Writing an Element of a Classical Group in a Non-Natural Representation as a Word in its Generators

Ann Cook 2007 Prize Entry

Elliot Costi

March 2007

1 $\mathrm{SL}(d,q)$ in its natural representation

The algorithms outlined here form part of a larger body of work in Computational Group Theory: *The Matrix Recognition Project.* This project requires an ability to compute efficiently with simple groups, a major case of which is the classical groups. As well as the natural representation, other representations in the same characteristic and cross characteristic need to be dealt with.

Given a generating set X for a group G, a word in X is a string of symbols and their inverses in X. Given a group G the two tasks that we wish to complete are:

1. find a standard generating set for G as words in a given generating set for G;

2. write a given element of G as a word in this standard generating set.

It is the latter of these two tasks that we will outline here.

By writing an element of a group G as a word in its generators, homomorphisms can be readily formed from G to an arbitary group H. This is achieved by defining the image of the generators of G in H under the homomorphism, writing an element g of G as a word in the generators of G and then evaluating the word on the generators of H. For example, let $G = \langle g_1, g_2, g_3\rangle$, $\phi : G \to H$ and $\phi(g_i) = h_i \in H$. If you can write $g \in G$ as $g = g_2^2 g_3^{-1} g_1 g_3$, then $\phi(g)$ can be found by evaluating $h_2^2 h_3^{-1} h_1 h_3$ in H.

Consider $\mathrm{SL}(d,q)$ in its natural representation. That is to say, $\mathrm{SL}(d,q)$ is the set of all $d \times d$ matrices of determinant 1 over a finite field of size q acting on the corresponding vector space $(\mathbb{F}_q)^d$.

We wish to write an arbitary element g of $\mathrm{SL}(d,q)$ as a word in a specific generating set. The generating set we wish to use is $\{t, u, v, \delta\}$ and is defined as follows:

$$t = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & I_{d-2} \end{pmatrix}, \text{ a transvection.} \qquad u = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & I_{d-2} \end{pmatrix}$$

$$v = \begin{pmatrix} 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix} \qquad \delta = \begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega^{-1} & 0 \\ 0 & 0 & I_{d-2} \end{pmatrix}$$

The elements u and v generate a subgroup of $C_2 \wr \mathrm{Sym}(d)$ of index 2 that contains $\mathrm{Sym}(d)$, the permutation group on d-symbols. Hence, $\langle u, v\rangle$ and can be used to permute the d columns and rows. t can be used to add row/column 1 to row/column 2. We can therefore proceed by using row and column operations to kill the entries in g to reduce it to the identity matrix. We will then have $x_1 x_2 \cdots x_n g x_{n+1} x_{n+2} \cdots x_m = I$, where the x_i are elements of the generating set. We then rearrange this equation to get g on one side and hence the problem has been solved.

This procedure has been implemented in the computer algebra package MAGMA and most of the other classical groups have been implemented in a similar way.

2 Non-natural Representations of $\mathrm{SL}(d, q)$

2.1 Introduction to the General Ideas

Definition 2.1 *For the purposes of this presentation, a module is a vector space V over a finite field $\mathbb{F}_q$ with a matrix group acting on it on the right. A submodule U of V is a subspace of V that is also a module in its own right.*

Let us say that we have a group $E < \mathrm{SL}(n, q)$, $n > d$ where $E \cong G = \mathrm{SL}(d, q)$ (or possibly $\mathrm{PSL}(d, q)$, which is $\mathrm{SL}(d, q)$ with the scalar matrices quotiented out). We say that E is a non-natural representation of G, the vector space in this case being $(\mathbb{F}_q)^n$.

When we are in a non-natural representation of G, the problem becomes much harder. It is more difficult to use the same machinary as before to reduce $g \in E$ to the identity. As will be discussed here, we will go part of the way in killing g before using a trick to find the pre-image of g in G.

Example of a non-natural representation: $n = \begin{pmatrix} d \\ 2 \end{pmatrix}$ and the representation in question is the exterior square of the natural module. The exterior square can be defined in the following way. Choose a basis $\{v_i\}$ for $V = (\mathbb{F}_q)^d$ and then form the tensor square $V \otimes V$. This is the vector space generated by the basis $\{v_i \otimes v_j\}$. We then quotient out the symmetric elements. That is to say, we define $v \otimes v = 0$, for all $v \in V$. Let the symbol $\wedge$ denote this product. This definition implies that $v \wedge w = w \wedge v$, for all $v, w \in V$. $V \wedge V$ is a vector space of dimension $n = \begin{pmatrix} d \\ 2 \end{pmatrix}$ and $E \cong \mathrm{PSL}(d, q)$ is the group defined by the acting algebra on this space. For example, if $G = \mathrm{SL}(4, 7)$ generated by:

$$\begin{pmatrix} -1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix} \quad \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{then } E < \mathrm{SL}(6, 7) \text{ is generated by:}$$

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Some of the more commonly defined other non-natural representations of classical groups include:

1. $V \vee V$ - the symmetric square of V (similar definition to the exterior square)
2. $V \otimes V^{\phi}$ - the tensor product of V with itself twisted by a field automorphism
3. $V \otimes V^*$ - the tensor product of V with its dual representation

2.2 Solving the Problem

Let ϕ be the isomorphism from $\mathrm{SL}(d,q)$ to E. Computer code already exists to provide a generating set for E that is the image under ϕ of $\{t,u,v,\delta\}$, so we will assume that the generating set that we have for E is this image.

Now consider the subgroup $H \leq \mathrm{SL}(d,q)$.

$$H = \begin{pmatrix} det^{-1} & 0 & 0 & \cdots & 0 \\ * & & & & \\ * & & & & \\ * & & \mathrm{GL}(d-1,q) & & \\ * & & & & \end{pmatrix}$$

Here, the asterisks, represent any elements of $\mathbb{F}_q$ that you like and det^{-1} represents the inverse of the determinant of the $\mathrm{GL}(d-1,q)$ portion of the matrix in order to make the elements of H have determinant 1. H is the stabilizer of the subspace U of V spanned by the first basis vector. We say that the subspace U is a submodule afforded by H.

Now consider $\phi(H)$. Just as H in the natural dimension affords a submodule, a theorem from representation theory (omitted here) states that, as $\phi(H)$ contains a p-group, it affords a non-trivial submodule U of ${F_q}^n$. For the example of the exterior square, the submodule in question has dimension $d-1$. Let g be the element of E that we wish to find as a word in the generating set and set $W = gU$.

Example: $G = \mathrm{SL}(4,7)$, E is the exterior square and

$$g = \begin{pmatrix} 4 & 5 & 0 & 4 & 4 & 5 \\ 2 & 6 & 5 & 2 & 1 & 5 \\ 6 & 6 & 4 & 0 & 1 & 1 \\ 5 & 1 & 0 & 5 & 1 & 3 \\ 5 & 1 & 0 & 2 & 6 & 4 \\ 2 & 0 & 3 & 1 & 3 & 2 \end{pmatrix}$$

Then $U = \langle e_1, e_2, e_4 \rangle < (F_q)^n$ and $gU = W = \langle (1 \quad 3 \quad 0 \quad 1 \quad 0 \quad 0), (0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 6), (0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 3) \rangle$.

The idea is to find an element k of E such that $kgU = U$. This means that $kg \in H$ and hence we must have killed the top row of g, if you were able to consider it in its natural dimension.

The problem outlined here is that we are performing processes on the non-natural representation that, by solely looking at what is going on in this non-natural representation, it would be impossible to tell that it is getting us to where we wish to be. We are using the fact that we know the general shape of the pre-image of g in the natural representation in order to obtain full information about this pre-image. Processes that work with group elements in this way are known as "grey box algorithms".

We will use an algorithm developed by Ruth Schwingel, a former Queen Mary's PhD student and a supervisee of Charles Leedham-Green, to find out the first row and column of the pre-image of $g \in SL(d,q)$. As the algorithm was the second to feature in Ruth's thesis, it has been colloquially dubbed Ruth2.

3 Ruth2

Ruth2 takes as input a matrix p-group K and the aforementioned submodule U as defined in the previous section. It then returns a canonical element $\bar{U}$ in the orbit of U under K together with an element $x \in K$ that maps U to $\bar{U}$. Originally, Ruth2 only worked if the input gorup K was written over a prime field. By considering the way in which the input submodule U was canonised, I modified the algorithm to work for matrix groups written over prime power fields and also so that a word in the generators for K is returned.

We define K to be the image in E under ϕ of the set of matrices in G that look like this:

$$K = \begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & & & & \\ 0 & & & & \\ \vdots & & I_{d-1} & & \\ 0 & & & & \end{pmatrix}, \text{ where the * represent elements of } \mathbb{F}_q.$$

Assuming that the pre-image of g in G does not have a 0 in the first entry of the matrix (in which case we apply other techniques, omitted here), U and W will be in the same orbit under K and hence we can find an element z of K that maps W back to U. Hence, we have $zgU = U$, meaning that $zg \in \phi(H)$ and so we have reduced the top row of the pre-image of g in G to $\begin{pmatrix} y & 0 & 0 & \cdots & 0 \end{pmatrix}$. Dualising this process, we can reduce the first column in the same way.

We then can work out the remaining entries in the pre-image of g by conjugating the generators of K with our reduced g to work out the other entries of g in the natural representation. For example, assume that $y = 1$, K_1 is the first generator of K and look at what is happening in the natural representation of $\mathrm{SL}(4, q)$:

$$K_1^g = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & & & \\ 0 & & A^{-1} & \\ 0 & & & \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & & & \\ 0 & & A & \\ 0 & & & \end{pmatrix} = \begin{pmatrix} 1 & a_1 & a_2 & a_3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

which is in K.

I created an algorithm to write an element of K as a word in its generators in E. Therefore, despite the fact we are unable to see this construction in the lower dimension, we can obtain the values of a_1, a_2 and a_3 by performing K_1^g in the non-natural representation and solving the word problem on the result. Hence, we can work out the pre-image of g in the lower dimension. We then apply the algorithm as mentioned in section 1 in order to complete the process and write g as a word in the generating set.

3.1 What's Next?

Having completed this for $\mathrm{SL}(d, q)$. I am currently working on similar methods for the other classical groups.