence, compute the eigenvalues of g over F_{q^d}. For a zero $s \in F_{q^d}$ of one of the irreducible divisors of $c(x)$ largest degree, compute s^m. If the value is 1 or if the computation of linear factors returns FAIL, then discard g and return computing $c(x)$. Return g and its eigenvalues over F_{q^d} (Corr, 2014).

Lemma 3.1: There is a Las Vegas algorithm which finds a suitable $g \in G$ in

$$O((\xi_G + \rho_q d^9 + \rho_q d^3 \log q + \rho_{q^d}\ d^4 \log^2 d \log(dq)) \log d^2 \log q \log \epsilon^{-1})$$

time.

Proof: We have the bound $P > \frac{1}{3d^2 \log q}$ (proportion of special elements in G) and we obtain $\frac{2}{P} < 6d^2 \log q$. The characteristic polynomial $c(x)$ of g is computed by using the algorithm of Dumas et al. (2005) in $O(\xi_H + \rho_q d^9)$ time. Step (ii) costs $O(\rho_q d^3 \log q)$ and (iii) runs faster than (ii). The distinct linear factors of $c(x)$ in F_{q^d} are obtained using a Las Vegas algorithm of Beals et al. (2005) in

$$O\big(\rho_{q^d} n \log n \log(nq^d) \log\log n \log \epsilon^{-1}\big) = O\big(\rho_{q^d} d^4 \log^2 d \log(dq) \log \epsilon^{-1}\big)$$

time. Taking mth powers of the eigenvalues of s requires $O\big(\rho_{q^d}\, \mathrm{d}^{3/2} \log q\big)$ time. And then the Las

Vegas algorithm for finding special element has complexity

$$O\big((\xi_G + \rho_q d^9 + \rho_q d^3 \log q + \rho_{q^d}\ d^4 \log^2 d \log(dq))\, d^2\ \log q \log \epsilon^{-1}\big).$$

In the last step of our algorithm, we find the image of g which is a matrix in $GL(d, F_{q^d})$. Hovever, aim of the final stage of our algorithm is to rewrite the output as a $d \times d$ matrix over F. How to be done this is showed in Magaard et al. (2008, Lemma 4.6).

Lemma 3.2: Let $h \in H$ and let $A = (a_{ij})$ be the matrix of h in the basis $\mathfrak{E}$. For $i, j \in \{1, \dots, d\}$,

$$a_{i+1,j+1} = a_{ij}^q$$

where the index $d+1$ is interpreted as 1 (Magaard et al., 2008, Lemma 4.7).

Lemma 3.3: Let $h \in H$ and let $A = (a_{ij})$ be the matrix of h in the basis $\mathfrak{E}$.

i. For $i, j \in \{1, \dots, d\}$, $\mathrm{Prob}(a_{ij} = 0) < 4/q^d$. If $q \geq 3$ then $\mathrm{Prob}(a_{ij} = 0) < 2/q^d$.

ii. Prob(all $a_{ij} \neq 0) > 5/8$

For proof, see Magaard et al. (2008, Lemma 4.8).

One of the common steps is also **avoiding division by zero**. For details about this, see Magaard et al. (2008)

4. Labelling the Eigenvalues l_{ijk}

In this section, we aim to produce a suitable labelling of orbits of eigenvalues under the Frobenius map σ and to find a basis for W of s-eigenvectors. Let $l_i = w^{q^{i-1}}$, for $1 \leq i \leq d$, be s- eigenvalues in its action on $V \otimes F_{q^d}$. Its eigenspaces on W are $\langle e_{i,j,k} \rangle$ for $1 \leq i, j, k \leq d$. We know the set by $\{l_{i,j,k} := l_i l_j l_k \,|\, 1 \leq i, j, k \leq d\}$ for the eigenvalues of s in its action on W. We identify the indices as $(i, j, k) \mapsto l_{i,j,k}$ and choose a basis $F_W = \{f_{i,j,k}\}$, $f_{i,j,k} \in \langle e_{i,j,k} \rangle$.

Some properties about W can be given as follows:

Let W be $\Gamma_{1,1,0,\dots}, \Gamma_{0,1,0,\dots,1}, \Gamma_{2,1,0,\dots}$ irreducible representations. We consider the sets for the eigenvalues of s in its action on W by

$$\{l_{i,j,k} := l_i l_j l_k \,|\, 1 \leq i < j < k \leq d, \mathrm{i} = \mathrm{j}\ or\ i = k\},$$
$$\{l_{i,j,k} := l_i l_j l_k^{-1} \,|\, 1 \leq i, j, k \leq d, i \neq j \neq k\ and\ i < j\},$$
$$\{l_{i,i,j} := l_i^2 l_j^{-1} \,|\, 1 \leq i, j \leq d, i \neq j\},$$

respectively. Their eigenspaces on W are $\langle e_{i,j,k} = e_i \otimes (e_j \wedge e_k) \rangle$, $\langle e_{i,j,k} = (e_i \wedge e_j) \otimes e_k^* \rangle$, $\langle e_{i,i,j} = e_i{}^2 \otimes e_j^* \rangle$.

Lemma 4.1. 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 irreducible representations as given above. There are suitable labellings $l_{i,j,k}$ of the eigenvalues of s on W with a basis $F_W = \{f_{i,j,k}\}$. The cost of this labelling procedure is $O(\rho_{q^d} d^{11} \log q)$ where ρ_{q^d} is the cost of a field operation in F_{q^d}.

Proof 4.1. We can give the proof for each of W respectively as the following.

If W is $\Gamma_{(1,1,0,\dots)}$ irreducible representation then we construct the orbits of eigenvalues under the Frobenius map σ and choose an orbıt and label an element of this orbit as $l_1 l_1 l_2$. Taking $q-th$ powers determines $l_2 l_2 l_3, l_3 l_3 l_4$. We compute $l_{212}^{q+2} = l_{112}^{2q+1}$, so l_{212} is determined and we compute $l_{113} = l_{112}^{1-q} l_{212}^q$ and $l_{313} = l_{212}^{q-1} l_{112}$. For $4 \leq k \leq d$, we determine the general terms as $l_1 l_1 l_k = (l_1 l_1 l_{k-1})^{q+1} / (l_1 l_1 l_{k-2})^q$ and $l_{k1k} = (l_{k-1} l_1 l_{k-1})^{q+1} / (l_{k-2} l_1 l_{k-2})^q$. We choose an arbitrary $l_{1,1,k}, l_{k,1,k} \in \Omega$ from each orbit Ω and compute its eigenspace $\langle e_{i,j,k} \rangle$. For other eigenvalues $l_{i,j,k}^{\sigma^r}$, we compute $f_{i+r,j+r,k+r} := f_{i,j,k}^{\sigma^r}$.

If W is $\Gamma_{(0,1,0,\dots,0,1)}$ irreducible representation then we choose an orbit and label an element of this orbit as $l_{1,2,3}$ and taking $q-th$ powers, determine $l_{234}, l_{d-1,d,1}$. We have equalities $l_1 l_{124}^{q^{d-1}} = l_{123} l_{d-1,d,1}^q$ and $l_2 l_{124} = l_{123} l_{234}$ where we have $l_2 = l_1^q$, so l_{124} is obtained by these equalities. Then, we obtain l_{134} using equality $l_{134}^{q+1} = l_{124} l_{123}^{q^2}$.

For $k \in \{5, \dots, d\}$, $l_{1,2,k} = (l_{1,2,k-1})^{q+1} / (l_{1,2,k-2})^q$ is determined. For $k \in \{4, \dots, d-1\}$, $l_{1,k,k+1} = (l_{1,k-1,k})^{q+1} / (l_{1,k-2,k-1})^q$. For $k \in \{3, \dots, d-2\}$ and $r \in \{2, \dots, d-k\}$,

$$l_{1,k,k+r} = (l_{1,k,k+r-1})^{q+1} / (l_{1,k,k+r-2})^q.$$

For $j \in \{2, \dots, d-k-r\}$, $r \in \{1, \dots, d-k-j\}$ and $k \in \{1, \dots, d-r\}$, we determine $l_{j,j+k,j+k+r} := l_{j-1,j+k-1,j+k+r-1}^q$ and then we determine $l_{d+1-k-r,d+1-r,1} := l_{d-k-r,d-r,d}^q$. We choose an arbitrary $l_{1,j,k} \in \Omega$ from each orbit Ω and compute its eigenspace $\langle e_{i,j,k} \rangle$. For other eigenvalues $l_{i,j,k}^{\sigma^r}$, we compute $f_{i+r,j+r,k+r} := f_{i,j,k}^{\sigma^r}$.

If W is $\Gamma_{(2,1,0,\dots)}$ irreducible representation then we choose one of this orbits and label the first element as $l_{1,1,2}$. For $i \in \{2, \dots, d-1\}$, $l_{i,i,i+1} = l_{i-1,i-1,i}^q$, and $l_{d,d,1} = l_{d-1,d-1,d}^q$. For $k \in \{1, \dots, d-1\}$, we perform the followings:

i. we have $l_1 l_{113}^{q^{d-1}} = l_{112} l_{\mathrm{d,d,1}}$ and $l_2 l_{113} = l_{112} l_{223}$ where we have $l_2 = l_1^q$, so l_{113} is obtained by these equalities.

ii. For $k \notin \{1,2,3\}$, we determine $l_{1,1,k} = l_{1,1,k-1}^{1+q} / l_{1,1,k-2}^q$.

iii. For $j \in \{2, \dots, d-k\}$, we determine $l_{j,j,j+k} := l^q_{j-1,j-1,j+k-1}$ and then we determine $l_{d+1-k,d+1-k,1} := l^q_{d-k,d-k,d}$.

iv. For $j \in \{d+2-k, \dots, d\}$, we determine $l_{j,j,j-d+k} := l^q_{j-1,j-1,j-d+k-1}$.

We choose an arbitrary $l_{i,i,j} \in \Omega$ from each orbit Ω and compute its eigenspace $\langle e_{i,j,k} \rangle$.

Proposition 4.2 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 needs not to a scalar multiple (Magaard et al.,2008).

5. Finding images

This section's goal is to construct the image of an arbitrary $g \in G$. We describe the procedure for constructing the matrix a_{ij} representing an arbitrary $g \in G$. Firstly, we compute $K = (\kappa_{ijk,lmn})$, the matrix representation defined with the action of g on W. We then compute the a_{ij} since we know $K = (\kappa_{ijk,lmn})$.

Lemma 5.1. 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 $O((\xi_G + \rho_{q^d}(d^9 + d^2 \log q)) \log \epsilon^{-1})$ where ξ_G is the cost of choosing a random element of G, and ρ_{q^d} is the cost of a field operation in K.

Proof. The basic equation for $\kappa_{ijk,lmn}$ is $\kappa_{iik,lmn} = a_{il} a_{im} a_{kn}$. We choose an arbitrary nonzero entry $\kappa_{i_0 j_0 k_0, l_0 m_0 n_0}$ in K. The matrix with (i,l) entry $\kappa_{i j_0 k_0, l m_0 n_0} = a_{il} a_{j_0 m_0} (a_{k_0 n_0})$ is a projective image of g.

If W is $\Gamma_{(0,1,0,\dots,0,1)}$ irreducible representation, the basic equation for $\kappa_{ijk,lmn}$ is

$$\kappa_{ijk,lmn} = a_{il} a_{jm} a^*_{kn} \quad (2.1)$$

We may use (2.1) for $i \neq j \neq k$ and $l \neq m \neq n$ and so we find $a^*_{11} a_{il} a_{jm}$ for any i, l, j, m by using the following equations:

$\kappa_{ij1,lm1} = a_{il} a_{jm} a^*_{11}$ for $i \neq j \neq 1, l \neq m \neq 1$,

$\kappa_{ij2,lm2} = a_{il} a_{jm} a^*_{22}$ for $i \neq j \neq 2, l \neq m \neq 2$,

$\kappa_{ij3,lm3} = a_{il} a_{jm} a^*_{33}$ for $i \neq j \neq 3, l \neq m \neq 3$,

$a^*_{11}/a^*_{22} = \kappa_{ij1,lm1}/\kappa_{ij2,lm2}$ for distinct i,j and l,m $i,j,l,m \notin \{1,2\}$,

$a^*_{11}/a^*_{33} = \kappa_{ij1,lm1}/\kappa_{ij3,lm3}$ for distinct i,j and l,m $i,j,l,m \notin \{1,3\}$,

$\kappa_{i21,l21} = a_{il} a_{22} a^*_{11}$ for $i,l \notin \{1,2\}$

$\kappa_{i31,l31} = a_{il} a_{33} a^*_{11}$ for $i,l \notin \{1,3\}$

$\kappa_{i41,l41} = a_{il} a_{44} a^*_{11}$ for $i,l \notin \{1,4\}$

$\kappa_{132,l32} = a_{1l} a_{33} a^*_{22}$ for $l \notin \{2,3\}$

$\kappa_{k32,132} = a_{k1} a_{33} a^*_{22}$ for $k \notin \{2,3\}$

$\kappa_{133,233} = a_{12} a_{33} a^*_{33}$

$\kappa_{233,133} = a_{21} a_{33} a^*_{33}$

$a_{22}/a_{33} = \kappa_{i21,l21}/\kappa_{i31,l31}$ for $i,l \notin \{1,2,3\}$,

$a_{22}/a_{44} = \kappa_{i21,l21}/\kappa_{i41,l41}$ for $i,l \notin \{1,2,4\}$.

If W is $\Gamma_{(2,0,\dots,0,1)}$ irreducible representation we may use (2.1) for $i = j \neq k$ and $l = m \neq n$ and so we find $a^*_{11} a_{il} a_{il}$ for any i,l by using the following equations:

$\kappa_{ii1,ll1} = a^2_{il} a^*_{11}$ for $i \neq 1, l \neq 1$,

$\kappa_{ii2,ll2} = a^2_{il} a^*_{22}$ for $i \neq 2, l \neq 2$,

$\kappa_{ii3,ll3} = a^2_{il} a^*_{33}$ for $i \neq 3, l \neq 3$,

$\kappa_{112,ll2} = a^2_{1l} a^*_{22}$ for $l \neq 2$,

$\kappa_{kk2,112} = a^2_{k1} a^*_{22}$ for $k \neq 2$,

$\kappa_{113,223} = a^2_{12} a^*_{33}$

$\kappa_{223,113} = a^2_{21} a^*_{33}$

$a^*_{11}/a^*_{22} = \kappa_{ii1,ll1}/\kappa_{ii2,ll2}$ for $i,l \notin \{1,2\}$,

$a^*_{11}/a^*_{33} = \kappa_{ij1,lm1}/\kappa_{ij3,lm3}$ for $i,l \notin \{1,3\}$

If W is $\Gamma_{(1,1,0,\dots)}$ irreducible representation, we choose an arbitrary nonzero entry $\kappa_{i_0 j_0 k_0, l_0 m_0 n_0}$ in K. The matrix with (i,l) entry $\kappa_{i j_0 k_0, l m_0 n_0} = a_{il}(a_{j_0 m_0})(a_{k_0 n_0})$ is image of g. In this case, we apply a procedure as above.

Corresponding Author:
Assoc. Prof. Dr. Nurullah ANKARALIOĞLU
Mathematics Department,
Faculty of Science, Ataturk University,
25240, Erzurum, Turkey
E-mail: ankarali@atauni.edu.tr

References

1. Babai L. Local expansion of vertex-transitive graphs and random generation in finite groups.in: Theory of Computing, Los Angeles, (Association for Computing Machinery, New York, 1991). 1991; pp. 164-174.
2. Beals R, Leedham-Green CR, Niemeyer AC, Prager CE, Seress Á. A black-box group algorithm for recognizing finite symmetric and alternating groups I. Trans. Amer. Math. Soc. 2003;355, 2097–2113.
3. Beals R, Leedham-Green CR, Niemeyer AC, Prager CE, Seress Á. Constructive recognition of finite alternating and symmetric groups acting as matrix groups on their natural permutation modules. Journal of Algebra, 2005;292 (1):4-46
4. Corr BP. Estimation and computation with matrices over finite fields. Phd Thesis, The University of Western Australia Department of Mathematics. January, 2014;180.
5. Dumas JG, Pernet C, Wan Z. Efficient computation of the characteristic polynomial. In Proceedings of the 2005 international symposium on Symbolic and algebraic computation, pages 2005;140-147. ACM.

6. Fulton W, Harris J. Representation Theory A First Course. Graduate Texts in Mathematics, Springer. 1999:551.
7. Kantor WM, Seress Á. Black box classical groups. Mem. Amer. Mat. Soc. 2001 :149,168.
8. Magaard K, O'Brien E, Seress A. Recognition of small dimensional representations of general lineer groups. J. Avustralian Math. Soc., 2008;85, 229-250.
9. Neumann PM, Praeger CE. A recognition algorithm for special linear groups.
10. Proc. London Math. Soc. 1992;65, 555–603.
11. Niemeyer AC, Praeger CE. A recognition algorithm for classical groups over finite fields. Proceedings of the London Mathematical Society, 1998;77(1):117-169.
12. Pak I. The product replacement algorithm is polynomial. in: 41st Ann. Symp. on Foundations of Computer Science, (Redondo Beach, CA, 2000, IEEE Computer Society Press, Los Alamitos, CA) 2000; 476-485.
13. Seress Á. Permutation Group Algorithms. Cambridge University Press. 2003:274.

9/26/2014