1 Introduction

Let $A$ be a linear transformation with minimum polynomial $m_A(t)$ and characteristic polynomial $c_A(t)$. We say that $A$ is cyclic if $m_A(t) = c_A(t)$, semisimple if $m_A(t)$ has no repeated factors, and separable if it is both cyclic and semisimple. The proportions of elements of $GL(d,q)$ which are cyclic or separable have been investigated by, amongst others, Neumann and Praeger [7], Wall [10], and Fulman [4] who also studies semisimple elements. Making use of their results, we gave estimates in [1] for these proportions in $SL(d,q)$.

Fulman, Neumann and Praeger [5] have recently found good estimates for the corresponding proportions in the finite classical groups, $U(d,q^2)$, $Sp(2m,q)$ and $O^\pm(d,q)$. They raise the question of whether similar methods may be used to calculate the proportions in various subgroups and supergroups of the classical groups. In a series of three papers, we shall show how this may be done. In this, the first paper, we deal with the special unitary groups $SU(d,q^2)$, consisting of unitary transformations with determinant 1. In the second paper [2] we shall focus on the conformal groups $GSp(2m,q)$ and $GO^\pm(d,q)$, and in the third paper [3] we shall consider how the method may be extended to a number of groups of orthogonal type, including the special orthogonal group and the derived group of the orthogonal group.

Our method in [1] involved the vector space cycle index of Kung [6] and Stong [8], which we describe briefly in Section 2. Similarly, in the current series
of papers, we make use of Fulman’s cycle indices for classical groups [4]. The cycle index for the unitary group is described briefly in Section 3, in which we also show how it may be adapted to the special unitary group.

After discussing some generating function identities in Section 4, we derive our main results in Section 5. For a set $T$ of linear transformations, we write $C_T$ for the proportion of cyclic elements in $T$, $SS_T$ for the proportion of semisimple elements, and $S_T$ for the proportion of separable elements. We will write $C_{U(\infty,q^2)}$ for $\lim_{d \to \infty} C_{U(d,q^2)}$, and so on. Our results depend upon the work of Fulman, Neumann and Praeger on unitary groups [5, Sections 2.1, 3.1], in which are given the following limiting proportions:

\[
C_{U(\infty,q^2)} = 1 - q^{-3} - q^{-5} + q^{-6} - 2q^{-7} + 3q^{-8} - 5q^{-9} + 8q^{-10} - 11q^{-11} + 21q^{-12} + O(q^{-13})
\]

\[
S_{U(\infty,q^2)} = 1 - q^{-1} - 2q^{-3} + 4q^{-4} - 6q^{-5} + 14q^{-6} - 28q^{-7} + 52q^{-8} - 106q^{-9} + O(q^{-10})
\]

\[
SS_{U(\infty,q^2)} = 1 - q^{-1} - q^{-3} + 2q^{-4} - 2q^{-5} + 5q^{-6} - 9q^{-7} + 11q^{-8} - 20q^{-9} + O(q^{-10}).
\]

The rate of convergence to these limits is exponential: if $0 < r < q$, then except for small values of $d$,

\[
|C_{U(\infty,q^2)} - C_{U(d,q^2)}| < r^{-2d},
\]

\[
|S_{U(\infty,q^2)} - S_{U(d,q^2)}| < r^{-d},
\]

\[
|SS_{U(\infty,q^2)} - SS_{U(d,q^2)}| < r^{-d}.
\]

We shall show that the same limiting values hold for the special unitary groups, and that the rates of convergence to the limits are of the same order.

In Section 6 we calculate the sizes of certain sets of polynomials, which are then used in Section 7 where we give explicit bounds for the proportions $C_{SU(d,q^2)}$ and $SS_{SU(d,q^2)}$. We shall not give explicit bounds for $SS_{SU(d,q^2)}$.

The research for this paper was conducted under the supervision of Dr Peter Neumann, to whom the author would like to express his great gratitude. The author was funded by a studentship of the Engineering and Physical Sciences Research Council.
2 The cycle index

Recall that a linear transformation $A$ may be represented by a matrix $R_A$ in rational canonical form. For each monic irreducible polynomial $f$ dividing $c_A$, there is a block of $R_A$ of the form

$$\text{diag}(\gamma(f^{\alpha_1}), \gamma(f^{\alpha_2}), \ldots, \gamma(f^{\alpha_t})),$$

where $\gamma(f^{\alpha_i})$ is the companion matrix of $f^{\alpha_i}$. The multiplicity of $f$ as a factor of $c_A$ is given by the sum $\sum_{i=1}^{t} \alpha_i$. The $t$-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_t)$ constitutes a partition of this multiplicity, and is denoted $\lambda_A(f)$; for polynomials not dividing $c_A$, this partition is the empty partition $\emptyset$. Two transformations $A$ and $B$ are similar if and only if $\lambda_A(f) = \lambda_B(f)$ for every monic irreducible polynomial $f$.

To simplify notation in several rather complicated expressions later on, here we introduce some notational devices which will be constantly useful. The field with $q$ elements we denote by $\mathbb{F}_q$, and its multiplicative group by $\mathbb{F}_q^\times$.

**Definition 2.1.** We define $\Phi_q$ to be the set of monic irreducible polynomials in $\mathbb{F}_q[t]$, and $\Phi_q^+$ the subset $\Phi_q \setminus \{t\}$.

**Definition 2.2.** We define $\Lambda$ to be the set of all partitions of positive integers. For a partition $\lambda \in \Lambda$, we shall write $|\lambda|$ for the sum of the parts of $\lambda$.

We are now in a position to define the cycle index. This definition is due to Stong [8]; it is a slight generalization of an earlier version by Kung [6], which did not distinguish between different irreducible polynomials of the same degree.

**Definition 2.3 (The cycle index).** For a set $T$ of linear transformations, the cycle index $Z_T$ of $T$ is the polynomial in variables $\{x_{f, \lambda} \mid f \in \Phi_q, \lambda \in \Lambda\}$ defined by

$$Z_T := \frac{1}{|T|} \sum_{A \in T} \prod_{f \in \Phi_q} x_{f, \lambda_A(f)}.$$

The usefulness of the cycle index for the study of cyclic, separable and semisimple transformations is explained by the following proposition:
Proposition 2.4. The proportion of semisimple transformations in $T$ is obtained by specializing the variables in $Z_T$ as follows:

$$x_{f,\lambda} \mapsto \begin{cases} 
1 & \text{if } \lambda \text{ has no part greater than } 1, \\
0 & \text{otherwise.} 
\end{cases}$$

The proportion of cyclic transformations in $T$ is obtained by specializing the variables in $Z_T$ as follows:

$$x_{f,\lambda} \mapsto \begin{cases} 
1 & \text{if } \lambda \text{ has no more than one part,} \\
0 & \text{otherwise.} 
\end{cases}$$

The proportion of separable transformations in $T$ is obtained by specializing the variables in $Z_T$ as follows:

$$x_{f,\lambda} \mapsto \begin{cases} 
1 & \text{if } |\lambda| \leq 1, \\
0 & \text{otherwise.} 
\end{cases}$$

The proof of this proposition is straightforward, since the given specializations of $x_{f,\lambda}$ relate in an obvious way to the conditions on characteristic and minimum polynomials by which we define cyclic, separable and semisimple transformations.

3 The unitary group cycle index

Definition 3.1. Let $g$ be a monic polynomial of degree $d$ over $F_{q^2}$, with non-zero constant term, whose roots (in a splitting field) are $\alpha_1, \ldots, \alpha_d$. We define $g^*$ to be the polynomial whose roots are $\alpha_1^{-q}, \ldots, \alpha_d^{-q}$.

It is clear that $g^*$ is well-defined, that it has degree $d$, that it is irreducible if and only if $g$ is, and that $g^{**} = g$. There is an alternative description of $g^*$ in terms of the coefficients of $g$. Suppose the coefficient of $t^i$ in $g(t)$ is $a_i$. Then the coefficient of $t^i$ in $g^*(t)$ is \( \left( \frac{a_i}{a_0} \right)^q \).

Given a partition $\lambda$, define $m_s$ to be the number of parts of $\lambda$ of size $s$, and define

$$k(\lambda) := \sum_{s \leq t} sm_s m_t + \frac{1}{2} \sum_s (s - 1)m_s^2.$$
The following quantities arise as the sizes of centralizers of elements of unitary groups, which were calculated by Wall [9]. They play a crucial role in Fulman’s factorization formula.

**Definition 3.2.**

\[
C_{U,f}(\lambda) = \begin{cases} 
q^{2k(\lambda)\deg f} \prod |U(m_s, q^{2\deg f})| & \text{if } f = f^*, \\
q^{4k(\lambda)\deg f} \prod |GL(m_s, q^{2\deg f})| & \text{if } f \neq f^*.
\end{cases}
\]

We can now state the factorization formula itself ([4, Theorem 10]). (We should perhaps alert the reader to the fact that our notation differs from Fulman’s.)

**Theorem 3.3 (Fulman).**

\[
1 + \sum_{d=1}^{\infty} Z_{U(d,q^2)} u^d = \prod_{\substack{f \in \Phi_+^n \\text{if } f = f^*}} \left(1 + \sum_{\lambda \in \Lambda} \frac{x_f,\lambda x_f U^{2\deg f} \lambda}{C_{U,f}(\lambda)} \right) \times \prod_{\substack{(f, f^*) \\text{if } f \neq f^*}} \left(1 + \sum_{\lambda \in \Lambda} \frac{x_f,\lambda x_f U^{2\deg f} \lambda}{C_{U,f}(\lambda)} \right).
\]

The method by which, in [1], we derived the identity of Theorem 2.7 as an analogy to Theorem 2.3, may be employed in this case to derive an analogy to Theorem 3.3 for the special unitary groups. We shall constantly employ the following notation:

**Definition 3.4.** We define \( \Omega_n \) to be the set of complex roots of \( t^n - 1 \).

Our method, in its simplest form, uses the following function, which was defined in [1]. Presently we shall replace it with a slightly more sophisticated device (Definition 3.6).

**Definition 3.5.** Let \( \eta \) be a generator of the cyclic group \( \mathbb{F}_{q^2}^\times \). For a monic polynomial \( g \), define \( r(g) \) to be the element of \( \mathbb{Z}_{q^2-1} \) such that \( \eta^{r(g)} = (-1)^{\deg(g)} g(0) \).

We note that

\[
\sum_{\omega \in \Omega_n} \omega^r = \begin{cases} 
n & \text{if } r \equiv 0 \text{ mod } n \\
0 & \text{otherwise},
\end{cases}
\]
and hence, for a transformation $A$ with characteristic polynomial $c_A$,

$$\sum_{\omega \in \Omega_{q^2-1}} \omega^{\tau(c_A)} = \begin{cases} q^2 - 1 & \text{if } \det A = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Now

$$r(c_A) = \sum_{f \in \Phi_{q^2}} r(f)|\lambda_A(f)|,$$

and it is not hard to show from these facts that

$$q + 1 + \sum_{d=1}^{\infty} Z_{SU(d,q^2)} u^d = \frac{1}{q - 1} \sum_{\omega \in \Omega_{q^2-1}} L_\omega(u), \quad \text{(1)}$$

where

$$L_\omega(u) = \prod_{f \in \Phi_{q^2}} \left( 1 + \sum_{\lambda \in \Lambda} \frac{\omega^{\tau(f)|\lambda|} u^{\deg f|\lambda|}}{C_{U,f}(\lambda)} \right)$$

$$\times \prod_{\{f,f^*\}} \left( 1 + \sum_{\lambda \in \Lambda} \frac{\omega^{\tau(f)+\tau(f^*)|\lambda|} u^{2\deg f|\lambda|}}{C_{U,f}(\lambda)} \right).$$

This identity can be simplified a little. Let $E_{q+1}$ be the cyclic subgroup of order $q + 1$ in $\mathbb{F}_{q^2}^*$. It follows from the definition of $f^*$, and from the fact that $(-1)^{\deg f} f(0)$ is the product of the roots of $f$, that

$$f^*(0) = f(0)^{-q}.$$

In particular, it is clear that if $f = f^*$ then $f(0) \in E_{q+1}$, whereas if $f \neq f^*$ then $f(0)f^*(0) \in E_{q+1}$.

**Definition 3.6.** Let $\zeta$ be a generator of the group $E_{q+1}$. For $g \in \Phi_{q^2}^+$, we define $\zeta^*(g) \in \mathbb{Z}_{q+1}$ by

$$\zeta^*(g) = \begin{cases} (-1)^{\deg g} g(0) & \text{if } g = g^* \\ g(0)g^*(0) & \text{if } g \neq g^*. \end{cases}$$

We define

$$R_\omega(u) := \prod_{f \in \Phi_{q^2}} \left( 1 + \sum_{\lambda \in \Lambda} \frac{\omega^{\tau(f)|\lambda|} u^{\deg f|\lambda|}}{C_{U,f}(\lambda)} \right).$$
\[ S_\omega(u) := \prod_{\{f, f^*\} \atop f \neq f^*} \left( 1 + \sum_{\lambda \in \Lambda} \frac{\omega^\sigma(f)|\lambda|_{x_f, \lambda} x_f^* \lambda u^{2 \deg f}|\lambda|}{C_{U_f}(\lambda)} \right), \]

\[ K_{U, \omega}(u) := R_\omega(u) S_\omega(u). \]

Now it is straightforward to show:

**Theorem 3.7.**

\[ q + 1 + \sum_{d=1}^{\infty} Z_{SU(d, q^2)} u^d = \sum_{\omega \in \Omega_{q+1}} K_{U, \omega}(u). \]

The term in the sum on the right-hand side corresponding to \( \omega = 1 \) is equal to Fulman’s cycle index for the unitary groups (Theorem 3.3). We therefore note the following corollary:

**Corollary 3.8.**

\[ q + \sum_{d=1}^{\infty} \left( Z_{SU(d, q^2)} - Z_{U(d, q^2)} \right) u^d = \sum_{\omega \in \Omega_{q+1}} K_{U, \omega}(u). \]

### 4 Some identities

Our arguments will make essential use of the following generating function identities, the case \( \omega = 1 \) of which are also used in [5]. They are analogues of those proved in [1] at the corresponding stage in the argument.

**Definition 4.1.** For \( \sigma \in \{+, -\} \), define

\[ V^\sigma_\omega(u) := \prod_{f \in \Phi_{q^2}^+} \left( 1 + \sigma \omega^\sigma(f) u^{\deg f} \right), \]

\[ W^\sigma_\omega(u) := \prod_{\{f, f^*\} \atop f \neq f^*} \left( 1 + \sigma \omega^\sigma(f) u^{2 \deg f} \right). \]

**Identity 4.2.**

\[ V^-_\omega(u) W^-_\omega(u) = \begin{cases} 1 & \text{if } \omega \neq 1, \\ \frac{1 - qu}{1 + u} & \text{if } \omega = 1. \end{cases} \]
Identity 4.3.

\[ V_{\omega}^+(u)W_{\omega}^+(u) = \begin{cases} 
1 & \text{if } \omega \neq \pm 1, \\
\frac{1-qu^2}{1+u^r} & \text{if } \omega = -1, \\
\frac{(1+u^r)(1-qu^2)}{(1+u^r)(1-qu)} & \text{if } \omega = 1.
\end{cases} \]

For the proof of Identity 4.2, we note that \( V_{\omega}^+(u)W_{\omega}^+(u) \) is equal to

\[
\sum_{\substack{g \in \mathbb{F}_{q}[t] \\ \text{deg } g = d}} \omega^a(g) u^{\text{deg } g}. \tag{2}
\]

For each positive integer \( d \), let \( D_{d,\alpha} \) be the number of polynomials \( g \) of degree \( d \), such that \( g = g^* \) and \( g(0) = \alpha \). From the description (given after Definition 3.1) of \( g^* \) in terms of the coefficients of \( g \), it is easy to calculate that \( D_{d,\alpha} = q^{d-1} \) for any \( \alpha \in \mathbb{F}_{q+1} \). The coefficient of \( u^d \) in the power series (2) is \((q+1)q^{d-1}\) if \( \omega = 1 \), and 0 otherwise. Clearly the constant coefficient is 1 for any value of \( \omega \). It is clear from this that the identity is correct when \( \omega \neq 1 \), and not hard to show that the generating function \( \frac{1-qu^2}{1+u^r} \) yields the correct coefficients in the case \( \omega = 1 \). Identity 4.3 follows easily from Identity 4.2, since

\[ V_{\omega}^+(u)W_{\omega}^+(u) = \frac{V_{\omega}^+(u^2)W_{\omega}^+(u^2)}{V_{\omega}^+(u)W_{\omega}^+(u)}. \]

We define \( N(d, q) \) to be the number of monic irreducible polynomials of degree \( d \) over \( \mathbb{F}_q \). We also define \( N^*(d, q) \) to be the number of monic irreducible polynomials \( f \) of degree \( d \) over \( \mathbb{F}_{q^2} \) such that \( f = f^* \), and \( M(d, q) \) to be the number of pairs \( \{f, f^*\} \) of monic irreducible polynomials of degree \( d \) over \( \mathbb{F}_{q^2} \) such that \( f \neq f^* \). Formulae for these quantities can be given, and it will be convenient for our purposes to make use of these to define functions \( N(d, z) \), \( N^*(d, z) \) and \( M(d, z) \) of the complex variable \( z \). The formula for \( N(d, q) \) is well-known. For a proof of the formula for \( N^*(d, q) \) see [4].

**Definition 4.4.**

\[ N(d, z) := \frac{1}{d} \sum_{a|d} \mu(a) z^{\frac{d}{a}} \]
\[ N^*(d, z) := \begin{cases} \frac{1}{d} \sum_{a|d} \mu(a) \left( z^{\frac{d}{a}} + 1 \right) & \text{if } d \text{ is odd,} \\ 0 & \text{if } d \text{ is even,} \end{cases} \]

\[ M(d, z) := \frac{1}{2} \left( N(d, z^2) - N^*(d, z) \right). \]

where \( \mu \) is the Möbius function.

We state analogues to Identities 4.2 and 4.3 in the case \( \omega = 1 \).

Identity 4.5. If \( |u| < 1 \) and \( |z| < \frac{1}{|u|} \) then
\[
\prod_{d=1}^{\infty} (1 - u^d)^{N^*(d, z)} (1 - u^{2d})^{M(d, z)} = \frac{1 - zu}{1 + u}.
\]

Identity 4.6. If \( |u| < 1 \) and \( |z| < \frac{1}{|u|} \) then
\[
\prod_{d=1}^{\infty} (1 + u^d)^{N^*(d, z)} (1 + u^{2d})^{M(d, z)} = \frac{(1 - zu^2)(1 + u)}{(1 + u^2)(1 - zu)}.\]

Identity 4.5 may be proved by taking the logarithm of the left hand side, expressing it as a power series in \( u \) and manipulating it into the desired form. However, we shall omit the details here. Identity 4.6 is an obvious corollary.

Finally we state the following identities (proved in [1] where they appear as Identities 3.7 and 3.8).

Identity 4.7. Let \( |u| < 1 \) and \( |z| < \frac{1}{|u|} \). Then
\[
\prod_{d=1}^{\infty} (1 - u^d)^{N(d, z)} = 1 - zu.
\]

Identity 4.8. Let \( |u| < 1 \) and \( |z| < \frac{1}{|u|} \). Then
\[
\prod_{d=1}^{\infty} (1 + u^d)^{N(d, z)} = \frac{1 - zu^2}{1 - zu}.
\]

5 Cyclic, separable and semisimple elements in the special unitary groups

The following notation will be convenient.
Definition 5.1. Let $\phi(u)$ and $\psi(u)$ be complex functions given by the power series $\sum_{i=0}^{\infty} a_i u^i$ and $\sum_{i=0}^{\infty} b_i u^i$ respectively. We write

$$\phi \ll \psi,$$

if $|a_i| \leq |b_i|$ for all $i$.

In analysing convergence of power series, we shall make use of the following well-known fact.

Proposition 5.2. Let $(a_i)$ be a sequence of non-negative real numbers, and $(b_i)$ a sequence of non-negative integers. If $\sum_i a_i b_i$ converges, then so does $\prod_i (1 + a_i)^{b_i}$.

We shall now analyse separable elements in $\text{SU}(d,q^2)$ by making the relevant substitution (from Proposition 2.4) in the cycle index. We define

$$\mathcal{R}_\omega(u) := \prod_{f \in \Phi^+} \left(1 + \frac{\omega^s(f) u^{\deg f}}{q^{\deg f} + 1}\right),$$

$$\mathcal{S}_\omega(u) := \prod_{\{f,f'\} \in \Phi^+_{\neq}} \left(1 + \frac{\omega^s(f) u^{2\deg f}}{q^{2\deg f} - 1}\right),$$

$$\mathcal{K}_{U,\omega}(u) = \mathcal{R}_\omega(u) \mathcal{S}_\omega(u).$$

Now by Corollary 3.8,

$$q + \sum_{d=1}^{\infty} \left( S_{\text{SU}(d,q^2)} - S_{\text{U}(d,q^2)} \right) u^d = \sum_{\omega \in \Omega_{\neq}} \mathcal{K}_{U,\omega}(u).$$

We analyse the convergence of the infinite product $\mathcal{K}_{U,\omega}(u)$ using Identity 4.3. Suppose $\omega \neq 1$. If we write

$$A_\omega(u) = \begin{cases} \frac{1 - \frac{u^2}{q^{\deg f} + 1}}{1 + \frac{u^2}{q^{\deg f} + 1}} & \text{if } \omega = -1, \\ 1 & \text{otherwise,} \end{cases}$$

then

$$\mathcal{K}_{U,\omega}(u) = A_\omega(u) \mathcal{R}_\omega(u) V^+_\omega \left( \frac{u}{q} \right)^{-1} \mathcal{S}_\omega(u) W^+_\omega \left( \frac{u}{q} \right)^{-1}.$$
Clearly $A_\omega(u)$ is always analytic at least in a disc of radius $q$. Now by straight-forward manipulation,
\[
\mathcal{R}_\omega(u) V^+_{\omega}(u) - \frac{1}{q} = \prod_{\substack{f \in \Phi^+_{\omega} \\ f \neq f^*}} \left( 1 - \frac{\omega^*(f) \deg f}{(q^{\deg f} + 1)(q^{\deg f} + \omega^*(f) \deg f)} \right)
\]
\[
\ll \prod_{d=1}^{\infty} \left( 1 + \frac{u^d}{(q^d + 1)(q^d - u^d)} \right)^{N^*(d,q)}
\]
which, since $N^*(d,q) = O(q^d)$, converges if
\[
\sum_{d=1}^{\infty} \frac{u^d}{(q^d + 1)(q^d - u^d)}
\]
does. This is certainly the case if $|u| < q$. Similarly,
\[
\mathcal{S}_\omega(u) W^+_{\omega}(u) - \frac{1}{q} = \prod_{\substack{\{f,f^*\} \\ f \in \Phi^+_{\omega} \\ f \neq f^*}} \left( 1 + \frac{\omega^*(f) \deg f}{(q^{2\deg f} - 1)(q^{2\deg f} + \omega^*(f) \deg f)} \right)
\]
\[
\ll \prod_{d=1}^{\infty} \left( 1 + \frac{u^{2d}}{(q^{2d} - 1)(q^{2d} - u^{2d})} \right)^{\frac{1}{2}M(d,q)}
\]
which, since $M(d,q) = O(q^{2d})$, converges if
\[
\sum_{d=1}^{\infty} \frac{u^{2d}}{(q^{2d} - 1)(q^{2d} - u^{2d})}
\]
does. This is the case if $|u| < q$.

We have proved that $\mathcal{R}_{U,\omega}(u)$ converges at least in a disc of radius $q$. This is sufficient to establish the following theorem:

**Theorem 5.3.** $\sum_{d=1}^{\infty} (S_{SU(d,q^2)} - S_{U(d,q^2)}) u^d$ is convergent at least in a disc of radius $q$.

In particular, this implies:

**Corollary 5.4.**

\[
S_{SU(\infty,q^2)} = S_{U(\infty,q^2)},
\]

and whenever $0 < r < q$,

\[
|S_{U(d,q^2)} - S_{SU(d,q^2)}| < o(r^d).
\]
Turning next to cyclic transformations, let us define

\[ \hat{R}_\omega(u) := \prod_{f \in \Phi^+_{n^2}, f = f^*} \left( 1 + \sum_{j=1}^{\infty} \frac{\omega^{j \deg f} u^j \deg f}{q^{(j-1) \deg f} (q^{\deg f} + 1)} \right), \]

\[ \hat{S}_\omega(u) := \prod_{\{f, f^*\} \in \Phi^+_{n^2} \setminus f = f^*} \left( 1 + \sum_{j=1}^{\infty} \frac{\omega^{j \deg f} u^j 2 \deg f}{q^{2 \deg f} (q^{2 \deg f} + 1)} \right), \]

\[ \hat{K}_{U, \omega}(u) = \hat{R}_\omega(u) \hat{S}_\omega(u). \] (5)

Then it follows from Corollary 3.8 that

\[ q + \sum_{d=1}^{\infty} C_{SU(d, q^2)} u^d - \sum_{d=1}^{\infty} C_{U(d, q^2)} u^d = \sum_{\omega \in \Omega_{n^2+1}} \hat{K}_{U, \omega}(u). \]

Suppose \( \omega \neq 1 \). By straightforward manipulation,

\[ \hat{R}_\omega(u) = \prod_{f \in \Phi^+_{n^2}, f = f^*} \left( 1 + \frac{\omega^{\deg f} u^{\deg f}}{(q^{\deg f} + 1) \left( 1 - \frac{\omega^{\deg f} u^{\deg f}}{q^{\deg f}} \right)} \right), \]

\[ \hat{S}_\omega(u) = \prod_{\{f, f^*\} \in \Phi^+_{n^2} \setminus f = f^*} \left( 1 + \frac{\omega^{2 \deg f} u^{2 \deg f}}{(q^{2 \deg f} - 1) \left( 1 - \frac{\omega^{2 \deg f} u^{2 \deg f}}{q^{2 \deg f}} \right)} \right). \]

and furthermore, it is easy to obtain from this the fact that

\[ \hat{R}_\omega(u)V_{\omega}^{-\frac{u}{q}} = \prod_{f \in \Phi^+_{n^2}, f = f^*} \left( 1 - \frac{\omega^{\deg f} u^{\deg f}}{q^{\deg f} (q^{\deg f} + 1)} \right), \] (6)

\[ \hat{S}_\omega(u)W_{\omega}^{-\frac{u}{q}} = \prod_{\{f, f^*\} \in \Phi^+_{n^2} \setminus f = f^*} \left( 1 + \frac{\omega^{2 \deg f} u^{2 \deg f}}{q^{2 \deg f} (q^{2 \deg f} - 1)} \right). \] (7)

Recall that if \( f \) is irreducible and \( f = f^* \) then \( \deg f \) is odd. It follows from
(6) that
\[ \hat{R}_\omega(u) V^-_{\omega} \left( \frac{u}{q} \right) = \prod_{f \in \Phi^+_2 \atop f = f^*} \left( 1 + \frac{\omega(f)(-\frac{u}{q})^{\deg f}}{q^{\deg f} + 1} \right) \]
\[ = \overline{R}_\omega \left( \frac{-u}{q} \right), \]
and it can also be seen that
\[ \hat{S}_\omega(u) W^-_{\omega} \left( \frac{u}{q} \right) = \overline{S}_\omega \left( \frac{-u}{q} \right). \]
So, by Identity 4.2,
\[ \hat{K}_{U,\omega}(u) = \overline{K}_{U,\omega} \left( \frac{-u}{q} \right) \quad (8) \]
which converges in a disc of radius \( q^2 \), since we have already established that \( \overline{K}_{U,\omega}(u) \) converges in a disc of radius \( q \). This gives the following theorem:

**Theorem 5.5.** \( \sum_{d=1}^{\infty} (C_{SU(d,q^2)} - C_{U(d,q^2)}) u^d \) is convergent at least in a disc of radius \( q^2 \).

In particular, this implies:

**Corollary 5.6.**
\[ C_{SU(\infty,q^2)} = C_{U(\infty,q^2)}, \]
and whenever \( 0 < r < q \),
\[ |C_{U(d,q^2)} - C_{SU(d,q^2)}| < o(r^{2d}). \]

Finally, we look at semisimple transformations. Define
\[ \tilde{R}_\omega(u) := \prod_{f \in \Phi^+_2 \atop f = f^*} \left( 1 + \sum_{j=1}^{\infty} \frac{\omega^{\deg f}(u)^j}{U(j, q^{2\deg f})} \right), \]
\[ \tilde{S}_\omega(u) := \prod_{\{f, f^*\} \atop f \in \Phi^+_2 \atop f \neq f^*} \left( 1 + \sum_{j=1}^{\infty} \frac{\omega^{\deg f}(u)^j}{GL(j, q^{2\deg f})} \right), \]
\[ \tilde{K}_{U,\omega}(u) = \tilde{R}_\omega(u) \tilde{S}_\omega(u). \]
Then from Corollary 3.8,
\[ q + \sum_{d=1}^{\infty} SS_{U(d,q^2)} u^d - \sum_{d=1}^{\infty} SS_{U(d,q^2)} u^d = \sum_{\omega \in \Omega_{U+1}} K_{U,\omega}(u). \]

Suppose \( \omega \neq 1 \). Then by Identity 4.2,
\[ \tilde{K}_{U,\omega}(u) = A_\omega(u) \tilde{R}_\omega(u) V_{\omega}^+ \left( \frac{u}{q} \right) - 1 \tilde{S}_\omega(u) W_{\omega}^+ \left( \frac{u}{q} \right) - 1. \]

where \( A_\omega(u) \) is as defined at (4) above, and is analytic in a disc of radius \( q \). The product \( \tilde{R}_\omega(u) V_{\omega}^+ \left( \frac{u}{q} \right) \) is equal to
\[ \prod_{f \in \Phi_{+}^*} \left( 1 - \frac{\omega^r(f) u^{\deg f}}{(q^d + 1)(q^d - \omega^r(f) u^{\deg f})} \right) + \left( 1 + \frac{\omega^r(f) u^{\deg f}}{q^{\deg f}} \right)^{-1} \left( \sum_{j=2}^{\infty} \frac{\omega^r(f) u^{j \deg f}}{|U(j, q^2 \deg f)|} \right). \]

We crudely estimate:
\[ \sum_{j=2}^{\infty} \frac{u^{j d}}{|U(j, q^2 \deg f)|} \ll \sum_{j=2}^{\infty} \frac{u^{j d}}{q^{j d}(q^d - 1)^j} = \frac{u^{2d}}{q^{2d}(q^d - 1)^2} \left( \frac{1}{1 - \frac{u^{d}}{q^{d}(q^d - 1)}} \right). \]

Hence by straightforward manipulation,
\[ \tilde{R}_\omega(u) V_{\omega}^+ \left( \frac{u}{q} \right) \ll \prod_{d=1}^{\infty} \left( 1 + \frac{u^{d}}{(q^d + 1)(q^d - u^d)} \right) \sum_{d=1}^{\infty} \frac{q^d u^{d}}{(q^d + 1)(q^d - u^d)} \]
\[ \ll \prod_{d=1}^{\infty} \left( 1 + \frac{u^{2d}}{(q^d - 1)(q^d - u^d)(q^d(q^d - 1) - u^d)} \right) N^*(d,q), \]

which converges if
\[ \sum_{d=1}^{\infty} q^d \frac{u^{d}}{(q^d + 1)(q^d - u^d)} \]
and
\[ \sum_{d=1}^{\infty} q^d \frac{u^{2d}}{(q^d - 1)(q^d - u^d)(q^d(q^d - 1) - u^d)} \]
both converge. This is certainly the case if \( |u| < q \). A very similar argument gives us that \( \tilde{S}_\omega(u) W_{\omega}^+ \left( \frac{u}{q} \right) \) also converges in the disc of radius \( q \). So we have the following theorem:
Theorem 5.7. \( \sum_{d=1}^{\infty} (SS_{SU(d, q^2)} - SS_{U(d, q^2)}) u^d \) is convergent at least in a disc of radius \( q \).

In particular, this implies:

**Corollary 5.8.**

\( SS_{SU(\infty, q^2)} = SS_{U(\infty, q^2)} \),

and whenever \( 0 < r < q \),

\[ |SS_{U(d, q^2)} - SS_{SU(d, q^2)}| < o(r^d). \]

### 6 Analysis of the function \( \delta \)

In this section we analyse the behaviour of the function \( \delta \) (recall Definition 3.6) on the sets of self-dual and non-self-dual irreducible polynomials of degree \( d \).

We introduce the following notation:

\[
\begin{align*}
    n_{d,s} &:= |\{f \in \Phi_{q^2}^+ \mid f = f^*, \delta(f) = s\}|, \\
    m_{d,s} &:= \frac{1}{2}|\{f \in \Phi_{q^2}^+ \mid f \neq f^*, \delta(f) = s\}|.
\end{align*}
\]

In Section 7 we shall require estimates for the variation of \( n_{d,s} \) and \( m_{d,s} \) as \( s \) varies. It happens that exact formulae are obtainable by straightforward methods, and we shall derive them here. This section should perhaps be regarded as a brief diversion; although some of the results given here will be of use later, our principal reason for including them is our belief that these quantities are of intrinsic interest.

Let \( d \) be odd, and let \( f \) be an irreducible polynomial of degree \( d \) over \( \mathbb{F}_{q^2} \). Let \( \alpha \) be a root of \( f \) in \( \mathbb{F}_{q^2} \). Then \( f = f^* \) if and only if \( \alpha \) lies in \( \mathbb{E}_{q^d+1} \), the subgroup of order \( q^d + 1 \) in \( \mathbb{F}_{q^2}^\times \). Recall that the norm map, \( \mathcal{N}_d : \mathbb{F}_{q^d}^\times \to \mathbb{F}_{q^2}^\times \), is a surjective homomorphism. The image of the subgroup \( \mathbb{E}_{q^d+1} \) under \( \mathcal{N}_d \) is \( \mathbb{E}_{q^d} \). Let \( \zeta \) generate \( \mathbb{E}_{q^d} \) as in Definition 3.6. Then it is clear that if \( f = f^* \) then \( \zeta^{\delta(f)} = \mathcal{N}_d(\alpha) \). We define \( e_{d,s} \) to be the number of elements in the pre-image of \( \zeta^s \) which are primitive (as elements of the extension \( \mathbb{F}_{q^d} : \mathbb{F}_{q^2} \)). Then since each such element has \( d \) conjugates, we see that

\[ n_{d,s} = \frac{e_{d,s}}{d}. \] (9)
In order to calculate $e_{d,s}$, let us extend our notation by letting $e_{d,a,s}$ be the number of elements in the pre-image $\mathfrak{N}_d^{-1}(\zeta^s)$ whose minimum polynomial over $\mathbb{F}_{q^2}$ has degree $a$. Then

$$\sum_{a|d} e_{d,a,s} = |\mathfrak{N}_d^{-1}(\zeta^s)| = \frac{q^d + 1}{q + 1}. \quad (10)$$

Now if $a|d$, then the norm maps $\mathfrak{N}_d$ and $\mathfrak{N}_a$ are related by the formula

$$\mathfrak{N}_a(\alpha) = \mathfrak{N}_d(\alpha)^{\frac{q^d - 1}{q^a - 1}} = \mathfrak{N}_d(\alpha)^{\frac{q^d}{q^a - 1}},$$

since

$$\frac{q^{2d} - 1}{q^{2a} - 1} \equiv a \mod q + 1.$$ 

It follows that

$$e_{d,a,s} = \sum_{t \in \mathbb{F}_{q+1}^{\times}} e_{a,t}.$$ 

Let $b$ divide $d$, and let $I_b$ be the image of $\mathbb{E}_{q^b+1}$ under $\mathfrak{N}_d$. By considering the size of the intersection of $\mathbb{E}_{q^b+1}$ and $\mathfrak{N}_d^{-1}(\zeta^s)$, we obtain the following generalization of (10).

$$\sum_{a|b} e_{d,a,s} = \begin{cases} \frac{q^b + 1}{|I_b|} & \text{if } \zeta^s \in I_b, \\ 0 & \text{otherwise.} \end{cases} \quad (11)$$

By straightforward calculation, we see that $|I_b| = \frac{q^b + 1}{\text{hcf}(q + 1, d)}$, and that $\zeta^s \in I_b$ if and only if $\text{hcf}(q + 1, d)$ divides $s$. For convenience, let us define $\chi_b$ by

$$\chi_b = \begin{cases} 1 & \text{if } \text{hcf}(q + 1, d)|s, \\ 0 & \text{otherwise.} \end{cases}$$

(Note here that in order to simplify notation, we shall not generally distinguish between a natural number $n$ and its modular reduction $n + (q + 1)\mathbb{Z}$.) Now for all divisors $b$ of $d$,

$$\sum_{a|b} e_{d,a,s} = \chi_b \text{hcf}(q + 1, \frac{d}{b}) \frac{q^b + 1}{q + 1},$$

and it follows by Möbius Inversion that

$$e_{d,b,s} = \sum_{a|b} \mu(a) \chi_b \text{hcf}(q + 1, \frac{da}{b}) \frac{q^b + 1}{q + 1},$$

16
and in particular, that
\[ e_{d,s} = e_{d,d,s} = \sum_{a \mid d} \mu(a) \chi_{\frac{d}{\gcd(q+1,a)}} q^{\frac{d}{\gcd(q+1,a)}} + 1. \]

Combining this formula with (9) give us the following proposition:

**Proposition 6.1.**
\[ n_{d,s} = \frac{1}{d(q+1)} \sum_{a \mid d} \mu(a) \gcd(q+1,a)(q^{\frac{d}{\gcd(q+1,a)}} + 1). \]

We now consider the behaviour of \( n_{d,s} \) as \( s \) varies.

**Proposition 6.2.** Let \( p \) be prime. Then
\[ n_{d,ps} = \begin{cases} n_{d,s} - \frac{p}{d} & \text{if } p \mid q+1, p \mid d \text{ and } p \nmid s, \\ n_{d,s} & \text{otherwise.} \end{cases} \]

**Corollary 6.3.** Considered as a function of \( s \), the quantity \( n_{d,s} \) is maximized when \( \gcd(q+1,s) = 1 \) and minimized when \( s = 0 \).

To prove Proposition 6.2, suppose \( p \mid s \). If \( a \) is such that \( \gcd(q+1,a) \mid ps \) but \( \gcd(q+1,a) \nmid s \), then it follows that \( p^2 \mid \gcd(q+1,a) \). Thus \( p^2 \mid a \) and so \( \mu(a) = 0 \).

From Proposition 6.1 then, we see that if \( p \mid s \) then \( n_{d,ps} = n_{d,s} \). We may assume therefore that \( \gcd(p,s) = 1 \). We may also assume that \( p \mid \gcd(q+1,d) \), for it is clear from Proposition 6.1 that if \( p \nmid q+1 \) or if \( p \nmid d \) then \( n_{d,ps} = n_{d,s} \). Now, given these assumptions, we may calculate that
\[ n_{d,ps} = \frac{1}{d(q+1)} \sum_{a \mid d} \mu(a) \left( \gcd(q+1,a)(q^{\frac{d}{\gcd(q+1,a)}} + 1) - p \gcd(q+1,a)(q^{\frac{d}{\gcd(q+1,a)}} + 1) \right) \]
\[ = n_{d,s} - \frac{p}{d(q+1)} \sum_{a \mid \frac{d}{\gcd(q+1,a)}} \mu(a) \gcd(q+1,a)(q^{\frac{d}{\gcd(q+1,a)}} + 1) \]
\[ = n_{d,s} - n_{d,s}. \]

This proves the proposition; the corollary follows easily, since \( n_{d,ps} \leq n_{d,s} \).

Now suppose that \( f \) is a monic irreducible polynomial of degree \( d \) over \( \mathbb{F}_{q^2} \), and that \( f \neq f^* \). In this case, \( d \) may be either even or odd. Suppose \( \alpha \) is a
root of $f$. Then we see from Definition 3.6 that $\zeta^{\alpha(f)} = 4q_{d}(\alpha)^{1-q}$. We therefore consider the group homomorphism $H : \mathbb{F}_{q^{d}}^{\times} \rightarrow \mathbb{E}_{q^{d+1}}$ given by

$$H(\alpha) = 4q_{d}(\alpha)^{1-q}.$$

For $s \in \mathbb{Z}_{q+1}$ we define $E_{d,s}$ to be the number of primitive elements of $\mathbb{F}_{q^{d}}^{\times}$ in the pre-image $H^{-1}(\zeta^{s})$. We define $E_{d,s}^{*}$ to be the number of primitive elements in the intersection of $H^{-1}(\zeta^{s})$ with $\mathbb{E}_{q^{d+1}}$. We shall not give details of the calculation of $E_{d,s}$ or $E_{d,s}^{*}$, since in each case the procedure is essentially the same as that for $e_{d,s}$ given above. The relation stated between these values and $m_{d,s}$ is clear.

**Theorem 6.4.**

$$E_{d,s} = \frac{1}{q+1} \sum_{\substack{a|d \\ \text{hcf}(q+1,a)|s}} \mu(a)\text{hcf}(q+1,a)(q^{\frac{2a}{d}} - 1),$$

$$E_{d,s}^{*} = \frac{1}{q+1} \sum_{\substack{a|d \\ \text{hcf}(q+1,2a)|s}} \mu(a)\text{hcf}(q+1,2a)(q^{\frac{2a}{d}} + 1),$$

$$m_{d,s} = \begin{cases} \frac{1}{2d}E_{d,s} & \text{if } d \text{ is even,} \\ \frac{1}{2d}(E_{d,s} - E_{d,s}^{*}) & \text{if } d \text{ is odd.} \end{cases}$$

We state without proof some results similar to Proposition 6.2.

**Proposition 6.5.** Let $p$ be prime. Then

$$E_{d,ps} = \begin{cases} E_{d,s} - pE_{d,p,s} & \text{if } p|q+1, p|d \text{ and } p \nmid s \\ E_{d,s} & \text{otherwise.} \end{cases}$$

Let $d$ be odd. Then except in the case that $q$ is odd, $p = 2$ and $2 \nmid s$,

$$E_{d,ps}^{*} = \begin{cases} E_{d,s}^{*} - pE_{d,p,s}^{*} & \text{if } p|q+1, p|d \text{ and } p \nmid s, \\ E_{d,s}^{*} & \text{otherwise.} \end{cases}$$

The case given as exceptional in Proposition 6.5 is unavoidably so, since when $q$ is odd and $2 \nmid s$ it can be seen easily from Theorem 6.4 that $E_{d,s}^{*} = 0$, whereas $E_{d,2s}$ is non-zero.

Writing this as far as possible in terms of $m_{d,s}$, we get:
Proposition 6.6. 
\[ m_{d,ps} = \begin{cases} 
  m_{d,s} - m_{d,s}^p, & \text{if } p | q + 1, p | d \text{ and } p \nmid s, \text{ and either } p \neq 2 \text{ or } 4 | d, \\
  m_{d,s} - \frac{1}{d} E_{d,s}^p, & \text{if } q \text{ is odd, } p = 2, 2 \nmid s \text{ and } d \equiv 2 \mod 4, \\
  m_{d,s} - \frac{1}{2d} E_{d,2s}^p, & \text{if } q \text{ is odd, } p = 2, 2 \nmid s, \text{ and } d \text{ is odd,} \\
  m_{d,s}, & \text{otherwise.} 
\end{cases} \]

Corollary 6.7. Considered as a function of \( s \), the quantity \( m_{d,s} \) is maximized when \( \gcd(q + 1, s) = 1 \) and minimized when \( s = 0 \).

7 Explicit bounds for cyclic and separable transformations

We shall now derive explicit bounds for the differences \( |S_{U(d,q^2)} - S_{U(d,q^2)}| \) and \( |C_{U(d,q^2)} - C_{SU(d,q^2)}| \). There is a price to be paid for this explicitness, inasmuch as our bounds will not reflect the rates of convergence given in Theorems 5.3 and 5.5. Nonetheless, we believe the results given in this section are good enough for practical purposes, even for fairly small values of \( d \).

We shall assume that \( \omega \neq 1 \). We start by expressing \( K_{U,\omega}(u) \), which we defined at (3), in the form
\[ K_{U,\omega}(u) = \prod_{d=1}^{\infty} \prod_{s \in \mathbb{Z}_{q+1}} \left( 1 + \frac{\omega^s u^d}{q^d + 1} \right)^{n_{d,s}} \left( 1 + \frac{\omega^s u^{2d}}{q^{2d} - 1} \right)^{m_{d,s}}. \]
Let \( n_d \) and \( m_d \) be the smallest values as \( s \) varies of \( n_{d,s} \) and \( m_{d,s} \) respectively. Define
\[ P_{\omega}(u) = \prod_{d=1}^{\infty} \prod_{s \in \mathbb{Z}_{q+1}} \left( 1 + \frac{\omega^s u^d}{q^d + 1} \right)^{n_{d,s}} \left( 1 + \frac{\omega^s u^{2d}}{q^{2d} - 1} \right)^{m_{d}}, \]
\[ Q_{\omega}(u) = \prod_{d=1}^{\infty} \prod_{s \in \mathbb{Z}_{q+1}} \left( 1 + \frac{\omega^s u^d}{q^d + 1} \right)^{n_{d,s} - n_d} \left( 1 + \frac{\omega^s u^{2d}}{q^{2d} - 1} \right)^{m_{d,s} - m_d}. \]
Clearly \( K_{U,\omega}(u) = P_{\omega}(u)Q_{\omega}(u) \). Now if \( a \) is the multiplicative order of \( \omega \), then
\[ P_{\omega}(u) = \prod_{d=1}^{a} \left( 1 - \frac{(-1)^a u^d}{q^d + 1} \right)^{\frac{a+1}{2} n_d} \left( 1 - \frac{(-1)^a u^{2d}}{q^{2d} - 1} \right)^{\frac{a+1}{2} m_d}, \]
\[ Q_{\omega}(u) \ll \prod_{d=1}^{a} \left( 1 + \frac{u^d}{q^d + 1} \right)^{\frac{a+1}{2} n_d} \left( 1 + \frac{u^{2d}}{q^{2d} - 1} \right)^{\frac{a+1}{2} m_d}. \]
It is not hard to show that, since $a \geq 2$,

$$\left(1 + \frac{u^{2da}}{(q^{2d}-1)^a}\right)^{\frac{q+1}{a}} \ll \left(1 + \frac{u^{2da}}{q^{2da}}\right)^{q+1}. $$

Now $(q+1)m_d \leq M(d, q)$ and $(q+1)n_d \leq N^*(d, q)$. So

$$P_\omega(u) \ll \prod_{d=1}^{\infty} \left(1 + \frac{u^{da}}{q^{da}}\right)^{N^*(d, q)} \left(1 + \frac{u^{2da}}{q^{2da}}\right)^{M(d, q)},$$

by Identity 4.2. It is not hard to deduce from this that

$$P_\omega(u) \ll \frac{1 + \frac{u}{q}}{1 - \frac{u}{q^2}}. \quad (12)$$

It is clear that this estimate is very crude; it is analytic only in a disc of radius $\sqrt{q}$, whereas we might expect $P_\omega(u)$ to be analytic at least in a disc of radius $q$. It is possible that a more subtle analysis would give a more realistic estimate.

In particular, we observe that if $q$ is even, then the multiplicative order $a$ of $\omega$ in the calculation above is strictly greater than 2. To take account of this would give a larger radius of analyticity.

We turn now to the function $Q_\omega(u)$. We give two estimates, the first of which is not valid for $q \leq 3$. The second is valid for all $q$, but inferior in most cases. From Propositions 6.1 and 6.4 we observe that

$$n_{d,s} - n_d = O(q^{\frac{d}{2}}),$$

$$m_{d,s} - m_d = O(q^{d}).$$

We also see that

$$N(d, q^{\frac{d}{2}}) = \frac{1}{d}q^{\frac{d}{2}} + O(q^{\frac{d}{2}}),$$

$$N^*(d, q^{\frac{d}{2}}) = \frac{1}{d}q^{\frac{d}{2}} + O(q^{\frac{d}{2}}),$$

$$M(d, q^{\frac{d}{2}}) = \frac{1}{2d}q^{d} + O(q^{\frac{d}{2}}).$$

Let us suppose that $q > 3$. Then there exists a constant $\kappa_q$ such that for all $d$,

$$\sum_{s \in \mathbb{Z}_{q+1}} (n_{d,s} - n_d) \leq \kappa_q N^*(d, q^{\frac{d}{2}}), \quad (13)$$
and
\[ \sum_{s \in \mathbb{Z}_{q+1}} (m_{d,s} - m_d) \leq \frac{q^{2d} - 1}{q^{2d}} \kappa_q M(d, q^{\frac{1}{2}}). \]

(This fails for \( q \leq 3 \) since \( M(1, q^{\frac{1}{2}}) \) turns out to be negative.) We note here that if \( q \) is even we can do better than we have stated, since in this case
\[ n_{d,s} - n_d = O(q^{\frac{1}{2}}), \]
\[ m_{d,s} - m_d = O(q^{\frac{2d}{2}}). \]

where \( b \) is the smallest prime factor of \( q + 1 \). However we shall not pursue this line of argument any further.

It follows from our definition of \( \kappa_q \) that
\[ Q_\omega(u) \ll \prod_{d=1}^{\infty} \left( 1 + \frac{u^d}{q^d} \right)^{\kappa_q N^*(d, q^{\frac{1}{2}})} \left( 1 + \frac{u^{2d}}{q^{2d}} \right)^{\kappa_q M(d, q^{\frac{1}{2}})} \]
\[ = \left( \frac{1 - \frac{u^2}{q^2}}{1 + \frac{u^2}{q^2}} \right)^{\kappa_q} \]
by Identity 4.6. It is not hard to deduce that
\[ Q_\omega(u) \ll \left( \frac{1 + \frac{u}{q}}{1 - \frac{u}{q^{\frac{1}{2}}}} \right)^{\kappa_q}. \]

It follows from the foregoing discussion that
\[ \hat{K}_{U,\omega}(u) \ll \left( \frac{1 + \frac{u}{q}}{1 - \frac{u}{q^{\frac{1}{2}}}} \right)^{\kappa_q + 1}. \]

The corresponding result for cyclic transformations may be deduced from this fact. Recall the definition of \( \hat{K}_{U,\omega}(u) \) given at (5). From (8) we obtain:
\[ \hat{K}_{U,\omega}(u) \ll \left( \frac{1 + \frac{u}{q}}{1 - \frac{u}{q^{\frac{1}{2}}}} \right)^{\kappa_q + 1}. \]

Now since
\[ \sum_{d=1}^{\infty} |S_{SU(d,q)} - S_{U(d,q)}| u^d = \sum_{\omega \in \Omega_{q+1}} \hat{K}_{U,\omega}(u) \]

21
we obtain the following estimates by binomial expansion:

**Theorem 7.1.** Let \( q > 3 \), and let \( \kappa_q \) be a constant such that, for all \( d \), the conditions (13) and (14) are satisfied. Then

\[
|S_{SU(d,q)} - S_{U(d,q)}| \leq q(1 + \frac{1}{q^2})^{\kappa_q + 1}(\kappa_q + 1) \ldots (\kappa_q + d) \frac{d!}{q^{d^2}},
\]

\[
|C_{SU(d,q)} - C_{U(d,q)}| \leq q(1 + \frac{1}{q^2})^{\kappa_q + 1}(\kappa_q + 1) \ldots (\kappa_q + d) \frac{d!}{q^{2d}}.
\]

For our second estimate for \( Q_\omega(u) \) we observe that there exists a constant \( \lambda_q \) such that for all \( d \),

\[
\sum_{s \in \mathbb{Z}_{q+1}} (n_{d,s} - n_d) \leq \lambda_q N(d, q^{\frac{1}{2}}),
\]

and

\[
\sum_{s \in \mathbb{Z}_{q+1}} (m_{d,s} - m_d) \leq \frac{q^{2d} - 1}{q^{2d}} \lambda_q N(d, q).
\]

Now

\[
Q_\omega(u) \ll \prod_{d=1}^{\infty} \left( 1 + \frac{u^d}{q^d} \right)^{\lambda_q N(d, q^{\frac{1}{2}})} \left( 1 + \frac{u^{2d}}{q^{2d}} \right)^{\lambda_q N(d, q)}
\]

\[
= \left( \frac{1 - \frac{u^2}{q^2}}{1 - \frac{u}{q^{\frac{1}{2}}}} \right)^{\kappa_q} \left( \frac{1 - \frac{u^2}{q^2}}{1 - \frac{u}{q}} \right)^{\kappa_q}
\]

by Identity 4.8.

It follows from this and from (12) that

\[
\mathcal{K}_{U,\omega}(u) \ll \frac{1 + \frac{u}{q}}{(1 - \frac{u}{q^{\frac{1}{2}}})^{\lambda_q + 1} (1 - \frac{u^2}{q})^{\lambda_q}}.
\]
From (8) the corresponding result for cyclic transformations is:

$$K_{U,\omega}(u) \ll \frac{1 + \frac{u}{q^2}}{(1 - \frac{u}{q^2})^{\lambda_q+1}} \left(1 - \frac{u^2}{q^2}\right)^{\lambda_q}.$$ 

Now since

$$\sum_{d=1}^{\infty} |S_{SU(d,q)} - S_{U(d,q)}| u^d = \sum_{\omega \in \Omega_{q+1}}^{\omega \neq 1} K_{U,\omega}(u) \ll \frac{q(1 + \frac{u}{q})}{(1 - \frac{u}{q^2})^{\lambda_q+1}} \left(1 - \frac{u^2}{q^2}\right)^{\lambda_q} \ll q(1 + \frac{1}{q^2})(1 - \frac{u}{q^2})^{-2\lambda_q-1},$$

we obtain the following estimates by binomial expansion:

**Theorem 7.2.** Let $q > 3$, and let $\lambda_q$ be a constant such that, for all $d$, the conditions (15) and (16) are satisfied. Then

$$|S_{SU(d,q)} - S_{U(d,q)}| \leq \frac{q(1 + \frac{1}{q^2})(2\lambda_q + 1) \ldots (2\lambda_q + d)}{d! q^{\frac{d}{2}}},$$

$$|C_{SU(d,q)} - C_{U(d,q)}| \leq \frac{q(1 + \frac{1}{q^2})(2\lambda_q + 1) \ldots (2\lambda_q + d)}{d! q^{\frac{d}{2}}}.$$

It remains only to calculate suitable values of $\kappa_q$ and $\lambda_q$. This may be done without difficulty for any given $q$ using the results of Propositions 6.1 and 6.4, and Corollaries 6.3 and 6.7. We shall not attempt to present these calculations here, but we present a table showing the smallest integer values which may be used. It is worth noting that Theorem 7.2 gives better results than Theorem 7.1 in the case $q = 5$.

**References**


23
<table>
<thead>
<tr>
<th>$q$</th>
<th>$\kappa_q$</th>
<th>$\lambda_q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>NA</td>
<td>5</td>
</tr>
<tr>
<td>even, $\geq 4$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>NA</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>11</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>odd, $\geq 13$</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

Smallest integer values for $\kappa_q$ and $\lambda_q$


Pembroke College
Cambridge
CB2 1RF