Membership Testing in Classical Groups

Elliot Costi

2008

Suppose that the field that these matrices are defined over is $F = \mathrm{GF}(q)$. Then ω is the primitive element of F. For the Unitary groups defined over the field $\mathrm{GF}(q^2)$, $\alpha = \omega^{\frac{q+1}{2}}$. For $\Omega^-(2n, q)$, let γ be the primitive element of $GF(q^2)$. Then the variables A, B and C given in the definition have the following values, with α defined as for the Unitary groups:

$$\begin{aligned} A &= \frac{1}{2}(\gamma^{q-1} + \gamma^{-q+1}) \\ B &= \frac{1}{2}\alpha(\gamma^{q-1} - \gamma^{-q+1}) \\ C &= \frac{1}{2}\alpha^{-1}(\gamma^{q-1} - \gamma^{-q+1}). \end{aligned}$$

Group	s	t	δ	u	v	x	y
$\mathrm{SL}(n, q)$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$	I_2	$\begin{pmatrix} 0 & 1 \\ -I_n & 0 \end{pmatrix}$	I_4	I_4
$\mathrm{Sp}(2n, q)$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	$(e_1, e_2, \ldots, e_n)(f_1, f_2, \ldots, f_n)$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$	I_4
$\mathrm{SU}(2n, q)$	$\begin{pmatrix} 0 & \alpha \\ \alpha^{-q} & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega^{q+1} & 0 \\ 0 & \omega^{-(q+1)} \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	$(e_1, e_2, \ldots, e_n)(f_1, f_2, \ldots, f_n)$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^{-q} & 0 & 0 \\ 0 & 0 & \omega^{-1} & 0 \\ 0 & 0 & 0 & \omega^q \end{pmatrix}$
$\mathrm{SU}(2n+1, q)$	$\begin{pmatrix} 0 & \alpha \\ \alpha^{-q} & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega^{q+1} & 0 \\ 0 & \omega^{-(q+1)} \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	$(e_1, e_2, \ldots, e_n)(f_1, f_2, \ldots, f_n)$	$\begin{pmatrix} 1 & -1/2 & 1 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega^{q-1} & 0 \\ 0 & 0 & \omega^{-q} \end{pmatrix}$

Table 1: Standard generators for non-orthogonal classical groups

Group	s	t	δ	u	v
$\Omega^+(2n, q)$	$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^{-1} & 0 & 0 \\ 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & \omega^{-1} \end{pmatrix}$	I_4	$(e_1, e_2, \ldots, e_n)^{\epsilon_n}(f_1, f_2, \ldots, f_n)^{\epsilon_n}$
	s'	t'	δ'		
	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^{-1} & 0 & 0 \\ 0 & 0 & \omega^{-1} & 0 \\ 0 & 0 & 0 & \omega \end{pmatrix}$		
Group	t	t'	δ	u	v
$\Omega^-(2n, q)$	$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^{-1} & 0 & 0 \\ 0 & 0 & A & B \\ 0 & 0 & C & A \end{pmatrix}$	$(e_1, e_2)^-(f_1, f_2)^-$	$(e_1, \ldots, e_{n-1})^{\epsilon_{n-1}}(f_1, \ldots, f_{n-1})^{\epsilon_{n-1}}$
Group	s	t	δ	u	v
$\Omega(2n+1, q)$	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega^2 & 0 & 0 \\ 0 & \omega^{-2} & 0 \\ 0 & 0 & 1 \end{pmatrix}$	I_4	$(e_1, \ldots, e_n)^{\epsilon_n}(f_1, \ldots, f_n)^{\epsilon_n}$

Table 2: Standard generators for orthogonal groups