POWERS IN FINITE ORTHOGONAL AND SYMPLECTIC GROUPS: 
A GENERATING FUNCTION APPROACH

SAIKAT PANJA AND ANUPAM SINGH

Abstract. For an integer $M \geq 2$ and a finite group $G$, an element $\alpha \in G$ is called an $M$-th power if it satisfies $A^M = \alpha$ for some $A \in G$. In this article, we will deal with the case when $G$ is finite symplectic or orthogonal group over a field of order $q$. We introduce the notion of $M^*$-power SRIM polynomials. This, amalgamated with the concept of $M$-power polynomial, we provide the complete classification of the conjugacy classes of regular semisimple, semisimple, cyclic and regular elements in $G$, which are $M$-th powers, when $(M, q) = 1$. The approach here is of generating functions, as worked on by Jason Fulman, Peter M. Neumann, and Cheryl Praeger in the memoir “A generating function approach to the enumeration of matrices in classical groups over finite fields”. As a byproduct, we obtain the corresponding probabilities, in terms of generating functions.

1. Introduction

1.1. Question in the general context. The motivation behind this work dates back to the work of two of the great mathematicians of the last century, A. Borel and E. Waring. Given an element $w \in F_l$ (the free group on $l$ generators), the map associated with $w$ by plugging elements of $G^l$ in $w$, is called a word map. It was proved by A. Borel (in [1]) (and later by Larsen independently in [4]) that given a semisimple algebraic group $G$ and a word map $w : G^l \rightarrow G$, it is a dominant map. The image of $w$ will be denoted as $w(G)$ hereafter. The result due to Borel reveals the surprising result that $w(G)^2 = G$. On the other hand, it was E. Waring, who mentioned in his paper “Meditationes Algebraicae” that, “every natural number is a sum of at most 9 cubes; every natural number is a sum of at most 19 fourth powers; and so on”. These two problems gave rise to the following general question in the context of group theory.

Question 1.1. Given a group $G$ and a word $w$ on $l$ generators, does there exists a $m(w) \in \mathbb{N}$ such that $(w(G))^{m(w)} = G$?

2010 Mathematics Subject Classification. 20G40, 20P05.

Key words and phrases. orthogonal, symplectic, power map.

The first named author has been supported by NBHM PhD scholarship. The second named author is funded by SERB through CRG/2019/000271 for this research.
This question is known as *Waring type problem* in group theory and has attracted an ample amount of attention from mathematicians in the past half-century. Substantial progress has been made and many fundamental questions are solved, using a wide spectrum of tools, including representation theory, probability, and geometry. A recent breakthrough in this direction is the affirmation of Ore’s conjecture (which states that the commutator map corresponding to the word $xyx^{-1}y^{-1} \in F_2$ is surjective in the case of finite non-abelian simple groups), by Liebeck, O’Brien, Shalev and Tiep [15], using the methods from character theory. They proved that if $G$ is any quasisimple classical group over a finite field, then every element of $G$ is a commutator, using character-theoretic results due to Frobenius. In [16], the results about the product of squares in the finite non-abelian simple groups are proved. It was proved that every element of a non-abelian finite simple group $G$ is a product of two squares. For a survey of these results and further problems in the context of group theory, we refer the reader to the excellent survey article due to Shalev [21].

In this article, we will be interested in the map associated with $w = x^M \in F_1$ where $M \geq 2$ is an integer. This is a part of the ongoing project, where we intend to draw a conclusion about the image size of the power maps for finite groups of Lie type. The complete solution to this for the case of $\text{GL}(n, q)$ has been described in [13]. But the existence of a root in the general linear group does not guarantee the existence of a root in the symplectic or orthogonal group. This has been a great motivation behind this work. The asymptotics of the powers in finite reductive groups has been pursued in [12]. Indeed, the authors therein estimate the proportion of regular semisimple, semisimple and regular which are $M$-th powers in the concerned groups, as $q$ tends to infinity.

We will be giving the exact ratio for the symplectic and orthogonal groups over a finite field $F_q$. We restrict ourselves to the case $(M, q) = 1$, as the case $(M, q) \neq 1$ is more intricate and will be followed up in future work. Our main results are Theorem 5.5 (and Theorem 5.6), Theorem 6.3 (and Theorem 6.4), Theorem 7.9 (and Theorem 7.11) concerning generating function for the probability of a separable, semisimple, cyclic, and regular element respectively to be an $M$-th power in symplectic groups (and orthogonal groups). In follow-up work, we will be also looking into the case of power maps in exceptional groups of Lie type.

1.2. **Methodology.** We take the methods of statistical group theory, where generating functions play a key role. Before describing this, note that if $x \in G$ is an $M$-th power, then so are all conjugates of $x$. Hence to solve the question, it is admirable that we first find the conjugacy classes, which are $M$-th powers. The conjugacy class of finite orthogonal and symplectic groups is given by the combinatorial data consisting of self-reciprocal monic polynomials and signed symplectic or orthogonal partitions. The first description of conjugacy classes in these groups was discussed in the paper of Wall (see...
The enumeration for the conjugacy classes is done with the machinery of generating functions along with the results of G. Wall.

Coming back to the viewpoint of statistical group theory, another way of looking into conjugacy classes is via cycle indices, which was introduced by Pólya for the symmetric group in the paper [20]. This can be briefly described as follows. For \( \pi \in S_n \), let \( a_i(\pi) \) denotes the number of \( i \)-cycles in \( \pi \). Recall that in \( S_n \), the number of elements with \( a_i \) many \( i \)-cycles is given by \( n!/\prod_{i=1}^{n} a_i!i^{a_i} \). This along with the Taylor expansion of \( e^z \) gives that

\[
\sum_{n=0}^{\infty} \frac{u^n}{n!} \sum_{\pi \in S_n} \prod_{i} x_i^{a_i(\pi)} = \prod_{m=1}^{\infty} e^{x_m u^m/m}.
\]

Since then the concept of cycle index has been developed for various groups and has been used to derive exemplary results. For example in [7] cycle indices for the finite classical groups more precisely for unitary, symplectic, and orthogonal groups are studied. In the symplectic and in the orthogonal case it is assumed that \( q \) is odd. For the orthogonal groups a mixed cycle index is defined, taking into account both groups \( O^+(n, q) \) and \( O^-(n, q) \) at the same time. In the memoir [8], the authors consider probabilistic properties for classical groups over a fixed finite field of cardinality \( q \) when the rank goes to infinity. The results are about the asymptotics of corresponding probability. These results are very important and already have been used in many contexts, including the design of algorithms in group theory, random generation of simple groups, monodromy groups of curves, and derangements. Similar works have been pursued in an enormous amount of texts and a philomath is suggested to look into [3], [2], [4], [7], [10], [9] to have better understanding of this direction. We will be using these cycle indices for finite orthogonal and symplectic groups, drawn from [10] and some special polynomials to conclude our result. For reasons coming from the theory of cycle indices, the results for orthogonal groups rely on the results about symplectic groups.

1.3. Organization of the paper. Throughout the article \( q = p^a \), a power of a prime. In Section 2, we will be recalling the description of the central objects of this paper, the finite orthogonal and symplectic groups. The key role in calculating the generating functions are played by the conjugacy classes and centralizers of these groups, which will be discussed in Section 3. In Section 4, we introduce the notion of \( M^* \) polynomials and count the number of such polynomials over a finite field. This section has been coupled with examples to have a better understanding of the proposed definitions. Section 5, 6, 7 and 8 are devoted to calculating generating functions for separable, semisimple, cyclic, and regular matrices in symplectic and orthogonal groups respectively. This article is based on a part of Ph.D. thesis of the first named author. A more elaborate versions of the results can be found in [19].
Acknowledgment. The authors thank B. Sury and Amit Kulshrestha for their interest in this work.

2. ORTHOGONAL AND SYMPLECTIC GROUPS

In this section, we briefly recall the orthogonal and symplectic groups over a finite field \( \mathbb{F}_q \), mainly to set the notation for the rest of the paper. The treatment here closely follows that of [8], [26] and [5].

2.1. Orthogonal groups. Let \( V \) be an \( m \)-dimensional vector space over a finite field \( \mathbb{F}_q \). Then there are at most two non-equivalent non-degenerate quadratic forms on \( V \). The orthogonal group consists of elements of \( \text{GL}(V) \) which preserve a non-degenerate quadratic form \( Q \).

When \( m = 2n \) for some \( n \geq 1 \), up to equivalence there are two such forms denoted as \( Q^+ \) and \( Q^- \). These are as follows. Fix \( a \in \mathbb{F}_q \) such that \( t^2 + t + a \in \mathbb{F}_q[t] \) is irreducible. Then the two non-equivalent forms are given by

\[
(1) \quad Q^+(x_1, \ldots, x_m) = x_1x_2 + x_3x_4 + \cdots + x_{2n-1}x_{2n}, \quad \text{and} \\
(2) \quad Q^-(x_1, \ldots, x_m) = x_1^2 + x_1x_2 + ax_2^2 + x_3x_4 + \cdots + x_{2n-1}x_{2n}.
\]

The orthogonal group preserving \( Q^+ \) will be denoted as \( O^+(m, q) \), and the orthogonal group preserving \( Q^- \) will be denoted as \( O^-(m, q) \).

When \( m = 2n + 1 \), for \( q \) even there is only one (up to equivalence) quadratic form, namely \( Q(x_1, \ldots, x_m) = x_1^2 + \sum_{i=1}^{n} x_{2i}x_{2i+1} \) and hence there is only one (up to conjugacy) orthogonal group. If \( q \) is odd, then up to equivalence, there are two non-degenerate quadratic forms. But, these two forms give isomorphic orthogonal groups. We take \( Q(x_1, \ldots, x_m) = x_1^2 + \cdots + x_{m}^2 \). Thus, in case \( m = 2n + 1 \), up to conjugacy, we have only one orthogonal group. This will be denoted as \( O^0(m, q) \).

As it is common in literature, we will use the notation \( O^\varepsilon(m, q) \) to denote any of the orthogonal group above where \( \varepsilon \in \{0, +, -\} \). With respect to an appropriate basis, we will fix the matrices of the symmetric bilinear forms (associated to the quadratic forms \( Q^\varepsilon \)) as follows:

\[
J_0 = \begin{pmatrix} 0 & 0 & \Lambda_n \\ 0 & \alpha & 0 \\ \Lambda_n & 0 & 0 \end{pmatrix}, \quad J_+ = \begin{pmatrix} 0 & \Lambda_n \\ \Lambda_n & 0 \end{pmatrix}, \quad J_- = \begin{pmatrix} 0 & 0 & \Lambda_{n-1} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -\delta & 0 \\ \Lambda_{n-1} & 0 & 0 & 0 \end{pmatrix}
\]
where \( \alpha \in \mathbb{F}_q^\times, \delta \in \mathbb{F}_q \setminus \mathbb{F}_q^2, \) and \( \Lambda_l = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}, \) an \( l \times l \) matrix. Then, the orthogonal group in matrix form is

\[
O^\epsilon(m, q) = \{ A \in \text{GL}(m, q) \mid {}^tA J \epsilon A = J \epsilon \}.
\]

Adapting the notations of [8], we define the type of an orthogonal space as follows.

**Definition 2.1.** The type of an orthogonal space \((V, Q)\) of dimension \(m\) is

\[
\tau(V) = \begin{cases} 
1 & \text{if } m \text{ is odd, } q \equiv 1 \pmod{4}, Q \sim \sum x_i^2, \\
-1 & \text{if } m \text{ is odd, } q \equiv 1 \pmod{4}, Q \sim b \sum x_i^2, \\
\iota^m & \text{if } m \text{ is odd, } q \equiv 3 \pmod{4}, Q \sim \sum x_i^2, \\
(-\iota)^m & \text{if } m \text{ is odd, } q \equiv 3 \pmod{4}, Q \sim b \sum x_i^2,
\end{cases}
\]

where \(\iota \in \mathbb{C}\) satisfies \(\iota^2 = -1\), and \(b \in \mathbb{F}_q \setminus \mathbb{F}_q^2\).

More generally, when \(V\) is orthogonal direct sum \(V_1 \oplus V_2 \oplus \cdots \oplus V_l\), the type is defined by

\[
\tau(V) = \prod_{i=1}^l \tau(V_i).
\]

### 2.2. Symplectic group.

Let \(V\) be a vector space of dimension \(2n\) over \(\mathbb{F}_q\). There is a unique non-degenerate alternating bilinear form on \(V\). We consider the form given by

\[
\langle (x_i)_{i=1}^{2n}, (y_j)_{j=1}^{2n} \rangle = \sum_{j=1}^{n} x_j y_{2n+1-j} - \sum_{i=0}^{n-1} x_{2n-i} y_{i+1}.
\]

The symplectic group is the subgroup of \(\text{GL}(V)\) consisting of those elements which preserve this alternating form on \(V\). By fixing an appropriate basis, the matrix of the form is

\[
J = \begin{pmatrix} 0 & \Lambda_n \\ -\Lambda_n & 0 \end{pmatrix}
\]

where \(\Lambda_n = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}\) and

\[
\text{Sp}(2n, q) = \{ A \in \text{GL}(2n, q) \mid {}^tA J A = J \}.
\]

Since all alternating forms are equivalent over \(\mathbb{F}_q\), the symplectic groups obtained with respect to different forms are conjugate within \(\text{GL}(2n, q)\).
2.3. Main Question. We recall some definitions here. Let $G = \text{Sp}(2n, q)$ or $O'((m, q)$ defined as above where $m = 2n$ or $2n + 1$ depending on $m$ is even or odd. Then, $n$ is the Lie rank of $G$. An element $A \in G$ is said to be

1. **separable** if the characteristic polynomial of $A$ is separable over $\mathbb{F}_q$,
2. **semisimple** if the minimal polynomial of $A$ is separable over $\mathbb{F}_q$,
3. **cyclic** if the minimal polynomial of $A$ is same as the characteristic polynomial of $A$, and,
4. **regular** if the centraliser of $A$ in $G$ has dimension equal to the Lie rank of $G$.

We say an element $g \in G$ is an $M$th power in $G$ or it has $M$th-root in $G$ if the equation $X^M = g$ has a solution. As in [13], we would like to study if separable, semisimple, cyclic or regular elements are $M$th powers. More precisely, we are interested in the generating functions of the following quantities for these groups:

1. $cs_G^M(n, q)$, $css_G^M(n, q)$, $cc_G^M(n, q)$ and $cr_G^M(n, q)$ which denote the ratio of the number of separable, semisimple, cyclic and regular conjugacy class, respectively, of $G$ which are $M$-th power, to the number of all conjugacy classes.
2. $s_G^M(n, q)$, $ss_G^M(n, q)$, $c_G^M(n, q)$ and $r_G^M(n, q)$ which denote the ratio of the number of separable, semisimple, cyclic and regular elements in $G$ which are $M$-th power, with respect to the $|G|$.

Further, the associated generating functions will be defined in the later sections accordingly. The main question here is to determine these generating functions using the canonical forms of elements in these groups.

3. Conjugacy classes in Orthogonal and Symplectic group

As mentioned in the introduction, if an element is an $M$th power, so is the conjugacy class containing that element. Thus, it is necessary that we know the conjugacy classes in detail for these groups. This is achieved using the combinatorial data consisting of monic polynomials, and signed partitions attached to these polynomials. This is the classic work of [26]. We recall briefly the results therein, which will be used further.

**Definition 3.1.** A *symplectic signed partition* is a partition of a number $k$, such that the odd parts have even multiplicity and even parts have a sign associated with it. The set of all symplectic signed partitions will be denoted as $D_{Sp}$.

**Definition 3.2.** An *orthogonal signed partition* is a partition of a number $k$, such that all even parts have even multiplicity, and all odd parts have a sign associated with it. The set of all orthogonal signed partitions will be denoted as $D_O$.

**Example 3.3.**
1. The partition $6^+2^34^2^−3^1^2$ is a symplectic signed partition of 32.
2. The partition $7^+2^−2^7^+3^2^6^1^−2$ is an orthogonal signed partition of 51.
Definition 3.4. The dual of a monic degree \( r \) polynomial \( f(x) \in k[x] \) satisfying \( f(0) \neq 0 \), is the polynomial given by \( f^*(x) = f(0)^{-1}x^rf(x^{-1}) \). The polynomial \( f \) will be called *-symmetric (or self reciprocal) if \( f = f^* \). A monic polynomial \( f(x) \in \mathbb{F}_q[x] \), will be called to be *--irreducible if and only if it does not have any proper self-reciprocal factor.

It can be shown that characteristic polynomial of symplectic or orthogonal matrix is self reciprocal. Indeed if \( \lambda \) is a root of the characteristic polynomial of a symplectic (or orthogonal) matrix, so is \( \lambda^{-1} \). We follow J. Milnor’s terminology [18] to distinguish between the *-irreducible factors of the characteristic polynomials. We call a *-irreducible polynomial \( f \) to be

1. Type 1 if \( f = f^* \) and \( f \) is irreducible polynomial of even degree;
2. Type 2 if \( f = gg^* \) and \( g \) is irreducible polynomial satisfying \( g \neq g^* \);
3. Type 3 if \( f(x) = x \pm 1 \).

According to [20], [22], the conjugacy classes of \( \text{Sp}(2n, q) \) are parameterized by the functions \( \lambda : \Phi \to \mathcal{P}^{2n} \cup \mathcal{D}^n_{\text{Sp}} \), where \( \Phi \) denotes the set of all monic, non-constant, irreducible polynomials, \( \mathcal{P}^{2n} \) is the set of all partitions of \( 1 \leq k \leq 2n \) and \( \mathcal{D}^n_{\text{Sp}} \) is the set of all symplectic signed partitions of \( 1 \leq k \leq 2n \). Such a \( \lambda \) represent a conjugacy class of \( \text{Sp}(2n, q) \) if and only if

1. \( \lambda(x) = 0 \),
2. \( \lambda_{\varphi^*} = \lambda_\varphi \),
3. \( \lambda_\varphi \in \mathcal{D}^n_{\text{Sp}} \) iff \( \varphi = x \pm 1 \) (we distinguish this \( \lambda \), by denoting it \( \lambda^\pm \)),
4. \( \sum_{\varphi} |\lambda_\varphi| \deg(\varphi) = 2n \).

Also from [20], [22], we find out that similar kind of statement is true for the groups \( \text{O}'(n, \mathbb{F}_q) \). The conjugacy classes of \( \text{O}'(n, \mathbb{F}_q) \) are parameterized by the functions \( \lambda : \Phi \to \mathcal{P}^n \cup \mathcal{D}^n_{\text{O}} \), where \( \Phi \) denotes the set of all monic, non-constant, irreducible polynomials, \( \mathcal{P}^n \) is the set of all partitions of \( 1 \leq k \leq n \) and \( \mathcal{D}^n_{\text{O}} \) is the set of all symplectic signed partitions of \( 1 \leq k \leq n \). Such a \( \lambda \) represent a conjugacy class of \( \text{Sp}(2n, q) \) if and only if

1. \( \lambda(x) = 0 \),
2. \( \lambda_{\varphi^*} = \lambda_\varphi \),
3. \( \lambda_\varphi \in \mathcal{D}^n_{\text{O}} \) iff \( \varphi = x \pm 1 \) (we distinguish this \( \lambda \), by denoting it \( \lambda^\pm \)),
4. \( \sum_{\varphi} |\lambda_\varphi| \deg(\varphi) = n \).

Class representative corresponding to given data can be found in [24], [23], [11] and we will mention them whenever needed. We mention the following results about the conjugacy class size (and hence the size of the centraliser) of elements corresponding to given data, which can be found in [26].
Lemma 3.5 ([26], pp. 36). Let \( X \in \text{Sp}(2n, q) \) be a matrix corresponding to the data \( \Delta_X = \{ (\phi, \mu_{\phi}) : \phi \in \Phi_X \subset \Phi \} \). Then the conjugacy class of \( X \) in \( \text{Sp}(2n, q) \) is of size \( \frac{|\text{Sp}(2n, q)|}{\prod_{\phi} B(\phi)} \) where \( B(\phi) \) and \( A(\phi^\mu) \) are defined as follows

\[
A(\phi^\mu) = \begin{cases} 
|U(m_{\mu}, Q)| & \text{if } \phi(x) = \phi^*(x) \neq x \pm 1 \\
|\text{GL}(m_{\mu}, Q)|^{\frac{1}{2}} & \text{if } \phi \neq \phi^* \\
|\text{Sp}(m_{\mu}, q)| & \text{if } \phi(x) = x \pm 1, \mu \text{ odd} \\
|q^{\frac{1}{2}m_{\mu}} \text{O}^\epsilon(m_{\mu}, q)| & \text{if } \phi(x) = x \pm 1, \mu \text{ even}
\end{cases}
\]

where \( \epsilon \) gets determined by the sign of the corresponding partition, \( Q = q^{\phi}, m_{\mu} = m(\phi^\mu) \) and

\[
B(\phi) = Q^{\sum_{\nu<\mu} \mu m_{\nu} + \frac{1}{2} \sum_{\nu} (\mu - 1) m_{\nu}^2} \prod_{\mu} A(\phi^\mu).
\]

Lemma 3.6 ([26], pp. 39). Let \( X \in \text{O}'(n, q) \) be a matrix corresponding to the data \( \Delta_X = \{ (\phi, \mu_{\phi}) : \phi \in \Phi_X \subset \Phi \} \). Then the conjugacy class of \( X \) in \( \text{O}'(n, q) \) is of size \( \frac{|\text{Sp}(2n, q)|}{\prod_{\phi} B(\phi)} \) where \( B(\phi) \) and \( A(\phi^\mu) \) are defined as before, except when \( \phi(x) = x \pm 1 \),

\[
A(\phi^\mu) = \begin{cases} 
|\text{O}'(m_{\mu}, q)| & \text{if } \mu \text{ odd} \\
q^{\frac{1}{2}m_{\mu} |\text{Sp}(m_{\mu}, q)|} & \text{if } \mu \text{ even}
\end{cases}
\]

where \( \epsilon' \) in \( \text{O}'(m_{\mu}, q) \) gets determined by the corresponding sign of the part, of the partition.

With all the basic tools now in place, we are ready to move to the next section, where we determine when a matrix \( A \) whose characteristic polynomial is a \( \ast \)-irreducible polynomial of type 1 or 2, is an \( M \)-th power. This information is further used in subsequent chapters to determine the desired generating functions, with the help of the concept of central join of two matrices, following [24], [23].

4. \( M \)-POWER AND \( M^\ast \)-POWER POLYNOMIAL

In [13], the concept of \( M \)-power polynomial has been introduced, which plays a crucial role of identifying matrices of \( \text{GL}(n, q) \) which are \( M \)-th powers, in terms of the combinatorial data. We will be encountering another kind of polynomials, which are irreducible factors of characteristic polynomials for identifying matrices in \( \text{Sp}(2n, q), \text{O}'(n, q) \).
4.1. Special polynomials.

Lemma 4.1. (1) Each Self reciprocal irreducible monic (SRIM) polynomial of degree $2n$ ($n \geq 1$) over $\mathbb{F}_q$ is a factor of the polynomial

\[
H_{q,n}(x) := x^{2^n} - 1 \in \mathbb{F}_q[x],
\]

(2) Each irreducible factor of degree $\geq 2$ of $H_{q,n}(x)$ is a SRIM-polynomial of degree $2d$, where $d$ divides $n$ such that $\frac{n}{d}$ is odd.

Example 4.2. (1) The SRIM polynomials of degree 4 over $\mathbb{F}_5$, are factors of $x^{26} - 1 \in \mathbb{F}_5[x]$. Using [25], it can be found out that in $\mathbb{F}_5[x]$, we have $x^{26} - 1 = (x + 1)(x + 4)(x^4 + x^3 + 4x^2 + x + 1)(x^4 + 2x^3 + 2x + 1)(x^4 + 2x^3 + x^2 + 2x + 1)(x^4 + 3x^3 + 3x + 1)(x^4 + 3x^3 + x^2 + 3x + 1)(x^4 + 4x^3 + 4x^2 + 4x + 1)$. This gives all the SRIM polynomial of degree 4 over $\mathbb{F}_5$.

(2) Also using [25], we have that in $\mathbb{F}_2[x]$ the polynomial $x^{26+1} - 1$ factorizes as $(x + 1)(x^4 + x^3 + x^2 + x + 1)(x^{12} + x^8 + x^7 + x^6 + x^5 + x^4 + 1)(x^{12} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1)(x^{12} + x^{11} + x^9 + x^7 + x^6 + x^5 + x^3 + x + 1)(x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$. This gives all the SRIM polynomial of degree 12 over $\mathbb{F}_2$.

Definition 4.3. A SRIM polynomial $f \in \mathbb{F}_q[x]$ of degree $2k$, $k \geq 1$, is said to be an M*-power SRIM polynomial if and only if $f(x^M)$ has a SRIM factor $g \in \mathbb{F}_q[x]$, of degree $2k$. Denote the set of M*-power SRIM polynomial (of degree $\geq 2$) by $\Phi^*_{M}$.

Definition 4.4. [13] A monic irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree $k$, $k \geq 1$, is said to be an M-power polynomial if and only if $f(x^M)$ has a monic irreducible factor $g \in \mathbb{F}_q[x]$, of degree $k$. Denote the set of M-power polynomial (≠ x) by $\Phi^*_{M}$.

Example 4.5. (a) Consider $\mathbb{F}_5$ and the polynomial $x^4 + 3x^3 + 3x + 1 \in \mathbb{F}_5[x]$. Then $x^8 + 3x^6 + 3x^2 + 1 = (x^4 + 2x^3 + x^2 + 2x + 1)(x^4 + 3x^3 + x^2 + 3x + 1)$. Hence $x^4 + 3x^3 + 3x + 1$ is a 2*-power SRIM polynomial.

(b) Consider $\mathbb{F}_5$ and the polynomial $x^4 + 3x^3 + 1x^2 + 3x + 1 \in \mathbb{F}_5[x]$. Then $x^8 + 3x^6 + x^4 + 3x^2 + 1 = (x^4 + 2x^3 + x^2 + 3x + 1)(x^4 + 3x^3 + x^2 + 2x + 1)$. Thus it is a 2-power polynomial but not a 2*-power SRIM polynomial.

Proposition 4.6. Let $N^*_M(q, 2k)$ denotes the number of M*-power SRIM polynomial of degree $2k$, $k \geq 1$. Then

\[
N^*_M(q, 2k) = \frac{1}{2k(M, q^{2k} - 1)} \sum_{\substack{l \text{ odd} \ \lvert \ 2k}} \mu(l)(M(q^{2k/l} - 1), q^k + 1).
\]
Proof. Let $f$ be an $M^*$-power SRIM polynomial of degree $2k$. Then $f(x^M)$ has a SRIM factor $g$ of degree $2k$. Consider $f, g \in \mathbb{F}_{q^2k}$. Then $f = \prod_{i=1}^{2k} (x - \alpha_i), g = \prod_{i=1}^{2k} (x - \beta_i)$. As discussed before, without loss of generality we may assume that $\beta_i^M = \alpha_i$. Considering the map $\theta_M : \mathbb{F}_{q^2k} \rightarrow \mathbb{F}_{q^2k}$, we have $\alpha_i \in \text{im}(\theta_M)$, for all $i$. Since $f$ is SRIM, using Lemma 4.1 we have that $\alpha_i^{q^k+1} = 1$ for all $i$. Thus $\beta_i$ for all $i$, satisfies $\beta_i^{M(q^k-1)} = \beta_i^{q^k+1} = 1$ and $\beta_i^M = \alpha_i$ generates $\mathbb{F}_{q^{2k}}$ over $\mathbb{F}_q$.

Conversely suppose $\alpha$ satisfies that, $\alpha^{q^k+1} = 1$ and generates $\mathbb{F}_{q^{2k}}$ over $\mathbb{F}_q$. If $\varphi$ is the monic minimal polynomial of $\alpha$, then $\varphi$ is of degree $2k$. Also if $\eta$ is any root of $\varphi$, then $\eta = \alpha^l$, for some $l$, whence $\eta^{q^k+1} = 1$. Thus $\varphi$ is SRIM. So, if $N_M^*(q, 2k)$ denotes the number of $M^*$-power SRIM polynomial of degree $2k$, then

$$N_M^*(q, 2k) = \frac{1}{2k} |\{\alpha \in \mathbb{F}_{q^2k} : \alpha^{q^k+1} = 1, \alpha = \theta_M(\eta) \text{ for some } \eta \in \mathbb{F}_{q^{2k}}, \mathbb{F}_{q^{2k}} = \mathbb{F}_q(\alpha)\}|,$$

as sets of roots, of distinct irreducible polynomials, are disjoint. Since $|\theta_M^{-1}(1)| = (M, q^{2k} - 1)$, we have that,

$$N_M^*(q, 2k) = \frac{1}{2k(M, q^{2k} - 1)} |\{\alpha \in \mathbb{F}_{q^{2k}} : \alpha^{q^k+1} = 1, \mathbb{F}_{q^{2k}} = \mathbb{F}_q(\alpha^M)\}|.$$

To ensure $\mathbb{F}_{q^{2k}} = \mathbb{F}_q(\alpha^M)$, we should have that $\alpha^M \not\in \mathbb{F}_q^l$ for any $l|2k, l > 1$. Since $\alpha^{q^k+1} = 1$, we have that $\alpha^q + 1$ if and only if $l$ is odd (because $x^m + 1$ divides $x^n + 1$ if and only if $\frac{n}{m}$ is odd). Thus $\alpha^M \in \mathbb{F}_{q^{2k/l}}$ if and only if $l$ is odd. For $l$ odd, define $E_l = \{\alpha \in \mathbb{F}_{q^{2k}} : \alpha^{q^k+1} = 1, \mathbb{F}_{q^{2k/l}} = \mathbb{F}_q(\alpha^M)\}$. Then $|E_l| = (M(q^{2k/l} - 1), q^{k+1})$, whence by inclusion-exclusion principle the proof is done.

This settles down the case, when a single block is an $M$-power. Now let us proceed for the case when there are more than one block of same type.

Example 4.7. We can show that, if $A$ is a matrix corresponding to the conjugacy class data $(x^{12} + 2x^{11} + 2x^{10} + 2x^9 + x^8 + x^6 + x^4 + 2x^3 + 2x^2 + 2x + 1, 1)$ in $\text{Sp}(12, \mathbb{F}_3)$, then $A^{73}$ has conjugacy class data $(x^4 + x^3 + x^2 + x + 1, 1^3)$.

Now we consider the case when $A$ has more than one block of type 1 but is an $M$-th power of some $\alpha$. Since we are interested in the image of the map $x \mapsto x^M$, we will be considering the case when any $M$-th root of $A$ (if exists) has single Jordan block of type 1. Thus if minimal polynomial of $A$ (of degree $\frac{2n}{k}$ for some odd $k$), has root $\gamma$, we must have that $M$-th root of $\gamma$ must exist in $\mathbb{F}_{q^{2n}}$ and not in any proper subfield of $\mathbb{F}_{q^{2n}}$. Thus we want to calculate the number of SRIM polynomials of degree $\frac{2n}{k}$, over $\mathbb{F}_q$ such that if $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}_{q^{2n}}$, then there exists $\beta \in \mathbb{F}_{q^{2n}}$ such that $\min_{\mathbb{F}_q}(\beta)$ is SRIM.
polynomial of order \(2n\). Let \(N_M^*(q, 2n, \frac{2n}{k})\) denotes the number of SRIM polynomial of degree \(\frac{2n}{k}\) such that if \(f(\alpha) = 0\) for some \(\alpha \in \mathbb{F}_{q^{2n}}\), then any \(M\)-th root of \(\alpha\), say \(\beta\), lies in \(\mathbb{F}_{q^{2n}}\) with the property that \(\mathbb{F}_{q^{2n}} = \mathbb{F}_q[\beta]\) and \(\beta^{q^n+1} = 1\).

**Proposition 4.8.** We have \(N_M^*(q, 2n, \frac{2n}{k})\) to be equal to

\[
\frac{1}{2k} \sum_{s < k, s = \text{odd}, s|k} \mu(s) \frac{1}{(M, q^{\frac{2n}{s}} - 1)} \left( \sum_{l = \text{odd}, l|\frac{2n}{s}} \mu(l) \left( M \left( q^{\frac{n}{l}} + 1 \right), q^{\frac{n}{l}} + 1 \right) \right).
\]

**Proof.** For \(k\) odd and \(k|2n\), consider the set

\[
E_{2n, \frac{2n}{k}} = \left\{ \alpha \in \mathbb{F}_{q^{2n}} \mid \alpha^{\frac{2n}{k}} + 1 = 1, \alpha = \beta^M, \beta \in \mathbb{F}_{q^{2n}}, \beta^{q^n+1} = 1, [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \frac{2n}{k} \right\}.
\]

To enumerate this set let us find the number of \(\beta \in \mathbb{F}_{q^{2n}}\), such that \(\beta^M \in E_{2n, \frac{2n}{k}}\). Then \(\beta\) satisfies the equations \(\beta^{q^n+1} = 1, \beta^{M(\frac{2n}{s})+1} = 1\). Number of \(\beta\) satisfying these two equations is given by \((M(q^{\frac{n}{l}} + 1), q^n + 1)\). But we should have that \([\mathbb{F}_q(\beta^M) : \mathbb{F}_q] = \frac{2n}{k}\). Hence \(\beta^M \notin \mathbb{F}_{q^{\frac{2n}{s}}}, l > 1\) being odd. Hence by inclusion-exclusion principle, the number of \(\beta \in \mathbb{F}_{q^{2n}}\), such that \(\beta^M \in E_{2n, \frac{2n}{k}}\) is \(\sum_{l = \text{odd}, l|\frac{2n}{s}} \mu(l) \left( M \left( q^{\frac{n}{l}} + 1 \right), q^n + 1 \right)\). Since \(|\theta_M^{-1}(1)| = (M, q^{2n} - 1)\) where \(\theta_M : \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^{2n}}\) is the map \(\theta_M(x) = x^M\), we have that

\[
|E_{2n, \frac{2n}{k}}| = \frac{1}{(M, q^{2n} - 1)} \sum_{l = \text{odd}, l|\frac{2n}{s}} \mu(l) \left( M \left( q^{\frac{n}{l}} + 1 \right), q^n + 1 \right).
\]

Now we want to consider only those \(\alpha \in E_{2n, \frac{2n}{k}}\) such that it doesn’t have any \(M\)-th root in any proper subfield of \(\mathbb{F}_{q^{2n}}\). Since an \(M\)-th root, say \(\beta\), also has minimal polynomial to be SRIM (by hypothesis), we have that \(\beta \in \mathbb{F}_{q^{\frac{2n}{s}}}\) if and only if \(s\) is odd. Hence \(\beta \in E_{2n, \frac{2n}{k}} \setminus \bigcup_{s = \text{odd}, s|\frac{2n}{k}} E_{2n/s, \frac{2n}{k}}\). Thus we have that

\[
N_M^* \left( q, 2n, \frac{2n}{k} \right) = \frac{1}{2k} \sum_{s < k, s = \text{odd}, s|\frac{2n}{k}} \mu(s) \frac{1}{(M, q^{\frac{2n}{s}} - 1)} \sum_{l = \text{odd}, l|\frac{2n}{s}} \mu(l) \left( M \left( q^{\frac{n}{l}} + 1 \right), q^{\frac{n}{l}} + 1 \right),
\]

since the sets of roots of irreducible polynomials are disjoint. \(\square\)

**Definition 4.9.** For a divisor \(k\) of \(n\), we will call a polynomial \(f(x) \in \mathbb{F}_q[x]\) of degree \(\frac{n}{k}\) which is not an \(M\)-power polynomial, to be **degenerate** \((M, n, \frac{n}{k})\) polynomial if and only if minimal polynomial of \(\beta\) over \(\mathbb{F}_q\) is of degree \(n\), where \(f(\beta^M) = 0\). Denote the set of degenerate \((M, n, \frac{n}{k})\) polynomials \((\neq x)\) by \(\Phi_{M,n,\frac{n}{k}}^u\). Denote by \(\Phi_{M,n,\frac{n}{k}}^{u*}\) the subset of SRIM polynomials having same property.
Lemma 4.13. Let $e$ the exponent is unique data attached to the polynomial $f$ of degree 2, which is defined to be the multiplicative order of a root of $f$. Then minimal polynomial of $f$ should not divide any $q^e - x$. Hence note that a root of $f$ is odd. Since we are considering SRIM polynomials, by inclusion-exclusion we have that number of primitive elements in $F_{q^n}$ of exponent $e$ is

Remark 4.10. The quantity $N_M^*(q, 2n, \frac{2n}{k})$ counts the number of degenerate $(M, 2n, \frac{2n}{k})$ SRIM polynomials over $\mathbb{F}_q$.

Remark 4.11. We have that $N_M^*(q, 2r) = N_M^*(q, 2r, 2r)$.

In case a polynomial is degenerate $(M, n, \frac{n}{r})$ polynomial, there are $M$-th roots of $\alpha$, where $f(\alpha) = 0$, which lies in $\mathbb{F}_{q^n}$ and not in any proper subfield of it. But there might be other $M$-th roots which lie in other extensions, as illustrated by the following examples.

Example 4.12. Using $[25]$, we have that $x^{132} + 2x^{77} + x^{66} + 2x^{55} + 1 = (x^{12} + x^{11} + x^{10} + x^9 + 2x^6 + x^3 + x^2 + x + 1)(x^{60} + x^{58} + 2x^{57} + 2x^{56} + 2x^{55} + 2x^{54} + 2x^{53} + x^{51} + x^{49} + x^{48} + 2x^{46} + x^{44} + x^{43} + 2x^{42} + x^{41} + x^{40} + x^{39} + x^{38} + 2x^{36} + x^{34} + x^{32} + 2x^{31} + x^{30} + x^{27} + x^{26} + 2x^{25} + x^{23} + 2x^{21} + 2x^{19} + x^{17} + x^{16} + x^{15} + x^{13} + 2x^{11} + 2x^7 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 1)(x^{60} + 2x^{59} + 2x^{58} + 2x^{57} + 2x^{56} + 2x^{55} + 2x^{54} + 2x^{53} + 2x^{52} + 2x^{49} + x^{47} + x^{45} + x^{44} + x^{43} + 2x^{41} + 2x^{39} + x^{37} + 2x^{35} + x^{34} + x^{33} + x^{30} + 2x^{29} + x^{28} + x^{26} + 2x^{24} + x^{22} + x^{21} + x^{20} + x^{19} + 2x^{18} + 2x^{17} + x^{16} + x^{15} + 2x^{14} + x^{12} + 2x^{11} + x^{9} + 2x^{7} + 2x^{6} + 2x^{5} + 2x^{4} + 2x^{3} + x^{2} + 1)$ in $\mathbb{F}_3[x]$. Hence note that a root of $x^{12} + 2x^{11} + x^6 + 2x^5 + 1$ has 11-th root in different degree field extensions.

Now assume that $f(\beta^M) = 0$ for some $\beta \in \mathbb{F}_{q^k}$, where $f \in \mathbb{F}_{q^n}[x]$ is a SRIM polynomial of degree 2n. Then minimal polynomial of $\beta$ must divide $f(x^M)$. Hence to determine all possible k, we should know about the irreducible factors of $f(x^M)$. From [6] we know that the irreducible factors of $f(x^M)$ solely depends on the degree and the exponent of the irreducible polynomial, which is defined to be the multiplicative order of a root of $f$ is the splitting field of $f$. Since all the roots are conjugate to each other, we have that the exponent is unique data attached to the polynomial $f$. This necessitates to find the number of irreducible polynomial which has exponent $e$. We have the following.

Lemma 4.13. Let $N_M^*(q, 2n, e)$ denotes the number of SRIM polynomials of degree 2n and exponent $e$ which are not $M$-power SRIM polynomial. Then we have

$$N_M^*(q, 2n) = \frac{1}{2n} \sum_{l=odd \ n \ | \ 2n} \mu(l)\phi(e) - \frac{1}{2n(M, q^{2n} - 1)} \sum_{l=odd \ n \ | \ 2n} \mu(l)(M(q^{2n}/l - 1), e).$$

Proof. Let us first find out number of SRIM polynomials of degree 2n and exponent $e$ in $\mathbb{F}_q[x]$. Note that $e$ must divide $q^n + 1$ as $\alpha^{q^n + 1} = 1$ (by Lemma 4.1). Since $\mathbb{F}_{q^{2n}}$ is cyclic group the number of elements of order $e$ is given by $\phi(e)$. But we want to have that such an element should not belong to any proper subfield of $\mathbb{F}_{q^{2n}}$ i.e. $e$ should not divide any $q^\frac{n}{l} + 1$ where $l$ is odd. Since we are considering SRIM polynomials, by inclusion-exclusion we have that number of primitive elements in $\mathbb{F}_{q^{2n}}$ of exponent $e$ is...
POWERS IN FINITE ORTHOGONAL AND SYMPLECTIC GROUPS

\[ \sum_{\substack{l \text{ odd} \\mod 2n}} \mu(l)\phi(e), \text{ whence number of irreducible polynomials of degree } 2n \text{ and exponent } e \]

in \( \mathbb{F}_q[x] \) is \( \frac{1}{2n} \sum_{\substack{l \text{ odd} \\mod 2n}} \mu(l)\phi(e) \).

Next we find out the number of \( M^* \)-power SRIM polynomial of degree \( 2n \) and exponent \( e \). As in the remarks preceding 4.6, replacing \( \alpha^{q^n+1} = 1 \) by the condition \( \alpha^{e} = 1 \), we have that number of \( M^* \)-power SRIM polynomial of degree \( 2n \) and exponent \( e \) is

\[ \frac{1}{2n(M,q^{2n} - 1)} \sum_{\substack{l \text{ odd} \\mod 2n}} \mu(l)(M(q^{2n/l} - 1), e). \]

Hence the result follows. \( \square \)

By similar line of arguments and the fact that \( x \in \mathbb{F}_{q^n} \) if and only if \( x^{q^n - 1} = 1 \), we have the following lemmas, which will help us in counting. These are some generalized results of [13], proof of which are as same as above.

**Lemma 4.14.** Let \( N_M(q,k) \) denotes the number of \( M \)-power polynomial of degree \( k \). Then

\[ (4.5) \quad N_M(q,k) = \frac{1}{k(M,q^k - 1)} \sum_{l|k} \mu(l)(M(q^{k/l} - 1), q^k - 1). \]

**Lemma 4.15.** Let \( k|n \) and \( N_M(q,n \frac{n}{k}) \) denotes the number of irreducible monic polynomial \( f \) over \( \mathbb{F}_q \) of degree \( \frac{n}{k} \), such that any \( M \)-th root of \( \alpha \) (where \( f(\alpha) = 0 \)) lies in \( \mathbb{F}_q^{n} \), but not in any proper subfield of \( \mathbb{F}_q^{n} \). Then

\[ (4.6) \quad N_M(q,n \frac{n}{k}) = \frac{1}{k} \sum_{s \in \mathbb{F}_q^{n \frac{n}{k}}} \frac{1}{(M,q^{n/s} - 1)} \sum_{l|\frac{n}{s}} \mu(l) \left( M \left( q^{\frac{n}{s}} - 1 \right), q^n - 1 \right). \]

**Lemma 4.16.** Let \( N_M(q,n) \) denotes the number polynomials of degree \( n \) and exponent \( e \) which are not \( M \)-power polynomial. Then we have

\[ N_M(q,n) = \frac{1}{n} \sum_{l|n} \mu(l)\phi(e) - \frac{1}{n(M,q^n - 1)} \sum_{l|2n} \mu(l)(M(q^{n/l-1}), e). \]

Let \( R_M^*(q,2n) \) denotes the number of pairs \( \{\phi, \phi^*\} \), where \( \phi (\neq \phi^*) \) is an irreducible monic polynomial of degree \( n \geq 2 \) and \( \phi \) is an \( M \)-power polynomial. Then

\[ R_M^*(q,2n) = \begin{cases} \frac{1}{2} N_M(q,n) & \text{if } n \text{ is odd} \\ \frac{1}{2} \left( N_M(q,n) - N_M^*(q,n) \right) & \text{if } n \text{ is even} \end{cases} \]

Let \( k|n \) and \( R_M^*(q,2n \frac{2n}{k}) \) denotes the number of pairs \( \{\phi, \phi^*\} \), where \( \phi (\neq \phi^*) \) is an irreducible monic polynomial \( f \) over \( \mathbb{F}_q \) of degree \( \frac{n}{k} \), such that any \( M \)-th root of \( \alpha \) (where
\( f(\alpha) = 0 \) lies in \( \mathbb{F}_{q^n} \), but not in any proper subfield of \( \mathbb{F}_{q^n} \). Then

\[
R^*_M(q, 2n, \frac{2n}{k}) = \begin{cases} 
\frac{1}{2} (N_M(q, n, n/k) - N^*_M(q, n, n/k)) & \text{if } n \text{ is even, } k \text{ is odd} \\
\frac{1}{2} N_M(q, n, n/k) & \text{otherwise}
\end{cases}
\]

Let \( R^*_M(q, 2n) \) denotes the number of pairs \( \{\phi, \phi^*\} \), where \( \phi (\neq \phi^*) \) is an irreducible polynomial of degree \( n \geq 2 \), which is not an \( M \)-power polynomial. Then we have

\[
R^*_M(q, 2n) = \begin{cases} 
\frac{1}{2} N^e_M(q, n) & \text{if } n \text{ is odd} \\
\frac{1}{2} (N^e_M(q, n) - \frac{1}{m(M, q^n - 1)} \sum_{l|k} \mu(l)(Mq^e, q^n + 1)) & \text{if } n \text{ is even}
\end{cases}
\]

With the counting in hand we now move to next section, where we calculate the generating functions in the indeterminate \( u \).

4.2. Auxiliary results. Before proceeding further, we note down the following lemma, which helps in defining the indicator function (see 4.23) corresponding to a class of irreducible polynomials having same degree and exponent.

**Lemma 4.17.** Let \( f_1, f_2 \in \mathbb{F}_q[x] \) be monic irreducible polynomials of degree \( n \) and exponent \( e \). Then \( f_1(x^M) \) has a SRIM factor of degree \( 2l \) if and only if \( f_2(x^M) \) has a SRIM factor of degree \( 2l \).

**Proof.** Since \( f_1 \) and \( f_2 \) are of same degree and same exponent, by [6] the roots of \( f_1(x^M) \) and \( f_2(x^M) \) have same order. Hence the result follows from Lemma 4.1. \( \square \)

**Lemma 4.18.** Let \( f = gg^* \) be a type 2 polynomial. Then all irreducible factors of \( g(x^M) \) are of type 2.

**Proof.** On the contrary if possible let \( h \) be a type 1 polynomial, which is an irreducible polynomial of degree \( 2m \). Let \( \alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_1^{-1}, \alpha_2^{-1}, \ldots, \alpha_n^{-1} \) be a set of roots of \( h \) in the splitting field of \( h \). Then \( \alpha_1^M, \alpha_2^M, \ldots, \alpha_n^M, \alpha_1^{-M}, \alpha_2^{-M}, \ldots, \alpha_n^{-M} \) are roots of \( g \). Then as in Lemma 5.1, these elements are the only roots of \( g \). Now if for all \( 1 \leq i \leq n \), \( \alpha_i^M \neq \alpha_i^{-M} \), then \( g \) will be a self-reciprocal polynomial. Hence there exists \( j \) such that \( \alpha_j^M = \alpha_j^{-M} \), which implies that \( \alpha_j^M = \pm 1 \). This is a contradiction, since \( \pm 1 \) are not roots of \( g \). \( \square \)

**Corollary 4.19.** Let \( f = gg^* \) be a type 2 polynomial of degree \( 2n \). Then \( \alpha^M = C_f \) has a solution in \( Sp(2n, q) \) if and only if \( g \) is an \( M \)-power polynomial.

**Proof.** Follows from the same line of proof as of Lemmas 5.1 and 5.2. \( \square \)

**Lemma 4.20.** Let \( f \) be a type 1 polynomial. Then all irreducible factors of \( f(x^M) \) are of type 1.
Proof. If possible, on contrary assume the $h = gg^*$ is a factor of $f(x^M)$ of type 2. Then there exists a root $\alpha$ of $g$ such that $\alpha^{-1}$ is not a root of $g$. As in Lemma 5.1, if $\Lambda = \{\alpha = \alpha_1, \alpha_2, \ldots, \alpha_k\}$ are roots of $g$, we get that the only roots of $f$ are $\Lambda^M = \{\alpha^M_1, \alpha^M_2, \ldots, \alpha^M_k\}$. Since $f$ is of type 1, we have that $\pm 1$ is not a root of $f$. Since the $M$-th powers might be the same, we choose a complete set of roots from $\Lambda^M$ of $f$, say $\{\alpha^M_1, \alpha^M_2, \ldots, \alpha^M_j\}$, after reindexing the set, if necessary. Note that for all $\alpha_m \in \Lambda$, we have $\alpha^M_m \neq \alpha^{-M}_m$. Since $\Lambda^M$ is closed under taking inverses, we see that there exists $\alpha_l$ such that $\alpha^M_1 = \alpha^{-M}_l$ which implies that $\alpha^M_1 = \alpha^{-M}_1$, which is a contradiction.

Now we want to calculate the number of $M^\ast$-power SRIM polynomial, which contributes to finding out the generating function for the number of separable conjugacy classes in $\text{Sp}(2n, q)$.

**Definition 4.21.** For a polynomial $f \in \mathbb{F}_q[x]$, define $M$-**power spectrum of** $f$ to be the set of degrees, of the irreducible factors of $f(x^M)$. Denote the set $M$-power spectrum of $f$ by $\mathcal{D}_M(f)$. Define the $M^\ast$-**power spectrum of** $f$ to be the set $\{l \in \mathcal{D}_M(f) : f(x^M)$ has a SRIM factor of degree $l\}$, which will be denoted as $\mathcal{D}^\ast_M(f)$.

**Remark 4.22.** We have that $f$ is an $M$-power polynomial (or $M^\ast$-power polynomial) if and only if $M \in \mathcal{D}_M(f)$.

**Definition 4.23.** For a non $M^\ast$-power SRIM polynomial $f$, define the infinite product

$$G_f(u) = \frac{1}{\prod_{i \in \mathcal{D}_M(f)} (1 - u^2^i) \prod_{j \in \mathcal{D}_M(f) \setminus \mathcal{D}^\ast_M(f)} (1 - u^j)}.$$

Define the indicator function corresponding to $f$ be the function $I_M(f) : \mathbb{N} \to \{0, 1\}$ as follows

$$I_M(f)(k) = \begin{cases} 1 & \text{if coefficient of } u^k \text{ in } G_f(u) \neq 0 \\ 0 & \text{otherwise} \end{cases}.$$

**Remark 4.24.** Because of 4.17 the indicator function is same for all irreducible polynomial $f$ of degree $n$ and exponent $e$. Hence we will denote it by $I_{n,e}$.

We end this section with the following notations, which will be used throughout frequently.

**Notation 4.25.** For a given matrix $X \in G(m, \mathbb{F}_q)$, we will use

1. $\Delta_X$ to denote the attached combinatorial data,
2. $c_X(t)$ to denote the characteristic polynomial of $X$,
3. $m_X(t)$ to denote the minimal polynomial of $X$. 

5. Generating Functions for Separable Matrices

From this section onward we will be providing the generating functions for different class of elements. The route is as follows. First we work with the conjugacy classes and then make use of orbit-stabilizer theorem to obtain the corresponding generating functions concerning probability. We will start with the case of a matrix being separable.

Lemma 5.1. Let \( f \) be an SRIM polynomial of degree \( 2k, k \geq 1 \) and \( \alpha^M = C_f \). Then \( f(x^M) \) has an SRIM factor of degree \( 2k \).

Proof. Let \( f \) be a SRIM polynomial of degree \( 2d \) over \( \mathbb{F}_q \). Hence \( f(x) = 1 + a_1x + a_2x^2 + \cdots + a_{d-1}x^{d-1} + x^d(a_d + a_{d-1}x + a_{d-2}x^2 + \cdots + a_1x^{d-1} + x^d) \). Then considering \( C_f \in \text{Sp}(2d, \mathbb{F}_q) \) we have that \( C_f \) is conjugate to the matrix

\[
\begin{pmatrix}
\lambda_1 & & \\
& \ddots & \\
& & \lambda_d
\end{pmatrix}
\]

where \( \{\lambda_i^{\pm 1}\}_{i=1}^d \) is the set of roots of \( f \). Let \( \alpha^M = C_f \) for some \( \alpha \in \text{Sp}(2d, \mathbb{F}_q) \). Since \( \alpha \) is conjugate to the matrix

\[
\begin{pmatrix}
\alpha_1 & & \\
& \ddots & \\
& & \alpha_d
\end{pmatrix}
\]

in \( \text{Sp}(2d, \mathbb{F}_q) \), where \( \{\alpha_i^{\pm 1}\}_{i=1}^d \) is the set of roots of \( \min_{\mathbb{F}_q}(\alpha) \), we have that \( \alpha_i^M = \lambda_{j(i)} \). Without loss of generality, we may assume that \( \alpha_i^M = \lambda_i^\epsilon \), \( \epsilon = \pm 1 \). Hence \( f(\alpha_i^\pm M) = 0 \) for all \( i \). Considering \( H(x) = f(x^M) \), we see that \( H(\alpha_i^{\pm 1}) = 0 \) for all \( i \), in particular \( g = \min_{\mathbb{F}_q}(\alpha) \) divides \( H \).

Since \( \alpha \in \text{Sp}(2d, q) \), we have that \( g \) is self reciprocal monic polynomial. If \( g = g_1g_2 \) for nontrivial factors \( g_1, g_2 \) of \( g \), then \( \min_{\mathbb{F}_q}(\alpha^M) = f \) is not irreducible. Thus, we conclude that \( g \) is an SRIM polynomial.

Lemma 5.2. Let \( f \) be an SRIM polynomial of degree \( 2k, k \geq 1 \) and \( f(x^M) \) has an SRIM factor of degree \( 2k \). Then there exists \( \alpha \in \text{Sp}(2k, q) \) such that \( \alpha^M = C_f \).

Proof. We aim to show that \( C_{g^M}^f \) is conjugate to \( C_f \), where \( g \) is a SRIM factor of degree \( 2k \), of \( f(x^M) \). This is equivalent to showing that the sets \( A = \{\alpha_i^M : i = 1, 2, \cdots, 2k\} \) and \( \Lambda = \{\lambda_i : i = 1, 2, \cdots, 2k\} \) are in bijective correspondence, where \( \{\alpha_i\}_{i=1}^{2k} \) is the set of roots of \( g \) and \( \{\gamma_i\}_{i=1}^{2k} \) is the set of roots of \( f \). Since \( f \) is separable, we have that \( |\Lambda| = 2k \).
Note that in \( \mathbb{F}_{q^2} \), we have \( f(x) = \prod_{i=1}^{2k} (x - \lambda_i) \), \( g(x) = \prod_{i=1}^{2k} (x - \alpha_i) \). Since \( g(x) \) divides \( f(x^M) \), we have that, for all \( j \), \( 0 = f(\alpha_j^M) = \prod_{i=1}^{2k} (\alpha_j^M - \lambda_i) \). Hence \( \alpha_j^M = \lambda_i \) for some \( i \).

After some permutation, we may assume that \( i = 1 \). Note that if \( h \) is the characteristic polynomial of \( C_{M} \), then \( h(\alpha_1) = 0 \). Since minimal polynomial of \( \alpha_1 \) is \( f \), we have that \( f = h \). Since \( f \) is separable, we have that \( |A| = |\Lambda| = 2k \). \( \square \)

**Corollary 5.3.** Let \( A \in \text{Sp}(2n, q) \) has characteristic polynomial \( f \), which is SRIM of degree \( 2n \). Then \( \alpha^M = A \), has a solution in \( \text{Sp}(2n, q) \), if and only if \( f \) is \( M^* \)-power SRIM polynomial.

**Proposition 5.4.** Let \( c_{\text{Sp}}^M(n, q) \) denotes the number of \( M \)-power separable conjugacy classes in \( \text{Sp}(2n, q) \) and \( c_{\text{Sp}}^S(n, u) = 1 + \sum_{m=1}^{\infty} c_{\text{Sp}}^S(m, q) u^m \). Then

\[
(5.1) \quad c_{\text{Sp}}^S(q, u) = \prod_{d=1}^{\infty} \left( 1 + u^d \right)^{N_\ast^d(q, 2d)} \prod_{d=1}^{\infty} \left( 1 + u^d \right)^{R_\ast^d(q, 2d)}.
\]

**Proof.** Let \( X \in \text{Sp}(2n, q) \) be a separable matrix. Then \( c_X(t) \) is separable and is a product of \( \ast \)-irreducible polynomials. Since \( c_X(t) \) is separable we have that each of the factor in \( c_X(t) \) occurs exactly once. Considering the fact that \( X \) has determinant 1, any \( \ast \)-irreducible polynomial of type 3 must occur twice. Hence none of the polynomial \( t \pm 1 \) is a factor of \( c_X(t) \). Let \( \Delta_X = \{ (f, \lambda_f) : f \in \Phi \} \). Then \( \Delta_X \) represents a separable class if and only if

1. \( \lambda_{t \pm 1} = 0 \),
2. \( \lambda_f = \lambda_{f^*} \in \{0, 1\} \),
3. \( \sum_{f \in \Delta_X} \deg f = 2n \).

Hence using Corollary 5.3, we have that \( X \) is an \( M \)-th power separable element if and only if

1. for all \( (f, 1) \in \Delta_X \) and \( f = f^* \), \( f \in \Phi_M^* \),
2. for all \( (f, 1) \in \Delta_X \) and \( f \neq f^* \), \( f \in \Phi_M \).

Thus \( c_X(t) = \prod_{i=1}^{r} f_i \prod_{j=1}^{s} g_j g_j^* \), where \( f_i \) is an \( M^* \)-power SRIM polynomial and \( g_j \neq g_j^* \) is an \( M \)-power polynomial. Considering the fact that each of the factors \( f_i \) and \( g_j g_j^* \) is of
even degree, we have that
\[
e S^M_{Sp}(q, u) = \prod_{f \in \Phi^*_M} \left(1 + u^{\deg f} \right) ^{\frac{1}{2}} \prod_{g \in \Phi^*_M \setminus \Phi^*_M} \left(1 + u^{\deg g} \right) ^{\frac{1}{2}}
\]
\[
= \prod_{d=1}^{\infty} \left(1 + u^d \right)^{N^*_M(q, 2d)} \prod_{d=1}^{\infty} \left(1 + u^d \right)^{R^*_M(q, 2d)} .
\]

**Theorem 5.5.** Let \( s^M_{Sp}(n, q) \) denotes the probability of an element to be \( M \)-power separable in \( Sp(2n, q) \) and \( S^M_{Sp}(q, u) = 1 + \sum_{m=1}^{\infty} s^M_{Sp}(m, q)u^m \). Then
\[
(5.2) \quad S^M_{Sp}(q, u) = \prod_{d=1}^{\infty} \left(1 + \frac{u^d}{q^d + 1} \right)^{N^*_M(q, 2d)} \prod_{d=1}^{\infty} \left(1 + \frac{u^d}{q^d - 1} \right)^{R^*_M(q, 2d)} .
\]

**Proof.** From Lemmas 3.5 and 3.6 it follows that
(1) for \( X \in Sp(2n, q) \), if \( c_X(t) \) is a SRIM polynomial then the centraliser of \( X \) inside \( Sp(2n, q) \) is of order \( q^n + 1 \),
(2) for \( X \in Sp(2n, q) \), if \( c_X(t) \) is \( * \)-irreducible polynomial of type 2 then the centraliser of \( X \) inside \( Sp(2n, q) \) is of order \( q^n - 1 \).
Hence using Proposition 5.4 and the fact that centraliser of a general block diagonal matrix is a direct sum of each of the corresponding centralisers, we have
\[
S^M_{Sp}(q, u) = \prod_{d=1}^{\infty} \left(1 + \frac{u^d}{q^d + 1} \right)^{N^*_M(q, 2d)} \prod_{d=1}^{\infty} \left(1 + \frac{u^d}{q^d - 1} \right)^{R^*_M(q, 2d)} .
\]

\( \square \)

The next theorem is proved along the same line of proof of Theorem 2.3.1 of [5].

**Theorem 5.6.** Let \( s^M_{O^e}(n, q) \) denotes the probability of an element to be \( M \)-power separable in \( O^e(2n, q) \) with \( e \in \{ \pm \} \) and \( s^M_{O^0}(n, q) \) denotes the probability of an element to be \( M \)-power separable in \( O^0(2n + 1, q) \). Define
\[
S^M_{O^+(q, u)} = 1 + \sum_{m \geq 1} s^M_{O^+(m, q)}u^m
\]
\[
S^M_{O^-(q, u)} = \sum_{m \geq 1} s^M_{O^-(m, q)}u^m
\]
\[
S^M_{O^0(q, u)} = 1 + \sum_{m \geq 1} s^M_{O^0(m, q)}u^m .
\]
Then

\[(5.3) \quad S^M_{O^+(u^2)} + S^M_{O^-(u^2)} + 2uS^M_{O^0(u^2)} = (1 + u)^{o(M,q)} S^M_{Sp}(u^2),\]

\[(5.4) \quad S^M_{O^+(u^2)} - S^M_{O^-(u^2)} = X^M_{O^0}(u^2),\]

where

\[X^M_{O^0}(q, u) = \prod_{d=1}^{\infty} \left(1 - \frac{u^d}{q^d+1}\right)^{N^*_M(q,2d)} \prod_{d=1}^{\infty} \left(1 + \frac{u^d}{q^d-1}\right)^{R^*_M(q,2d)},\]

where

\[o(M, q) = \begin{cases} 
1 & \text{if } M \text{ even} \\
2 & \text{otherwise}
\end{cases} .\]

Proof. The proof is similar to that of the previous theorem. But if \(X\) is a separable orthogonal matrix, then \(t \pm 1\) can divide \(c_X(t)\). The multiplicity of \(t \pm 1\) in \(c_X(t)\) can be at most 1, because \(c_X(t)\) is separable. Since center of \(O^n(q, m)\) is \(\{\pm 1\}\), we have that the block corresponding to \(t + 1\), of size \(1 \times 1\) is an \(M\)-th power if and only if \(M\) is odd. Now suppose \(M\) is even. Consider the product

\[(1 + u) \prod_{d=1}^{\infty} \left(1 + \frac{u^d}{q^d+1}\right)^{N^*_M(q,2d)} \prod_{d=1}^{\infty} \left(1 + \frac{u^d}{q^d-1}\right)^{R^*_M(q,2d)}.\]

For the case \(M\) being even, write \((1+u)\) as \((1+\frac{u}{2}+\frac{u}{2})\) and this tracks the possibility of \(t-1\) dividing \(c_X(t)\). Each term \(\frac{u}{2}\), appears for the distinct conjugacy classes corresponding to \(t-1\), each having order of centraliser 2. Note that in this case \(-1\) is not an \(M\)-th power. Hence \(e(M, q) = 1\). Now for \(n\) even positive, the coefficient of \(u^n\) is \(s^M_{O^+(n, q)} + s^M_{O^-(n, q)}\), where as for \(n\) being odd positive the coefficient is \(e(q)s^M_{O^0(n, q)}\) for \(e(q)\) many types of forms over \(\mathbb{F}_q^n\).

For the case \(M\) being odd and \(q\) being odd, consider the product

\[(1 + u)^2 \prod_{d=1}^{\infty} \left(1 + \frac{u^d}{q^d+1}\right)^{N^*_M(q,2d)} \prod_{d=1}^{\infty} \left(1 + \frac{u^d}{q^d-1}\right)^{R^*_M(q,2d)}.\]

Then writing \((1 + u)\) as \((1+\frac{u}{2}+\frac{u}{2})\) we get the possibility of \(t-1\) dividing \(c_X(t)\). But there are two such conjugacy classes each having centraliser of size 2. The same argument applies for the polynomial \(t + 1\) as well. Hence the power 2. This proves the first equation.

We will prove the second equation by modifying first equation. For each of the factor \(1 + C_f u^{2d}\) in the right hand side of the first equation, where \(C_f\) is the reciprocal of the size of the corresponding centraliser, replace it by \(1 + \tau_f C_f u^{2d}\), where \(\tau_f = \tau(V_f)\) and \(V_f\) denotes the component of \(V\) corresponding to \(f\), in the primary decomposition as an \(\mathbb{F}_q[X]\) module. Then since for \(q\) odd, each of the term \(\frac{u}{2}\) corresponds to conjugacy class with \(\tau_f\) values being negative to each other, the term \((1 + u)\) vanishes. Now, since
\( \tau_f = -1 \), when \( f \) is of type 1 and \( \tau_f = +1 \), when \( f \) is of type 2, the factors \( 1 + \frac{u^{2d}}{q^d + 1} \) are replaced by \( 1 - \frac{u^{2d}}{q^d + 1} \), whereas the factor \( 1 + \frac{u^{2d}}{q^d - 1} \) remains as it is. Hence the product becomes

\[
\prod_{d=1}^{\infty} \left( 1 - \frac{u^d}{q^d + 1} \right)^{N_M(q,2d)} \prod_{d=1}^{\infty} \left( 1 + \frac{u^d}{q^d - 1} \right)^{R_M(q,2d)},
\]

which on expanding gives \( S_{O+}^M(u^2) - S_{O-}^M(u^2) \). \( \square \)

**Remark 5.7.** Let \( cs_{O+}^M(n, q) \) denotes the probability of a conjugacy class to be \( M \)-power separable in \( O'\langle 2n, q \rangle \) with \( \epsilon \in \{\pm\} \) and \( cs_{O^0}^M(n, q) \) denotes the probability of a conjugacy class to be \( M \)-power separable in \( O^0\langle 2n + 1, q \rangle \). Define

\[
c_{S_{O+}^M}(q, u) = 1 + \sum_{m \geq 1} cs_{O+}^M(m, q)u^m,
\]

\[
c_{S_{O-}^M}(q, u) = \sum_{m \geq 1} cs_{O-}^M(m, q)u^m,
\]

\[
c_{S_{O^0}^M}(q, u) = 1 + \sum_{m \geq 1} cs_{O^0}^M(m, q)u^m.
\]

Then

\[
c_{S_{O+}^M}(u^2) + c_{S_{O-}^M}(u^2) + 2uc_{S_{O^0}^M}(u^2) = (1 + 2u)^{o(M,q)}c_{S_{Sp}^M}(u^2),
\]

\[
c_{S_{O+}^M}(u^2) - c_{S_{O-}^M}(u^2) = c_{X_{O^0}^M}(u^2),
\]

where

\[
c_{X_{O^0}^M}(q, u) = \prod_{d=1}^{\infty} \left( 1 - u^d \right)^{N_M(q,2d)} \prod_{d=1}^{\infty} \left( 1 + u^d \right)^{R_M(q,2d)}.
\]

6. **Generating Functions for Semisimple Matrices**

Before moving towards the determination of generating functions for semisimple case, we find out the cases where \( M \)-th root of \( -1 \) exists. This is certainly true, whenever \( M \) is odd. The next lemma discusses the scenario, when \( M \) is even.

We first note that for a number \( M = 2^nM' \) for \( (M', 2) = 1 \), we have

\[
x^M + 1 = (x^{2^n} + 1)(x^{2^n(M'-1)} - x^{2^n(M'-2)} + \cdots + 1).
\]

Let us call the second factor in the above decomposition \( F \). If we can prove that all irreducible factors of \( F \) have degree which is multiple of degree of the factors of \( x^{2^n} + 1 \), we can conclude about factors of \( x^M + 1 \). We note the following result from [17].

**Proposition 6.1** (Theorem 1, [17]). Let \( q \equiv 3 \pmod{4} \), i.e., \( q = 2^A m - 1 \), \( A \geq 2 \), \( m \) odd. Let \( n \geq 2 \).
(1) If \( n < A \), then \( x^{2^n} + 1 \) is the product of \( 2n - 1 \) irreducible trinomials over \( \mathbb{F}_q \)

\[
x^{2^n} + 1 = \prod_{\gamma \in \Gamma} (x^2 + \gamma x + 1),
\]

where \( \Gamma \) is the set of all roots of the Dickson polynomial \( D_{2^{n-1}}(x, 1) \).

(2) If \( n \geq A \), then \( x^{2^n} + 1 \) is the product of \( 2^{A-1} \) irreducible polynomials over \( \mathbb{F}_q \)

\[
x^{2^n} + 1 = \prod_{\delta \in \Delta} (x^{2^{n-A+1}} + \delta x^{2n-A} - 1),
\]

where \( \Delta \) is the set of all roots of the Dickson polynomial \( D_{2^{A-1}}(x, -1) \).

Suppose \( M = 2^n \), for some \( n \). Then the block \( \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \) is an \( M \)-th root in the first case. For the second case the \( L \times L \) matrix \( -I_L \) is an \( M \)-th power if and only if \( L \) is a multiple of \( 2^{n-A+2} \).

**Proposition 6.2.** Let \( css_{Sp}^M(2n, q) \) denotes the number of \( M \)-power semisimple conjugacy classes in \( Sp(2n, q) \) and \( css_{Sp}^M(q, u) = 1 + \sum_{m=1}^{\infty} css_{Sp}^M(2m, q)u^m \). Then \( css_{Sp}^M(q, u) \) is given by

\[
\frac{1}{(1 - u^{(M,q)})(1 - u)} \prod_{d=1}^{\infty} (1 - u^d)^{-N_M^*(q,2d)} \prod_{d=1}^{\infty} (1 - u^d)^{-R_M^*(q,2d)}
\]

\[
\times \prod_{d=1}^{\infty} \prod_{e|q^2+1} \left( 1 + \sum_{m=1}^{\infty} I_{e,2d}(2dm)u^{dm} \right)^{N_{e,d}^*(q,2d)} \prod_{d=1}^{\infty} \prod_{e|q^2-1} \left( 1 + \sum_{m=1}^{\infty} I_{e,d}(dm)u^{dm} \right)^{R_{e,d}^*(q,2d)},
\]

where \( r(M,q) = \begin{cases} 1 & \text{if } M \text{ is odd} \\ 2 & q \equiv 3 \pmod{4}, n < A \\ 2^{n-A+1} & q \equiv 3 \pmod{4}, n \geq A \end{cases} \).

**Proof.** Let \( X \in Sp(2n, q) \) be semisimple. Then \( m_X(t) \) is a product of distinct \( * \)-irreducible polynomials. Considering that \( X \) has determinant 1, we have that \( (t+1) \) has even multiplicity in \( c_X(t) \). This forces to have multiplicity of \( t-1 \) to be even in \( c_X(t) \).

Let \( \Delta_X = \{(f, \lambda_f) : f \in \Phi\} \). Then \( X \) is semisimple if and only if

1. \( \lambda_{t+1} \in \{0, 1^{2r_1}\}, \lambda_{t-1} \in \{0, 1^{2r-1}\}, \)
2. \( \lambda_f = \lambda_f^* \in \{0, 1^{l_f}\}, \)
3. \( \sum |\lambda_f| = 2n, \)

where \( r_1, r, l_f \in \mathbb{Z}_{>0} \). Hence using Corollary 5.3 and discussion preceding Lemma 4.13, \( X \) is an \( M \)-th power if and only if

1. \( \lambda_{t-1} \in \{0, 1^{2r_1}\}, r_1 \in \mathbb{Z}_{>0}, \)
2. \( \lambda_{t+1} \in \{0, 1^{2r-1}\}, \) where \( r_{-1} \in r(M,q)\mathbb{Z}_{>0}, \)

where \( c_X(t) \). This forces to have multiplicity of \( t-1 \) to be even in \( c_X(t) \).
(3) for \( f \), an \( M^* \)-power SRIM polynomial of degree \( d \) we have \( \lambda_f \in \{0, 1^m : m \in \mathbb{Z}_{>0} \} \),

(4) for \( f \neq f^{*} \), an \( M \)-power polynomial of degree \( d \) we have

\[
\lambda_f = \lambda_{f^{*}} \in \{0, 1^m : m \in \mathbb{Z}_{>0} \}
\]

(5) for \( f \), a type 1 polynomial which is not an \( M^* \)-power polynomial,

\[
\lambda_f \in \{0, 1^m : m \in \sum_{i \in \mathcal{D}_M(f)} \mathbb{Z}_{>0}i\},
\]

(6) for \( f \), a type 2 polynomial which is not an \( M \)-power polynomial

\[
\lambda_f = \lambda_{f^{*}} \in \{0, 1^m : m \in \sum_{i \in \mathcal{D}_M(f)} \mathbb{Z}_{>0}i\}.
\]

Hence \( cSS_s^{M}(q, u) \) is given by

\[
\left(1 + \sum_{m=1}^{\infty} u^m\right) \left(1 + \sum_{m=1}^{\infty} u^{\frac{m\deg f}{2}}\right)^{e(q)-1}
\]

\[
\times \prod_{f=f^{*} \atop f \in \Phi_M^*} \left(1 + \sum_{m=1}^{\infty} u^{\frac{m\deg f}{2}}\right) \prod_{f \neq f^{*} \atop f \in \Phi_M} \left(1 + \sum_{m=1}^{\infty} u^{m\deg f}\right)
\]

\[
\times \prod_{f=f^{*} \atop f \notin \Phi_M^{*}} \prod_{f \neq f^{*} \atop f \notin \Phi_M} \left(1 + \sum_{m=1}^{\infty} \mathcal{I}_M(f)(m\deg f)\frac{u^{\deg f}}{2} u^{m\deg f}\right)
\]

where

(1) the first term accounts for the polynomial \( t - 1 \),

(2) the second term accounts for the polynomial \( t + 1 \), which vanishes when \( (q, 2) \neq 1 \) and hence the power \( e(q) - 1 \),

(3) the third and fourth term appear for the polynomials in \( \Phi_M^{*} \) and \( \Phi_M \) respectively,

(4) the fifth term appears for the type 1 polynomial which are not \( M^* \)-th power SRIM.

Note that in this case \( f(x^M) \) has factors of degrees belonging to \( \mathcal{D}_M(f) \). Suppose \( k_i \in \mathcal{D}_M(f) \) and \( g_{k_i} \) be a factor of \( f(x^M) \), of degree \( k_i \) with \( i = 1, 2, \ldots \). Then clearly \( \deg f|k_i \) and \( (f, 1^{\deg f}) \) is an \( M \)-th power for all \( k_i \in \mathcal{D}_M(f) \). Then for any integer \( m \in \sum_{i \in \mathbb{Z}_{>0}} \frac{k_i}{\deg f} \), the class \( (f, 1^m) \) is an \( M \)-th power.

In this case two kinds of polynomials can occur in factorization of \( f(x^M) \). It can be of either type 1 or type 2. For this the function \( G_f \) has two components corresponding to each type. Hence we associate the function \( \mathcal{I}_M(f) \) which indicates if \( m \in \sum_{i \in \mathbb{Z}_{>0}} \frac{k_i}{\deg f} \) or not.
(5) the sixth term appears for the type 2 polynomial which are not $M$-th power (applying similar kind of argument as in the previous case).

Hence plugging in the formulae for number of each kind of polynomials and taking into consideration 4.17 we get the result. □

**Theorem 6.3.** Let $SS^M_{Sp}(n,q)$ denotes the probability of an element to be $M$-power semisimple in $Sp(2n,q)$ and $SS^M_{Sp}(q,u) = 1 + \sum_{m=1}^{\infty} ss^M_{Sp}(2m,q)u^m$. Then

$$SS^M_{Sp}(q,u) = \left(1 + \sum_{m \geq 1} \frac{u^m r(M,q)}{|Sp(mr(M,q),F_q)|}\right) \left(1 + \sum_{m \geq 1} \frac{u^m}{|Sp(2m, F_q)|}\right) \prod_{d=1}^{\infty} \left(1 + \sum_{m \geq 1} \frac{u^{dm}}{|U(m, F_{q^d})|}\right) R^*_M(q,2d)$$

$$\times \prod_{d=1}^{\infty} \left(1 + \sum_{m \geq 1} \frac{u^{dm}}{|GL(m, F_{q^d})|}\right) N^*_M(q,2d)$$

$$\times \prod_{d=1}^{\infty} \prod_{e|q^d-1} \left(1 + \sum_{m=1}^{\infty} I_{e,d}(dm) \frac{u^{dm}}{|U(m, F_{q^d})|}\right) R^*_{M,e}(q,2d)$$

$$\times \prod_{d=1}^{\infty} \prod_{e|q^d+1} \left(1 + \sum_{m=1}^{\infty} I_{e,2d}(2dm) \frac{u^{dm}}{|U(m, F_{q^d})|}\right) N^*_{M,e}(q,2d)$$

where $r(M,q)$ is the function defined in Proposition 6.2.

**Proof.** Since $\pm 1_{2n}$ are in the center of $Sp(2n,q)$, their centralisers are $Sp(2n,q)$ itself. From Lemmas 3.5 and 3.6 we have that

1. if $f \in \Phi^*$ is of degree $2k$ and $\mu_f = 1^m$, then the centraliser of $X$ inside $Sp(2km,F_q)$ is of order $|U(m,q^k)|$,
2. if $f \in \Phi^\perp$ is of degree $k$ and $\mu_f = 1^m$, then the centraliser of $X$ inside $Sp(2dm,F_q)$ is of order $|GL(m,q^d)|$.

Hence using Proposition 6.2 and the fact that centraliser of a general block diagonal matrix is direct sum of each of the corresponding centralisers, we have the result. □
We define the following functions for simplifying the statements in the case of orthogonal groups. These are motivated by the definitions in Chapter 3 of [8].

\[ Y_{1}^{*,M}(u, q) = \prod_{d=1}^{\infty} \left( 1 + \sum_{m \geq 1} \frac{u^{dm}}{|U(m, q^{d})|} \right)^{N_{M}(q, 2d)} \prod_{d=1}^{\infty} \left( 1 + \sum_{m \geq 1} \frac{u^{dm}}{|GL(m, q^{d})|} \right)^{N_{M}^{c}(q, 2d)} \times \prod_{d=1}^{\infty} \prod_{e|q^{d}+1} \left( 1 + \sum_{m=1}^{\infty} I_{e,2d}(2dm) \frac{u^{dm}}{|U(m, q^{d})|} \right)^{N_{M}^{c}(q, 2d)} \times \prod_{d=1}^{\infty} \prod_{e|q^{d}+1} \left( 1 + \sum_{m=1}^{\infty} I_{e,d}(dm) \frac{u^{dm}}{|GL(m, q^{d})|} \right)^{R_{M}(q, 2d)} \right), \]

\[ Y_{2}^{*,M}(u, q) = \prod_{d=1}^{\infty} \left( 1 + \sum_{m \geq 1} \frac{(-1)^{m} u^{dm}}{|U(m, q^{d})|} \right)^{N_{M}(q, 2d)} \prod_{d=1}^{\infty} \left( 1 + \sum_{m \geq 1} \frac{u^{dm}}{|GL(m, q^{d})|} \right)^{R_{M}(q, 2d)} \times \prod_{d=1}^{\infty} \prod_{e|q^{d}+1} \left( 1 + \sum_{m=1}^{\infty} I_{e,2d}(2dm) \frac{(-1)^{m} u^{dm}}{|U(m, q^{d})|} \right)^{N_{M}^{c}(q, 2d)} \times \prod_{d=1}^{\infty} \prod_{e|q^{d}+1} \left( 1 + \sum_{m=1}^{\infty} I_{e,d}(dm) \frac{u^{dm}}{|GL(m, q^{d})|} \right)^{R_{M}(q, 2d)} \right), \]

\[ F_{+1}(u, q) = 1 + \sum_{m \geq 1} \frac{1}{|O^{+}(2m, q)|} + \frac{1}{|O^{-}(2m, q)|} u^{m}, \]

\[ F_{+1}(u, q) = 1 + \sum_{m \geq 1} \left( \frac{1}{|O^{+}(2m, q)|} - \frac{1}{|O^{-}(2m, q)|} \right) u^{m}, \]

\[ F_{+1}(u, q) = 1 + \sum_{m \geq 1} \frac{u^{m}}{|Sp(2m, q)|}, \]

\[ F_{+1}(u, q) = 1 + \sum_{m \geq 1} \frac{1}{|O^{+}(mr(M, q), q)|} + \frac{1}{|O^{-}(mr(M, q), q)|} u^{m \frac{r(M, q)}{2}}, \]

\[ F_{+1}(u, q) = 1 + \sum_{m \geq 1} \left( \frac{1}{|O^{+}(mr(M, q), q)|} - \frac{1}{|O^{-}(mr(M, q), q)|} \right) u^{m \frac{r(M, q)}{2}}, \]

\[ F_{+1}(u, q) = 1 + \sum_{m \geq 1} \frac{u}{|Sp(mr(M, q), q)|}. \]

The next theorem is proved along the same as Theorem 3.1.6 of [8].
Theorem 6.4. Let $ss_{O^\epsilon}(n,q)$ denotes the probability of an element to be $M$-power semisimple in $O^\epsilon(2n,q)$ with $\epsilon \in \{\pm\}$ and $s_{O^0}(n,q)$ denotes the probability of an element to be $M$-power semisimple in $O^0(2n+1,q)$.

Define

\[ SS_{O^+}(q,u) = 1 + \sum_{m \geq 1} ss_{O^+}(m,q)u^m \]
\[ SS_{O^-}(q,u) = \sum_{m \geq 1} ss_{O^-}(m,q)u^m \]
\[ SS_{O^0}(q,u) = 1 + \sum_{m \geq 1} ss_{O^0}(m,q)u^m. \]

Then

\[ SS_{O^+}(u^2) + SS_{O^-}(u^2) + 2uSS_{O^0}(u^2) = \left(F_{+,+1}(u^2) + uF_{+,1}(u^2)\right) \times \left(F_{-,+1}(u^2) + uF_{-,1}(u^2)\right)^{\epsilon(q)-1}Y_{1,+}^*,M(u^2), \]
\[ S_{O^+}(u^2) - S_{O^-}(u^2) = F_{+,+1}(u^2)[F_{-,+1}(u^2)]^{\epsilon(q)-1}Y_{2,1}^*,M(u^2). \]

Proof. Using similar argument as in Theorem 5.6, the proof follows. □

7. Generating Functions for Cyclic Matrices

Before we give the generating function for the cyclic conjugacy classes we find out which matrices with eigenvalue 1 (or $-1$) are $M$-th power. Note that two matrices $A$ and $B$ are conjugate if and only if $-A$ and $-B$ are conjugate. Hence, conjugacy classes of matrices with all eigenvalue 1 is in bijection with conjugacy classes of matrices with all eigenvalue $-1$. Recall that an element $X \in \text{Sp}(2n,q)$ is cyclic if and only if $c_X(t) = m_X(t)$. Hence we concentrate on single Jordan block with eigenvalue 1. Since Jordan blocks of odd size should occur even times, they do not contribute to cyclic elements (refer [10], pp 48). Although, we have the following

Lemma 7.1. If $(M,q) = 1$, then every unipotent conjugacy class is an $M$-th power.

Let us denote by $U_{f,n} = \begin{pmatrix} C_f & 1 \\ C_f & 1 \\ \vdots & \vdots \\ C_f & 1 \end{pmatrix}$, also sometimes by $U_{C_f,n}$, the matrix of size $n \deg f \times n \deg f$, where $f$ is a monic irreducible polynomial and $C_f$ is the...
standard companion matrix of $f$. Now we want to find the structure of semisimple part $\alpha_s$ of $\alpha$, where $\alpha^M = U_{t+1,n}$ and $\alpha \in \text{GL}(n,q)$. We have the following

**Lemma 7.2.** Let $(M,q) = 1$ and there exists $\alpha \in \text{GL}(n,q)$ satisfying $\alpha^M = U_{t+1,n}$. Then $\alpha_s$ is a scalar matrix.

**Proof.** Let $\alpha$ be conjugate to $UCf_{1,n}$ for some monic irreducible polynomial $f$. Then since $(M,q) = 1$, we have that $\alpha^M$ is conjugate to $UCf_{1,n}$. Now $\alpha^M = U_{t+1,n}$ implies that $C_{1,n} = -1$, whence $UCf_{1,n}$ is conjugate to $\gamma U_{t-1,n}$, where $C_{1,n}$ is denoted as $\gamma$ (as it is a $1 \times 1$ matrix). So $\alpha_s = \gamma I$, is a scalar matrix, as claimed. □

**Corollary 7.3.** Let $(M,q) = 1$ and $U_{Sp_{t+1,n}} \in \text{Sp}(2m,q)$ where $U_{Sp_{t+1,n}}$ is conjugate to $U_{Sp_{t+1,n}}$ in $\text{GL}(2m,q)$. Then $U_{Sp_{t+1,n}}$ is an $M$-th power if and only if $M$ is odd.

**Proof.** Let $M$ be odd. Note that $-U_{Sp_{t+1,n}}$ is a unipotent element and hence has an $M$-th root, say $\alpha$. Then $(-\alpha)^M = U_{Sp_{t+1,n}}$.

Conversely suppose $\alpha^M = U_{Sp_{t+1,n}}$ for some $\alpha \in \text{Sp}(2m,q)$. Also $U_{Sp_{t+1,n}} \in \text{GL}(2m,q)$ implies that $\alpha_s$ is a scalar matrix. Then we have that $\alpha_s = -I$, since $\text{Sp}(2m,q)$ contains only the scalar matrices $\{\pm I\}$. Hence $M$ should be odd. □

**Corollary 7.4.** Let $(M,q) = 1$. Any matrix $X \in \text{Sp}(2n,q)$ with combinatorial data $(t + 1, m^\pm)$ is an $M$-th power if and only if $M$ is odd.

**Proof.** This follows from 7.1 and proof of 7.3. □

From Chapter 3 of [5], we use tensor product construction to study the $\pm 1$-potent conjugacy classes and denote them by $[J_{a,\epsilon}]$. From Lemma 3.4.7 [5], we have

**Lemma 7.5.** A unipotent element of type $[J_{a,\epsilon}]$ fixes a pair of complementary maximal totally isotropic subspaces of the natural $\text{Sp}_{ab}(q)$-module if and only if $\epsilon = +$.

**Corollary 7.6.** We have that $[J_{a,\epsilon}]^M = [J_{a,\epsilon}]$.

**Proof.** Let $\epsilon = +$. Then there are complementary maximally totally isotropic subspaces $W_1, W_2$ of dimension $\frac{b}{2}$ such that $J_a \otimes I_b$ fixes $U \otimes W_1$ and $U \otimes W_2$. Then $J_a^M \otimes I_b^M$ fixes $U \otimes W_1$ and $U \otimes W_2$ and hence the result follows in this case.

For $\epsilon = -$, on the contrary assume $[J_{a,-}]^M$ has the property that it fixes a pair of complementary maximally totally isotropic subspaces. Since $[J_{a,-}]$ has power coprime to $M$, we have that $[J_{a,-}]$ fixes a pair of complementary maximally totally isotropic subspaces, which is a contradiction. □

**Corollary 7.7.** For $M$ odd, we have that $-[J_{a,\epsilon}]^M = [-J_{a,\epsilon}]$. 


Proposition 7.8. Let $cC^M_{Sp}(2n, q)$ denote the number of $M$-power cyclic conjugacy classes in $Sp(2n, q)$ and $cC^M_{Sp}(q, u) = 1 + \sum_{m=1}^{\infty} cC^M_{Sp}(2m, q)u^m$. Then $cC^M_{Sp}(q, u)$ is given by

\[
(7.1) \quad \left(\frac{2}{1-u} - 1 - u\right)^{h(q, M)} \prod_{d=1}^{\infty} \left(1-u^d\right)^{-N^*_M(q,2d)} \prod_{d=1}^{\infty} \left(1-u^d\right)^{-R^*_M(q,2d)},
\]

where

\[ h(q, M) = \begin{cases} 2 & \text{if } M \text{ is odd} \\ 1 & \text{otherwise} \end{cases} \]

Proof. Let $X \in Sp(2n, q)$ be cyclic. Then $cX(t) = mX(t)$. Since the space $\mathbb{F}_q^{2n}$, considered as an $X$-module will be cyclic, we have that the primary decomposition of $\mathbb{F}_q^{2n}$ should be of the form $\bigoplus_{f \in \Phi} \mathbb{F}_q^{\langle f(t)^a \rangle}$, with each $f \in \Phi$ occurring at most once. Let $\Delta_X = \{(f, \lambda_f) : f \in \Phi\}$. Then $\Delta_X$ represents a cyclic class if and only if

1. $\lambda_{t \pm 1} \in 2\mathbb{Z}$,
2. $\lambda_f = \lambda_f^* \in \mathbb{Z}_{\geq 0}$.

We divide the proof in two cases depending on the value of $(M, q)$.

We start with the case when $(M, q) = 1$. In this case using the fact that $U^M_{C_f,n}$ is conjugate to $U^M_{C_f}$, we have that $X$ is an $M$-th power cyclic polynomial if and only if

1. $\lambda_{t-1} \in 2\mathbb{Z}$,
2. $\lambda_{t+1} \in 2\mathbb{Z}$ if $M$ is odd and $\lambda_{t+1} = 0$ if $M$ is even,
3. $(f, \lambda_f) \in \Delta_X$, $f$ is of type 1 and $\lambda_f \neq 0$, then $f \in \Phi^*_M$,
4. $(f, \lambda_f) \in \Delta_X$, $f$ is of type 2 and $\lambda_f \neq 0$, then $f \in \Phi_M \setminus \Phi^*_M$.

We should keep in mind that there are two conjugacy classes corresponding to the polynomials $t \pm 1$. Hence, we have that

\[
cC^M_{Sp}(q, u) = \left(1 + 2 \sum_{m \geq 1} u^m\right)^{h(q, M)} \prod_{f \in \Phi^*_M} \left(1 + \sum_{m \geq 1} u^{m\deg f}\right) \prod_{g \in \Phi_M \setminus \Phi^*_M} \left(1 + \sum_{m \geq 1} u^{m\deg g}\right)^{\frac{1}{2}},
\]

where

1. the first term accounts for the terms corresponding to $t \pm 1$, with a power 1 if $M$ is even and 2 if $M$ is odd,
2. the second term accounts for polynomial of type 1 and
3. the third term accounts for polynomial of type 2, with a power $\frac{1}{2}$, as for each $g \neq g^*$, the term $\left(1 + \sum_{m \geq 1} u^{m\deg g}\right)$ occurs twice.

Then grouping the polynomials with same degree of type 1 or 2, the result follows for the case $(M, q) = 1$. \qed
Theorem 7.9. Let $c^M_{Sp}(n, q)$ denotes the probability of an element to be $M$-power cyclic in $Sp(2n, q)$ and $C^M_{Sp}(q, u) = 1 + \sum_{m=1}^{\infty} c^M_{Sp}(2m, q)u^m$. Then $C^M_{Sp}(q, u)$ is given by

\begin{equation}
\left(\frac{1}{1 - \frac{u}{q}}\right) h(q, M) \prod_{d=1}^{\infty} \left(1 + \frac{u^d}{(q^d + 1)(1 - \frac{u^d}{q^d})}\right) \prod_{d=1}^{\infty} \left(1 + \frac{u^d}{(q^d - 1)(1 - \frac{u^d}{q^d})}\right) \frac{R^*_M(q, 2d)}{R^*_M(q, 2d)}
\end{equation}

if $(q, M) = 1$, where $h(q, M)$ is as in 7.8.

Proof. It follows from Lemmas 3.5 and 3.6 that

1. for $m \geq 2$, the cyclic matrices corresponding to $t \pm 1$, in $Sp(2m, F_q)\), form two conjugacy classes, with each of the corresponding centraliser of order $2q^m$,

2. if $f$ is of type 1 of degree $2m$, then order of the centraliser in $Sp(2ml, F_q)$ of a matrix $X$, with $\Delta_X = \{(f, l)\}$ is $q^{2d(l-1)}(q^d + 1)$,

3. if $f$ is of type 2 of degree $m$, then order of the centraliser in $Sp(2ml, F_q)$ of a matrix $X$, with $\Delta_X = \{(f, l), (f^*, l)\}$ is $q^{2d(l-1)}(q^d - 1)$.

Hence using Proposition 7.8 and the fact that the centraliser of a general block diagonal matrix is a direct sum of each of the corresponding centralisers, we have the result. \qed

Analogous statements as in 7.3, 7.8 are true in case of $O^r(n, q)$, whenever $(M, q) = 1$. Hence we consider the case when $(q, 2) = 1 \neq (M, q)$. From [11], we know that for unipotent elements of $O^r(m, q)$ all even Jordan block sizes occur with even multiplicity. Hence for cyclic $-1$-potent element (i.e. elements $X$ with $c_X(t) = (t + 1)^k$), we consider unipotent elements which have odd Jordan block size, with multiplicity 1. The corresponding conjugacy class has representative

\[
A_\epsilon = \begin{pmatrix}
1 \\
1 & 1 \\
\vdots & \vdots & \ddots \\
1 & 1 & \cdots & 1 \\
1 & 1 & \cdots & 1 & 1 \\
-\epsilon & -\epsilon & \cdots & -\epsilon & -2\epsilon & 1 \\
& & & & & -1 & 1 \\
& & & & & -1 & 1 \\
& & & & & \cdots & \cdots \\
& & & & & \cdots & \cdots \\
& & & & & -1 & 1
\end{pmatrix},
\]

where $\epsilon = 1$ or is a non-square in $F_q$. But then $A^M_\epsilon$ is not cyclic $-1$-potent element.

Before writing down the generating functions for the cyclic elements, let us introduce the following functions:
Definition 7.10. We define
\[
Z_0(u) = \prod_{d=1}^{\infty} \left( 1 + \frac{u^d}{(q^d + 1)(1 - \left(\frac{u^2}{q}\right)^d)} \right)^{N_{\mathcal{O}}^-(q, 2d)} \left( 1 + \frac{u^d}{(q^d - 1)(1 - \left(\frac{u^2}{q}\right)^d)} \right)^{R_{\mathcal{O}}^+(q, 2d)},
\]
\[
Z_0'(u) = \prod_{d=1}^{\infty} \left( 1 - \frac{u^d}{(q^d + 1)(1 + \left(\frac{u^2}{q}\right)^d)} \right)^{N_{\mathcal{O}}^+(q, 2d)} \left( 1 + \frac{u^d}{(q^d - 1)(1 - \left(\frac{u^2}{q}\right)^d)} \right)^{R_{\mathcal{O}}^-(q, 2d)}.
\]

Theorem 7.11. Let \( c_{\mathcal{O}}^M(n, q) \) denotes the probability of an element to be \( M \)-power cyclic in \( \mathcal{O}(2n, q) \) with \( \epsilon \in \{\pm\} \) and \( c_{\mathcal{O}}^M(n, q) \) denotes the probability of an element to be \( M \)-power cyclic in \( \mathcal{O}(2n + 1, q) \). Define
\[
C_{\mathcal{O}}^+(q, u) = 1 + \sum_{m \geq 1} c_{\mathcal{O}}^+(m, q)u^m,
\]
\[
C_{\mathcal{O}}^-(q, u) = \sum_{m \geq 1} c_{\mathcal{O}}^-(m, q)u^m,
\]
\[
C_{\mathcal{O}}^M(q, u) = 1 + \sum_{m \geq 1} c_{\mathcal{O}}^M(m, q)u^m.
\]
Then
\[
(7.3) \quad C_{\mathcal{O}}^+(u^2) + C_{\mathcal{O}}^-(u^2) + 2uC_{\mathcal{O}}^0(u^2) = 1 + \frac{u^2}{1 - \frac{u^2}{q}} Z_0(u^2),
\]
where \( h(q, M) \) is as in \( 7.8 \) and
\[
(7.4) \quad C_{\mathcal{O}}^M(u^2) - C_{\mathcal{O}}^M(u^2) = Z_0'(u^2).
\]

Proof. We divide the proof in several cases. The first case is when \( M, q \) are odd. Then consider the product
\[
\left( 1 + \frac{u}{1 - \frac{u^2}{q}} \right)^2 \prod_{d=1}^{\infty} \left( 1 + \frac{u^{2d}}{(q^d + 1)(1 - \left(\frac{u^2}{q}\right)^d)} \right)^{N_{\mathcal{O}}^+(q, 2d)} \left( 1 + \frac{u^{2d}}{(q^d - 1)(1 - \left(\frac{u^2}{q}\right)^d)} \right)^{R_{\mathcal{O}}^+(q, 2d)}.
\]
Since \( M \) is odd, all of cyclic unipotent or \(-1\)-potent elements are \( M \)-th power. Now if for a cyclic orthogonal matrix \( X \), \( c_X(t) \) has factor \( t \pm 1 \), then the multiplicity should be odd. There are two conjugacy classes corresponding to each polynomial \((t \pm 1)^{2l+1}\), with size of centraliser equal to \( 2q^l \). Hence each of \((t \pm 1)^{2l+1}\), has generating function
\[
1 + \frac{2u}{2q} + \frac{2u^3}{2q^2} + \frac{2u^5}{2q^3} + \cdots = 1 + \frac{u}{1 - \frac{u^2}{q}}.
\]
Hence using arguments similar to \( 5.6 \) we have that the product on expansion gives \( C_{\mathcal{O}}^+(u^2) + C_{\mathcal{O}}^-(u^2) + 2uC_{\mathcal{O}}^0(u^2) \).

Next suppose \( q \) is odd and \( M \) is even. Then all the cyclic unipotent matrices are \( M \)-th power, where as none of the cyclic \(-1\)-potent are \( M \)-th power. Since unipotent
component in cyclic matrices has odd size, we see that none of the cyclic matrices in $O^\pm$, has unipotent part. This along with arguments as before, we have that in this case $C_{O^+}(u^2) + C_{O^-}(u^2) + 2uC_{O^0}(u^2)$ is given by

$$\left(1 + \frac{u}{1 - \frac{u^2}{q}}\right) \prod_{d=1}^{\infty} \left(1 + \frac{u^{2d}}{(q^d + 1)(1 - (\frac{u^2}{q})^d)}\right)^{N_{M}^{*}(q,2d)} \left(1 + \frac{u^{2d}}{(q^d - 1)(1 - (\frac{u^2}{q})^d)}\right)^{R_{M}^{*}(q,2d)}.$$  

For the last equation argument similar to 5.6 does the job. □

8. Generating Functions for Regular Matrices

Since in case of $Sp(2n,q)$, an element $X \in Sp(2n,q)$ is regular if and only if $X$ is cyclic, we concentrate on the case of $O^\epsilon(m,q)$. We will need the following definition from [8].

**Definition 8.1.** Let $U$ be a finite dimensional vector space over $\mathbb{F}_q$ and $X \in \text{Aut}(U, \varphi)$ and $c_X(t) = (t - \mu)^n$ where $\varphi$ is an orthogonal form and $\mu = \pm 1$. Then call $X$ to be **nearly cyclic** if and only if either $U = \{0\}$ or there is an $X$-invariant orthogonal decomposition $U = U_0 \oplus U_1$, in which dim $U_0 = 1$ and $U_1$ is a cyclic $X$-module.

To understand the structure of regular conjugacy classes we state Theorem 3.2.1 from [8], which is as follows.

**Theorem 8.2.** Let $q$ be odd and $X \in O^\epsilon(m,q)$. Then $X$ is regular if and only if

1. for every monic irreducible polynomial $\phi$ other than $t \pm 1$, the $\phi$-primary component of $X$ is cyclic,
2. for $\mu = \pm 1$, the $t - \mu$ component of $X$ is cyclic if it is odd dimensional and nearly cyclic if it is even dimensional.

**Theorem 8.3.** Assume $q$ to be odd and Let $r_{O^\epsilon}^M(n,q)$ denotes the probability of an element to be $M$-power regular in $O^\epsilon(2n,q)$ with $\epsilon \in \{\pm\}$ and $r_{O^\epsilon_0}^M(n,q)$ denotes the probability of an element to be $M$-power regular in $O^0(2n+1,q)$. Define

$$R_{O^+}^M(q,u) = 1 + \sum_{m \geq 1} r_{O^+}^M(m,q)u^m$$

$$R_{O^-}^M(q,u) = \sum_{m \geq 1} r_{O^-}^M(m,q)u^m$$

$$R_{O^0}^M(q,u) = 1 + \sum_{m \geq 1} r_{O^0}^M(m,q)u^m.$$
Then

\[ R^M_{O^+}(u) + R^M_{O^-}(u) + 2uR^M_{O^0}(u) = \left( 1 + \frac{u}{1 - \frac{u^2}{q^2}} + \frac{qu^2}{q^2 - 1} + \frac{u^4}{q^2(1 - \frac{u^2}{q^2})} \right)^{h'(M)} \]

\[ \left( 1 + \frac{u^2}{2(q-1)} + \frac{u^2}{2(q+1)} \right)^{h''(M)} Z_O(u^2), \]

where \( h'(M) = 1 \) if \( M \) is even and 2 otherwise and \( h''(M) = 1 \) if \( M = 2 \) and 0 otherwise.

**Proof.** We divide the proof in two parts on the basis of parity of \( M \) modulo 2. Before that, note that

\[ F^M_1(u) = 1 + \left( \frac{u}{1} + \frac{u^3}{q} + \frac{u^5}{q^2} + \cdots \right) + \left( \frac{u^2}{2(q-1)} + \frac{u^2}{2(q+1)} + \frac{u^4}{4q^2} + \frac{u^6}{4q^3} + \cdots \right) \]

\[ = \left( 1 + \frac{u}{1 - \frac{u^2}{q}} + \frac{qu^2}{q^2 - 1} + \frac{u^4}{q^2(1 - \frac{u^2}{q^2})} \right). \]

Using same argument and [7,8] we find that

\[ F^M_{-1}(u) = \begin{cases} 
1 + \frac{u}{1 - \frac{u^2}{q}} + \frac{qu^2}{q^2 - 1} + \frac{u^4}{q^2(1 - \frac{u^2}{q})} & \text{if } M \text{ odd} \\
\frac{u^2}{2(q-1)} + \frac{u^2}{2(q+1)} & \text{if } M = 2 \\
1 & \text{otherwise}
\end{cases} \]

\[ Z_O(u^2), \]

\[ \square \]
9. Concluding remarks and further question

9.1. Existence of root in \( \text{GL}(2n, q) \) versus existence of root in \( \text{Sp}(2n, q) \). Recall from Example 4.5 that the matrix \( A \in \text{Sp}(4, 5) \) corresponding to the combinatorial data \( \{x^4 + 3x^3 + x^2 + 3x + 1, 1\} \) has a square root \( \text{GL}(4, 5) \) but not in \( \text{Sp}(4, 5) \). This exhibits an example of a matrix that shows that having a square root (more generally an \( M \)-th root) in general linear group does not imply the existence of a square root in symplectic group. Hence the notion of \( M^* \)-power polynomial is different from that of \( M \)-power polynomial.

9.2. Closed formula. In the memoir \([8]\), the works are based on using generating functions and getting precise estimates. These results are one of the great works after that of G. E. Wall and complement the work of Guralnick and Lubeck. In the later part of the book, the authors go on finding analytic continuity of the generating functions beyond the unit disc (with probable poles at 1 and some few more points). An important ingredient of finding these results heavily relies on one of the famous Rogers-Ramanujan identities, viz.

\[
1 + \sum_{n \geq 1} \frac{1}{|\text{GL}(n, q)|} = \prod_{m \equiv 1 \pmod{5}} \frac{1}{1 - q^{-m}},
\]

for proving results about the limiting probabilities in the case of \( \text{GL}(n, q) \). To date, analog result is not known to have conclusive results for symplectic and orthogonal groups. It will be highly desirable to have closed formula for the generating functions for \( M \)-th powers in the symplectic and orthogonal groups.

We should also keep in mind that generating functions are used for constructing new modular forms. Famous examples include explicit formulas for the number of representations of a positive integer as a sum of four and eight squares, whose generating functions are modular forms of weight 2 and 4, respectively, or the partition function \( p(n) \), whose generating function is essentially a modular form of weight \(-1/2\). It will not be surprising if the above generating functions give new modular forms and such a result will be of high interest to a greater audience.

9.3. Product of \( M \)-th powers. As mentioned in the introduction we will be happy to draw similar conclusions as discussed in \([16]\) for finite groups of Lie type, at least asymptotically (as \( q \rightarrow \infty \) or \( n \rightarrow \infty \)). Our paper is the first step towards the same, as it sheds light on the scenario for powers in the concerned groups.

References

[1] A. Borel, *On free subgroups of semisimple groups*, Enseign. Math. (2), 29 (1983), pp. 151–164.
[2] J. R. Britnell, *Cyclic, separable and semisimple matrices in the special linear groups over a finite field*, J. London Math. Soc. (2), 66 (2002), pp. 605–622.
[3] Cycle index methods for finite groups of orthogonal type in odd characteristic, J. Group Theory, 9 (2006), pp. 753–773.

[4] Cyclic, separable and semisimple transformations in the special unitary groups over a finite field, J. Group Theory, 9 (2006), pp. 547–569.

[5] T. C. Burness and M. Giudici, Classical groups, derangements and primes, 25 (2016), pp. xviii+346.

[6] M. C. R. Butler, The irreducible factors of $f(x^m)$ over a finite field, J. London Math. Soc., 30 (1955), pp. 480–482.

[7] J. Fulman, Cycle indices for the finite classical groups, J. Group Theory, 2 (1999), pp. 251–289.

[8] J. Fulman, P. M. Neumann, and C. E. Praeger, A generating function approach to the enumeration of matrices in classical groups over finite fields, Mem. Amer. Math. Soc., 176 (2005), pp. vi+90.

[9] J. Fulman, J. Saxl, and P. H. Tiep, Cycle indices for finite orthogonal groups of even characteristic, Trans. Amer. Math. Soc., 364 (2012), pp. 2539–2566.

[10] J. E. Fulman, Probability in the classical groups over finite fields: Symmetric functions, stochastic algorithms, and cycle indices, (1997), p. 148. Thesis (Ph.D.)–Harvard University.

[11] S. Gonshaw, M. W. Liebeck, and E. A. O’Brien, Unipotent class representatives for finite classical groups, J. Group Theory, 20 (2017), pp. 505–525.

[12] A. Kulshrestha, R. Kundu, and A. Singh, Asymptotics of the powers in finite reductive groups, Journal of Group Theory, (2021), p. 000010151520200206.

[13] R. Kundu and A. Singh, Generating functions for the powers in $GL(n,q)$, Israel Journal of Mathematics, (2022), p. To appear.

[14] M. Larsen, Word maps have large image, Israel J. Math., 139 (2004), pp. 149–156.

[15] M. W. Liebeck, E. A. O’Brien, A. Shalev, and P. H. Tiep, The Ore conjecture, J. Eur. Math. Soc. (JEMS), 12 (2010), pp. 939–1008.

[16] Products of squares in finite simple groups, Proc. Amer. Math. Soc., 140 (2012), pp. 21–33.

[17] H. Meyn, Factorization of the cyclotomic polynomial $x^n + 1$ over finite fields, Finite Fields Appl., 2 (1996), pp. 439–442.

[18] J. Milnor, On isometries of inner product spaces, Invent. Math., 8 (1969), pp. 83–97.

[19] S. Panja, Powers and skew braces for classical groups, (2022), p. 114. Thesis (Ph.D.)–Indian Institute of Science Education and Research Pune.

[20] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, Acta Math., 68 (1937), pp. 145–254.

[21] A. Shalev, Word maps, conjugacy classes, and a noncommutative Waring-type theorem, Ann. of Math. (2), 170 (2009), pp. 1383–1416.

[22] K.-i. Shinoda, The characters of Weil representations associated to finite fields, J. Algebra, 66 (1980), pp. 251–280.

[23] D. E. Taylor, Conjugacy classes in finite orthogonal groups, (2020).

[24] Conjugacy classes in finite symplectic groups, (2020).

[25] The Sage Developers, Sagemath, the Sage Mathematics Software System (Version 0.6.0), (2021). https://www.sagemath.org.

[26] G. E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, J. Austral. Math. Soc., 3 (1963), pp. 1–62.
Email address: panjasaikat300@gmail.com

Email address: anupamk18@gmail.com

IISER Pune, Dr. Homi Bhabha Road, Pashan, Pune 411 008, India