Derivation of the Cycle Index Formula of the Affine Square($q$) Group Acting on $GF(q)$

Geoffrey Ngovi Muthoka

Pure and Applied Sciences Department
Kirinyaga University, P. O. Box 143-10300, Kerugoya, Kenya

Ireri Kamuti

Department of Mathematics and Actuarial Science
Kenyatta University, P. O. Box 43844-00100, Nairobi, Kenya

Mutie Kavila

Department of Mathematics and Actuarial Science
Kenyatta University, P. O. Box 43844-00100, Nairobi, Kenya

This article is distributed under the Creative Commons by-nc-nd Attribution License. Copyright © 2019 Hikari Ltd.

Abstract

The concept of the cycle index of a permutation group was discovered by [7] and he gave it its present name. Since then cycle index formulas of several groups have been studied by different scholars. In this study the cycle index formula of an affine square($q$) group acting on the elements of $GF(q)$ where $q$ is a power of a prime $p$ has been derived using a method devised by [4]. We further express its cycle index formula in terms of the cycle index formulas of the elementary abelian group $P_q$ and the cyclic group $C_{q-1}$ since the affine square($q$) group is a semidirect product group of the two groups.

Keywords: Cycle index, Affine square($q$) group, Semidirect product group
1 Introduction

[1] The set \( P_q = \{ x + b, \text{ where } b \in GF(q) \} \) forms a normal subgroup of the affine\((q)\) group and the set \( C_{q-1} = \{ ax, \text{ where } a \text{ is a non zero square in } GF(q) \} \) forms a cyclic subgroup of the affine\((q)\) group under multiplication. The semidirect product \( P_q \rtimes C_{q-1} \) form a group known as the affine square\((q)\) group denoted by \( \text{Aff} □(q) \). The elements of \( \text{Aff} □(q) \) are of the form \( \{ ax + bsuchthatb \in GF(q)\text{ and }a\text{ is a non zero square in }GF(q)\} \). In this study we derive the cycle index formula of the affine square\((p)\) group acting on \( GF(q) \) and express it in terms of the cycle index formulas of the elementary abelian group \( P_q \) and the cyclic group \( C_{q-1} \).

2 Preliminary Notes

Definition 2.1. [2] A group \( G \) is said to be a semidirect product group of \( N \) by \( H \) if; \( N \triangleleft G \) and \( H < G \), \( N \cap H = \{ e \} \) and \( NH = G \). We symbolically express this as \( G = N \rtimes H \).

Definition 2.2. [4] The Möbius function of any \( n \in N \) is given by,
\[
\mu(n) = \begin{cases} 
-1 & \text{if } n \text{ is a square free with an odd number of prime factors} \\
0 & \text{if } n \text{ has a squared prime factor} \\
1 & \text{if } n \text{ is a square free with an even number of prime factors.}
\end{cases}
\]

Definition 2.3. [3] The cycle index of the action of \( G \) on \( X \) is the polynomial (say over the rational field \( Q \)) in \( t_1, t_2, \ldots, t_n \) given by;
\[
Z(G) = Z_{G,x}(t_1, t_2, \ldots, t_n) = \frac{1}{|G|} \sum_{g \in G} \{ \text{mon}(g) \}
\]
Note that if \( G \) has conjugacy classes \( K_1, K_2, \ldots, K_m \) with \( g_i \in K_i \) then
\[
Z(G) = \frac{1}{|G|} \sum_{i=1}^{m} |K_i| \text{mon}(g_i).
\]

Theorem 2.4. [6] Let \( x \) be a permutation with cycle type \( (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n) \) then;
\[
\text{i. the number } \pi(x^i) \text{ of cycles of length one in } x^i \text{ is } \sum_{i|l} i\alpha_i.
\]
\[
\text{ii. } \alpha_l = \sum_{i|l} \pi \left( x^i \right) \mu(i) \text{ where } \mu \text{ is the Möbius function.}
\]
3 Main Results

3.1 The cycle index of the affine square(q) group

**Lemma 3.1.** Let \( g \in Aff \square(q) \) be such that \( g \) fixes only one element in \( GF(q) \), then \( C_G(g) = C_{\frac{q-1}{2}} \).

**Proof.** Since the Affine square(q) group acts transitively on \( GF(q) \) [5], then the stabilizers of each of the elements in \( GF(q) \) are conjugate and only intersect at the identity so it is enough to find the centralizer of any one element. The elements of \( Aff \square(q) \) which fix 0 \( \in GF(q) \) are of the form \( \alpha x + 0 \) where \( \alpha \in GF(q) \). This can be written as; \( M = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \).

A general element of \( Aff \square(q) \) is of the form \( \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \) such that \( a \) is a non zero square element of \( GF(q) \) and \( \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} \).

Now, \( \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & -ab + b \\ 0 & 1 \end{pmatrix} \).

For the element \( \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \) to centralize \( \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \) then, \( -ab + b = 0 \), implying \( b(1 - \alpha) = 0 \Rightarrow b = 0 \) or \( \alpha = 1 \).

If \( \alpha = 1 \), then \( \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \) is the identity which is centralized by every element of the group and so the centralizers of \( \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \) are of the form \( \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \) where \( a \) is a non zero square element in \( GF(q) \) thus the centralizer has order \( (q-1) \) which is a cyclic multiplicative group \( C_{\frac{(q-1)}{2}} \) of order \( \frac{(q-1)}{2} \). \( \square \)

**Lemma 3.2.** Let \( g \in Aff \square(q) \) be such that \( g \) does not fix any element in \( GF(q) \), then \( C_G(g) = P_q \).

**Proof.** Since the Affine square(q) group acts transitively on \( GF(q) \) [5], then the stabilizers of each of the elements in \( GF(q) \) are conjugate and only intersect at the identity so it is enough to find the centralizer of any one element. The elements of \( Aff \square(q) \) which do not fix any element of \( GF(q) \) are of the form \( x + \alpha \) where \( \alpha \in GF(q) \). This can be written as; \( M = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \).

A general element of \( Aff \square(q) \) is of the form \( \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \) such that \( a \) is a non zero square element in \( GF(q) \) and \( \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} \).
Geoffrey Ngovi Muthoka, Ireri Kamuti and Mutie Kavila

Now \( \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{a} & \frac{-b}{a} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha a \\ 0 & 1 \end{pmatrix} \).

For the element \( \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \) to centralize \( \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \) then, \( \alpha a = \alpha \), implying \( \alpha(a - 1) = 0 \Rightarrow \alpha = 0 \) or \( a = 1 \).

If \( \alpha = 0 \), then \( \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \) is the identity which is centralized by every element of the group and so the centralizers of \( \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \) are of the form \( \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \) where \( b \in GF(q) \) thus the centralizer has order \( q \) which is the elementary abelian group \( P_q \).

**Theorem 3.3.**

Let \( p > 2 \) be a prime and \( q = p^r \), the cycle index formula of the affine square \( (q) \) group \( G \) acting on the \( q \) elements of \( GF(q) \) is given by;

\[
Z_G(X, X) = \frac{1}{|G|} \left( t_1^{q} + (q - 1) t_0^{q^2} + q \sum_{1 \neq d | \frac{q-1}{2}} \phi(d) t_1^{\frac{q-1}{2}} \right),
\]

where \( |G| = \frac{1}{2}q(q-1) \), \( \phi(d) \) is the Euler’s phi function and \( X \) the \( q \) elements of the \( GF(q) \).

**Proof.**

The elements of the \( Aff_{\square}(q) \) group are partitioned into \( I, \tau_1 \) (the set of elements that fix one element on the field \( GF(q) \)) and \( \tau_0 \) (the set of elements that do not fix any element of \( GF(q) \)). To derive the cycle index formula we need to find the number of \( \tau_0 \) and \( \tau_1 \) elements and the respective cycle types.

Let \( g \in \tau_1 \). Then from Lemma 3.1 \( C_G(g) = C_{\frac{q-1}{2}} \).

\[
\Rightarrow |C^g| = \frac{1}{2}q(q-1) = q
\]

where \( C^g \) is the conjugacy class in \( G \) containing \( g \).

Let \( g \in \tau_0 \), then from Lemma 3.2 \( C_G(g) = P_q \)

\[
\Rightarrow |C^g| = \frac{1}{2}q(q-1) = q - \frac{1}{2}
\]

The subgroup \( N_G \left( C_{\frac{q-1}{2}} \right) = C_{\frac{q-1}{2}} \), implying there are \( \frac{1}{2}q(q-1) = q \) conjugate cyclic groups \( C_{\frac{q-1}{2}} \) in \( G \).

These cyclic groups intersect only at the identity.

Thus;

\[
|\tau_1| = \left( \frac{q-1}{2} - 1 \right) q
\]
We find the number of $\tau_0$ elements by subtracting the number of $\tau_1$ elements and the identity from the order of $G$.

It follows that:

$$|\tau_0| = \left[q \frac{q-1}{2} - \left(\frac{q-1}{2} - 1\right) q - 1\right] = q - 1 \quad (4)$$

Since the length of a conjugacy class of $g \in \tau_0$ is $\frac{q-1}{2}$ from Equation 2 and the number of $\tau_0$ elements are $q - 1$ from 4, then there are two conjugacy classes of elements in $\tau_0$ but each element in $\tau_0$ is of order $q$.

Therefore:

$$Z_{(G,X)} = \frac{1}{|G|} \left(t_1^q + \frac{q-1}{2} \cdot \text{mon}(x_1) + \frac{q-1}{2} \cdot \text{mon}(x_2)
+ q\left( \text{summation of all monomials of the nontrivial elements in cyclic subgroups } C_{\frac{q-1}{2}} \right) \right),$$

where $x_1$ and $x_2$ are representatives of elements in the first and the second conjugacy classes respectively but since all $\tau_0$ are of order $p$ then they will have the same monomial and thus $Z_{(G,X)}$ can be written as:

$$Z_{(G,X)} = \frac{1}{|G|} \left(t_1^q + (q - 1) \cdot \text{monomial of an element in } \tau_0
+ q\left( \text{summation of all monomials of the nontrivial elements in cyclic subgroups } C_{\frac{q-1}{2}} \right) \right)$$

That is,

$$Z_{(G,X)} = \frac{1}{|G|} \left(t_1^q + (q - 1) \cdot \text{mon}(x) + q \sum_{g \in C_{q-1}\backslash \{I\}} \text{mon}(g) \right) \quad (5)$$

where $x_1 \in \tau_0$.

Let $x \in \tau_0$, then $\pi(x) = 0$

It follows from Theorem 2.4 that,

$\pi(x^p) = q$ and

if $l < p$, $\pi(x^l) = 0$

Now if $0 < l < p$ then,

$$\alpha_l = \frac{1}{l} \sum_{i|l} \pi\left(x^\frac{i}{l}\right) \mu(i)$$

$$= \frac{1}{l} \sum_{i|l} 0\mu(i) = 0$$
and
\[
\alpha_p = \frac{1}{p} \sum_{i|p} \pi\left(x^{\frac{i}{p}}\right) \mu(i) \\
= \frac{1}{p} [\pi(x^p) - \pi(x)] \\
= \frac{1}{p} [q - 0] = \frac{q}{p}.
\]

Therefore the resulting monomial is;
\[
t_{\frac{q}{p}}^p
\]  
(6)

If \(g \in \tau_1\), then \(\pi(g) = 1\),
\(\pi(g^d) = q\) where \(d\) is the order of \(g\),
\(\pi(g^l) = 1\) when \(l < d\)

\[
\alpha_l = \frac{1}{l} \sum_{i|l} \pi\left(g^{\frac{i}{l}}\right) \mu(i) \\
= \frac{1}{l} \sum_{i|l} (1) \mu(i) \\
= \frac{1}{l} \sum_{i|l} \mu(i) = 0
\]

\[
\alpha_d = \frac{1}{d} \sum_{i|d} \pi\left(g^{\frac{i}{d}}\right) \mu(i) \\
= \frac{1}{d} \left[ \pi(g^d) \mu(1) + \sum_{1 \neq i|d} \pi\left(g^{\frac{i}{d}}\right) \mu(i) - \pi(g) \right] \\
= \frac{1}{d} \left[ \pi(g^d) - \pi(g) \right] \\
= \frac{1}{d} [q - 1] = \frac{q - 1}{d}
\]

Thus the resulting monomial is;
\[
t_1t_{\frac{d-1}{d}}
\]  
(7)

Substituting for \(\text{mon}(x)\) (in 6) and \(\text{mon}(g)\) (in 7) in Equation 5 we get;
\[
Z(\alpha,X) = \frac{1}{|G|} \left( t_1^q + (q - 1) t_{\frac{q}{p}}^p + q \sum_{1 \neq d|q} \theta(d) t_1 t_{d^{-1}} \right)
\]
Example 3.1.1
Let $p = 5$, $r = 2 \Rightarrow q = 5^2$, $X = GF(25)$ and $|G| = 300$.
Possible values of $d$ are; 2, 3, 4, 6 and 12.
Then
\[ \emptyset (2) = 1, \emptyset (3) = 2, \emptyset (4) = 2, \emptyset (6) = 2 \text{ and } \emptyset (12) = 4. \]
Substituting in Theorem 3.3, we have;
\[ Z_{(Aff \square (25),X)} = \frac{1}{300} \left( t_1^{25} + 24t_5^2 + 25t_1t_2^{12} + 50t_1t_3^8 + 50t_1t_4^6 + 100t_1t_6^2 \right). \]

3.2 Expressing the cycle index of the Affine square(q) group in terms of the cycle index of the elementary abelian group $P_q$ and the cyclic group $C_{q^2-1}$

The equation in Theorem 3.3 can be simplified as;
\[
Z_{(G,X)} = \frac{1}{|G|} \left( t_1^q + (q - 1) t_p^q + q \sum_{1 \neq d \mid \frac{q-1}{2}} \emptyset(d)t_1t_d^{\frac{q-1}{d}} \right)
\]
\[\begin{align*}
&= \frac{1}{q \left(\frac{q-1}{2}\right)} \left( t_1^q + (q - 1) t_p^q \right) + \frac{1}{q \left(\frac{q-1}{2}\right)} \left( qt_1^q + q \sum_{1 \neq d \mid \frac{q-1}{2}} \emptyset(d)t_1t_d^{\frac{q-1}{d}} \right) - \frac{1}{2} t_1^q \\
&= \frac{1}{q-1} Z_{(P_q,X)} + \frac{1}{q-1} \left( t_1^q + \sum_{1 \neq d \mid \frac{q-1}{2}} \emptyset(d)t_1t_d^{\frac{q-1}{d}} \right) - \frac{1}{2} t_1^q \\
&= \frac{1}{q-1} Z_{(P_q,X)} + Z_{(C_{\frac{q^2-1}{2}},X)} - \frac{1}{2} t_1^q \\
&= \frac{1}{\left| C_{\frac{q^2-1}{2}} \right|} Z_{(P_q,X)} + Z_{(C_{\frac{q^2-1}{2}},X)} - \frac{1}{\left| C_{\frac{q^2-1}{2}} \right|} Z_{(1,X)}. \quad (8)
\]

Example 3.2.1
Let $p = 3$, $r = 2 \Rightarrow q = 3^2$, $X = GF(9)$ and $|G| = 36$ and
\[ Z_{(G,X)} = \frac{1}{36} \left( t_1^3 + 8t_3^3 + 9 \sum_{1 \neq d \mid 4} \emptyset(d)t_1t_d^{\frac{8}{d}} \right) \quad \text{(from Theorem 3.3)}
\]
which can be simplified as;

\[ Z_{(G,X)} = \frac{1}{9(4)} \left( t_1^9 + 8t_3^3 \right) + \frac{1}{9(4)} \left( 9t_1^9 + 9 \sum_{d \neq 7} \phi(d)t_1^7 t_3^d \right) - \frac{1}{4} t_1^9 \]

\[ = \frac{1}{4} Z_{(P_9,X)} + Z_{(C_4,X)} - \frac{1}{4} t_1^9 \]

\[ = \frac{1}{4} Z_{(P_9,X)} + Z_{(C_4,X)} - \frac{1}{4} Z_{(1,X)} \text{ (from Equation 8).} \]

Acknowledgements. Supported by National Research Fund; NRF

References


Received: August 3, 2019; Published: September 3, 2019