Powers and Skew Braces for Classical Groups

A thesis
submitted in partial fulfillment of the requirements
of the degree of

Doctor of Philosophy

by

Saikat Panja
ID: 20173547

INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH PUNE

September 23, 2022

Dedicated to
the four pillars of my life

Certificate

Certified that the work incorporated in the thesis entitled "*Powers and skew braces for classical groups*", submitted by *Saikat Panja* was carried out by the candidate, under my supervision. The work presented here or any part of it has not been included in any other thesis submitted previously for the award of any degree or diploma from any other university or institution.

Date: September 23, 2022

Dr. Anupam Kumar Singh
Thesis Supervisor

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that violation of the above will be cause for disciplinary action by the institute and can also, evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Saikat Panja

Date: September 23, 2022

Saikat Panja
Roll Number: 20173547

Acknowledgements

An expedition in the Himalayas might fail without a well-experienced guide. Similarly, my Ph. D. Journey would not have been this beautiful without my supervisors support at each naive step of mine. He has guided me through the routes well and encouraged me to grow mathematically. As the sherpas take a call for the summit push, my supervisor has always taken the correct academic decisions for me during my tenure. The first part of the thesis has been made possible because of his continuous support. He has allowed me to venture into different areas as well. The second part of the thesis is an outcome of that support. I am more thankful to him because of his support during the COVID-19 years. I would like to take this opportunity to thank him wholeheartedly.

Next, I would like to thank the four pillars of my life. Ma and Baba, without your lessons for life, I wouldn't have survived this journey. My maternal grandmother, although I haven't gotten much chance of spending time with her, has been a strong lady throughout her life. She has been a major inspiration for me during the time of fall. Finally, the one and the strongest, who has been my old friend for a long time and will be staying with me all the time, thank you. It has been possible because of you people. I hope I have made you people proud.

Besides my supervisor, I would like to thank the rest of my research advisory committee: Prof. B. Sury and Dr. Vivek Mohan Mallick for their insightful comments and encouragement. I had the opportunity to talk about mathematics with several people. In particular, I would like to thank Dr. Anindya Goswami, Dr. Rama Mishra, Dr. Steven Spallone, and Dr. Supriya Pisolkar, for sharing their insights into mathematics. I have learned a lot of mathematics from a lot of people, especially Prof Satya Deo from Harish Chandra Research Institute, Prof. Asok Nanda, Dr. Rajib Dutta, Dr. Saugata Bandyopadhyay, Dr. Shibananda Biswas, from IISER Kolkata, Prof. Amiya Mukherjee from ISI Kolkata, Prof.

Anant Shastri from IIT Bombay, Prof. Venkata Balaji T E from IIT Madras, Dr. Angom Tiken Singh from North Eastern Hill University, Prof. Parvati Shastri from the University of Bombay, and Dr. Hemant Kumar Singh from the University of Delhi. A special mention goes to Namrata Arvind from IISER Pune, who agreed upon working on a project with me. I would also like to thank Gaurav Kumar Shant from the University of Delhi and Sachchidanand Prasad from IISER Kolkata, for agreeing on learning parts of Mathematics together.

The next set of people is the one with whom I had the privilege of sharing food and life in different institutes and to them, I owe my sincere thanks. They were just a phone call away, whenever needed. This includes Sandip Murmu from IISER Kolkata, Firdousi Parvez, Narayanan P., Rajeshwari B. R. from IISER Pune.

I would like to thank all the friends in the department for helping me with the things I was not good about, be it math or something else. A special mention is to Saikat Goswami from TCG CREST, for showing endless love towards mathematics, which certainly kept me motivated during these years. It would not be fair if I don't mention people who were (mis)fortunate to taste food prepared by me. This includes a lot of people, but special mention goes to Dhruv Khatri, Digvijay Patil, Dilpreet Kaur, Narayanan P, Ratna Pal, and Swagata Dutta. I have missed a long list of people, whom I should've mentioned. I hope I will be forgiven.

Trekking has made it possible to meet new people from different parts of India and they have given me a new perspective of looking into life. Mentions are due to Arpit Muley, Apurv Shrivastabha, Devansh Shah. Shohag Biswas has a special place among all of them, for we have walked together miles and discussed things flawlessly during our course at Himalayan Mountaineering Institute.

My sincere thanks go to Sameer Inamdar from Dhrupad Academy and Naveen from CPR, for you two have taught me things outside academics, which has made my Ph. D. life a little easier. I am thankful to two anonymous people, one who had one hand amputated and was enthusiastic about cycling, another being a person in her sixties and trying two learn to swim. You have given me an enormous amount of strength.

I am thankful to NBHM for the financial support in the form of the research fellowship. I would like to acknowledge the support of the institute, its library staff members, its administrative staff members for their cooperation, special thanks are due to, Ms. Sayalee Damle, Mrs. Suvarna Bharadwaj, Mrs. Tanuja Sapre, Mr.

Tushar Kurulkar and Mr. Yogesh Kolap.

Finally, I would like to thank the reviewers for reading the thesis and giving their valuable comments. This has certainly helped to improve the exposure and readability of this thesis. Also, thanks are due to the anonymous referee of the paper "Hopf-Galois Realizability of $\mathbb{Z}_n \rtimes \mathbb{Z}_2$", which has helped to write some parts of the thesis more clearly.

September 23, 2022 *Saikat Panja*

Abstract

This thesis is divided into two parts. The first part concerns generating functions for M-powers ($M \geq 2$) in finite symplectic and orthogonal group. We will be giving generating functions for the separable, semisimple, cyclic, and regular conjugacy classes (and hence elements) in the concerned group. This enables us to find the corresponding probability with the help of generating functions.

The second part is concerned with skew braces corresponding to the groups of the form $\mathbb{Z}_n \rtimes \mathbb{Z}_2$. Fixing this group to be the additive group (resp. multiplicative group), we find the multiplicative group (resp. additive group), such that they form a skew brace when n is odd. A complete classification is obtained when we assume that the radical $\mathrm{Ra}(n)$ is a Burnside number.

Introduction

Waring type problem in the context of groups:

The British mathematician E. Waring, in his paper "Meditationes Algebraicae" [Wa91], stated 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$\cdots$

Legends are that he believed that, for every natural number $n \geq 2$, there exists a number $N(n)$ such that every positive integer m can be written as sum of $N(n)$ many n-powers, namely for any $x \in \mathbb{N}$, there exist $a_i \in \mathbb{N} \cup \{0\}$ such that

$$x = \sum_{i=1}^{N(n)} a_i^n.$$

This can be generalized in the contexts of groups as follows.

Question 1. *Given a group G and $n \in \mathbb{N}$ does there exist $N(n) \in \mathbb{N}$ such that each element of G is a product of $N(n)$ many n powers?*

This can be further generalized, which is known as word problems in group theory. By a word we mean an element $w = w(x_1, ..., x_d)$ of the free group F_d on the free generators $x_1, ..., x_d$. Given a word w and a group G, we consider the *word map*

$$w = w_G : G^d = \underbrace{G \times G \times \cdots \times G}_{d \text{ times}} \to G, \quad (g_1, ..., g_d) \mapsto w(g_1, ..., g_d).$$

The image of this map, namely the set of all group elements of the form $w(g_1, ..., g_d)$ (where $g_i \in G$) is denoted by $w(G)$. Two important questions studied extensively are: (i) How large $w(G)$ is, and (ii) what is the w-width of G?. Here the w-width of G is the minimal k such that $w(G)^k = \{x_1 x_2 \cdots x_k : x_i \in w(G)\} = \langle w(G) \rangle$, namely every element of the subgroup generated by $w(G)$ is a product of length k of elements of $w(G)$ (there is also a slightly different definition of width which allows also inverses of elements of $w(G)$). Another interesting question is to study the fibers of the word map w and in particular its kernel, namely the inverse image of 1. There are several motivations for the research directions described above. One is related to the classical Waring problem in Number Theory. Hilbert's solution to this problem shows that every natural number is a sum of $g(k)$ many k-th powers, where g is a suitable function. In recent years there has been much interest in word maps on groups, with various motivations and applications. Substantial progress has been made and many fundamental questions were solved, using a wide spectrum of tools, including representation theory, probability, and geometry. For example, famous Ore's conjecture (1951) asks whether every element of a non-abelian finite simple group is a commutator. This was solved by A. Shalev et al in [LiBrShTi10]. Indeed the authors prove 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. Later they proved results about the product of squares in finite non-abelian simple group in [LiBrShTi12]. They proved that every element of a nonabelian finite simple group G is a product of two squares. For more recent advancements and possible generalization, the survey article by A. Shalev [Sh13] is a good read.

Another motivation is Serre's question from the 1960s, whether every finite index subgroup of a (topologically) finitely generated profinite group is open. Other motivations for the study of word maps come from the study of residual properties of free groups, as well as certain questions in subgroup growth and representation varieties. A useful result proved by Borel in the 1980s states that word maps on simple algebraic groups are dominant maps [Bo83]. This can be applied in the study of word maps on finite simple groups of Lie type.

Power map - A special kind of word map:

To study Question 1, we need to first understand the powers of elements in a group. Let $M \geq 2$ be an integer. Then the map defined as

$$w : G \longrightarrow G, \quad g \longrightarrow g^M,$$

will be referred to as *power map*. Thus to answer Question 1, we need to find the image of this power map first. Hence we ask the following question.

Question 2. *Let G be a group and $M \geq 2$ be an integer. For which elements $g \in G$, there exists $y \in G$ such that $y^M = x$?*

This question has been answered for symmetric groups in a series of papers in [Be+Go89], [Bl74], [BoGl80], for $\mathrm{GL}(n, q)$ in [KuSi22] and for the wreath product of groups in [KuMo22]. Asymptotics of the powers in finite reductive group is studied in [KuKuSi21] and a formula is obtained. The generating functions for the corresponding probability has been obtained. For example, for $M = 2$ and $G = S_n$, if $P_2(n)$ denotes the probability of an element to be a square in S_n, we have that [Bl74, Lemma 1]

$$1 + \sum_{n=1}^{\infty} P_2(n) z^n = \left(\frac{1+z}{1-z}\right)^{\frac{1}{2}} \prod_{k=1}^{\infty} \cosh\left(\frac{u^{2k}}{2k}\right).$$

For $\mathrm{GL}(n, q)$ if $M \geq 2$ is an integer and $(q, M) = 1$, then the generating function for probability of a regular semisimple element being M-th power is given by [KuSi22, Theorem 5.2]

$$\prod_{d=1}^{\infty} \left(1 + \frac{z^d}{q^d - 1}\right)^{N_M(q,d)},$$

where $N_M(q, d)$ denotes the number of M-power polynomials in $\mathbb{F}_q[t]$. The cases for semisimple, cyclic and general case have also been studied in the same paper. This motivated the following question.

Main question 1. *Let G be one of the finite symplectic and orthogonal groups over fields of cardinality q. Let $M \geq 2$ be an integer. Let $g \in G$ be either of regular semisimple, semisimple, cyclic, or regular elements. Then, does there exist an element $h \in G$ such that $h^M = g$?*

We have mostly addressed the case $(M,q)=1$. Some partial answers for the case $(M,q)\neq 1$ have also been mentioned near the end of the first part. We will use the method of generating functions. Jason Fulman's [FuNePr05] work on generating functions for the conjugacy classes is of much help. For example, in case of the Symplectic group the probability of an element being regular is given by

$$\prod_{d=1}^{\infty}\left(1+\frac{z^d}{q^d+1}\right)^{N^*(q,2d)}\prod_{d=1}^{\infty}\left(1+\frac{z^d}{q^d-1}\right)^{M^*(q,d)},$$

where $N^*(q,2d)$ denotes the number of self reciprocal polynomials of degree $2d$ and $M^*(q,d)$ is the number of the polynomials of degree d which are not self reciprocal. We provide the generating functions for the probability of an element being M-power, in case the element is regular, regular semisimple, semisimple or cyclic. Before stating our main results, we will need the following functions.

$$\begin{aligned}
F_{+,+1}(u,q) =& 1+\sum_{m\geq 1}\left(\frac{1}{|\mathrm{O}^+(2m,\mathbb{F}_q)|}+\frac{1}{|\mathrm{O}^-(2m,\mathbb{F}_q)|}\right)u^m,\\
F_{-,+1}(u,q) =& 1+\sum_{m\geq 1}\left(\frac{1}{|\mathrm{O}^+(2m,\mathbb{F}_q)|}-\frac{1}{|\mathrm{O}^-(2m,\mathbb{F}_q)|}\right)u^m,\\
F_{+1}(u,q) =& 1+\sum_{m\geq 1}\frac{u^m}{|\mathrm{Sp}(2m,\mathbb{F}_q)|},\\
F^M_{+,-1}(u,q) =& 1+\sum_{m\geq 1}\left(\frac{1}{|\mathrm{O}^+(mr(M,q),\mathbb{F}_q)|}+\frac{1}{|\mathrm{O}^-(mr(M,q),\mathbb{F}_q)|}\right)u^{m\frac{r(M,q)}{2}},\\
F^M_{-,-1}(u,q) =& 1+\sum_{m\geq 1}\left(\frac{1}{|\mathrm{O}^+(mr(M,q),\mathbb{F}_q)|}-\frac{1}{|\mathrm{O}^-(mr(M,q),\mathbb{F}_q)|}\right)u^{m\frac{r(M,q)}{2}},\\
F_{-1}(u,q) =& 1+\sum_{m\geq 1}\frac{u^{\frac{mr(M,q)}{2}}}{|\mathrm{Sp}(mr(M,q),\mathbb{F}_q)|},\\
Z_{\mathrm{O}}(u) =& \prod_{d=1}^{\infty}\left(1+\frac{u^d}{(q^d+1)(1-(\frac{u}{q})^d)}\right)^{N^*_M(q,2d)}\left(1+\frac{u^d}{(q^d-1)(1-(\frac{u}{q})^d)}\right)^{R^*_M(q,2d)},\\
Z'_{\mathrm{O}}(u) =& \prod_{d=1}^{\infty}\left(1-\frac{u^d}{(q^d+1)(1+(\frac{u}{q})^d)}\right)^{N^*_M(q,2d)}\left(1+\frac{u^d}{(q^d-1)(1-(\frac{u}{q})^d)}\right)^{R^*_M(q,2d)}.
\end{aligned}$$

By $e(q)$ we mean the number of square roots of 1 in $\mathbb{F}_q$. The following are our main results regarding Main Question 1.

Theorem 1. *Let* $s^M_{\mathrm{Sp}}(n,q)$ *be the probability of an element to be* M*-power separable in* $\mathrm{Sp}(2n,\mathbb{F}_q)$ *and* $S^M_{\mathrm{Sp}}(q,u) = 1 + \sum\limits_{m=1}^{\infty} s^M_{\mathrm{Sp}}(m,q)u^m$*. Then*

$$S^M_{\mathrm{Sp}}(q,u) = \prod_{d=1}^{\infty}\left(1+\frac{u^d}{q^d+1}\right)^{N^*_M(q,2d)} \prod_{d=1}^{\infty}\left(1+\frac{u^d}{q^d-1}\right)^{R^*_M(q,2d)}.$$

Theorem 2. *Let* $s^M_{\mathrm{O}^\epsilon}(n,q)$ *be the probability of an element to be* M*-power separable in* $\mathrm{O}^\epsilon(2n,\mathbb{F}_q)$ *with* $\epsilon \in \{\pm\}$ *and* $s^M_{\mathrm{O}^0}(n,q)$ *denotes the probability of an element to be* M*-power separable in* $\mathrm{O}^0(2n+1,\mathbb{F}_q)$*. Define*

$$\begin{aligned} S^M_{\mathrm{O}^+}(q,u) &= 1 + \sum_{m\geq 1}^{\infty} s^M_{\mathrm{O}^+}(m,q)u^m \\ S^M_{\mathrm{O}^-}(q,u) &= \sum_{m\geq 1}^{\infty} s^M_{\mathrm{O}^-}(m,q)u^m \\ S^M_{\mathrm{O}^0}(q,u) &= 1 + \sum_{m\geq 1}^{\infty} s^M_{\mathrm{O}^0}(m,q)u^m. \end{aligned}$$

Then

$$\begin{aligned} &S^M_{\mathrm{O}^+}(u^2) + S^M_{\mathrm{O}^-}(u^2) + e(q)uS^M_{\mathrm{O}^0}(u^2) = (1+u)^{o(M,q)}S^M_{\mathrm{Sp}}(u^2), \\ &S^M_{\mathrm{O}^+}(u^2) - S^M_{\mathrm{O}^-}(u^2) = X^M_{\mathrm{O}^0}(u^2), \end{aligned}$$

where

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

$e(q)$ *as before and*

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

Theorem 3. *Let* $ss^M_{\mathrm{Sp}}(n,q)$ *be the probability of an element to be* M*-power semisim-*

ple in $\mathrm{Sp}(2n,\mathbb{F}_q)$ *and* $SS^M_{\mathrm{Sp}}(q,u)=1+\sum\limits_{m=1}^{\infty} ss^M_{\mathrm{Sp}}(2m,q)u^m$. *Then*

$$\begin{aligned}
SS^M_{\mathrm{Sp}}(q,u) &= \left(1+\sum_{m\geq 1}\frac{u^{m\frac{r(M,q)}{2}}}{|\mathrm{Sp}(mr(M,q),\mathbb{F}_q)|}\right)^{e(q)-1}\left(1+\sum_{m\geq 1}\frac{u^m}{|\mathrm{Sp}(2m,\mathbb{F}_q)|}\right)\\
&\times\prod_{d=1}^{\infty}\left(1+\sum_{m\geq 1}\frac{u^{dm}}{|\mathrm{U}(m,\mathbb{F}_{q^d})|}\right)^{N^*_M(q,2d)}\prod_{d=1}^{\infty}\left(1+\sum_{m\geq 1}\frac{u^{dm}}{|\mathrm{GL}(m,\mathbb{F}_{q^d})|}\right)^{R^*_M(q,2d)}\\
&\times\prod_{d=1}^{\infty}\prod_{e|q^d+1}\left(1+\sum_{m=1}^{\infty}\mathcal{I}_{e,2d}(2dm)\frac{u^{dm}}{|\mathrm{U}(m,\mathbb{F}_{q^d})|}\right)^{N^{*,e}_M(q,2d)}\\
&\times\prod_{d=1}^{\infty}\prod_{e|q^d-1}\left(1+\sum_{m=1}^{\infty}\mathcal{I}_{e,d}(dm)\frac{u^{dm}}{|\mathrm{GL}(m,\mathbb{F}_{q^d})|}\right)^{R^{*,e}_M(q,2d)}
\end{aligned}$$

where

$$r(M,q)=\begin{cases}2 & \textit{if } M=2\\ s & \textit{if there exists } n \textit{ such that } 2M|(q^n+1),(M,q)=1\\ 2s & 2M\nmid(q^n+1) \textit{ for any } n,(M,q)=1\\ r\left(\frac{2M}{(2M,q)},q\right) & \textit{when } (M,q)\neq 1\end{cases},$$

where $s\in\mathbb{N}$ *is the smallest number satisfying* $q^s\equiv 1(\mathrm{mod}\ 2M)$.

Theorem 4. *Let* $ss^M_{\mathrm{O}^\epsilon}(n,q)$ *denotes the probability of an element to be* M*-power semisimple in* $\mathrm{O}^\epsilon(2n,\mathbb{F}_q)$ *with* $\epsilon\in\{\pm\}$ *and* $s^M_{\mathrm{O}^0}(n,q)$ *denotes the probability of an element to be* M*-power semisimple in* $\mathrm{O}^0(2n+1,\mathbb{F}_q)$.

Define

$$\begin{aligned}
SS^M_{\mathrm{O}^+}(q,u) &= 1+\sum_{m\geq 1}^{\infty} ss^M_{\mathrm{O}^+}(m,q)u^m\\
SS^M_{\mathrm{O}^-}(q,u) &= \sum_{m\geq 1}^{\infty} ss^M_{\mathrm{O}^-}(m,q)u^m\\
SS^M_{\mathrm{O}^0}(q,u) &= 1+\sum_{m\geq 1}^{\infty} ss^M_{\mathrm{O}^0}(m,q)u^m.
\end{aligned}$$

Then

$$\begin{aligned}
&SS^M_{\mathrm{O}^+}(u^2) + SS^M_{\mathrm{O}^-}(u^2) + e(q)uSS^M_{\mathrm{O}^0}(u^2)\\
&= \left(F^M_{+,+1}(u^2) + uF_{+1}(u^2)\right)\left(F^M_{+,-1}(u^2) + uF_{-1}(u^2)\right)^{e(q)-1} Y_1^{*,M}(u^2),\\
&S^M_{\mathrm{O}^+}(u^2) - S^M_{\mathrm{O}^-}(u^2) = F_{-,+1}(u^2)[F^M_{-,-1}(u^2)]^{e(q)-1}Y_2^{*,M}(u^2).
\end{aligned}$$

Theorem 5. *Let $c^M_{\mathrm{Sp}}(n,q)$ be the probability of an element to be M-power cyclic in $\mathrm{Sp}(2n,\mathbb{F}_q)$ and $C^M_{\mathrm{Sp}}(q,u) = 1 + \sum\limits_{m=1}^{\infty} c^M_{\mathrm{Sp}}(2m,q)u^m$. Then $C^M_{\mathrm{Sp}}(q,u)$ is given by*

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

if $(q,M)=1$,

$$h(q,M) = \begin{cases} 0 & \text{if } (M,q) \neq 1\\ 2 & \text{if } (M,q) = 1, M = odd, (q,2) = 1\\ 1 & otherwise \end{cases}$$

and

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

if $(q,M) \neq 1$.

Theorem 6. *Let $c^M_{\mathrm{O}^\epsilon}(n,q)$ be the probability of an element to be M-power cyclic in $\mathrm{O}^\epsilon(2n,\mathbb{F}_q)$ with $\epsilon \in \{\pm\}$ and $c^M_{\mathrm{O}^0}(n,q)$ denotes the probability of an element to be M-power cyclic in $\mathrm{O}^0(2n+1,\mathbb{F}_q)$. Define*

$$\begin{aligned}
C^M_{\mathrm{O}^+}(q,u) &= 1 + \sum_{m\geq 1}^{\infty} c^M_{\mathrm{O}^+}(m,q)u^m\\
C^M_{\mathrm{O}^-}(q,u) &= \sum_{m\geq 1}^{\infty} c^M_{\mathrm{O}^-}(m,q)u^m\\
C^M_{\mathrm{O}^0}(q,u) &= 1 + \sum_{m\geq 1}^{\infty} c^M_{\mathrm{O}^0}(m,q)u^m.
\end{aligned}$$

Then

$$C_{\mathrm{O}^+}(u^2) + C_{\mathrm{O}^-}(u^2) + 2uC_{\mathrm{O}^0}(u^2) = \left(1 + \eta(q)u + \frac{u^2}{1-\frac{u^2}{q}}\right)^{h(q,M)} Z_{\mathrm{O}}(u^2),$$

where

$$h(q,M) = \begin{cases} 0 & \text{if } (M,q) \neq 1 \\ 2 & \text{if } (M,q) = 1, M = \text{odd}, (q,2) = 1 \\ 1 & \text{otherwise} \end{cases}$$

and $\eta(q) = \begin{cases} 0 & \text{if } (q,2) = 1 \\ 1 & \text{otherwise} \end{cases}$,

and

$$C^M_{\mathrm{O}^+}(u^2) - C^M_{\mathrm{O}^+}(u^2) = Z'_O(u^2).$$

Theorem 7. *For an odd integer q, let $r^M_{\mathrm{O}^\epsilon}(n,q)$ be the probability of an element to be M-power regular in $\mathrm{O}^\epsilon(2n,\mathbb{F}_q)$ with $\epsilon \in \{\pm\}$ and $r^M_{\mathrm{O}^0}(n,q)$ denotes the probability of an element to be M-power regular in $\mathrm{O}^0(2n+1,\mathbb{F}_q)$. Define*

$$R^M_{\mathrm{O}^+}(q,u) = 1 + \sum_{m\geq 1}^{\infty} r^M_{\mathrm{O}^+}(m,q)u^m$$
$$R^M_{\mathrm{O}^-}(q,u) = \sum_{m\geq 1}^{\infty} r^M_{\mathrm{O}^-}(m,q)u^m$$
$$R^M_{\mathrm{O}^0}(q,u) = 1 + \sum_{m\geq 1}^{\infty} r^M_{\mathrm{O}^0}(m,q)u^m.$$

Then

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

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

The first part of the thesis is dedicated to answering the Main Question 1 and is organized as follows. In Chapter 1 we recall some concepts from the theory of finite groups of Lie type. The second chapter describes the conjugacy classes of the concerned group in terms of generating functions. In the third chapter, we mention the theory of the cycle index. The concept of M^*-power polynomial is defined in Chapter 4 and will be used throughout the chapter to answer the concerned question. A substantial amount of this part has been put into the paper [PaSi22].

Skew braces:

A set theoretical solution of the Yang-Baxter equation is a pair (X, r) where

$$r : X \times X \longrightarrow X \times X$$

is a bijective map satisfying

$$(r \times id)(id \times r)(r \times id) = (id \times r)(r \times id)(id \times r).$$

The map r is closely related to braid relations in braid group and sometimes called as *braiding.* Such a solution will be called *non-degenerate* if the coordinate maps are bijective. The solution will be called *involutive* if r^2 is the identity map. Braces were introduced by W. Rump to study set theoretic non-degenerate solutions of the Yang Baxter equations, particularly the involutive solution in [Ru07]. Rump showed that every involutive non-degenerate solution of the Yang-Baxter equation can be in a good way embedded in a brace, and that on the other hand, every brace gives a solution of the quantum Yang-Baxter equation. Later, the classification of non-degenerate involutive set-theoretic solutions of the Yang-Baxter equation was reduced to the classification of braces by Bachiller, Cedo, Jespers, and Okninski in [CeJeOk14] and [BaFeJe16]. This was generalized in a non-commutative setting by L. Guarnieri and L. Vendramin as Skew braces, which initially appeared in D. Bachiller Ph.D. thesis, were recently studied extensively by Guarnieri, Smoktunowicz, and Vendramin (also Byott) [GuVe17], [SmVe18]. This was used further to develop an algorithm to construct and enumerate classical and non-classical braces of comparatively smaller size, taking into account the work of Bachiller, Catino and Rizzo.

Given a skew brace $(B, \cdot, \circ)$, we have two associated groups $(B, \circ)$ and $(B, \cdot)$ satisfying some compatibility condition among them. One of such condition can be given by

$$(B, \cdot) \hookrightarrow \mathrm{Hol}(B, \circ),$$

where $\mathrm{Hol}(G) = G \rtimes_{id} \mathrm{Aut}(G)$ for a group G. Note that both of $(B, \cdot)$ and $(B, \circ)$ are of same order. Hence it is natural to ask the following question.

Question 3. *Let G_1 and G_2 be two groups of same order k. Then does there exist a skew brace $(B, \cdot, \circ)$, such that $(B, \cdot) \cong G_1$ and $(B, \circ) \cong G_2$?*

As k increases, the number of groups also increases significantly and hence it becomes difficult to catch hold of two groups, which can fit together to construct a skew brace.

A much more powerful tool that can be deployed to study this question is via the theory of Hopf-Galois modules. As we will see in chapter 6, these two are closely related. We will see that given two groups G, N of the same order, if there exists a Hopf-Galois structure with group G of type N, then there is a skew brace $(B, \cdot, \circ)$ such that $(B, \circ) \cong G$ and $(B, \cdot) \cong N$. The method of crossed homomorphism was introduced by Cindy Tsang in [Ts19]. This was further used to study the non-existence of Hopf-Galois structure for a certain class of groups. Using the correspondence between Hopf-Galois structure and skew-braces those results can be translated in terms of skew braces. For example [Ts22, Theorem 1.6].

If $(B, \cdot, \circ)$ is a skew brace such that $(B, \circ)$ is a cyclic group and $(B, \cdot)$ is a non-C-group, then $(B, \cdot)$ is isomorphic to a group of the form $M \rtimes_\alpha P$, for some C-group M of odd order and (P, α) satisfying one of the following conditions:

1. $P = D_4$ or $P = Q_8$ with $\alpha(P)$ has order 1 or 2;

2. $P = D_{2^m}$ with $m \geq 3$ or $P = Q_{2^m}$ with $m \geq 4$ and $\alpha(r) = Id_M$;

where α is the determining homomorphism and r is the rotation in the presentation of dihedral or quaternion group.

This has motivated the following question.

Main question 2. *Let $G = \mathbb{Z}_n \rtimes \mathbb{Z}_2$. What are all the skew braces $(B, \cdot, \circ)$ such that either $(B, \cdot) \cong G$ or $(B, \circ) \cong G$?*

We answer this question in the second part of the thesis, for the case, n being odd and give some partial result towards the case $n \equiv 2 \pmod 4$. The main results are as follows.

Theorem 8. *Let N be a group of order $2n$, where n is odd and the pair $(\mathbb{Z}_n \rtimes \mathbb{Z}_2, N)$ is realizable. Then $N \cong (\mathbb{Z}_k \rtimes \mathbb{Z}_l) \rtimes \mathbb{Z}_2$ where $(k, l) = 1, lk = n$.*

Theorem 9. *Let G be a group of order $2n$ such that the pair $(G, \mathbb{Z}_n \rtimes \mathbb{Z}_2)$ is realizable. Then $G = (\mathbb{Z}_k \rtimes \mathbb{Z}_l) \rtimes \mathbb{Z}_2$ for some $(k, l) = 1, kl = n$.*

We will start by recalling the basic concepts of skew braces in Chapter 5. Thereafter in Chapter 6, we will mention the relation between Hopf-Galois theory and bijective crossed homomorphisms. The seventh Chapter is concerned with proof of the main results. This part of the thesis appears in the article [ArPa22b].

Part I

Results in Power Maps

Chapter 1

Finite groups of Lie type

The exposition here follows closely the texts [MaTe11] by G. Malle, D. Testerman, [Wi17] by W. A. Graff, [Sp09] by T. A. Springer and [Hu75] by J. E. Humphreys.

1.1 Prerequisite from algebraic geometry

Let k be an alebgraically closed field. A subset $X \subseteq k^n$ is called an *algebraic set* if there exists an ideal $I \subseteq k[x_1, x_2, \cdots, x_n]$ such that

$$X = \{(a_1, a_2, \cdots, a_n) \in k^n : f(a_1, a_2, \cdots, a_n) = 0 \text{ for all } f \in I\}.$$

The set $\{(a_1, a_2, \cdots, a_n) \in k^n : f(a_1, a_2, \cdots, a_n) = 0 \text{ for all } f \in I\}$ is denoted as $V(I)$ and is called the *zero set of the ideal I*. Again for a subset $S \subseteq k^n$, define the *vanishing ideal*

$$I(S) = \{f \in k[x_1, x_2, \cdots, x_n] : f(s) = 0 \text{ for all } s \in S\}.$$

Since $I(S)$ is an ideal of $k[x_1, x_2, \cdots, x_n]$, the quantity $k[x_1, x_2, \cdots, x_n]/I(S)$ makes sense. This will be called the *affine algebra of S*.

Example 1.1.1. 1. Let $t = (t_1, t_2) \in k^2$. Then $\{t\} = V(\langle x_1 - t_1, x_2 - t_2\rangle)$ is an algebraic set. The vanishing ideal of $\{t\}$ is given by $\langle x_1 - t_1, x_2 - t_2\rangle \subseteq k[x_1, x_2]$. The affine algebra is given by $k[x_1, x_2]/\langle x_1 - t_1, x_2 - t_2\rangle$.

2. Let

$$S = \left\{ \begin{bmatrix} t_1 & t_2 \\ t_3 & t_4 \end{bmatrix} : t_i \in k, t_1t_4 - t_2t_3 \neq 0 \right\}.$$

Then S is in bijection with the set $U = \{(u_1, u_2, u_3, u_4, u_5) \in k^5 : (u_1u_4 - u_2u_3)u_5 = 1\}$. Hence S is an algebraic set with vanishing ideal $\langle (x_1x_4 - x_2x_3)x_5 \rangle$. The affine algebra of S is given by $k[x_1, x_2, x_3, x_4, x_5]/\langle (x_1x_4 - x_2x_3)x_5 \rangle$.

Considering $\{S_\lambda\}$, a collection of algebraic sets corresponding to ideals $\{I_\lambda\}$, it is routine to check that

$$\begin{aligned} S_{\lambda_1} \cup S_{\lambda_2} &= V(I_{\lambda_1} \cap I_{\lambda_2}) \\ S_{\lambda_1} \cap S_{\lambda_2} &= V(\langle I_{\lambda_1} \cup I_{\lambda_2} \rangle). \end{aligned}$$

Hence the collection of algebraic sets corresponds to the collection of closed sets in topology. This topology on k^n will be called as *Zariski topology*. From now on k^n will be considered as a topological space under this topology and any subset of k^n will be considered with the induced topology. A topological space $\emptyset \neq T \subseteq k^n$ will be called *reducible* if there are nonempty proper closed subsets T_1, T_2 of T satisfying $T = T_1 \cup T_2$. Otherwise, T will be called *irreducible*. Moreover call T to be a *Noetherian space* if any sequence of closed sets $T_1, \cdots, T_n$ of T satisfies existence of m such that $T_{m+i} = T_m$ for all $i \in \mathbb{N}$. It can be proved [Hu75, 1.3, Proposition B] that there are only finitely many maximal closed irreducible subsets in a non-empty Noetherian topological space T. These are called *irreducible components* of T. Using Hilbert basis theorem we observe that an algebraic set is Noetherian in Zariski topology. Furthermore, it can be shown that an algebraic set S is irreducible if and only if the vanishing ideal is a prime ideal [Hu75, 1.3, proposition C].

Let $S \subseteq k^m, T \subseteq k^n$ be two algebraic sets. A set theoretic map $\psi : S \to T$ is called a *regular map* if there exist polynomials $f_1, f_2, \ldots, f_n \in k[x_1, x_2, \ldots, x_m]$ such that

$$\psi(x) = (f_1(x), f_2(x), \ldots, f_n(x)),$$

for all $x = (x_1, x_2, \ldots, x_m) \in S$.

1.2 Algebraic groups

Definition 1.2.1. Let $G \subseteq k^n$ be an algebraic variety. Then G will be called an algebraic group if the group operations viz. the multiplication map $m : G \times G \to G$

and the inversion map $i : G \to G$ given by $m(a, b) = ab$ and $i(a) = a^{-1}$ are regular maps.

Example 1.2.2. 1. Let $G = \{z \in \mathbb{C} : z^m = 1\}$. Then the group operations

$$m(x, y) = xy \qquad\qquad i(x) = x^{m-1}$$

are both regular maps. Hence this is an algebraic group as G is an affine closed set corresponding to the polynomial $t^m - 1 \in \mathbb{C}[t]$.

2. Let W be an m-dimensional vector space over k and $\mathrm{GL}(W)$ denote the group of invertible endomorphisms of W. Take the following set

$$\mathbb{C}^{n^2+1} = \{((a_{ij})_{1\leq i,j\leq n}, b) : a_{ij}, b \in k\}.$$

Then we have that

$$\mathrm{GL}(W) = \{((a_{ij}), b) : \det(a_{ij})b - 1 = 0\}$$

is an affine variety. Since the multiplication map and inversion map are regular maps, we get that $\mathrm{GL}(W)$ is an algebraic group. This will often be denoted as $\mathrm{GL}(n, k)$.

3. Let k does not have characteristic 2. Let G be the subset of $\mathrm{GL}(2n, k)$ consisting of A such that A satisfies the matrix equation

$$^{t}AJA = J, \quad \text{where } J = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \iddots & \vdots & \vdots \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Then this is an affine variety as it is a zero set of the polynomials determined by the set of polynomials, which are determined by comparing the matrix entries of two sides. Also as before, this is an algebraic group.

A topological space X is said to be *irreducible* if it can not be written as a union of two proper closed non-empty subsets. For an affine variety, it is equivalent to saying that any two non-empty open subsets intersect non-trivially or to the statement that the ring of functions $k[X]$ is an integral domain [MaTe11, Proposition 1.9]. Given two affine varieties X, Y we have that [MaTe11, Proposition 1.10]

1. If X, Y are irreducible then $X \times Y$ is also irreducible,

2. X is irreducible implies that the toplogical closure $\overline{X}$ is also irreducible,

3. X has only finitely many irreducible subsets (known as *irreducible components*).

A topological space is called connected if it can not be written as disjoint union of two proper closed subsets. It can be proved that for an algebraic group the concept of irreducible and connectedness are equivalent.

Example 1.2.3. 1. Since the ring of functions of the groups $\mathbb{G}_a$ and $\mathbb{G}_m$ are $k[t], k[t, t^{-1}]$ respectively, and are integral domain, they are connected (or irreducible).

2. GL_n is a connected algebraic group, since $k[\mathrm{GL}_n]$, being localization of the polynomial ring $k[t_{ij}]$ at the polynomial $\det(t_{ij})$, is an integral domain.

3. The orthogonal group is not connected as $\det^{-1}(\{1\})$ is a closed subgroup of index 2.

1.3 Jordan Decomposition

Recall that given an element $x \in M_n(k)$, there exists unique $s, n \in M_n(k)$, such that $x = s + n$ and $sn = ns$ [HoKu71, Chapter 7]. The element s is known as semisimple part and the element n is called the nilpotent part of x. There is a multiplicative analogue of this result. Given $x \in \mathrm{GL}_n(k)$, there exist unique $s, u \in \mathrm{GL}_n(k)$ such that s is semisimple (i.e. diagonalizable) and u is unipotent (i.e. $u - 1$ is nilpotent) satisfying $x = su = us$. The elements s, u are known as *semisimple, unipotent part of* x respectively. Now let G be a linear algebraic group. Then

1. If ϕ is an embedding of G in $\mathrm{GL}_n(k)$ and $g \in G$, then there exist $g_s, g_u \in G$ satisfying $g = g_s g_u = g_u g_s$ such that $\phi(g_s)$ is semisimple and $\phi(g_u)$ is unipotent [Hu75, Theorem 15.3(a)].

2. The decomposition of g into this product is independent of embedding [MaTe11, Theorem 2.5].

3. The semisimple and unipotent parts are preserved under morphism of algebraic groups [Hu75, Theorem 15.3(c)].

If G is an algebraic group and $g \in G$, then $g = g_s g_u = g_u g_s$ will be referrred to as *Jordan decomposition* of g. We call a group to be *unipotent* if all the elements are unipotent.

Example 1.3.1. The group $k_a = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in k \right\}$ is a unipotent group.

In general it can be shown that the group

$$U(n,k) = \left\{ \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ & 1 & \cdots & a_{2n} \\ & & \ddots & \vdots \\ & & & 1 \end{pmatrix} a_{ij} \in k, a_{ij} = 0 \text{ for all } i > j \right\},$$

is a unipotent group. Also given $G \subseteq \mathrm{GL}_n$ a unipotent group, it can be conjugated to a subgroup of U_n [Hu75, Corollary 17.5]. Since U_n is nilpotent, we deduce that any unipotent linear algebraic group is nilpotent, hence solvable. Jordan decomposition of elements lead to similar decomposition for commutative algebraic group. If G is a commutative linear algebraic group, then $G_s = \{g_s : g \in G\}$ and $G_u = \{g_u : g \in G\}$ are closed subgroups of G [MaTe11, Theorem 3.1]. In this case the product map $\pi : G_u \times G_s \longrightarrow G$ is an isomorphism of algebraic groups. Using this it can be proved that, if G is an algebraic group of dimension 1 then $G \cong \mathbb{G}_a$ or $G \cong \mathbb{G}_m$ [Hu75, Theorem 20.5].

1.4 Semisimple algebraic groups and their classification

A linear algebraic group of the form $\mathbb{G}_m \times \mathbb{G}_m \times \cdots \times \mathbb{G}_m$ will be called a *torus*. A *character* (resp. *cocharacter*) of G is a morphism of algebraic groups $\chi : G \longrightarrow \mathbb{G}_m$ (resp. $\gamma : \mathbb{G}_m \longrightarrow G$). The set of all characters (resp. cocharacters) forms a group and will be called as *character (resp. cocharacter) group*. Let T be a torus with charcater group X, cocharacter group Y. Then the map $\langle , \rangle : X \times Y \longrightarrow \mathbb{Z}$ (which is defined as $\chi(\gamma(t)) = t^{\langle \chi, \gamma \rangle}$) is a perfect pairing, i.e. any homomorphism $X \longrightarrow \mathbb{Z}$

(resp. $Y \longrightarrow \mathbb{Z}$) is of the form $\chi \mapsto \langle \chi, \gamma \rangle$ (resp. $\gamma \mapsto \langle \chi, \gamma \rangle$) for some $\gamma \in Y$ (resp. $\chi \in X$).

A maximal closed connected solvable subgroup B of G will be called a *Borel subgroup* of G. If G is a linear algebraic group we have that, all Borel subgroups are conjugate in G [Hu75, Theorem 21.3]. Since tori are contained in Borel subgroups, we get that all maximal tori are conjugate to each other [Hu75, Corollary 21.3]. By *radical of* G, to be denoted $R(G)$ we mean the maximal connected solvable normal subgroup of G. The set $R(G)_u$ is the maximal closed connected normal unipotent subgroup of G, which is known as *unipotent radical* of G, which is denoted as $R_u(G)$. In the case $R_u(G) = 1$, the linear algebraic group G is called *reductive*. When $R(G) = 1$, the group G will be called *semisimple*, provided G is connected.

For a k-algebra A, a k-linear map $\delta : A \longrightarrow A$ is called a derivation of A if $\delta(ab) = a\delta(b) + \delta(a)b$. The set of all derivations of A will be denoted as $D(A)$. A multiplication in this space can be defined as $\delta_1 \cdot \delta_2 = \delta_1\delta_2 - \delta_2\delta_1$. The *Lie algebra of* G is the subspace of left invariant derivations of $k[G]$, i.e.

$$\mathrm{Lie}(G) = \{\delta \in D(k[G]) : \delta\lambda_x = \lambda_x\delta\},$$

where $\lambda_x : k[G] \longrightarrow k[G]$ is the map $(\lambda_x(f))(g) = f(x^{-1}g)$. The Lie algebra of G is a vector space and can be classified via the associated combinatorial data, known as root system. An *abstract root system* in a finite dimensional real vector space V is a finite subset $\Phi \subseteq V$ such that $\alpha, c\alpha \in \Phi$ iff $c = \pm 1$, for each α there is $s_\alpha \in \mathrm{GL}(V)$ stabilizing Φ, and for $\alpha, \beta \in \Phi$ we have that $s_\alpha\beta - \beta \in \mathbb{Z}\alpha$. A root system is called indecomposable if it can not be written as a union of two non-empty proper mutually orthogonal subsets. Via the classification of root systems, it is known that if Φ is an indecomposable root system, then up to isomorphism it is one of the following types [Hu72, Thorem 11.4]:

$$A_n(n \geq 1), B_n(n \geq 2), C_n(n \geq 3), D_n(n \geq 4), E_6, E_7, E_8, F_4, G_2.$$

A quadruple $(X, \Phi, Y, \Phi^\vee)$ is called a *root datum* if

1. $X \cong \mathbb{Z}^n \cong Y$ with a perfect pairing $\langle , \rangle : X \times Y \longrightarrow \mathbb{Z}$;

2. $\Phi \subset X, \Phi^\vee \subset Y$ are abstract root system in the real vector spaces generated by ϕ and $\phi^\vee$ respectively;

3. a bijection exists $\Phi \longrightarrow \Phi^\vee$ satisfying $\langle \alpha, \alpha^\vee \rangle = 2$;

4. the reflections s_α of the root system Φ and $s_{\alpha^\vee}$ of $\Phi^\vee$ are given by

$$\begin{aligned} s_\alpha \cdot \chi &= \chi - \langle \chi, \alpha^\vee \rangle \alpha && \text{for all } \chi \in X \\ s_{\alpha^\vee} \cdot \gamma &= \gamma - \langle \alpha, \gamma \rangle \alpha^\vee && \text{for all } \gamma \in Y. \end{aligned}$$

The root system attached with the Lie algebra of an algebraic group will be called *Lie algebra of* G. Let Φ be the root system of a connected reductive group G with respect to the maximal torus T. Then setting $\Phi^\vee = \{\alpha^\vee : \alpha \in \Phi\}$, we get that $(X(T), \Phi, Y(T), \Phi^\vee)$ is a root datum. We are now ready to state the classification result due to Chevalley:

Theorem 1.4.1. *Two semisimple linear algebraic groups are isomorphic if and only they have isomorphic root data.*

1.5 Steinberg endomorphism and Classification of finite groups of Lie type

Given $F_q : k \longrightarrow k$ defined as $F_q(t) = t^q$, it induces an automorphism of GL_n given by $(a_{ij}) \longrightarrow (F_q(a_{ij}))$. This map is called the *standard Frobenius of* GL_n. Note that the fixed point group of this action is $\mathrm{GL}_n(\mathbb{F}_q)$. An endomorphism $F : G \longrightarrow G$ of a linear algebraic group G is called a *Steinberg endomorphism* of G, if for some $r \geq 1$, we have that $F^r : G \longrightarrow G$ is Frobenius morphism of the form F_{p^α}. Steinberg proved [St68, Theorem 10.13] that if G is a simple linear algebraic group, $\sigma : G \longrightarrow G$ is an endomorphism of G, then either of the following statements hold:

1. σ is an automorphism of G,

2. the group $G^\sigma := \{g \in G : \sigma(g) = g\}$ is a finite group.

Also, the second case occurs if and only if σ is a Steinberg endomorphism. Now if $F : G \longrightarrow G$ is a Steinberg endomorphism of a semisimple algebraic group, then the finite group of fixed points G^F will be called a *finite group of Lie type.*

Now, let G be a connected reductive linear algebraic group and $F : G \longrightarrow G$ a Steinberg endomorphism. Then it can be proved [MaTe11, Corollary 21.12] that there exist a pair $T \subseteq B$ consisting of F-stable torus and F-stable Borel subgroup.

The group $W := N_G(T)/T$ is called the *Weyl group of* G. Note that F acts on the character group X and cocharacter group Y as follows:

$$\begin{aligned} F(\chi)(t) &= \chi(F(t)) && \chi \in X, t \in T \\ F(\gamma)(c) &= F(\gamma(c)) && \gamma \in Y, c \in k^\times. \end{aligned}$$

Let $\Phi \subset X$ be a root system of G with respect to T and B. We fix an isomorphism $u_\beta : G_a \longrightarrow U_\beta$ for $\beta \in X$. We further set $X_\mathbb{R} = X \otimes_\mathbb{Z} \mathbb{R}$. Note that the Weyl group $N_G(T)/T$ is F-stable which defines a semidirect product $W\langle F\rangle$. Thus a finite group of Lie type (G, F) is determined upto isomorphism by the root datum of G, the coset $W\phi$ and q, where $\phi \in \operatorname{Aut}(X_\mathbb{R})$ stabilizes $\Phi \subset X, \Phi^\vee \subset Y$, in the sense that if $(G, F), (G', F')$ both correspond to $(X, \Phi, Y, \Phi^\vee, W\phi)$ and same q, there is an isomorphism $\sigma : G \longrightarrow G'$ satisfying $F' \circ \sigma = \sigma \circ F$. The ordered tuple $(X, \Phi, Y, \Phi^\vee, W\phi)$ is known as a *complete root datum.* The complete root datum along with the prime power q completely determines the finite group G^F up to isomorphism [MaTe11, Corollary 21.8].

Example 1.5.1. Recall that the orthogonal group O_{2n}, preserving the quadratic form $x_1x_{2n} + \cdots + x_nx_{n+1}$ on $\overline{\mathbb{F}_q}^{2n}$. Then $\mathrm{O}(2n, \mathbb{F}_q)$ is stable under standard Frobenius map $F_q(x) = x^q$. We write $\mathrm{O}(2n, \mathbb{F}_q)^+ := \mathrm{O}(2n, q)^{F_q}$ is the orthogonal group of $+$ type.

Example 1.5.2. It can be shown that there exists a Steinberg endomorphism F'_q, which induces non-trivial graph automorphism of order 2 on the Dynkin diagram of O_{2n} [MaTe11, Example 22.9]. The fixed point of this is known as the orthogonal group of $-$ type.

Chapter 2

Conjugacy classes and centralizer

This chapter follows the expositions in [Ta1], [Ta2] by D. E. Taylor, [Sh80] by K. Shinoda, [Mi69] by J. Milnor and the classic [Wa63] by G. E. Wall. The counting of the special polynomials is taken from the work [FuNePr05] by J. Fulman, P. M. Neumann, and C. Praeger.

2.1 Polynomials and partitions

The *dual* of a monic degree r polynomial $f(t) \in k[t]$ satisfying $f(0) \neq 0$, is the polynomial given by $f^*(t) = f(0)^{-1}t^r f(t^{-1})$. The polynomial f will be called $*$-*symmetric* if $f = f^*$. Note that $f(t) = a_0 + a_1 t + \cdots + t^d$ is $*$-symmetric if an only if

$$a_0 = \pm 1 \text{ and } a_{d-i} = a_0 a_i \text{ for } 0 < i < d.$$

We call f to be $*$*-irreducible or self reciprocal* if it is $*$-symmetric and has no proper $*$-symmetric factors. It can be proved that if f is a monic $*$-irreducible polynomial of odd degree then $f = t \pm 1$. In the even degree case we get that [Ta1, Lemma 1.5]:

1. if f is irreducible then $f(t) = t^d g(t + t^{-1})$ for an irreducible polynomial g of degree d,

2. if f is reducible then $f = gg^*$, for some irreducible polynomial g satisfying $g \neq g^*$.

A *partition* of a number Λ is a sequence of non-negative numbers $\lambda_1, \lambda_2, \cdots$ satisfying $\lambda_1 \geq \lambda_2 \geq \cdots \geq 0$, and $\Lambda = \sum \lambda_i$. Considering the multiplicities of the parts of λ we can write it as $1^{m_1}2^{m_2}\ldots$, removing i^{m_i}, whenever $m_i = 0$.

Definition 2.1.1. 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 $\pm$ associated with it. The set of all symplectic signed partitions will be denoted as $\mathcal{D}_{\mathrm{Sp}}$.

Definition 2.1.2. 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 partition will be denoted as $\mathcal{D}_{\mathrm{O}}$.

Example 2.1.3.

1. The partition $6^{+2}3^4 2^{-3}1^2$ is a symplectic signed partition of 32.

2. The partition $7^{+2}7^{-2}3^{+3}2^6 1^{-2}$ is an orthogonal signed partition of 51.

It can be shown that characteristic polynomial of symplectic or orthogonal matrix is $*$-symmetric (or self reciprocal). Indeed if λ is a root of the characteristic polynomial of a symplectic (or orthogonal) matrix, so is λ^{-1}. We follow J. Milnor's terminology [Mi69] 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 $f(t) = t \pm 1$.

Let $N^*(q, n)$ denotes the number of monic irreducible self-reciprocal polynomial $f(t)$ of degree n over $\mathbb{F}_q$ and let $R^*(q, n)$ denotes the number of unordered conjugate pairs $\{f, f^*\}$ of monic irreducible polynomials of degree n, over $\mathbb{F}_q$ such that $f \neq f^*$. We have the following result about the quantities $N^*(q, n)$ and $R^*(q, n)$ [FuNePr05, Lemma 1.3.16].

Lemma 2.1.4. *Let n be a positive integer.*

1.

$$N^*(q,n) = \begin{cases} e(q) & \textit{if } n = 1 \\ 0 & \textit{if } n \textit{ is odd and } n > 1 \\ \frac{1}{n} \sum\limits_{r|n, r \textit{ odd}} \mu(r)(q^{\frac{n}{2r}} + 1 - e(q)) & \textit{if } n \textit{ is even} \end{cases},$$

2.

$$M^*(q,n) = \begin{cases} \frac{1}{2}(q - e(q) - 1) & \textit{if } n = 1 \\ \frac{1}{2}N(q,n) & \textit{if } n \textit{ is odd and } n > 1 \\ \frac{1}{2}(N(q,n) - N^*(q,n)) & \textit{if } n \textit{ is even} \end{cases},$$

3.

$$N^*(q,2n) = \begin{cases} M^*(q,n) + 1 & \textit{if } n = 1 \\ M^*(q,n) & \textit{if } n \textit{ is odd and } n > 1 \\ M^*(q,n) + N^*(q,n) & \textit{if } n \textit{ is even} \end{cases}.$$

Note that here $e(q)$ is the number of square root of 1 *in the concerned field.*

2.2 Symplectic group

The symplectic group of Lie rank n is defined to be a subgroup of $\mathrm{GL}(2n, \mathbb{F}_q)$, which preserves a non-degenerate alternating form on $\mathbb{F}_q^{2n}$. We will be taking the alternating form to be $\left\langle (x_i)_{i=1}^{2n}, (y_j)_{j=1}^{2n} \right\rangle = \sum\limits_{j=1}^{n} x_j y_{2n+1-j} - \sum\limits_{i=0}^{n-1} x_{2n-i} y_{i+1}$. Fixing the usual basis of $\mathbb{F}_q^{2n}$, the matrix of the form is $J = \begin{pmatrix} 0 & \Lambda_n \\ -\Lambda_n & 0 \end{pmatrix}$ where $\Lambda_n = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \iddots & \vdots & \vdots \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$. Then a square matrix A of size $2n$ is said to be symplectic if and only if ${}^tAJA = J$. Since all the alternating forms are equivalent over $\mathbb{F}_q$, we have that Symplectic groups are unique up to conjugacy inside $\mathrm{GL}(2n, \mathbb{F}_q)$. We will be denoting the symplectic group by $\mathrm{Sp}(2n, \mathbb{F}_q)$ (of Lie rank n).

According to [Wa63, Example 2.6, case B], [Mi69, Theorem 3.2], the conjugacy classes of $\mathrm{Sp}(2n,\mathbb{F}_q)$ are parametrized by the functions $\lambda:\Phi\to\mathcal{P}^{2n}\cup\mathcal{D}^{2n}_{\mathrm{Sp}}$, where Φ denotes the set of all monic, non-constant, irreducible polynomials, $\mathcal{P}^{2n}$ is the set of all partitions of $1\le k\le 2n$ and $\mathcal{D}^{2n}_{\mathrm{Sp}}$ is the set of all symplectic signed partitions of $1\le k\le 2n$. Such a λ represents a conjugacy class of $\mathrm{Sp}(2n,\mathbb{F}_q)$ if and only if

1. $\lambda_x=0$,
2. $\lambda_{\varphi^*}=\lambda_\varphi$,
3. $\lambda_\varphi\in\mathcal{D}^n_{\mathrm{Sp}}$ iff $\varphi=x\pm 1$ (we distinguish this λ, by denoting it $\lambda^{\pm}$),
4. $\sum\limits_{\varphi}|\lambda_\varphi|\deg(\varphi)=2n$ where $|\lambda_\varphi|$ denotes the sum of the parts of the partition.

The data corresponding to the assignment will be denoted by $\{(f,\lambda_f)\}$ and will be called the *combinatorial data attached to conjugacy class*. Class representative corresponding to given combinatorial data attached to conjugacy class can be found in [Ta1], [Ta2], [GoLiBr] and we will mention them whenever needed. Without proof, we mention the following results about the conjugacy class size (and hence the size of the centralizer) of elements corresponding to given data, which can be found in [Wa63].

Lemma 2.2.1. *[Wa63, pp. 36] Let $X\in\mathrm{Sp}(2n,\mathbb{F}_q)$ be a matrix corresponding to the data $\Delta_X=\{(\phi,\lambda_\phi):\phi\in\Phi_X\subset\Phi\}$. Then the conjugacy class of X in $\mathrm{Sp}(2n,\mathbb{F}_q)$ is of size $\dfrac{|\mathrm{Sp}(2n,\mathbb{F}_q)|}{\prod\limits_{\phi}B(\phi)}$ where $B(\phi)$ and $A(\phi^\lambda)$ are defined as follows*

$$A(\phi^\lambda)=\begin{cases}|\mathrm{U}(m_\lambda,Q)| & \textit{if } \phi(t)=\phi^*(t)\neq t\pm 1\\ |\mathrm{GL}(m_\lambda,Q)|^{\frac12} & \textit{if } \phi\neq\phi^*\\ |\mathrm{Sp}(m_\lambda,\mathbb{F}_q)| & \textit{if } \phi(t)=t\pm 1,\ \lambda \textit{ odd}\\ |q^{\frac12 m_\lambda}\mathrm{O}^\epsilon(m_\lambda,\mathbb{F}_q)| & \textit{if } \phi(t)=t\pm 1,\ \lambda \textit{ even}\end{cases},$$

where ϵ gets determined by the sign of the corresponding partition, $Q=q^{|\phi|}$, $m_\lambda=m(\phi^\lambda)$ and

$$B(\phi)=Q^{\sum\limits_{\lambda<\nu}\lambda m_\lambda m_\nu+\frac12\sum\limits_{\lambda}(\lambda-1)m_\lambda^2}\prod_\lambda A(\phi^\lambda).$$

2.3 Orthogonal group

The orthogonal groups are defined to be a subgroup of $\mathrm{GL}(n, \mathbb{F}_q)$ which preserves a non-degenerate quadratic form Q on $\mathbb{F}_q^n$.

If $n = 2m$ for some $m \geq 1$, upto equivalence of forms over $\mathbb{F}_q$ (under action of $\mathrm{GL}(n, \mathbb{F}_q)$), there are two such forms. If $a \in \mathbb{F}_q$ is such that $t^2 + t + a \in \mathbb{F}_q[x]$ is irreducible, then the two non-equivalent forms are given by

1. $Q^+((x_i)_{i=1}^n) = \sum\limits_{i=1}^{m} x_{2i-1}x_{2i}$ and
2. $Q^-((x_i)_{i=1}^n) = x_1^2 + x_1x_2 + ax_2^2 + \sum\limits_{i=2}^{m} x_{2i-1}x_{2i}$.

The orthogonal group preserving Q^+ will be denoted as $\mathrm{O}^+(n, \mathbb{F}_q)$, whereas the orthogonal group preserving Q^- will be denoted as $\mathrm{O}^-(n, \mathbb{F}_q)$.

If $n = 2m + 1$, then for q even there is only one (upto equivalence) quadratic form, namely $Q((x_i)_{i=1}^n) = x_1^2 + \sum\limits_{i=1}^{m} x_{2i}x_{2i+1}$ and hence there is only one (upto conjugacy) orthogonal group. If q is odd, then upto equivalence there are only two non-degenerate quadratic forms given by

1. $Q_1((x_i)_{i=1}^n) = \sum\limits_{i=1}^{n} x_i^2$ and
2. $Q_\delta((x_i)_{i=1}^n) = \delta \sum\limits_{i=1}^{n} x_i^2$, where $\delta \in \mathbb{F}_q \setminus \mathbb{F}_q^2$.

But these two forms give isomorphic orthogonal groups. Thus, in case $n = 2m+1$, up to conjugacy there exists only one orthogonal group. This will be denoted as $\mathrm{O}^0(n, \mathbb{F}_q)$. We will use the notation $\mathrm{O}^\epsilon(n, \mathbb{F}_q)$ to denote any of the orthogonal group in general, with $\epsilon \in \{-, +, 0\}$. If we take $J_0 = \begin{pmatrix} 0 & 0 & \Lambda_m \\ 0 & \alpha & 0 \\ \Lambda_m & 0 & 0 \end{pmatrix}$, $J_+ = \begin{pmatrix} 0 & \Lambda_m \\ \Lambda_m & 0 \end{pmatrix}$ and $J_- = \begin{pmatrix} 0 & 0 & 0 & \Lambda_{m-1} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -\delta & 0 \\ \Lambda_{m-1} & 0 & 0 & 0 \end{pmatrix}$, with $\alpha \in \mathbb{F}_q^\times, \delta \in \mathbb{F}_q \setminus \mathbb{F}_q^2$, then $A \in \mathrm{O}^\epsilon(n, \mathbb{F}_q)$ if and only if ${}^tAJ_\epsilon A = J_\epsilon$. Adapting the notations of [FuNePr05] we define the type of an orthogonal space as follows.

Definition 2.3.1. The type of an orthogonal space (V, Q) of dimension n is

$$\tau(V) = \begin{cases} \epsilon 1 & \text{if } n \text{ is even and } V \text{ has type } \epsilon, \\ 1 & \text{if } n \text{ is odd and } q \text{ is even}, \\ 1 & \text{if } n \text{ is odd, } q \equiv_4 1, Q \sim \sum x_i^2, \\ -1 & \text{if } n \text{ is odd, } q \equiv_4 1, Q \sim b\sum x_i^2, \\ \iota^n & \text{if } n \text{ is odd, } q \equiv_4 3, Q \sim \sum x_i^2, \\ (-\iota)^n & \text{if } n \text{ is odd, } q \equiv_4 3, Q \sim b\sum x_i^2, \end{cases}$$

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

Remark 2.3.2. If V has orthogonal decomposition $V_1 \oplus V_2 \oplus \cdots \oplus V_l$, then $\tau(V) = \prod\limits_{i=1}^{l} \tau(V_i)$.

From [Wa63, Example 2.6, case C], [Mi69, Theorem 3.2], we find out that similar kind of statement is true for the groups $\mathrm{O}^\epsilon(n, \mathbb{F}_q)$. The conjugacy classes of $\mathrm{O}^\epsilon(n, \mathbb{F}_q)$ are parametrized by the functions $\lambda : \Phi \to \mathcal{P}^n \cup \mathcal{D}^n_{\mathrm{O}}$, where Φ 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 $\mathcal{D}^n_{\mathrm{O}}$ is the set of all symplectic signed partitions of $1 \leq k \leq n$. Such a λ represent a conjugacy class of $\mathrm{Sp}(2n, \mathbb{F}_q)$ if and only if

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

Lemma 2.3.3. *[Wa63, pp. 39] Let $X \in \mathrm{O}^\epsilon(n, q)$ be a matrix corresponding to the data $\Delta_X = \{(\phi, \lambda_\phi) : \phi \in \Phi_X \subset \Phi\}$. Then the conjugacy class of X in $\mathrm{O}^\epsilon(n, q)$ is of size $\dfrac{|\mathrm{Sp}(2n, \mathbb{F}_q)|}{\prod\limits_{\phi} B(\phi)}$ where $B(\phi)$ and $A(\phi^\lambda)$ are defined as before, except when $\phi(t) = t \pm 1$,*

$$A(\phi^\lambda) = \begin{cases} |\mathrm{O}^{\epsilon'}(m_\lambda, q)| & \textit{if } \lambda \textit{ odd} \\ q^{-\frac{1}{2}m_\lambda} |\mathrm{Sp}(m_\lambda, q)| & \textit{if } \lambda \textit{ even} \end{cases},$$

where ϵ' in $\mathrm{O}^{\epsilon'}(m_\lambda, q)$ gets determined by the corresponding sign of the part, of the partition.

2.4 Central Join

Suppose $A = \begin{pmatrix} P & Q \\ R & S \end{pmatrix} \in \mathrm{Sp}(2n, \mathbb{F}_q)$ where P, Q, R, S are $n \times n$ matrices and $B \in \mathrm{Sp}(2m, \mathbb{F}_q)$. Then A satisfies the equation ${}^tAJ_{2n}A = J_{2n}$, whence P, Q, R, S satisfy

$$\begin{aligned}
-{}^tR\Lambda_n P + {}^tP\Lambda_n R &= 0, \\
-{}^tR\Lambda_n Q + {}^tP\Lambda_n S &= \Lambda_n, \\
-{}^tS\Lambda_n P + {}^tQ\Lambda_n R &= -\Lambda_n, \\
-{}^tS\Lambda_n Q + {}^tQ\Lambda_n S &= 0.
\end{aligned}$$

Also B satisfies ${}^tBJ_{2m}B = J_{2m}$. Let us define

$$A \circ B = \begin{pmatrix} P & 0_{2m} & Q \\ 0_{2m} & B & 0_{2m} \\ R & 0_{2m} & S \end{pmatrix}.$$

Then

$$\begin{aligned}
{}^t(A \circ B)J_{2m+2n}(A \circ B) &= \begin{pmatrix} {}^tP & 0_{2m} & {}^tR \\ 0_{2m} & {}^tB & 0_{2m} \\ {}^tQ & 0_{2m} & {}^tS \end{pmatrix} \begin{pmatrix} 0_n & 0_{2m} & \Lambda_n \\ 0_{2m} & J_{2m} & 0_{2m} \\ -\Lambda_n & 0_{2m} & 0_n \end{pmatrix} \begin{pmatrix} P & 0_{2m} & Q \\ 0_{2m} & B & 0_{2m} \\ R & 0_{2m} & S \end{pmatrix} \\
&= \begin{pmatrix} -{}^tR\Lambda_n & 0_{2m} & {}^tP\Lambda_n \\ 0_{2m} & {}^tBJ_{2m} & 0_{2m} \\ -{}^tS\Lambda_n & 0_{2m} & {}^tQ\Lambda_n \end{pmatrix} \begin{pmatrix} P & 0_{2m} & Q \\ 0_{2m} & B & 0_{2m} \\ R & 0_{2m} & S \end{pmatrix} \\
&= \begin{pmatrix} -{}^tR\Lambda_n P + {}^tP\Lambda_n R & 0_{2m} & -{}^tR\Lambda_n Q + {}^tP\Lambda_n S \\ 0_{2m} & {}^tBJ_{2m}B & 0_{2m} \\ -{}^tS\Lambda_n P + {}^tQ\Lambda_n R & 0_{2m} & -{}^tS\Lambda_n Q + {}^tQ\Lambda_n S \end{pmatrix} \\
&= J_{2m+2n}.
\end{aligned}$$

Thus $A \circ B \in \mathrm{Sp}(2(m + n), \mathbb{F}_q)$.

Definition 2.4.1. [Ta1, pp 21] Given $A \in \mathrm{Sp}(2n, \mathbb{F}_q), B \in \mathrm{Sp}(2m, \mathbb{F}_q)$, we call the matrix $A \circ B$ to be *symplectic central join* of A and B.

Now suppose the matrices A, B are in two orthogonal groups preserving symmetric bilinear forms with matrices J_1, J_2 respectively. Then $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ preserves $\begin{pmatrix} J_1 & 0 \\ 0 & J_2 \end{pmatrix}$. But note that the matrix $\begin{pmatrix} J_1 & 0 \\ 0 & J_2 \end{pmatrix}$ is not of standard shape. Thus we will be needing functions that can convert the diagonal shape to the standard shape. This is achieved by *orthogonal central join* [Ta2, pp. 21], taking into consideration different Witt types of the bilinear forms. We will be considering the simplest case, when Witt type of J_1 is $\langle 0 \rangle$. Then we have that J_1 is of the form $\begin{pmatrix} 0 & \Lambda_m \\ \Lambda_m & 0 \end{pmatrix}$ for some m. Let A be a matrix of size $2m \times 2m$ and B a matrix of size $n \times n$. We can write

$$A = \begin{pmatrix} P & Q \\ R & S \end{pmatrix}.$$

Define

$$A \circ B = \begin{pmatrix} P & 0 & Q \\ 0 & B & 0 \\ R & 0 & S \end{pmatrix}.$$

Note that if $X = \begin{pmatrix} I_m & 0 & 0 \\ 0 & 0 & I_m \\ 0 & I_n & 0 \end{pmatrix}$, we have that $X^{-1} \begin{pmatrix} J_1 & 0 \\ 0 & J_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & \Lambda_m \\ 0 & J_2 & 0 \\ \Lambda_m & 0 & 0 \end{pmatrix}$. With this it can be easily shown that $X^{-1} \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} = A_1 \circ A_2$, and that $A_1 \circ A_2$ belongs to the orthogonal group of Witt type as same as J_2.

Using the central join of matrices, first, the study can be done for a block corresponding to a polynomial of the form f^m for some $*$-irreducible polynomial f, and later be put together to get the answer in the general case. This follows from the following result.

Lemma 2.4.2. *Let A, B be two elements of the symplectic group (or orthogonal group). Then for an integer $M \geq 2$, we have that $(A \circ B)^M = A^M \circ B^M$.*

Proof. See [Ta1], [Ta2]. □

Chapter 3

Generating functions and Cycle index

3.1 Generating function

By definition a *generating function attached to a sequence* (a_n) is the Taylor series in variable z, given by $\sum\limits_{n=0}^{\infty} a_n z^n$. For example the generating function for the sequence $(a_n = 1)_{n\geq 0}$ is given by

$$1 + z + z^2 + \ldots = \frac{1}{1-z}.$$

If $a_m = P(m)$ denotes the number of partitions of m, then it can be shown that

$$1 + \sum_{m=1}^{\infty} a_m z^m = \prod_{n=1}^{\infty} \frac{1}{1-z^n}.$$

Notation 3.1.1. For a given matrix $X \in \mathrm{G}(m, \mathbb{F}_q)$, where $\mathrm{G}(m, \mathbb{F}_q)$ is either the symplectic or orthogonal group over $\mathbb{F}_q$ of Lie rank m, we will use

1. Δ_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.

We will be describing here the generating functions for the number of different conjugacy classes (elements), viz. separable, semisimple, regular, cyclic in case of finite orthogonal and symplectic groups. Recall the definitions for the same. A matrix A will be called (a) *Separable* if $c_A(t)$ has distinct roots, (b) *Semisimple* if $m_A(t)$ has distinct roots, (c) *Cyclic* if $m_A(t) = c_A(t)$ (d) *Regular* if its centraliser in the corresponding algebraic group over the algebraic closure of $\mathbb{F}_q$ has dimension equal to the Lie rank of the group. Now we will describe the generating functions for the probability of an element being of a specific type in the concerned group. We start with the symplectic group, as the generating functions in the case of orthogonal groups will be given in terms of the generating function in the case of the symplectic group.

Symplectic group:

Let $S_{\mathrm{Sp}}(u)$ be the generating function for the probability of an element to be separable in $\mathrm{Sp}(2m, q)$ (to be denoted by s_{Sp}(2m,q)). Hence we have

$$S_{\mathrm{Sp}}(z) := 1 + \sum_{m\geq 1} s_{\mathrm{Sp}}(2m, q) z^m.$$

Then we have that this quantity factorizes [FuNePr05, Theorem 2.2.1] and we have the equality

$$S_{\mathrm{Sp}}(z) = \prod_{d=1}^{\infty} \left(1 + \frac{z^d}{q^d+1}\right)^{N^*(q,2d)} \prod_{d=1}^{\infty} \left(1 + \frac{z^d}{q^d-1}\right)^{M^*(q,d)}.$$

Similarly we have the following for cyclic matrices [FuNePr05, Theorem 2.2.7]

$$\begin{aligned} C_{\mathrm{Sp}}(z) = \left(\frac{1}{1-\frac{z}{q}}\right)^2 & \prod_{d=1}^{\infty} \left(1 + \frac{z^d}{(q^d+1)(1-\frac{z^d}{q^d})}\right)^{N^*(q,2d)} \\ & \times \prod_{d=1}^{\infty} \left(1 + \frac{z^d}{(q^d-1)(1-\frac{z^d}{q^d})}\right)^{M^*(q,d)}, \end{aligned}$$

for semisimple matrices [FuNePr05, Theorem 3.1.5]

$$\begin{aligned} SS_{\mathrm{Sp}}(z) = & \left(1 + 2\sum_{m=1}^{\infty} \frac{z^m}{|\mathrm{Sp}(2m, \mathbb{F}_q)|}\right)^2 \\ & \times \prod_{d=1}^{\infty} \left(1 + \sum_{m=1}^{\infty} \frac{z^{dm}}{|\mathrm{U}(m, \mathbb{F}_{q^d})|}\right)^{N^*(q,2d)} \prod_{d=1}^{\infty} \left(1 + \sum_{m=1}^{\infty} \frac{z^{dm}}{|\mathrm{GL}(m, \mathbb{F}_{q^d})|}\right)^{M^*(q,d)}, \end{aligned}$$

where C_{Sp} and SS_{Sp} denote the generating functions for the probability of an element to be cyclic, and semisimple respectively in the Symplectic group.

Orthogonal group:

Define the following functions for different orthogonal groups;

$$S_{\mathrm{O}^+}(z) = 1 + \sum_{m=1}^{\infty} s_{\mathrm{O}^+}(2m, q)z^m, S_{\mathrm{O}^-}(z) = 1 + \sum_{m=1}^{\infty} s_{\mathrm{O}^-}(2m, q)z^m,$$
$$S_{\mathrm{O}^0}(z) = 1 + \sum_{m=1}^{\infty} s_{\mathrm{O}^0}(2m+1, q)z^m$$

to denote the generating functions for the probability of an element to be separable in respective orthogonal groups. We define

$$X_{\mathrm{O}}(z) := \prod_{d=1}^{\infty}\left(1 - \frac{z^d}{q^d+1}\right)^{N^*(q,2d)} \prod_{d=1}^{\infty}\left(1 + \frac{z^d}{q^d-1}\right)^{M^*(q,d)}.$$

This leads to the equalities [FuNePr05, Theorem 2.3.1]

1. $S_{\mathrm{O}^+}(z^2) + S_{\mathrm{O}^-}(z^2) + 2zS_{\mathrm{O}}(z^2) = (1+z)^2 S_{\mathrm{Sp}}(z^2)$
2. $S_{\mathrm{O}^+}(z^2) - S_{\mathrm{O}^-}(z^2) = X_{\mathrm{O}}(z^2)$.

Further, define

$$X'_{\mathrm{O}}(z) := \prod_{d=1}^{\infty}\left(1 - \frac{z^d}{(q^d+1)\left(1+\left(\frac{u}{q}\right)^d\right)}\right)^{N^*(q,2d)} \prod_{d=1}^{\infty}\left(1 + \frac{z^d}{(q^d-1)\left(1-\left(\frac{u}{q}\right)^d\right)}\right)^{M^*(q,d)}.$$

Then in the case of cyclic matrices, we get [FuNePr05, Theorem 2.3.9]

1. $C_{\mathrm{O}^0}(z) = \left(1 - \frac{z}{q}\right) C_{\mathrm{Sp}}(z)$,
2. $C_{\mathrm{O}^\pm} = \frac{1}{2}\left(\left(1-\frac{z}{q}\right)^2 + z\right) C_{\mathrm{Sp}}(z) \pm \frac{1}{2} X'_{\mathrm{O}}(z)$.

For regular elements we have [FuNePr05, Theorem 3.2.2] that, for orthogonal groups of odd dimension

$$R_{\mathrm{O}}(z) = \left(1 + \frac{z}{q(q^2-1)} - \frac{z^2}{q^2(q^2-1)}\right) C_{\mathrm{Sp}}(z),$$

and for orthogonal groups of even dimension we have two equations, i.e.

1. $R_{\mathrm{O}^+}(z) + R_{\mathrm{O}^-}(z) = \left(\left(1 + \dfrac{z}{q(q^2-1)} - \dfrac{z^2}{q^2(q^2-1)}\right)^2 + z\right) C_{\mathrm{Sp}}(z),$

2. $R_{\mathrm{O}^+}(z) - R_{\mathrm{O}^-}(z) = \left(1 + \dfrac{z}{q^2-1}\right)^2 X'_{\mathrm{O}}(z).$

To write down the generating functions for the semisimple case, we will need the following functions.

$$Y_1^*(z) = \prod_{d=1}^{\infty}\left(1 + \sum_{m=1}^{\infty} \frac{z^{dm}}{|\mathrm{U}(m, \mathbb{F}_{q^d})|}\right)^{N^*(q,2d)} \prod_{d=1}^{\infty}\left(1 + \sum_{m=1}^{\infty} \frac{z^{dm}}{|\mathrm{GL}(m, \mathbb{F}_{q^d})|}\right)^{M^*(q,d)},$$

$$Y_2^*(z) = \prod_{d=1}^{\infty}\left(1 + \sum_{m=1}^{\infty} \frac{(-1)^m z^{dm}}{|\mathrm{U}(m, \mathbb{F}_{q^d})|}\right)^{N^*(q,2d)} \prod_{d=1}^{\infty}\left(1 + \sum_{m=1}^{\infty} \frac{z^{dm}}{|\mathrm{GL}(m, \mathbb{F}_{q^d})|}\right)^{M^*(q,d)},$$

$$F(z) = 1 + \sum_{m=1}^{\infty} \frac{z^m}{|\mathrm{Sp}(2m, \mathbb{F}_q)|},$$

$$F_+(z) = 1 + \sum_{m=1}^{\infty}\left(\frac{1}{|\mathrm{O}^+(2m, \mathbb{F}_q)|} + \frac{1}{\mathrm{O}^-(2m, \mathbb{F}_q)}\right) z^m,$$

$$F_-(z) = 1 + \sum_{m=1}^{\infty}\left(\frac{1}{|\mathrm{O}^+(2m, \mathbb{F}_q)|} - \frac{1}{\mathrm{O}^-(2m, \mathbb{F}_q)}\right) z^m.$$

Then we have [FuNePr05, Theorem 3.1.7] that

$$SS_{\mathrm{O}^+}(z^2) + SS_{\mathrm{O}^-}(z^2) + 2zSS_{\mathrm{O}}(z^2) = (F_+(z^2) + zF(z^2))^2 Y_1^*(z^2)$$
$$SS_{\mathrm{O}^+}(z^2) - SS_{\mathrm{O}^-}(z^2) = F_-(z^2)^2 Y_2^*(z^2).$$

Note that these results are the cases $M = 1$. We will be generalizing these ideas, to answer the cases $M \geq 2$. This line of study has been previously done in the work by Kundu and Singh in [KuSi22], for the group $\mathrm{GL}(n, \mathbb{F}_q)$. We mention some of the results here, before moving to the next subsection.

Theorem 3.1.2. *[KuSi22, Theorem 5.2] Let $M \geq 2$ be an integer and $(q, M) = 1$. For the group $\mathrm{GL}(n, \mathbb{F}_q)$, the generating function for regular and regular semisimple classes which are M-th power is*

1. $1 + \sum_{n=1}^{\infty} c(n, q, M)_{rg} u^n = \prod_{d=1}^{\infty} (1 - u^d)^{-N_M(q,d)};$

2. $1 + \sum_{n=1}^{\infty} c(n,q,M)_{rs} u^n = \prod_{d=1}^{\infty} (1+u^d)^{N_M(q,d)}$,

where $c(n,q,M)_{rg}$ and $c(n,q,M)_{rs}$ denote the number of regular and regular semisimple conjugacy classes in $\mathrm{GL}(n,\mathbb{F}_q)$ *respectively, $N_M(q,d)$ is the number of M-power polynomial of degree d over $\mathbb{F}_q$.*

Theorem 3.1.3. *[KuSi22, Theorem 6.2] Let $M = r^a$ be a prime power and $(q,M) = 1$. Then, we have the following generating function:*

$$1 + \sum_{n=1}^{\infty} c(n,q,M)_{ss} u^n = \prod_{i=0}^{a} \prod_{d \geq 1} (1 - u^{r^i d})^{-N_M^i(q,d)},$$

where $c(n,q,M)_{ss}$ denotes the number of semisimple conjugacy classes in $\mathrm{GL}(n,q)$ *and $N_M^i(q,d)$ is the number of irreducible polynomials $f \in \Phi$ of degree d with the property that all irreducible factors of $f(t^M)$ are of degree dr^i.*

3.2 Cycle index

A *cycle index* of a group G is a polynomial in several variables, defined in a way that information about how a group of permutations acts on a set can be found from the coefficients and exponents. We are interested in the cycle index of particular group action, viz. the conjugation action of a group G on itself. Note that in that case the orbits are the conjugacy classes and the stabilizers are the centralizer of an element. Polya first introduced the concept of cycle index for the symmetric group S_n in [PoRe87]. This can be briefly described as follows. For $\pi \in S_n$, let $a_i(\pi)$ denote the number of i-cycles in π. 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

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

Kung [Ku81] and Stong [St88] later developed a cycle index for the finite general linear group $\mathrm{GL}(n,\mathbb{F}_q)$, which can be described as follows. Let $x_{f,\lambda}$ be variable corresponding to the pair (f,λ) where $f \in k[t]$ and λ is a partition of a number.

Then the cycle index of $\mathrm{GL}(n, \mathbb{F}_q)$ is given by

$$1 + \sum_{n=1}^{\infty} \frac{u^n}{|\mathrm{GL}(n, \mathbb{F}_q)|} \sum_{\alpha \in \mathrm{GL}(n,q)} \prod_{f \neq t} x_{f, \lambda_f(\alpha)} = \prod_{f \neq t} \sum_{\lambda} x_{f,\lambda} \frac{u^{|\lambda| \deg(f)}}{c_{\mathrm{GL},f,q}(\lambda)},$$

where

$$c_{\mathrm{GL},f,q}(\lambda) = \prod_{i} \prod_{k=1}^{m_i} (q^{\deg(f) d_i - q^{\deg(f)(d_i - k)}})$$
$$\text{with } d_i = m_1 1 + m_2 2 + \cdots + m_{i-1}(i-1) + (m_i + m_{i+1} + \cdots + m_j) i.$$

We will be concerned with the cycle indices in the case of symplectic and orthogonal groups, which were developed in the Ph.D. thesis [Fu97] of Jason Fulman. Define the cycle index of the symplectic group to be

$$1 + \sum_{n=1}^{\infty} \frac{u^{2n}}{|\mathrm{Sp}(2n, \mathbb{F}_q)|} \sum_{\alpha \in \mathrm{Sp}(2n,q)} \prod_{f = t \pm 1} x_{f, \lambda_f^{\pm}(\alpha)} \prod_{f \neq t \pm 1} x_{f, \lambda_f(\alpha)}.$$

By the work of J. Fulman we have that this quantity factorizes as follows [Fu99, Theorem 12];

$$\prod_{f = t \pm 1} \left(\sum_{\lambda^p m} x_{f, \lambda^{\pm}} \frac{u^{|\lambda^{\pm}|}}{c_{\mathrm{Sp},f,q}(\lambda^{\pm})} \right) \prod_{\substack{f = f^* \\ f \neq t \pm 1}} \left(\sum_{\lambda} x_{f,\lambda} \frac{(-(u^{\deg f}))^{|\lambda|}}{c_{\mathrm{GL},t-1,-(q^{\deg f/2})}(\lambda)} \right)$$
$$\times \prod_{\substack{\{f, f^*\} \\ f \neq f^*}} \left(\sum_{\lambda} x_{f,\lambda} x_{f^*,\lambda} \frac{u^{2|\lambda| \deg f}}{c_{\mathrm{GL},t-1,q^{\deg f}}(\lambda)} \right).$$

In case of orthogonal groups, we take sum of the cycle indices of the different orthogonal groups of same rank together (note that for odd case $\mathrm{O}^+ = \mathrm{O}^-$) and define the cycle index to be as follows:

$$1 + \sum_{n=1}^{\infty} \left(\frac{u^n}{|\mathrm{O}^+(n, \mathbb{F}_q)|} \sum_{\alpha \in \mathrm{O}^+(n, \mathbb{F}_q)} \prod_{f = t \pm 1} x_{f, \lambda_f^{\pm}(\alpha)} \prod_{f \neq t, t \pm 1} x_{f, \lambda_f(\alpha)} \right)$$
$$+ \sum_{n=1}^{\infty} \left(\frac{u^n}{|\mathrm{O}^-(n, \mathbb{F}_q)|} \sum_{\alpha \in \mathrm{O}^-(n, \mathbb{F}_q)} \prod_{f = t \pm 1} x_{f, \lambda_f^{\pm}(\alpha)} \prod_{f \neq t, t \pm 1} x_{f, \lambda_f(\alpha)} \right),$$

and this factorizes as follows [Fu99, Theorem 14]:

$$\prod_{f=t\pm 1}\left(\sum_{\lambda^{\pm}} x_{f,\lambda^{\pm}}\frac{u^{|\lambda^{\pm}|}}{c_{O,f,q^{\deg f}}(\lambda^{\pm})}\right)\left(\sum_{\lambda} x_{f,\lambda}\frac{(-(u^{\deg f}))^{|\lambda|}}{c_{\mathrm{GL},t-1,-q^{\deg f/2}}(\lambda)}\right)$$

$$\prod_{\{f,f^*\},f\neq f^*}\left(\sum_{\lambda} x_{f,\lambda}x_{f^*,\lambda}\frac{u^{2|\lambda|\deg f}}{c_{\mathrm{GL},t-1,q^{\deg f}}(\lambda)}\right).$$

Chapter 4

Generating functions for M-th powers

In this chapter, we will find the desired generating functions. We start with the concept of M-power and M^*-power polynomials. The number of such polynomials has been counted in later sections. These polynomials play a key role in determining the generating functions for symplectic and orthogonal groups. In subsequent sections, we provide the generating functions for a number of the M-th power regular semisimple, semisimple, cyclic, and regular classes in orthogonal and symplectic groups.

4.1 M-power and M^*-power polynomial

Following the definitions of [KuSi22] we note down the following, which will be in further use:

Definition 4.1.1. 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 polynomials ($\neq x$) by Φ_M.

We recall the following theorem from [MeGo90].

Lemma 4.1.2. *[MeGo90, Theorem 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*

$$H_{q,n}(x) \coloneqq x^{q^n+1} - 1 \in \mathbb{F}_q[x], \tag{4.1.1}$$

2. *Each irreducible factor of degree ≥ 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 4.1.3. 1. The SRIM polynomials of degree 4 over $\mathbb{F}_5$, are factors of $x^{26} - 1 \in \mathbb{F}_5[x]$. Using SAGE, it can be found out that in $\mathbb{F}_5[x]$, we have $x^{26} - 1 = (x+1)(x+4)(x^4+x^3+4x^2+x+1)(x^4+2x^3+2x+1)(x^4+2x^3+x^2+2x+1)(x^4+3x^3+3x+1)(x^4+3x^3+x^2+3x+1)(x^4+4x^3+4x^2+4x+1)$. Hence the degree 4 SRIM polynomials over $\mathbb{F}_5$ are $(x^4+x^3+4x^2+x+1)$, (x^4+2x^3+2x+1), $(x^4+2x^3+x^2+2x+1)$, (x^4+3x^3+3x+1), $(x^4+3x^3+x^2+3x+1)$ and $(x^4+4x^3+4x^2+4x+1)$.

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

Definition 4.1.4. 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 an SRIM factor $g \in \mathbb{F}_q[x]$, of degree $2k$. Denote the set of M^*-power SRIM polynomials (of degree ≥ 2) by Φ_M^*.

Example 4.1.5. 1. 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.

2. 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 4.1.6. *Let $N^*_M(q,2k)$ denote the number of M^*-power SRIM polynomial of degree $2k$, $k \geq 1$. Then*

$$N^*_M(q,2k) = \frac{1}{2k(M,q^{2k}-1)} \sum_{\substack{l=\text{odd}\\ l|2k}} \mu(l)(M(q^{2k/l}-1), q^k+1). \tag{4.1.2}$$

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 $f, g \in \mathbb{F}_{q^{2k}}[x]$. 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 $\theta_M : \mathbb{F}_{q^{2k}} \to \mathbb{F}_{q^{2k}}$, we have $\alpha_i \in \text{im}(\theta_M)$, for all i. Since f is SRIM, using 4.1.2 we have that $\alpha_i^{q^k+1} = 1$ for all i. Thus β_i for all i, satisfies $\beta_i^{M(q^{2k}-1)} = \beta_i^{q^k+1} = 1$ and $\beta_i^M = \alpha_i$ generates $\mathbb{F}_{q^{2k}}$ over $\mathbb{F}_q$.

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

$$N^*_M(q,2k) = \frac{1}{2k}|\{\alpha \in \mathbb{F}_{q^{2k}} : \alpha^{q^k+1} = 1, \alpha = \theta_M(\eta) \text{ for some } \eta \in \mathbb{F}_{q^{2k}}, \mathbb{F}_{q^{2k}} = \mathbb{F}_q(\alpha)\}|, \tag{4.1.3}$$

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 $\alpha^M \notin \mathbb{F}_{q^l}$ for any $l|2k, l>1$. Since $\alpha^{q^k+1} = 1$, we have that $\alpha^{q^{\frac{k}{l}}+1}$ 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. Note the following example, where A has single block but A^{73} has 3 blocks with same conjugacy class data.

Example 4.1.7. Let A be 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 $\mathrm{Sp}(12,3)$, 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 α. 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 the minimal polynomial of A (of degree $2n/k$ for some odd k), has root γ, we have that M-th root of γ 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 $2n/k$, over $\mathbb{F}_q$ such that if $f(\alpha)=0$ for some $\alpha \in \mathbb{F}_{q^{2n/k}}$, then there exists $\beta \in \mathbb{F}_{q^{2n}}$ such that $\min_{\mathbb{F}_q}(\beta)$ is SRIM polynomial of order $2n$. Let $N^*_M(q,2n,2n/k)$ denotes the number of SRIM polynomial of degree $\frac{2n}{k}$ such that if $f(\alpha)=0$ for some $\alpha \in \mathbb{F}_{q^{2n/k}}$ then any M-th root of α, say β 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 4.1.8. *We have*

$$N^*_M(q,2n,2n/k) = \frac{1}{2k} \sum_{\substack{s<k \\ s=odd, s|k}} \mu(s) \frac{1}{(M, q^{\frac{2n}{s}}-1)} \sum_{\substack{l=odd \\ l|\frac{2n}{k}}} \mu(l) \left(M\left(q^{\frac{n}{kls}}+1\right), q^{\frac{n}{s}}+1\right). \tag{4.1.4}$$

Proof. For k odd and $k|2n$, consider the set

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

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

$$|E_{2n,2n/k}| = \frac{1}{(M,q^{2n}-1)} \sum_{\substack{l=\text{odd} \\ l|\frac{2n}{k}}} \mu(l)\left(M\left(q^{\frac{n}{kl}}+1\right), q^n+1\right).$$

Now we want to consider only those $\alpha \in E_{2n,2n/k}$ 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 β 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 $\beta \in E_{2n,2n/k} \setminus \bigcup\limits_{\substack{s<k \\ s=\text{odd}, \frac{2n}{k} \mid \frac{2n}{s}}} E_{2n/s,2n/k}$. Thus we have that

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

since the sets of roots of irreducible polynomials are disjoint. □

Definition 4.1.9. 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 β 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 $\Phi^u_{M,n,\frac{n}{k}}$. Denote by $\Phi^{*,u}_{M,n,\frac{n}{k}}$ the subset of SRIM polynomials having same property.

Remark 4.1.10. The quantity $N_M^*(q, 2n, 2n/k)$ counts the number of degenerate $(M, 2n, \frac{2n}{k})$ SRIM polynomials over $\mathbb{F}_q$.

Remark 4.1.11. We have that $N_M^*(q, 2r) = N_M^*(q, 2r, 2r)$.

In case a polynomial is degenerate $(M, n, \frac{n}{k})$ polynomial, there are M-th roots of α, 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 4.1.12.

1. Using SAGE, we have that $x^{132} + 2x^{77} + x^{66} + 2x^{55} + 1 = (x^{12} + x^{11} + x^{10} + x^9 + 2x^6 + x^3 + x^2 + x + 1)(x^{60} + x^{58} + 2x^{57} + 2x^{56} + 2x^{55} + 2x^{54} + 2x^{53} + x^{51} + x^{49} + x^{48} + 2x^{46} + x^{45} + x^{44} + 2x^{43} + 2x^{42} + x^{41} + x^{40} + x^{39} + x^{38} + 2x^{36} + x^{34} + x^{32} + 2x^{31} + x^{30} + x^{27} + x^{26} + 2x^{25} + x^{23} + 2x^{21} + 2x^{19} + x^{17} + x^{16} + x^{15} + x^{13} + 2x^{11} + 2x^7 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 1)(x^{60} + 2x^{59} + 2x^{58} + 2x^{57} + 2x^{56} + 2x^{55} + 2x^{53} + 2x^{49} + x^{47} + x^{45} + x^{44} + x^{43} + 2x^{41} + 2x^{39} + x^{37} + 2x^{35} + x^{34} + x^{33} + x^{30} + 2x^{29} + x^{28} + x^{26} + 2x^{24} + x^{22} + x^{21} + x^{20} + x^{19} + 2x^{18} + 2x^{17} + x^{16} + x^{15} + 2x^{14} + x^{12} + x^{11} + x^9 + 2x^7 + 2x^6 + 2x^5 + 2x^4 + 2x^3 + x^2 + 1)$ in $\mathbb{F}_3[x]$. Note that there are two different 60 degree irreducible factors of the polynomial, which shows that the 60-th roots are in different subfields.

2. Using SAGE, we have that $x^{88} + 2x^{66} + x^{44} + 2x^{22} + 1 = (x^4 + x^3 + 2x + 1)(x^4 + 2x^3 + x + 1)(x^{20} + 2x^{18} + x^{17} + 2x^{16} + 2x^{15} + 2x^{12} + 2x^{11} + 2x^{10} + 2x^9 + 2x^7 + x^6 + x^5 + 2x^2 + 2x + 1)(x^{20} + 2x^{18} + 2x^{17} + 2x^{16} + x^{15} + 2x^{12} + x^{11} + 2x^{10} + x^9 + x^7 + x^6 + 2x^5 + 2x^2 + x + 1)(x^{20} + x^{19} + 2x^{18} + 2x^{15} + x^{14} + x^{13} + x^{11} + 2x^{10} + x^9 + 2x^8 + x^5 + 2x^4 + 2x^3 + 2x^2 + 1)(x^{20} + 2x^{19} + 2x^{18} + x^{15} + x^{14} + 2x^{13} + 2x^{11} + 2x^{10} + 2x^9 + 2x^8 + 2x^5 + 2x^4 + x^3 + 2x^2 + 1)$ in $\mathbb{F}_3[x]$. Note that here there are two irreducible factors of degree 4 and four irreducible factors of degree 20. Hence the roots are in different subfields.

Now assume that $f(\beta^M) = 0$ for some $\beta \in \mathbb{F}_{q^k}$, where $f \in \mathbb{F}_q[x]$ is a SRIM polynomial of degree $2n$. Then minimal polynomial of β must divide $f(x^M)$. Hence to determine all possible k, we should know about the irreducible factors of $f(x^M)$. From [But55] 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 in 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 finding the number of irreducible polynomials which has exponent e. We have the following

Lemma 4.1.13. *Let $N_M^{*,e}(q, 2n)$ denote the number of SRIM polynomials of degree $2n$ and exponent e which are not M^*-power SRIM polynomial. Then we have*

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

Proof. Let us first find out the 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 4.1.2). 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 $\sum_{\substack{l = \text{odd} \\ l|2n}} \mu(l)\phi(e)$, whence number of irreducible polynomials of degree $2n$ and exponent e in $\mathbb{F}_q[x]$ is $\frac{1}{2n} \sum_{\substack{l = \text{odd} \\ l|2n}} \mu(l)\phi(e)$.

Next we find out the number of M^*-power SRIM polynomial of degree $2n$ and exponent e. As in the remarks preceding 4.1.6, 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 $\displaystyle\frac{1}{2n(M, q^{2n}-1)} \sum_{\substack{l=\text{odd}\\ l|2n}} \mu(l)(M(q^{2n/l}-1), e)$. Hence the result follows. □

By a 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 [KuSi22].

Lemma 4.1.14. *[KuSi22, Proposition 3.3] Let $N_M(q,k)$ denote the number of M-power polynomial of degree k. Then*

$$N_M(q,k) = \frac{1}{k(M, q^k-1)} \sum_{l|k} \mu(l)(M(q^{k/l}-1), q^k-1). \tag{4.1.5}$$

Lemma 4.1.15. *Let $k|n$ and $N_M(q,n,n/k)$ denote the number of irreducible monic polynomial f over $\mathbb{F}_q$ of degree n/k, such that any M-th root of α (where $f(\alpha)=0$) lies in $\mathbb{F}_{q^n}$, but not in any proper subfield of $\mathbb{F}_{q^n}$. Then*

$$N_M(q,n,n/k) = \frac{1}{k} \sum_{\substack{s<k,\\ \frac{n}{k}|\frac{n}{s}}} \mu(s) \frac{1}{(M, q^{\frac{n}{s}}-1)} \sum_{l|\frac{2n}{k}} \mu(l) \left(M\left(q^{\frac{n}{kls}}-1\right), q^{\frac{n}{s}}-1\right). \tag{4.1.6}$$

Proof. Same as in Proposition 4.1.8. □

Lemma 4.1.16. *Let $N_M^e(q,n)$ denote the number of polynomials of degree n and exponent e which are not M-power polynomial. Then we have*

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

Proof. Same as in Lemma 4.1.13. □

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

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

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

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

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

$$R^{*,e}_M(q, 2n) = \begin{cases} \frac{1}{2} N^e_M(q, n) & n \text{ is odd} \\ \frac{1}{2}(N^e_M(q, n) - \frac{1}{n(M,q^n-1)} \sum\limits_{l|k} \mu(l)(Mq^e, q^{\frac{n}{l}} + 1) & n \text{ is even} \end{cases}.$$

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

Before proceeding further, we note down the following lemma, which helps in defining the indicator function (see Definition 4.1.19) corresponding to a class of irreducible polynomials having the same degree and exponent.

Lemma 4.1.17. *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 [But55] the roots of $f_1(x^M)$ and $f_2(x^M)$ have same order. Hence the result follows from 4.1.2. □

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

Definition 4.1.18. 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^***-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 $\mathcal{D}^*_M(f)$.

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

Definition 4.1.19. For a non M^*-power SRIM polynomial f, define the infinite product

$$G_f(u) = \frac{1}{\prod\limits_{i \in \mathcal{D}^*_M(f)} \left(1 - u^{\frac{i}{2}}\right) \prod\limits_{j \in \mathcal{D}_M(f) \setminus \mathcal{D}^*_M(f)} (1 - u^j)}.$$

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

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

Remark 4.1.20. Because of 4.1.17 the indicator function is same for all irreducible polynomial f of degree n and exponent e. Hence we will denote it by $\mathcal{I}_{n,e}$.

Lemma 4.1.21. *Let f be an SRIM polynomial of degree $2k$, $k \geq 1$. Then $\alpha^M = C_f$, has a solution in* $\mathrm{Sp}(2n, q)$ *if and only if $f(x^M)$ has an SRIM factor of degree $2k$.*

Proof. Let f be a SRIM polynomial of degree $2d$ over $\mathbb{F}_q$. Hence $f(t) = 1 + a_1 t + a_2 t^2 + \cdots + a_{d-1} t^{d-1} + t^d(a_d + a_{d-1} t^1 + a_{d-2} t^2 + \cdots + a_1 t^{d-1} + t^d)$. Then considering $C_f \in \mathrm{Sp}(2d, \mathbb{F}_{q^{2d}})$ we have that C_f is conjugate to the matrix $\left(\begin{array}{ccc|ccc} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_d & & & \\ \hline & & & \lambda_d^{-1} & & \\ & & & & \ddots & \\ & & & & & \lambda_1^{-1} \end{array}\right)$, where $\{\lambda_i^{\pm 1}\}_{i=1}^d$ is the set of roots of f. Let $\alpha^M = C_f$ for some $\alpha \in \mathrm{Sp}(2d, \mathbb{F}_q)$. Since α is conjugate to the matrix $\left(\begin{array}{ccc|ccc} \alpha_1 & & & & & \\ & \ddots & & & & \\ & & \alpha_d & & & \\ \hline & & & \alpha_d^{-1} & & \\ & & & & \ddots & \\ & & & & & \alpha_1^{-1} \end{array}\right)$ in $\mathrm{Sp}(2d, \mathbb{F}_q^{2d})$, 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 $\alpha_i^{\epsilon M} = \lambda_i^{\epsilon}$, $\epsilon = \pm 1$. Hence $f(\alpha_i^{\pm M}) = 0$ for all i. Considering $G(x) = f(x^M)$, we see that $G(\alpha_i^{\pm 1}) = 0$ for all i, in particular $g = \min_{\mathbb{F}_q}(\alpha)$ divides G. Since $\alpha \in \mathrm{Sp}(2d, \mathbb{F}_q)$, we have that g is self reciprocal monic polynomial. If $g = g_1 g_2$ 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 a SRIM polynomial.

We aim to show that C_g^M is conjugate to C_f, where g is 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 $\Lambda = \{\lambda_i : 1, i = 1, 2, \cdots, 2k\}$ 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 $\mathbb{F}_{q^{2k}}$, we have $f(x) = \displaystyle\prod_{i=1}^{2k}(x - \lambda_i)$, $g(x) = \displaystyle\prod_{i=1}^{2k}(x - \alpha_i)$. Since $g(x)$ divides $f(x^M)$, we have that, for all j, $0 = f(\alpha_j^M) = \displaystyle\prod_{i=1}^{2k}(\alpha_j^M - \lambda_i)$. Hence $\alpha_1^M = \lambda_i$ for some i. After some permutation, we may assume that $i = 1$. Note that if h is the characteristic polynomial of C_g^M, then $h(\alpha_1) = 0$. Since minimal polynomial of α_1 is f, we have that $f = h$. Since f is separable, we have that $|A| = |\Lambda| = 2k$. □

Corollary 4.1.22. *Let $A \in \mathrm{Sp}(2n, \mathbb{F}_q)$ has characteristic polynomial f, which is SRIM of degree $2n$. Then $\alpha^M = A$, has a solution in $\mathrm{Sp}(2n, \mathbb{F}_q)$, if and only if f is M^*-power SRIM polynomial.*

Remark 4.1.23. Recall from Example 4.1.5 that the matrix $A \in \mathrm{Sp}(4, 5)$ corresponding to the combinatorial data $\{(x^4 + 3x^3 + x^2 + 3x + 1, 1)\}$ has a square root $\mathrm{GL}(4, 5)$ but not in $\mathrm{Sp}(4, 5)$. 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.

4.2 Separable matrices

Proposition 4.2.1. *Let $cs^M_{\mathrm{Sp}}(n,q)$ be the number of M-power separable conjugacy classes in* $\mathrm{Sp}(2n,\mathbb{F}_q)$ *and* $cS^M_{\mathrm{Sp}}(q,u) = 1 + \sum\limits_{m=1}^{\infty} cs^M_{\mathrm{Sp}}(m,q)u^m$*. Then*

$$cS^M_{\mathrm{Sp}}(q,u) = \prod_{d=1}^{\infty} \left(1+u^d\right)^{N^*_M(q,2d)} \prod_{d=1}^{\infty} \left(1+u^d\right)^{R^*_M(q,2d)}. \tag{4.2.1}$$

Proof. Let $X \in \mathrm{Sp}(2n,\mathbb{F}_q)$ be a separable matrix. Then $c_X(t)$ is separable and is product of $*$-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 $*$-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 Δ_X represents a separable class if and only if

1. $\lambda_{t\pm1} = 0$,
2. $\lambda_f = \lambda_{f^*} \in \{0,1\}$,
3. $\sum\limits_{f|c_X} \deg f = 2n$.

Hence using 4.1.22, 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 $c_X(t) = \prod\limits_{i=1}^{r} f_i \prod\limits_{j=1}^{s} g_j g_j^*$, 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

$$\begin{aligned} cS^M_{\mathrm{Sp}}(q,u) &= \prod_{f\in\Phi^*_M} \left(1+u^{\frac{\deg f}{2}}\right) \prod_{g\in\Phi_M\setminus\Phi^*_M} \left(1+u^{\deg g}\right)^{\frac{1}{2}} \\ &= \prod_{d=1}^{\infty} \left(1+u^d\right)^{N^*_M(q,2d)} \prod_{d=1}^{\infty} \left(1+u^d\right)^{R^*_M(q,2d)}. \end{aligned}$$

□

Theorem 4.2.2. *Let $s^M_{\mathrm{Sp}}(n,q)$ be the probability of an element to be M-power separable in* $\mathrm{Sp}(2n,\mathbb{F}_q)$ *and* $S^M_{\mathrm{Sp}}(q,u) = 1 + \sum\limits_{m=1}^{\infty} s^M_{\mathrm{Sp}}(m,q)u^m$. *Then*

$$S^M_{\mathrm{Sp}}(q,u) = \prod_{d=1}^{\infty}\left(1+\frac{u^d}{q^d+1}\right)^{N^*_M(q,2d)} \prod_{d=1}^{\infty}\left(1+\frac{u^d}{q^d-1}\right)^{R^*_M(q,2d)}. \tag{4.2.2}$$

Proof. From 2.2.1 and 2.3.3, it follows that

1. for $X \in \mathrm{Sp}(2n,\mathbb{F}_q)$, if $c_X(t)$ is SRIM polynomial then the centraliser of X inside $\mathrm{Sp}(2n,\mathbb{F}_q)$ is of order q^n+1,
2. for $X \in \mathrm{Sp}(2n,\mathbb{F}_q)$, if $c_X(t)$ is $*$-irreducible polynomial of type 2 then the centraliser of X inside $\mathrm{Sp}(2n,\mathbb{F}_q)$ is of order q^n-1.

Hence using 4.2.1 and the fact that the centralizer of a general block diagonal matrix is a direct sum of each of the corresponding centralizers, we have

$$S^M_{\mathrm{Sp}}(q,u) = \prod_{d=1}^{\infty}\left(1+\frac{u^d}{q^d+1}\right)^{N^*_M(q,2d)} \prod_{d=1}^{\infty}\left(1+\frac{u^d}{q^d-1}\right)^{R^*_M(q,2d)}.$$

□

The next theorem is proved along the same line of proof of Theorem 2.3.1 of [FuNePr05].

Theorem 4.2.3. *Let $s^M_{\mathrm{O}^\epsilon}(n,q)$ be the probability of an element to be M-power separable in* $\mathrm{O}^\epsilon(2n,\mathbb{F}_q)$ *with $\epsilon \in \{\pm\}$ and $s^M_{\mathrm{O}^0}(n,q)$ denote the probability of an element to be M-power separable in* $\mathrm{O}^0(2n+1,\mathbb{F}_q)$. *Define*

$$S^M_{\mathrm{O}^+}(q,u) = 1 + \sum_{m\geq 1}^{\infty} s^M_{\mathrm{O}^+}(m,q)u^m$$
$$S^M_{\mathrm{O}^-}(q,u) = \sum_{m\geq 1}^{\infty} s^M_{\mathrm{O}^-}(m,q)u^m$$
$$S^M_{\mathrm{O}^0}(q,u) = 1 + \sum_{m\geq 1}^{\infty} s^M_{\mathrm{O}^0}(m,q)u^m.$$

Then

$$S^M_{\mathrm{O}^+}(u^2) + S^M_{\mathrm{O}^-}(u^2) + e(q)uS^M_{\mathrm{O}^0}(u^2) = (1+u)^{o(M,q)}S^M_{\mathrm{Sp}}(u^2), \tag{4.2.3}$$
$$S^M_{\mathrm{O}^+}(u^2) - S^M_{\mathrm{O}^-}(u^2) = X^M_{\mathrm{O}^0}(u^2), \tag{4.2.4}$$

where

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

$e(q)$ as before and

$$o(M,q)=\begin{cases}1 & \textit{if } M \textit{ or } q \textit{ even}\\ 2 & \textit{otherwise}\end{cases}.$$

Proof. The proof is similar to that of 4.2.2. 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 $\mathrm{O}^\epsilon(m,\mathbb{F}_q)$ is $\{\pm 1\}$, we have that the block corresponding to $t+1$, of size 1×1 is an M-th power if and only if M is odd. Now suppose M is even or q is even. Consider the product

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

If q is even then the factor $1+u$ appears for the possibility of $t-1$ dividing $c_X(t)$. In this case the centraliser of the corresponding block has size 1. 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 $s^M_{\mathrm{O}^+}(n,q)+s^M_{\mathrm{O}^-}(n,q)$, where as for n being odd positive the coefficient is $e(q)s^M_{\mathrm{O}^0}(n,q)$ 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 the first one. For each of the factor $1+\Gamma_f u^{2d}$ in the right hand side of the first equation, where Γ_f is the reciprocal of the size of the corresponding centraliser, replace it by $1+\tau_f\Gamma_f u^{2d}$, where $\tau_f = \tau(V_f)$ and V_f denotes the component of V corresponding to f, in the primary decomposition as a $\mathbb{F}_q[X]$ module. Then since for q odd, each of the term $\frac{u}{2}$ corresponds to the conjugacy class with τ_f values being negative to each other, the term $(1+u)$ vanishes. For q even, we omit $(1+u)$, because we are dealing with even dimensional spaces only. Now, since $\tau_f = -1$, when f is of type 1 and $\tau_f = +1$, when f is of type 2, the factors $1+\dfrac{u^{2d}}{q^d+1}$ are replaced by $1-\dfrac{u^{2d}}{q^d+1}$, whereas the factor $1+\dfrac{u^{2d}}{q^d-1}$ remains as it is. Hence the product becomes $\prod_{d=1}^{\infty}\left(1-\dfrac{u^d}{q^d+1}\right)^{N_M^*(q,2d)}\prod_{d=1}^{\infty}\left(1+\dfrac{u^d}{q^d-1}\right)^{R_M^*(q,2d)}$, which on expanding gives $S^M_{\mathrm{O}^+}(u^2)-S^M_{\mathrm{O}^-}(u^2)$ because of 2.3.2. □

Proposition 4.2.4. *Let $cs^M_{\mathrm{O}^\epsilon}(n,q)$ denote the probability of a conjugacy class to be M-power separable in $\mathrm{O}^\epsilon(2n,\mathbb{F}_q)$ with $\epsilon\in\{\pm\}$ and $cs^M_{\mathrm{O}^0}(n,q)$ denotes the probability of a conjugacy class to be M-power separable in $\mathrm{O}^0(2n+1,\mathbb{F}_q)$. Define*

$$cS^M_{\mathrm{O}^+}(q,u) = 1+\sum_{m\geq 1}^{\infty} cs^M_{\mathrm{O}^+}(m,q)u^m$$
$$cS^M_{\mathrm{O}^-}(q,u) = \sum_{m\geq 1}^{\infty} cs^M_{\mathrm{O}^-}(m,q)u^m$$
$$cS^M_{\mathrm{O}^0}(q,u) = 1+\sum_{m\geq 1}^{\infty} cs^M_{\mathrm{O}^0}(m,q)u^m.$$

Then

$$cS^M_{\mathrm{O}^+}(u^2)+cS^M_{\mathrm{O}^-}(u^2)+e(q)ucS^M_{\mathrm{O}^0}(u^2) = (1+2u)^{o(M,q)}cS^M_{\mathrm{Sp}}(u^2), \tag{4.2.5}$$
$$cS^M_{\mathrm{O}^+}(u^2)-cS^M_{\mathrm{O}^-}(u^2) = cX^M_{\mathrm{O}^0}(u^2), \tag{4.2.6}$$

where

$$cX^M_{\mathrm{O}^0}(q,u) = \prod_{d=1}^{\infty}\left(1-u^d\right)^{N_M^*(q,2d)}\prod_{d=1}^{\infty}\left(1+u^d\right)^{R_M^*(q,2d)}.$$

4.3 Semisimple matrices

Before moving towards the determination of generating functions for semisimple cases, 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.

Lemma 4.3.1. *Let $q \neq 2^j$ and $r(M,q)$ denote the least size of matrix $-\mathbb{I}$ such that it has an M-th root in $\mathrm{Sp}(r(M,q),q)$. Then*

$$r(M,q) = \begin{cases} 2 & \text{if } M = 2 \\ s & \text{if there exists } n \text{ such that } 2M|(q^n+1), (M,q) = 1 \\ 2s & 2M \nmid (q^n+1) \text{ for any } n, (M,q) = 1 \\ r\left(\frac{2M}{(2M,q)}, q\right) & \text{when } (M,q) \neq 1 \end{cases},$$

where $s \in \mathbb{N}$ is the smallest number satisfying $q^s \equiv 1(\mathrm{mod}\ 2M)$.

Proof. First of all, note that $r(M,q)$ is always even as any matrix in $\mathrm{Sp}(2n,\mathbb{F}_q)$ has determinant 1. Let $M = 2$, then $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ implies that -1_{2k} has an M-th root for all $k \geq 1$.

Now consider the case $M \neq 2$ and $q \neq 2^l$ (as in this case $|\pm 1| = 1$)and -1_l has an M-th root in $\mathrm{Sp}(2n,\mathbb{F}_q)$, say α. Let γ be a root of $\min_{\mathbb{F}_q}(\alpha)$. Then γ is a primitive $2M$-th root of unity. Hence $\min_{\mathbb{F}_q}(\alpha)$ divides the $2M$-th cyclotomic polynomial Q_{2M} over $\mathbb{F}_q$. From [LiNi97], it is known that in case $(q,2M) = 1$ (which is true as $q \neq 2^s$ and (q,M)=1), Q_{2M} factors into $\frac{\phi(2M)}{d}$ (where ϕ is the Euler's totient function) distinct monic irreducible polynomial in $\mathbb{F}_q[x]$, of same degree d, where d is the least positive integer satisfying $q^d \equiv 1(\mathrm{mod}\ 2M)$.

If any of the irreducible factor is of type 1, then d is the required value of $r(M,q)$ (as we are considering the case of $\mathrm{Sp}(2n,\mathbb{F}_q)$), otherwise $r(M,q) = 2d$.

For the case $(q,2M) \neq 1$, let $(q,2M) = q'$ then $(q, \frac{2M}{q'}) = 1$. Then replacing $2M$, by $\frac{2M}{q'}$ we get the result, as q is odd. □

Corollary 4.3.2. *The matrix $-1_{2n\times 2n}$ has an M-th root in $\mathrm{Sp}(2n,\mathbb{F}_q)$ if and only if $r(M,q)|2n$.*

Proof. Follows from the factorization of the cyclotomic polynomial $Q_{\frac{2M}{(q,2M)}} \in \mathbb{F}_q[x]$, as all of the irreducible factors have same degree. □

Remark 4.3.3. The value $r(M,q)$ in the lemma above is always even.

Proposition 4.3.4. *Let $css^M_{\mathrm{Sp}}(2n,q)$ denote the number of M-power semisimple conjugacy classes in* $\mathrm{Sp}(2n,\mathbb{F}_q)$ *and* $cSS^M_{\mathrm{Sp}}(q,u) = 1 + \sum_{m=1}^{\infty} css^M_{\mathrm{Sp}}(2m,q)u^m$. *Then $cSS^M_{\mathrm{Sp}}(q,u)$ is given by*

$$\frac{1}{(1-u^{r(M,q)})^{e(q)-1}(1-u)}\prod_{d=1}^{\infty}(1-u^d)^{-N^*_M(q,2d)}\prod_{d=1}^{\infty}(1-u^d)^{-R^*_M(q,2d)}$$

$$\prod_{d=1}^{\infty}\prod_{e|q^d+1}\left(1+\sum_{m=1}^{\infty}\mathcal{I}_{e,2d}(2dm)u^{dm}\right)^{N^{*,e}_M(q,2d)}\prod_{d=1}^{\infty}\prod_{e|q^d-1}\left(1+\sum_{m=1}^{\infty}\mathcal{I}_{e,d}(dm)u^{dm}\right)^{R^{*,e}_M(q,2d)}$$

where $r(M,q)$ is as in 4.3.1 and $\mathcal{I}_{e,d}$ is as mentioned in Remark 4.1.20.

Proof. Let $X \in \mathrm{Sp}(2n,\mathbb{F}_q)$ 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 $t-1$ to have even multiplicity 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 $r_1, r_{-1}, l_f \in \mathbb{Z}_{>0}$. Hence using 4.1.22 and discussion preceding 4.1.13, 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 $r_{-1} \in r(M,q)\mathbb{Z}_{>0}$ (follows from 4.3.2),

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

6. for f, a type 2 polynomial which is not an M-power polynomial, $\lambda_f = \lambda_{f^*} \in \{0, 1^m : m \in \sum_{i \in \mathcal{D}_M(f)} \mathbb{Z}_{\geq 0} i\}$.

Hence $cSS^M_{\mathrm{Sp}}(q, u)$ is given by

$$\left(1+\sum_{m=1}^{\infty} u^m\right)\left(1+\sum_{m=1}^{\infty} u^{m\frac{r(M,q)}{2}}\right)^{e(q)-1}$$
$$\prod_{\substack{f=f^*\\ f\in\Phi^*_M}}\left(1+\sum_{m=1}^{\infty} u^{m\frac{\deg f}{2}}\right)\prod_{\substack{\{f\neq f^*\}\\ f\in\Phi_M}}\left(1+\sum_{m=1}^{\infty} u^{m\deg f}\right)$$
$$\prod_{\substack{f=f^*\\ f\notin\Phi^*_M}}\prod_{e|q^{\frac{\deg f}{2}}+1}\left(1+\sum_{m=1}^{\infty}\mathcal{I}_M(f)(m\deg f)u^{\frac{\deg f}{2}m}\right)$$
$$\prod_{\substack{\{f,f^*\}\\ f\neq f^*, f\notin\Phi_M}}\prod_{e|q^{\deg f}-1}\left(1+\sum_{m=1}^{\infty}\mathcal{I}_M(f)(m\deg f)u^{m\deg f}\right)$$

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 Φ^*_M and Φ_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 $i = 1, 2, \cdots$. Then clearly $\deg f | k_i$ and $(f, 1^{\frac{k_i}{\deg f}})$ is an M-th power for all $k_i \in \mathcal{D}_M(f)$. Then for any integer $m \in \sum_{c_i \in \mathbb{Z}_{\geq 0}} c_i \dfrac{k_i}{\deg f}$, the class $(f, 1^m)$ is an M-th power.

   In this case, two kinds of polynomials can occur in the factorization of $f(x^M)$. It can be of either type 1 or type 2. For this the function G_f (see Definition

4.1.19) has two components corresponding to each type. Hence we associate the function $\mathcal{I}_M(f)$ which indicates whether $m \in \sum\limits_{c_i \in \mathbb{Z}_{\geq 0}} c_i \dfrac{k_i}{\deg f}$ or not.

5. the sixth term appears for the type 2 polynomials 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 4.1.17 we get the result, as $1 + \sum\limits_{m=1}^{\infty} u^m = (1-u)^{-1}$. □

Theorem 4.3.5. *Let $ss^M_{\mathrm{Sp}}(n,q)$ be the probability of an element to be M-power semisimple in $\mathrm{Sp}(2n,\mathbb{F}_q)$ and $SS^M_{\mathrm{Sp}}(q,u) = 1 + \sum\limits_{m=1}^{\infty} ss^M_{\mathrm{Sp}}(2m,q)u^m$. Then*

$$
\begin{aligned}
SS^M_{\mathrm{Sp}}(q,u) = &\left(1 + \sum_{m\geq 1} \frac{u^{m\frac{r(M,q)}{2}}}{|\mathrm{Sp}(mr(M,q),\mathbb{F}_q)|}\right)^{e(q)-1} \left(1 + \sum_{m\geq 1} \frac{u^m}{|\mathrm{Sp}(2m,\mathbb{F}_q)|}\right) \\
&\prod_{d=1}^{\infty}\left(1 + \sum_{m\geq 1} \frac{u^{dm}}{|\mathrm{U}(m,\mathbb{F}_{q^d})|}\right)^{N^*_M(q,2d)} \prod_{d=1}^{\infty}\left(1 + \sum_{m\geq 1} \frac{u^{dm}}{|\mathrm{GL}(m,\mathbb{F}_{q^d})|}\right)^{R^*_M(q,2d)} \\
&\prod_{d=1}^{\infty}\prod_{e|(q^d+1)}\left(1 + \sum_{m=1}^{\infty} \mathcal{I}_{e,2d}(2dm)\frac{u^{dm}}{|\mathrm{U}(m,\mathbb{F}_{q^d})|}\right)^{N^{*;e}_M(q,2d)} \\
&\prod_{d=1}^{\infty}\prod_{e|(q^d-1)}\left(1 + \sum_{m=1}^{\infty} \mathcal{I}_{e,d}(dm)\frac{u^{dm}}{|\mathrm{GL}(m,\mathbb{F}_{q^d})|}\right)^{R^{*;e}_M(q,2d)}
\end{aligned}
$$

where $e(q)$, $r(M,q)$ are as in 4.3.4.

Proof. Since $\pm\mathbb{I}_{2n}$ are in the center of $\mathrm{Sp}(2n,\mathbb{F}_q)$, their centralisers are $\mathrm{Sp}(2n,\mathbb{F}_q)$ itself. From 2.2.1 and 2.3.3, we have that

1. if $f \in \Phi^*$ is of degree $2k$ and $\mu_f = 1^m$, then centraliser of X inside $\mathrm{Sp}(2km,\mathbb{F}_q)$ is of order $|\mathrm{U}(m,\mathbb{F}_{q^k})|$,

2. if $f \in \Phi \setminus \Phi^*$ is of degree k and $\mu_f = 1^m$, then centraliser of X inside $\mathrm{Sp}(2dm,\mathbb{F}_q)$ is of order $|\mathrm{GL}(m,\mathbb{F}_{q^d})|$.

Hence using 4.3.4 and the fact that the centralizer of a general block diagonal matrix is a direct sum of each of the corresponding centralizers, we have the result. □

The next theorem is proved along the same line of proof of the Theorem 3.1.6 of [FuNePr05].

Definition 4.3.6. We define the following functions for simplifying the statements in the case of orthogonal groups.

$$\begin{aligned}
Y_1^{*,M}(u,q) =&\prod_{d=1}^{\infty}\left(1+\sum_{m\geq 1}\frac{u^{dm}}{|\mathrm{U}(m,\mathbb{F}_{q^d})|}\right)^{N^*_M(q,2d)}\prod_{d=1}^{\infty}\left(1+\sum_{m\geq 1}\frac{u^{dm}}{|\mathrm{GL}(m,\mathbb{F}_{q^d})|}\right)^{R^*_M(q,2d)}\\
&\prod_{d=1}^{\infty}\prod_{e|q^d+1}\left(1+\sum_{m=1}^{\infty}\mathcal{I}_{e,2d}(2dm)\frac{u^{dm}}{|\mathrm{U}(m,\mathbb{F}_{q^d})|}\right)^{N^{*,e}_M(q,2d)}\\
&\prod_{d=1}^{\infty}\prod_{e|q^d-1}\left(1+\sum_{m=1}^{\infty}\mathcal{I}_{e,d}(dm)\frac{u^{dm}}{|\mathrm{GL}(m,\mathbb{F}_{q^d})|}\right)^{R^{*,e}_M(q,2d)},\\
Y_2^{*,M}(u,q) =&\prod_{d=1}^{\infty}\left(1+\sum_{m\geq 1}\frac{(-1)^m u^{dm}}{|\mathrm{U}(m,\mathbb{F}_{q^d})|}\right)^{N^*_M(q,2d)}\prod_{d=1}^{\infty}\left(1+\sum_{m\geq 1}\frac{u^{dm}}{|\mathrm{GL}(m,\mathbb{F}_{q^d})|}\right)^{R^*_M(q,2d)}\\
&\prod_{d=1}^{\infty}\prod_{e|q^d+1}\left(1+\sum_{m=1}^{\infty}\mathcal{I}_{e,2d}(2dm)\frac{(-1)^m u^{dm}}{|\mathrm{U}(m,\mathbb{F}_{q^d})|}\right)^{N^{*,e}_M(q,2d)}\\
&\prod_{d=1}^{\infty}\prod_{e|q^d-1}\left(1+\sum_{m=1}^{\infty}\mathcal{I}_{e,d}(dm)\frac{u^{dm}}{|\mathrm{GL}(m,\mathbb{F}_{q^d})|}\right)^{R^{*,e}_M(q,2d)},\\
F_{+,+1}(u,q) =&1+\sum_{m\geq 1}\left(\frac{1}{|\mathrm{O}^+(2m,\mathbb{F}_q)|}+\frac{1}{|\mathrm{O}^-(2m,\mathbb{F}_q)|}\right)u^m,\\
F_{-,+1}(u,q) =&1+\sum_{m\geq 1}\left(\frac{1}{|\mathrm{O}^+(2m,\mathbb{F}_q)|}-\frac{1}{|\mathrm{O}^-(2m,\mathbb{F}_q)|}\right)u^m,\\
F_{+1}(u,q) =&1+\sum_{m\geq 1}\frac{u^m}{|\mathrm{Sp}(2m,\mathbb{F}_q)|},\\
F^M_{+,-1}(u,q) =&1+\sum_{m\geq 1}\left(\frac{1}{|\mathrm{O}^+(mr(M,q),\mathbb{F}_q)|}+\frac{1}{|\mathrm{O}^-(mr(M,q),\mathbb{F}_q)|}\right)u^{m\frac{r(M,q)}{2}},\\
F^M_{-,-1}(u,q) =&1+\sum_{m\geq 1}\left(\frac{1}{|\mathrm{O}^+(mr(M,q),\mathbb{F}_q)|}-\frac{1}{|\mathrm{O}^-(mr(M,q),\mathbb{F}_q)|}\right)u^{m\frac{r(M,q)}{2}},\\
F_{-1}(u,q) =&1+\sum_{m\geq 1}\frac{u^{\frac{mr(M,q)}{2}}}{|\mathrm{Sp}(mr(M,q),\mathbb{F}_q)|}.
\end{aligned}$$

Theorem 4.3.7. *Let $ss^M_{\mathrm{O}^\epsilon}(n,q)$ denotes the probability of an element to be M-power semisimple in $\mathrm{O}^\epsilon(2n,\mathbb{F}_q)$ with $\epsilon \in \{\pm\}$ and $s^M_{\mathrm{O}^0}(n,q)$ denotes the probability of an element to be M-power semisimple in $\mathrm{O}^0(2n+1,\mathbb{F}_q)$.*

Define

$$\begin{aligned} SS^M_{\mathrm{O}^+}(q,u) &= 1 + \sum_{m\geq 1}^{\infty} ss^M_{\mathrm{O}^+}(m,q)u^m \\ SS^M_{\mathrm{O}^-}(q,u) &= \sum_{m\geq 1}^{\infty} ss^M_{\mathrm{O}^-}(m,q)u^m \\ SS^M_{\mathrm{O}^0}(q,u) &= 1 + \sum_{m\geq 1}^{\infty} ss^M_{\mathrm{O}^0}(m,q)u^m. \end{aligned}$$

Then

$$\begin{aligned} &SS^M_{\mathrm{O}^+}(u^2) + SS^M_{\mathrm{O}^-}(u^2) + e(q)uSS^M_{\mathrm{O}^0}(u^2) \\ &= \left(F^M_{+,+1}(u^2) + uF_{+1}(u^2)\right)\left(F^M_{+,-1}(u^2) + uF_{-1}(u^2)\right)^{e(q)-1} Y^{*,M}_1(u^2), \\ &S^M_{\mathrm{O}^+}(u^2) - S^M_{\mathrm{O}^-}(u^2) = F_{-,+1}(u^2)[F^M_{-,-1}(u^2)]^{e(q)-1}Y^{*,M}_2(u^2). \end{aligned}$$

Proof. Using similar argument as in 4.2.3, the proof follows. □

4.4 Cyclic matrices

Before giving the generating function for the cyclic conjugacy classes we first 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 eigenvalue 1 are in bijection with conjugacy classes of matrices with eigenvalue -1. Recall that an element $X \in \mathrm{Sp}(2n,\mathbb{F}_q)$ 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 [GoLiBr, Section 2.4]). In general, we have the following

Lemma 4.4.1. *Let $q = p^r$, for some prime p. An element $A \in \mathrm{Sp}(2n,\mathbb{F}_q)$ is unipotent if and only if order of A is p^s, for some $s \in \mathbb{N}$.*

Proof. Let $A \in \mathrm{Sp}(2n, \mathbb{F}_q)$ be of order p^s. Then A satisfies the polynomial $x^{p^s} - 1 = (x-1)^{p^s}$. Thus characteristic polynomial of A should divide $(x-1)^{p^s}$. Hence it has all the eigenvalues to be 1. Conversely, suppose A is an unipotent element. Then A is an element of the group of upper triangular matrices $\mathrm{UP}(2n, \mathbb{F}_q)$, whence $A^{q^{\frac{n(n-1)}{2}}} = 1$. □

Corollary 4.4.2. *If $(M, q) = 1$, then every unipotent conjugacy class is an M-th power.*

Let us denote the matrix $U_{C_f,n} = \begin{pmatrix} C_f & 1 & & & & \\ & C_f & 1 & & & \\ & & C_f & 1 & & \\ & & & \ddots & \ddots & \\ & & & & C_f & 1 \\ & & & & & C_f \end{pmatrix}$ of size $n \deg f \times n \deg f$ by $U_{C_f,n}$ (with all other entries to be 0), 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 α_s of α, where $\alpha^M = U_{t+1,n}$ and $\alpha \in \mathrm{GL}(n, q)$. We have the following

Lemma 4.4.3. *Let $(M, q) = 1$ and there exist $\alpha \in \mathrm{GL}(n, \mathbb{F}_q)$ satisfying $\alpha^M = U_{t+1,n}$. Then the semisimple part α_s is a scalar matrix.*

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

Corollary 4.4.4. *Let $(M, q) = 1$ and $U^{\mathrm{Sp}}_{t+1,n} \in \mathrm{Sp}(2m, \mathbb{F}_q)$ where $U^{\mathrm{Sp}}_{t+1,n}$ is conjugate to $U_{t+1,n}$ in $\mathrm{GL}(2m, \mathbb{F}_q)$. Then $U^{\mathrm{Sp}}_{t+1,n}$ is an M-th power in $\mathrm{Sp}(2m, \mathbb{F}_q)$ if and only if M is odd.*

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

Conversely suppose $\alpha^M = U^{\mathrm{Sp}}_{t+1,n}$ for some $\alpha \in \mathrm{Sp}(2m, \mathbb{F}_q)$. Also $U^{\mathrm{Sp}}_{t+1,n}$ and $\alpha \in \mathrm{GL}(2m, \mathbb{F}_q)$ implies that α_s is a scalar matrix. Then we have that $\alpha_s = -1$, since $\mathrm{Sp}(2m, \mathbb{F}_q)$ contains only the scalar matrices $\{\pm 1\}$. Hence M should be odd. □

Corollary 4.4.5. *Let $(M,q)=1$. Any matrix $X \in \mathrm{Sp}(2n,\mathbb{F}_q)$ with combinatorial data $(t+1,m^{\pm})$ is an M-th power if and only if M is odd.*

Proof. This follows from 4.4.2 and proof of 4.4.4. □

From [BuGi16, Section 3.4] we use tensor product construction to study the ±1-potent conjugacy classes and denote them by $[J_a^{b,\epsilon}]$. From Lemma 3.4.7 [BuGi16], we have

Lemma 4.4.6. *A unipotent element of type $[J_a^{b,\epsilon}]$ fixes a pair of complementary maximal totally isotropic subspaces of the natural $\mathrm{Sp}_{ab}(\mathbb{F}_q)$-module if and only if $\epsilon = +$.*

Corollary 4.4.7. *We have that $[J_a^{b,\epsilon}]^M = [J_a^{b,\epsilon}]$.*

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 $[J_a^{b,-}]^M$ has the property that it fixes a pair of complementary maximally totally isotropic subspaces. Since $[J_a^{b,-}]$ has power coprime to M, we have that $[J_a^{b,-}]$ fixes a pair of complementary maximally totally isotropic subspaces, which is a contradiction. □

Corollary 4.4.8. *For M odd, we have that $[-J_a^{b,\epsilon}]^M = [-J_a^{b,\epsilon}]$.*

Proposition 4.4.9. *Let $cc_{\mathrm{Sp}}^M(2n,q)$ denote the number of M-power cyclic conjugacy classes in $\mathrm{Sp}(2n,\mathbb{F}_q)$ and $cC_{\mathrm{Sp}}^M(q,u) = 1 + \sum_{m=1}^{\infty} cc_{\mathrm{Sp}}^M(2m,q)u^m$. Then $cC_{\mathrm{Sp}}^M(q,u)$ is given by*

$$\left(\frac{2}{1-u} - 1 - u\right)^{h(q,M)} \prod_{d=1}^{\infty}(1-\delta u^d)^{-\delta N_M^*(q,2d)} \prod_{d=1}^{\infty}(1-\delta u^d)^{-\delta R_M^*(q,2d)}, \tag{4.4.1}$$

where

$$h(q,M) = \begin{cases} 0 & \textit{if } (M,q) \neq 1 \\ 2 & \textit{if } (M,q)=1, M = \textit{odd}, (q,2)=1 \\ 1 & \textit{otherwise} \end{cases}$$

and

$$\delta = \begin{cases} 1 & \textit{if } (M,q)=1 \\ -1 & \textit{if } (M,q) \neq 1 \end{cases}.$$

Proof. Let $X \in \mathrm{Sp}(2n, \mathbb{F}_q)$ be cyclic. Then $c_X(t) = m_X(t)$. Since the space $\mathbb{F}_q^{2n}$, considered as an X-module is cyclic, we have that the primary decomposition of $\mathbb{F}_q^{2n}$ should be of the form $\bigoplus\limits_{f\in\Phi} \dfrac{\mathbb{F}_q[t]}{f(t)^a}$, with each $f \in \Phi$ occurring at most once. Let $\Delta_X = \{(f, \lambda_f) : f \in \Phi\}$. Then Δ_X represents a cyclic class if and only if

1. $\lambda_{t\pm1}$ is an even integer,

2. $\lambda_f = \lambda_{f^*} \in \mathbb{Z}_{\geq 0}$.

We divide the proof into 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 $U_{C_f^M}$, we have that X is an M-th power cyclic matrix if and only if

1. λ_{t-1} is an even integer,

2. λ_{t+1} is an even integer 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

$$cC^M_{\mathrm{Sp}}(q, u) = \left(1 + 2\sum_{m\geq1}^{\infty} u^m\right)^{h(q,M)} \prod_{f\in\Phi^*_M} \left(1 + \sum_{m\geq1}^{\infty} u^{m\frac{\deg f}{2}}\right) \prod_{g\in\Phi_M\setminus\Phi^*_M} \left(1 + \sum_{m\geq1}^{\infty} u^{m\deg g}\right)^{\frac{1}{2}},$$

where

1. the first term accounts for the terms corresponding to $t \pm 1$, with a power 1 if $q = 2^s$ or 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 $(1 + \sum\limits_{m\geq1}^{\infty} u^{m\deg g})$ occurs twice.

Then grouping the polynomials with same degree of type 1 or 2, the result follows for the case $(M, q) = 1$. The case $(M, q) \neq 1$ goes on the same lines and therefore omitted. □

Theorem 4.4.10. *Let $c^M_{\mathrm{Sp}}(n,q)$ be the probability of an element to be M-power cyclic in* $\mathrm{Sp}(2n,\mathbb{F}_q)$ *and* $C^M_{\mathrm{Sp}}(q,u) = 1 + \sum\limits_{m=1}^{\infty} c^M_{\mathrm{Sp}}(2m,q)u^m$*. Then $C^M_{\mathrm{Sp}}(q,u)$ is given by*

$$\left(\frac{1}{1-\frac{u}{q}}\right)^{h(q,M)} \prod_{d=1}^{\infty}\left(1+\frac{u^d}{(q^d+1)(1-\frac{u^d}{q^d})}\right)^{N^*_M(q,2d)} \prod_{d=1}^{\infty}\left(1+\frac{u^d}{(q^d-1)(1-\frac{u^d}{q^d})}\right)^{R^*_M(q,2d)}, \tag{4.4.2}$$

if $(q,M)=1$, where $h(q,M)$ is as in 4.4.9 and by

$$\prod_{d=1}^{\infty}\left(1+\frac{u^d}{q^d+1}\right)^{N^*_M(q,2d)} \prod_{d=1}^{\infty}\left(1+\frac{u^d}{q^d-1}\right)^{R^*_M(q,2d)}, \tag{4.4.3}$$

if $(q,M)\neq 1$.

Proof. For $(M,q)\neq 1$, the result is same as 4.2.2. Hence let us assume $(M,q)=1$. Then it follows from 2.2.1 and 2.3.3, that

1. for $m \geq 2$, the cyclic matrices corresponding to $t\pm 1$, in $\mathrm{Sp}(2m,\mathbb{F}_q)$ 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 $\mathrm{Sp}(2ml,\mathbb{F}_q)$ 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 $\mathrm{Sp}(2ml,\mathbb{F}_q)$ of a matrix X, with $\Delta_X = \{(f,l),(f^*,l)\}$ is $q^{2d(l-1)}(q^d-1)$.

Hence using 4.4.9 and the fact that the centralizer of a general block diagonal matrix is a direct sum of each of the corresponding centralizers, we have the result. □

Analogous statements as in 4.4.4, 4.4.9 are true in case of $\mathrm{O}^\epsilon(n,\mathbb{F}_q)$, whenever $(M,q)=1$. Hence we consider the case when $(q,2)=1\neq(M,q)$. From [GoLiBr, Section 2.5], we know that for unipotent elements of $O^\epsilon(m,\mathbb{F}_q)$ 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

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

where $\epsilon = 1$ or is a non-square in $\mathbb{F}_q$. But then A_ε^M is not cyclic -1-potent element. Also considering the representative for $(q,2) \neq 1$, from Section 3 of [GoLiBr], we have,

Lemma 4.4.11. *Let $(M,q) \neq 1$. Then none of the matrices $X \in \mathrm{O}^\epsilon(m, \mathbb{F}_q)$, with combinatorial data $\Delta_X = \{(t \pm 1, (2k+1)^\pm)\}$ with $|k| \geq 1$, is an M-th power.*

Before writing down the generating functions for the cyclic elements, let us introduce the following functions:

Definition 4.4.12. We define

$$Z_{\mathrm{O}}(u) = \prod_{d=1}^{\infty} \left(1 + \frac{u^d}{(q^d+1)(1-(\frac{u}{q})^d)}\right)^{N_M^*(q,2d)} \left(1 + \frac{u^d}{(q^d-1)(1-(\frac{u}{q})^d)}\right)^{R_M^*(q,2d)},$$

$$Z'_{\mathrm{O}}(u) = \prod_{d=1}^{\infty} \left(1 - \frac{u^d}{(q^d+1)(1+(\frac{u}{q})^d)}\right)^{N_M^*(q,2d)} \left(1 + \frac{u^d}{(q^d-1)(1-(\frac{u}{q})^d)}\right)^{R_M^*(q,2d)}.$$

Theorem 4.4.13. *Let $c^M_{\mathrm{O}^\epsilon}(n,q)$ be the probability of an element to be M-power cyclic in $\mathrm{O}^\epsilon(2n, \mathbb{F}_q)$ with $\epsilon \in \{\pm\}$ and $c^M_{\mathrm{O}^0}(n,q)$ denotes the probability of an element* *to be M-power cyclic in* $\mathrm{O}^0(2n+1,\mathbb{F}_q)$. *Define*

$$\begin{aligned} C^M_{\mathrm{O}^+}(q,u) &= 1+\sum_{m\geq 1}^{\infty} c^M_{\mathrm{O}^+}(m,q)u^m \\ C^M_{\mathrm{O}^-}(q,u) &= \sum_{m\geq 1}^{\infty} c^M_{\mathrm{O}^-}(m,q)u^m \\ C^M_{\mathrm{O}^0}(q,u) &= 1+\sum_{m\geq 1}^{\infty} c^M_{\mathrm{O}^0}(m,q)u^m. \end{aligned}$$

Then

$$C_{\mathrm{O}^+}(u^2)+C_{\mathrm{O}^-}(u^2)+2uC_{\mathrm{O}^0}(u^2) = \left(1+\eta(q)u+\frac{u^2}{1-\frac{u^2}{q}}\right)^{h(q,M)} Z_{\mathrm{O}}(u^2), \quad (4.4.4)$$

where $h(q,M)$ is as in 4.4.9 and $\eta(q) = \begin{cases} 0 & \textit{if } (q,2)=1 \\ 1 & \textit{otherwise} \end{cases}$, *and*

$$C^M_{\mathrm{O}^+}(u^2) - C^M_{\mathrm{O}^+}(u^2) = Z'_O(u^2). \quad (4.4.5)$$

Proof. We divide the proof in several cases. The first case is when M, q are odd and $(M,q)=1$. Then consider the product

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

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 $1+\frac{2u}{2}+\frac{2u^3}{2q}+\frac{2u^5}{2q^2}+\cdots = 1+\dfrac{u}{1-\frac{u^2}{q}}$. Hence using arguments similar to 4.2.3, we have that the product on expansion gives $C_{\mathrm{O}^+}(u^2)+C_{\mathrm{O}^-}(u^2)+2uC_{\mathrm{O}^0}(u^2)$.

Next assume that q is even, $(M,q)=1$. Hence M is odd, whence all unipotent elements are M-th power. In this case the cyclic unipotent matrix can be of order 1×1 or $2m\times 2m$. In the first case, order of the centraliser is 1. In the later case, there are two conjugacy classes each having centraliser of order $2q^{m-1}$. Hence in this case $C_{\mathrm{O}^+}(u^2) + C_{\mathrm{O}^-}(u^2) + 2uC_{\mathrm{O}^0}(u^2)$ is given by

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

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 have odd size, we see that none of the cyclic matrices in $\mathrm{O}^{\pm}$, has unipotent part. This along with arguments as before, we have that in this case $C_{\mathrm{O}^+}(u^2) + C_{\mathrm{O}^-}(u^2) + 2uC_{\mathrm{O}^0}(u^2)$ 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 final case of $(M, q) \neq 1$, since none of the cyclic unipotent or -1-potent elements are cyclic, we have that, $C_{\mathrm{O}^+}(u^2) + C_{\mathrm{O}^-}(u^2) + 2uC_{\mathrm{O}^0}(u^2)$ is given by

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

For the last equation argument similar to 4.2.3 does the job. □

4.4.1 Regular elements

Since in case of $\mathrm{Sp}(2n, \mathbb{F}_q)$, an element $X \in \mathrm{Sp}(2n, \mathbb{F}_q)$ is regular if and only if X is cyclic [NePr95], we concentrate on the case of $\mathrm{O}^{\epsilon}(m, \mathbb{F}_q)$. We will need the following definition from [FuNePr05].

Definition 4.4.14. Let U be a finite dimensional vector space over $\mathbb{F}_q$ and $X \in \mathrm{Aut}(U, \varphi)$ and $c_X(t) = (t - \mu)^n$ where, φ 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 $U = U_0 \oplus^{\perp} U_1$, 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 [FuNePr05], which is as follows.

Theorem 4.4.15. *Let q be odd and $X \in \mathrm{O}^\epsilon(m, \mathbb{F}_q)$. Then X is regular if and only if*

1. *for every monic irreducible polynomial ϕ other than $t \pm 1$, the ϕ-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 4.4.16. *Assume q to be odd and let $r^M_{\mathrm{O}^\epsilon}(n, q)$ be the probability of an element to be M-power regular in $\mathrm{O}^\epsilon(2n, \mathbb{F}_q)$ with $\epsilon \in \{\pm\}$ and $r^M_{\mathrm{O}^0}(n, q)$ denotes the probability of an element to be M-power regular in $\mathrm{O}^0(2n + 1, \mathbb{F}_q)$. Define*

$$R^M_{\mathrm{O}^+}(q, u) = 1 + \sum_{m \geq 1}^{\infty} r^M_{\mathrm{O}^+}(m, q) u^m$$

$$R^M_{\mathrm{O}^-}(q, u) = \sum_{m \geq 1}^{\infty} r^M_{\mathrm{O}^-}(m, q) u^m$$

$$R^M_{\mathrm{O}^0}(q, u) = 1 + \sum_{m \geq 1}^{\infty} r^M_{\mathrm{O}^0}(m, q) u^m.$$

Then

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

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

Proof. This follows the line of proof as in [FuNePr05, Theorem 3.2.2]. Note that

$$R^M_{\mathrm{O}^+}(u^2) + R^M_{\mathrm{O}^-}(u^2) + 2uR^M_{\mathrm{O}^0}(u^2) = F^M_1(u) F^M_{-1}(u) Z_{\mathrm{O}}(u^2),$$

where the functions F^M_1, F^M_{-1} have to be determined. Let us start with the case of M being odd. Corresponding to the polynomial $t - 1$, the component in the primary decomposition is either cyclic (odd dimensional) or nearly cyclic (even dimensional). Both of the cases can have ± types. Note that for the odd number

$2m{+}1$, there exists a single conjugacy class of unipotent cyclic elements of $\mathrm{O}^0(2m+1, \mathbb{F}_q)$ with centralizer having order $2q^m$ and this is always an M-th power. There is a single class of nearly cyclic unipotent elements in $\mathrm{O}^\epsilon(2, \mathbb{F}_q)$ consisting of 1 with order of the centralizer $2(q - \epsilon 1)$, $\epsilon \in \{\pm\}$. This class is also an M-th power. For $m \geq 2$, there are two classes of nearly cyclic unipotent matrices in $\mathrm{O}^\epsilon(2m, \mathbb{F}_q)$, $\epsilon \in \{\pm\}$. For each class, the corresponding primary decomposition has one 1 dimensional space and the other is a cyclic X-module. In this case, these are also M-th power. The centralizer in this case has order $4q^m$. Hence

$$\begin{aligned} F_1^M(u) &= 1 + \left(\frac{u}{1} + \frac{u^3}{q} + \frac{u^5}{q^2} + \cdots\right) + \left(\frac{u^2}{2(q-1)} + \frac{u^2}{2(q+1)} + 4\frac{u^4}{4q^2} + 4\frac{u^6}{4q^3} + \cdots\right) \\ &= \left(1 + \frac{u}{1 - \frac{u^2}{q}} + \frac{qu^2}{q^2-1} + \frac{u^4}{q^2(1 - \frac{u^2}{q})}\right). \end{aligned}$$

Using same argument and 4.4.9, we find that

$$F_{-1}^M(u) = \begin{cases} \left(1 + \dfrac{u}{1 - \frac{u^2}{q}} + \dfrac{qu^2}{q^2-1} + \dfrac{u^4}{q^2(1 - \frac{u^2}{q})}\right) & \text{if } M \text{ odd} \\ 1 + \dfrac{u^2}{2(q-1)} + \dfrac{u^2}{2(q+1)} & M = 2 \\ 1 & \text{otherwise} \end{cases}.$$

Hence multiplying the obtained functions, the result follows. □

Chapter 5

Further plans

In this part, we have come up with the generating functions for the probability of an element g being an M-th power in the case of g being separable, semisimple, regular, and cyclic where $g \in \mathrm{Sp}(2m, q), \mathrm{O}(m, q)^{\epsilon}$ with $\epsilon \in \{\pm, 0\}$. Most of the cases have been answered using the assumption $(M, q) = 1$.

In our future work, we will be working with the case $(M, q) \neq 1$ and also the general case. We are in the stage of finding a cycle index analogue of the generating functions. Recall that such cycle index has been provided in work of Jason Fulman. For example recall that

$$\begin{aligned}
&1 + \sum_{n=1}^{\infty} \frac{u^{2n}}{|\mathrm{Sp}(2n, q)|} \sum_{\alpha \in \mathrm{Sp}(2n,q)} \prod_{f = t \pm 1} x_{f, \lambda_f^{\pm}(\alpha)} \prod_{f \neq t \pm 1} x_{f, \lambda_f(\alpha)} \\
&= \prod_{f = t \pm 1} \left(\sum_{\lambda^p m} x_{f, \lambda^{\pm}} \frac{u^{|\lambda^{\pm}|}}{c_{\mathrm{Sp}, f, q}(\lambda^{\pm})} \right) \prod_{\substack{f = f^* \\ f \neq t \pm 1}} \left(\sum_{\lambda} x_{f, \lambda} \frac{(-(u^{\deg f}))^{|\lambda|}}{c_{\mathrm{GL}, t-1, -(q^{\deg f/2})}(\lambda)} \right) \\
&\times \prod_{\substack{\{f, f^*\} \\ f \neq f^*}} \left(\sum_{\lambda} x_{f, \lambda} x_{f^*, \lambda} \frac{u^{2|\lambda| \deg f}}{c_{\mathrm{GL}, t-1, q^{\deg f}}(\lambda)} \right).
\end{aligned}$$

We would like to ask the following question:

Question 4. *Does the cycle index for M-th powers in finite symplectic or orthogonal group factorizes as above?*

Question 5. *What will be the asymptotic values of the probability $\frac{G_{cc}^M}{|G|}$ where G_{cc}^M is the number of M-th power element of a particular type (for example semisimple, regular semisimple)?*

Note that we have mostly concentrated on the cases $(M, q) = 1$. The case $(M, q) \neq 1$ seems more tricky and difficult. So a question which naturally arises here is the following.

Question 6. *Is there any analogue for the case $(M, q) \neq 1$ to the results obtained in this thesis?*

Part II

Results in Skew Braces

Chapter 6

Skew braces

The Yang-Baxter equation first appeared in theoretical physics and statistical mechanics in the works of Yang [Ya67] and Baxter [Ba71]. Let $\mathcal{A}$ be an associative algebra over a field, with unit and R be an invertible element of $\mathcal{A} \otimes \mathcal{A}$. For $i, j \in \{1, 2, 3\}$ fix algebra homomorphisms $\psi_{i,j} : \mathcal{A} \otimes \mathcal{A} \longrightarrow \mathcal{A} \otimes \mathcal{A} \otimes \mathcal{A}$. Then *Yang-Baxter equation* for R is given by

$$R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12},$$

where $R_{ij} = \psi_{i,j}(R)$. A *set theoretic solution* to the Yang-Baxter equation is a pair (X, r), where

$$r : X \times X \longrightarrow X \times X \text{ given by } (x, y) \mapsto (\tau_x(y), \sigma_y(x))$$

is a bijection, satisfying

$$(r \times Id)(Id \times r)(r \times Id) = (Id \times r)(r \times Id)(Id \times r).$$

A solution is said to be *involutive* if r^2 is the identity map. Drinfield proposed to study the set-theoretic solutions to the Yang-Baxter equation, in an attempt to classify all the solutions to the Yang-Baxter equation. Note that if (X, r) is a set-theoretic solution to the Yang-Baxter equation, then it naturally induces a map from $V^{\otimes 2}$ to itself, where V is the vector space with basis X. Initially, this was studied by adjoining two groups, namely the structure group and the permutation group of a solution. Later these two were put together by Rump [Ru07] in a more natural setting, known as left brace.

6.1 Skew brace

A *left brace* is an algebraic structure $(B, +, \times)$ such that $(B, +)$ is an abelian group and $(B, \times)$ is a group, satisfying the left brace property

$$a \times (b + c) = a \times b - a + a \times c,$$

for all $a, b, c \in B$. A solution of Yang Baxter equation also gives some invariants of links. But if the solution is involutive, it gives a trivial invariant. Thus finding non-involutive solutions are of much importance. To study the non-involutive solutions of the Yang-Baxter equation, a parallel theory of left braces was proposed later. This was further generalized to define a new structure called the left skew brace. A *left skew brace* is an algebraic object $(B, \cdot, \circ)$ such that both $(B, \circ), (B, \cdot)$ are groups satisfying

$$a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c),$$

for all $a, b, c \in B$ where a^{-1} denotes the group theoretic inverse of a in the group $(B, \cdot)$.

Example 6.1.1. 1. Let $(G, +)$ be a group. If we take $\cdot = +$, then $(G, +, +)$ is a skew brace.

2. Let $(G, \cdot)$ be a group. Taking $a \circ b = b \cdot a$, we have for all $a, b, c \in G$

$$\begin{aligned} a \circ b \cdot (a^{-1}) \cdot a \circ c &= b \cdot a \cdot a^{-1} \cdot c \cdot a \\ &= b \cdot c \cdot a \\ &= a \circ (b \cdot c). \end{aligned}$$

Hence $(G, \cdot, \circ)$ is a skew brace.

3. [GuVe17, Example 1.5] Let M and N be two groups and $\beta : M \longrightarrow \mathrm{Aut}(N)$ be a group homomorphism $m \mapsto \beta_m$. Take $B = M \times N$ with

$$(m, n) \cdot (m', n') = (mm', nn'), (m, n) \circ (m', n') = (mm', n\beta_m(n')).$$

Then note that

$$(m, n) \circ ((m'm'', n'n'')) = (mm'm'', n\beta_m(n'n'')),$$

and

$$\begin{aligned}
&((m,n)\circ(m',n'))(m^{-1},n^{-1})((m,n)\circ(m'',n''))\\
=&(mm',n\beta_m(n'))(m^{-1},n^{-1})(mm'',\beta_m(n''))\\
=&(mm'm'',n\beta_m(n')n^{-1}\beta_m(n''))\\
=&(mm'm'',n\beta_m(n'n'')),
\end{aligned}$$

which shows that $(M \times N, \cdot, \circ)$ is a skew brace.

4. [SmVe18, Lemma 2.12, Example 2.13] Let A be a group and $\lambda : A \longrightarrow \mathrm{Aut}(A)$ be a map such that $\lambda_{a\lambda_a(b)} = \lambda_a\lambda_b$ for all $a, b \in A$. Then $a\circ b = a\lambda_a(b)$ provides a skew brace. Setting $G = S_3$ and $\lambda : G \longrightarrow S_G$ given by

$$\begin{aligned}
\lambda_{id} = \lambda_{(123)} = \lambda_{(132)} = id\\
\lambda_{(12)} = \lambda_{(23)} = \lambda_{(13)} = c_{(23)},
\end{aligned}$$

we get a skew brace of order 6.

Let $(B, \cdot, \circ)$ be a skew brace. Then it can be shown that the identity of both groups $(B, \circ)$ and $(B, \cdot)$ are same [SmVe18, Remark 2.4]. Also the following holds [SmVe18, Lemma 2.14]:

$$\begin{aligned}
a\circ(b^{-1}c) = a(a\circ b)^{-1}(a\circ c)\\
a\circ(bc^{-1}) = (a\circ b)(a\circ c)^{-1}a,
\end{aligned}$$

for all $a, b, c \in B$. For each $b \in B$ define the map

$$\beta_b : B \longrightarrow B,\ a \mapsto b^{-1}(b\circ a).$$

Then this map is bijective. We have the following.

Theorem 6.1.2. *[GuVe17, Proposition 1.9] Let G be a set such that $(G, \cdot)$ and $(G, \circ)$ are two groups. Assume the existence of a map $\lambda : G \longrightarrow S_G$ satisfying $\lambda_g(h) = g^{-1}\cdot(g\circ h)$ for all $g, h \in G$. Then the following statements are equivalent:*

1. *G is a skew brace.*

2. *$\lambda_{g\circ h}(a) = \lambda_g\lambda_h(a)$ for all $g, h, a \in G$.*

3. *$\lambda_g(hh') = \lambda_g(h)\lambda_g(h')$ for all $g, h, h' \in G$.*

Corollary 6.1.3. *[GuVe17, Corollary 1.10] Let* $(G, \cdot, \circ)$ *be a skew left brace. Then the map given by*

$$\begin{aligned} \lambda : (G, \circ) &\longrightarrow \mathrm{Aut}(G, \cdot) \\ g \mapsto \lambda_a, \lambda_a(b) &= a^{-1}(a \circ b), \end{aligned}$$

is a group homomorphism.

Suppose A, G are two groups and A is a left G-space by automorphisms. A *bijective* 1 *cocycle* is a bijective map $\pi : G \longrightarrow A$ satisfying

$$\pi(gh) = \pi(g)(g\pi(h)),$$

for all $g, h \in G$. Then we have the following

Proposition 6.1.4. *[GuVe17, Proposition 1.11] Over a group* $(A, \cdot)$ *the following are equivalent:*

1. *A group* G *and a bijective* 1 *cocycle from* G *to* A

2. *A skew left brace structure over* A.

Example 6.1.5. Let

$$\begin{aligned} D &= \langle r, s : r^4 = s^2 = srsr = 1 \rangle \\ Q &= \{\pm 1, \pm i, \pm j, \pm k\} \end{aligned}$$

be the dihedral and quaternion groups respectively of order 8. Define the following map $\pi : Q \longrightarrow D$

$$\begin{gathered} 1 \mapsto 1, -1 \mapsto r^2, -k \mapsto r^3 s, k \mapsto rs, \\ i \mapsto s, -i \mapsto r^2 s, j \mapsto r^3, -j \mapsto r. \end{gathered}$$

Then it can be easily seen that π is a bijective 1-cocycle.

6.2 Solution to Yang-Baxter equation

Given a skew brace $(B, \circ, \cdot)$, let us denote the inverse of b in $(B, \circ)$ by $\overline{b}$. Then we have the map $\lambda_a : B \longrightarrow B$ from Theorem 6.1.2. Define another map for $b \in B$, to be denoted as $\tau_b : B \longrightarrow B$ given by

$$\tau_b(a) = \overline{\lambda_a(b)} \circ a \circ b.$$

Then it can be easily seen that τ_b is a bijection for all $b \in B$. We have the following theorem

Theorem 6.2.1. *[SmVe18, Theorem 4.1] Let B be a skew left brace and $r : B \times B \longrightarrow B \times B$ be given by*

$$r(a, b) = (\lambda_a(b), \tau_b(a)),$$

for all $a, b \in B$. Then (B, r) is a solution to the Yang-Baxter equation.

An another way of producing solution to the Yang-Baxter equation is given by the following theorem.

Theorem 6.2.2. *[GuVe17, Proposition 1.9] Let A be a skew left brace. Define*

$$r : A \times A \longrightarrow A \times A, \quad r(a, b) = (\lambda_a(b), \lambda^{-1}_{\lambda_a(b)}((a \circ b)^{-1}a(a \circ b))),$$

for all $a, b \in A$. Then (A, r) is a non-degenerate solution of the Yang-Baxter equation. Furthermore, r is an involutive solution if and only if $(A, \cdot)$ is an abelian group.

Example 6.2.3. Consider a non-abelian group G and consider the skew left brace $(G, \cdot, \cdot)$. Then from the previous theorem a set theoretic solution to the Yang-Baxter equation is given by (G, r) with

$$r : G \times G \longrightarrow G \times G, \quad r(a, b) = (b, b^{-1}ab).$$

Chapter 7

Connection with Hopf-Galois structure

Let $\mathcal{R}$ be a commutative ring with unity and let $\mathcal{H}$ be an $\mathcal{R}$-bialgebra. Then $\mathcal{H}$ will be called an *$\mathcal{R}$-Hopf algebra* if there is an $\mathcal{R}$-module homomorphism $\lambda : \mathcal{H} \to \mathcal{H}$ (the antipode map), which is both an $\mathcal{R}$-algebra and an $\mathcal{R}$-coalgebra antihomomophism such that:

$$\lambda(h \otimes h') = \lambda(h) \otimes \lambda(h'),$$
$$\Delta\lambda(h) = (\lambda \otimes \lambda)\tau\Delta,$$
$$\mu(1 \otimes \lambda)\Delta = i\epsilon = \mu(\lambda \otimes 1)\Delta,$$

where Δ is the comultiplication map, τ is the switch map $\tau(h_1 \otimes h_2) = h_2 \otimes h_1$, $i : \mathcal{R} \hookrightarrow \mathcal{H}$ is the unit map and $\epsilon : \mathcal{H} \to \mathcal{R}$ is the counit map. Now assume that $\mathcal{H}$ is commutative. An $\mathcal{R}$-Hopf algebra $\mathcal{H}$ is called a *finite algebra* if it is finitely generated and a projective $\mathcal{R}$-module. Now if $\mathcal{S}$ is an $\mathcal{R}$-algebra which is an $\mathcal{H}$-module, then $\mathcal{S}$ is called an *$\mathcal{H}$-module algebra* if

$$h(st) = \sum h_{(1)}(s)h_{(2)}(t) \text{ and } h(1) = \epsilon(h)1$$

for all $h \in \mathcal{H}, s, t \in \mathcal{S}$, where $\Delta(h) = \sum\limits_{(h)} h_{(1)} \otimes h_{(2)} \in \mathcal{H} \otimes \mathcal{H}$ according to Sweedler's [Sw68] notation and $\epsilon : \mathcal{H} \to \mathcal{R}$ is the co-unit map.

Then $\mathcal{S}$, a finite commutative $\mathcal{R}$-algebra is called an *$\mathcal{H}$-Galois extension* over $\mathcal{R}$ if $\mathcal{S}$ is a left $\mathcal{H}$-module algebra and the $\mathcal{R}$-module homomorphism

$$j : \mathcal{S} \otimes_{\mathcal{R}} \mathcal{H} \to \mathrm{End}_{\mathcal{R}}(\mathcal{S}),$$

given by $j(s \otimes h)(s') = sh(s')$ for $s, s' \in \mathcal{S}, h \in \mathcal{H}$, is an isomorphism. Now we define a Hopf-Galois structure on a Galois field extension. Assume that K/F is a finite Galois field extension. An F-Hopf algebra $\mathcal{H}$, with an action on K such that K is an $\mathcal{H}$-module algebra and the action makes K into an $\mathcal{H}$-Galois extension, will be called a *Hopf-Galois structure* on K/F.

7.1 Greither-Pareigis theory and Byott's translation

Given a group G we define the *holomorph* of G as a semidirect product $G \rtimes_\psi \operatorname{Aut}(G)$, where ψ is the identity map. The holomorph of a group G (denoted by $\operatorname{Hol}(G)$) sits inside $\operatorname{Perm}(G)$ (set of permutations on G) as follows

$$\operatorname{Hol}(G) = \{\eta \in \operatorname{Perm}(G) : \eta \text{ normalizes } \lambda(G)\}$$

where λ is the left regular representation. We also recall that a subgroup $\Lambda \subseteq \operatorname{Perm}(\Omega)$ is called regular if $|\Lambda| = |\Omega|$ and Λ acts freely on Ω. The following result is due to Greither and Pareigis.

Proposition 7.1.1. *[Ch00, Theorem 6.8] Let K/F be a Galois extension of fields and $\Gamma = \operatorname{Gal}(K/F)$. Then there is a bijection between Hopf-Galois structures on K/F and regular subgroups G of $\operatorname{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$ where λ is the left regular representation.*

In the proof of the above proposition, given a regular subgroup $G \leq \operatorname{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$, the Hopf-Galois structure on K/F corresponding to G is $K[G]^\Gamma$. Here Γ acts on G by conjugation inside $\operatorname{Perm}(\Gamma)$ and it acts on K by field automorphism, which induces an action of Γ on $K[G]$. This G is called the *type* of the Hopf-Galois extension. Although Greither-Pareigis theory simplifies the problem of counting the number of Hopf-Galois structure for a given Galois extension, the size of $\operatorname{Perm}(\Gamma)$ is large ($|\Gamma|!$) in general. The next theorem (also known as *Byott's translation*) further simplifies the problem by considering regular embeddings in $\operatorname{Hol}(G)$, which is comparatively smaller in size. From the proof of [By96, Proposition 1] we have the following:

Let Γ be a finite group and G be a group of order $|\Gamma|$. Then there is a bijection between the following sets:

1. $\{\alpha : G \to \mathrm{Perm}(\Gamma)$ a monomorphism, $\alpha(G)$ is regular$\}$
2. $\{\beta : \Gamma \to \mathrm{Perm}(G)$ a monomorphism $\}$.

Let $e(\Gamma, G)$ be the number of regular subgroups in $\mathrm{Perm}(\Gamma)$ isomorphic to G which is normalized by $\lambda(\Gamma)$ i.e. the number of Hopf-Galois structures on K/F of type G. Let $e'(\Gamma, G)$ denote the number of subgroups Γ^* of $\mathrm{Hol}(G)$ isomorphic to Γ, such that the stabilizer in Γ^* of 1_G is trivial. Then we have the following result.

Theorem 7.1.2. *[By96, Proposition 1] With the notations as above we have,*

$$e(\Gamma, G) = \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|} e'(\Gamma, G).$$

The proof of this theorem explains the relationship between skew braces and Hopf-Galois structures. We will briefly mention it here.

Let G and N be two groups of same order. Take $\lambda_G : G \longrightarrow S_G$ be the left regular representation. Call an embedding of N in S_G to be *regular* if $\alpha : N \longrightarrow S_G$ is injective and $\alpha(N)$ is a regular subgroup of S_G. Then a regular embedding produces a bijection

$$\alpha_* : N \longrightarrow G, \quad n \mapsto \alpha(n) \cdot 1_G.$$

Then the map $\beta : G \longrightarrow S_N$ given by $\beta(g) = \alpha_*^{-1} \lambda_G(g) \alpha_*$ is a regular embedding. Thus we have a bijection between the sets:

$$\mathcal{N} = \{\text{regular embeddings } \alpha : N \longrightarrow S_G\},$$
$$\mathcal{G} = \{\text{regular embeddings } \beta : G \longrightarrow S_N\}.$$

By Childs' work [Ch00, pp. 48], this restricts to a bijection among the following two sets:

$$\mathcal{N}_0 = \{\alpha \in \mathcal{N} : \alpha(N) \text{ is normalized by } G\},$$
$$\mathcal{G}_0 = \{\beta \in \mathcal{G} : \beta(G) \subseteq \mathrm{Hol}(N)\}.$$

The action of $\mathrm{Aut}(N)$ on $\mathcal{N}_0$ translates to action on $\mathcal{G}_0$, by conjugation inside S_N. Two elements of $\mathcal{G}_0$ correspond to the same regular subgroup if and only if they are in the same orbit under the aforementioned action. Thus the Hopf-Galois structure with pair of groups (G, N) on K/F correspond bijectively to the $\mathrm{Aut}(N)$-conjugacy classes of $\mathcal{G}_0$. We now state the following result

Theorem 7.1.3. *[SmVe18, Proposition A.3] Let B be a group. Then there is a bijective correspondence between the classes of regular subgroups of* $\mathrm{Hol}(B)$ *of same order under* $\mathrm{Aut}(B)$*-conjugation and the isomorphism classes of skew braces with additive group B.*

Thus we have that for a pair of group (G, N), there exists a Hopf-Galois structure with Galois group G and type N, if and only if there is a skew brace with N additive group and G being multiplicative group. In such a case we say that the pair of group (G, N) is *realizable*.

Example 7.1.4.

1. [SmVe18, Example A.7] Let $G = C_{p^2}$ the cyclic group of order p^2. In this case it has been proved that if N is of order p^n and $\mathrm{Hol}(N)$ has an element of order p^n, then N is cyclic. Using this we have that every Hopf-Galois structure has cyclic type. Hence for skew brace with multiplicative group C_{p^2}, the additive group is also C_{p^2}. Note that the result holds for any odd prime p and $n \in \mathbb{N}$.

2. It has been proved that if G is a quasisimple group and (G, N) is realizable then $N \cong G$ [Ts19, Theorem 1.3]. Thus we have that if a skew brace has simple group as the multiplicative group, then the additive group should be isomorphic to the group and hence simple group.

7.2 Bijective crossed homomorphism

Let G, N be two groups of same size. Given $\mathfrak{f} \in \mathrm{Hom}(G, \mathrm{Aut}(N))$, a map $\mathfrak{g} \in \mathrm{Map}(G, N)$ will be called a *crossed homomorphism with respect to* $\mathfrak{f}$, if it satisfies

$$\mathfrak{g}(gh) = \mathfrak{g}(g) \cdot \mathfrak{f}(g)(\mathfrak{g}(h)), \quad \text{for all } g, h \in G.$$

We denote by $Z^1_{\mathfrak{f}}(G, N)$, the set of all such bijective maps. Then we have the following result.

Proposition 7.2.1. *[Ts19, Proposition 2.1] For* $\mathfrak{f} \in \mathrm{Map}(G, \mathrm{Aut}(N))$ *and* $\mathfrak{g} \in \mathrm{Map}(G, N)$*, define*

$$\beta_{(\mathfrak{f},\mathfrak{g})} : G \longrightarrow \mathrm{Hol}(N) \ \text{by}\ g \mapsto (\rho(\mathfrak{g}(g)), \mathfrak{f}(g)).$$

Then we have that the regular subgroups of $\mathrm{Hol}(N)$ *isomorphic to* G *are given by the set*

$$\{\beta_{\mathfrak{f},\mathfrak{g}} : \mathfrak{f} \in \mathrm{Hom}(G, \mathrm{Aut}(N)), \mathfrak{g} \in Z^1_{\mathfrak{f}}(G, N)\}.$$

Furthermore, each Hopf-Galois structure arises this way,

Example 7.2.2. 1. Let $\mathfrak{f}_0 \in \mathrm{Hom}(G, \mathrm{Aut}(N))$ be the trivial homomorphism. Then any $\mathfrak{g} \in Z^1_{\mathfrak{f}}(G, N)$ satisfies $\mathfrak{g}(ab) = \mathfrak{g}(a)\mathfrak{g}(b)$. This implies that $\mathfrak{g}$ is a group homomorphism. Since $\mathfrak{g}$ is a bijection , we conclude that

$$Z^1_{\mathfrak{f}}(G, N) = \begin{cases} \emptyset & \text{when } G \ncong N \\ \mathrm{Aut}(G) & \text{otherwise} \end{cases}.$$

Hence we get that (G, G) is realizable.

2. Let $\mathfrak{f} \in \mathrm{Hom}(G, \mathrm{Aut}(N))$. Given any $n \in N$, consider the principal crossed homomorphism

$$\mathfrak{g}_n(a) = n^{-1} \cdot \mathfrak{f}(a)(n).$$

Then $\mathfrak{g}_n$ is injective if and only if $\mathrm{Stab}(n) = 1_G$.

We close this chapter by mentioning the following result.

Proposition 7.2.3. *[Ts22, Proposition 2.2] Let* G, N *be two groups such that* $|G| = |N|$. *Let* $\mathfrak{f} \in \mathrm{Hom}(G, \mathrm{Aut}(N))$ *and* $\mathfrak{g} \in Z^1_{\mathfrak{f}}$ *be a bijective crossed homomorphism (i.e.* (G, N) *is realizable). Then if* M *is a characteristic subgroup of* N *and* $H = \mathfrak{g}^{-1}(M)$*, we have that the pair* (H, M) *is realizable.*

Chapter 8

Realizability of $\mathbb{Z}_n \rtimes \mathbb{Z}_2$

We start with an elementary observation.

Proposition 8.0.1. *Let G be a group of order $2n$ such that n is odd. Then G has a unique subgroup of order n.*

Proof. Let $g \in G$ be an element of order 2 (this exists by Cauchy's theorem). Consider the following compositions of the maps:

$$G \xrightarrow{\lambda} \mathrm{Perm}(G) \xrightarrow{\mathrm{sgn}} \{\pm 1\},$$

where λ represents the left regular representation and sgn is the sign representation of symmetric group. Note that $\lambda(g) = (a_1, ga_1)(a_2, ga_2)\dots(a_n, ga_n)$ for $a_1, a_2, \dots, a_n \in G$ such that $g^k a_l \neq a_m$ for all k, l, m. Since n is odd, we have that $\mathrm{sgn}(\lambda(g)) = -1$ and hence $\mathrm{sgn} \circ \lambda$ is surjective. Thus $H = \ker(\mathrm{sgn} \circ \lambda)$ is a subgroup of order n.

To prove that H is unique subgroup of order n, on the contrary assume that there is another subgroup $H' \neq H$ of order n. Then consider the following group homomorphism

$$\varphi : G \longrightarrow (G/H) \oplus (G/H') \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Since $H \neq H'$, we have that G surjects into $\mathbb{Z}_2 \times \mathbb{Z}_2$. Then 4 divides the order of the group, which is a contradiction. □

Corollary 8.0.2. *Let G be a group of order $2^k n$ such that $2 \not| n$. If the Sylow-2-subgroup of G is cyclic then G has subgroups of order $2^l n$ for all $0 \leq l \leq k$.*

Proof. Follows by induction, Proposition 8.0.1 and observing that a subgroup of a cyclic group is cyclic. □

Definition 8.0.3. A finite group G is called a $C-group$ if all the Sylow subgroups are cyclic. A group G is called *almost Sylow-cyclic* if its Sylow subgroups of odd order are cyclic, while either the Sylow-2-subgroup is trivial or they contain a cyclic subgroup of index 2.

We have the following theorem from Burnside's work [But55].

Proposition 8.0.4. *[But55] Let G be a finite group. Then all the Sylow subgroups are cyclic if and only if G is a semidirect product of two cyclic groups of coprime order.*

In recent work realizability of Cyclic groups has been characterized by the following two results. We mention them here as this will be the key ingredient to classify the same in case of groups of the form $\mathbb{Z}_n \rtimes \mathbb{Z}_2$.

Proposition 8.0.5. *[Ts22, Theorem 3.1] Let N be a group of odd order n such that the pair $(\mathbb{Z}_n, N)$ is realizable. Then N is a C-group.*

Proposition 8.0.6. *[Ru19, Theorem 1] Let G be a group of order n such that $(G, \mathbb{Z}_n)$ is realizable. Then G is solvable and almost Sylow-cyclic.*

8.1 On $\mathbb{Z}_n \rtimes \mathbb{Z}_2$ skew braces

Proposition 8.1.1. *Let $N = \mathrm{D}_{2n}$ and (G, N) is realizable. Then G is solvable.*

Proof. The non-trivial proper characteristic subgroups of $\mathrm{D}_{2n} = \langle r, s : r^n = s^2 = srsr = 1\rangle$ are given by

$$\langle r^d\rangle, \text{ where } d|n.$$

Then for all $\alpha|n$ the group G has a subgroup of order α, say H_α such that $(H_\alpha, \langle r^{\frac{n}{\alpha}}\rangle)$ is realizable. Since G has order $2n$ and H_n is a subgroup of index 2, then H_n is a normal subgroup of G. Let $n = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$. Now consider the series

$$G \geq H_n \geq H_{n/p_1} \geq H_{n/p_1^2} \geq \dots \geq H_{n/p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k - 1}} \geq 1.$$

Then each of $H_\alpha/H_{\alpha/p_j}$ is cyclic, hence abelian. □

Theorem 8.1.2. *Let N be a group of order $2n$, where n is odd and the pair $(\mathbb{Z}_n \rtimes \mathbb{Z}_2, N)$ is realizable. Then $N \cong (\mathbb{Z}_k \rtimes \mathbb{Z}_l) \rtimes \mathbb{Z}_2$ where $(k,l)=1$ and $lk=n$.*

Proof. By Proposition 8.0.1, N has a unique and hence characteristic subgroup H_n of order n. Then by Proposition 7.2.1 there exists a bijective crossed homomorphism $\mathfrak{g} \in Z^1_{\mathfrak{f}}(\mathbb{Z}_n \rtimes \mathbb{Z}_2, N)$ for some $\mathfrak{f} \in \operatorname{Hom}(\mathbb{Z}_n \rtimes \mathbb{Z}_2, \operatorname{Aut}(N))$. Hence, by Theorem 7.2.3 the pair $(\mathfrak{g}^{-1}H_n, H_n)$ is realizable. Note that $\mathbb{Z}_n \rtimes \mathbb{Z}_2$ has unique subgroup of order n, which is cyclic. It follows that $\mathfrak{g}^{-1}H_n = \mathbb{Z}_n$. This implies that $(\mathbb{Z}_n, H_n)$ is realizable. Hence by Proposition 8.0.5 we get that H_n is a C-group, whence it follows from [But55] that $H_n = \mathbb{Z}_k \rtimes \mathbb{Z}_l$ for $(k,l)=1, kl=n$. □

Theorem 8.1.3. *Let G be a group of order $2n$ such that the pair $(G, \mathbb{Z}_n \rtimes \mathbb{Z}_2)$ is realizable. Then $G = (\mathbb{Z}_k \rtimes \mathbb{Z}_l) \rtimes \mathbb{Z}_2$ for some $(k,l)=1, kl=n$.*

Proof. Given that the pair $(G, \mathbb{Z}_n \rtimes \mathbb{Z}_2)$ is realizable, by Proposition 7.2.1 there exists a bijective crossed homomorphism $\mathfrak{g} \in Z^1_{\mathfrak{f}}(G, \mathbb{Z}_n \rtimes \mathbb{Z}_2)$ for some $\mathfrak{f} \in \operatorname{Hom}(G, \operatorname{Aut}(\mathbb{Z}_n \rtimes \mathbb{Z}_2))$. Since $\mathbb{Z}_n$ is a characteristic subgroups of $\mathbb{Z}_n \rtimes \mathbb{Z}_2$, we get that $\mathfrak{g}^{-1}(\mathbb{Z}_n)$ is a subgroup of G and $(\mathfrak{g}^{-1}(\mathbb{Z}_n), \mathbb{Z}_n)$ is realizable. Then by Proposition 8.0.6, we have that $\mathfrak{g}^{-1}(\mathbb{Z}_n)$ is almost Sylow-cylic. Hence by [But55] $\mathfrak{g}^{-1}(\mathbb{Z}_n) = \mathbb{Z}_k \rtimes \mathbb{Z}_l$. Hence the result follows. □

Corollary 8.1.4. *Let n be an odd number such that* $\operatorname{Ra}(n)$ *is a Burnside number. Assume that $|G| = |N| = 2n$ and (G,N) is realizable. Then $G = \mathbb{Z}_n \rtimes_{\varphi} \mathbb{Z}_2$ if and only if $N = \mathbb{Z}_n \rtimes_{\psi} \mathbb{Z}_2$, where $\varphi, \psi : \mathbb{Z}_2 \longrightarrow \operatorname{Aut}(\mathbb{Z}_n)$ are group homomorphisms.*

Proof. Let $r_1, r_2 \in \mathbb{N}$ be two numbers such that $(r_1, r_2) = 1$ and $\operatorname{Ra}(r_1 r_2)$ is a Burnside number. Then $(r_1, \phi(r_2)) = 1$ (by definition), where ϕ is the Euler's totient function. Take $i \neq j$ and $i,j \in \{1,2\}$. Then the group homomorphism

$$\psi : \mathbb{Z}_{r_i} \to \operatorname{Aut}(\mathbb{Z}_{r_j})$$

is trivial, which shows that $\mathbb{Z}_{r_i} \rtimes \mathbb{Z}_{r_j} = \mathbb{Z}_{r_i} \oplus \mathbb{Z}_{r_j} = \mathbb{Z}_{r_1 r_2}$. Hence the result follows from previous two Theorems. □

Remark 8.1.5. It was shown in [ArPa22a, Theorem 1.3], that if $G = \mathrm{D}_{2n}$ then for any $\phi \in \operatorname{Hom}(\mathbb{Z}_2, \operatorname{Aut}(\mathbb{Z}_n))$ the pair $(\mathrm{D}_{2n}, \mathbb{Z}_n \rtimes_{\phi} \mathbb{Z}_2)$ is realizable. This along with the previous theorem implies that when $\operatorname{Ra}(n)$ is a Burnside number (recall that $m \in \mathbb{N}$ is called a Burnside number if $(m, \varphi(m)) = 1$ where φ is the Euler's totient function), these are all possible realizable pairs.

Corollary 8.1.6. *Let L/K be a finite Galois extension with Galois group isomorphic to D_{2n} where n is odd such that $\mathrm{Ra}(n)$ is a Burnside number. Then the number of Hopf-Galois structures on L/K is*

$$e(\mathrm{D}_{2n}) = \sum_{m=0}^{n} 2^m \chi(n-m),$$

where $\chi(w)$ is the coefficient of x^w in the polynomial $\prod\limits_{p_u \in \pi(n)} (x + p_u^{\alpha_u})$.

Proof. This follows from Theorem 8.1.4 and [ArPa22a, Corollary 4.1]. Then the result follows from Theorem 8.1.4 and Remark 8.1.5. □

Theorem 8.1.7. *Let $n \in \mathbb{N}$ such that $n \equiv 2 \pmod 4$. Suppose (G, D_{2n}) is realizable. Then there exists a short exact sequence*

$$0 \longrightarrow \mathbb{Z}_l \rtimes \mathbb{Z}_k \longrightarrow G \longrightarrow \mathbb{Z}_2 \longrightarrow 0,$$

for some $(k, l) = 1, kl = 2n$.

Proof. Given that the pair (G, D_{2n}) is realizable, we get that there exists $\mathfrak{f} \in \mathrm{Hom}(G, \mathrm{Aut}(\mathrm{D}_{2n}))$ and $\mathfrak{g} \in Z^1_{\mathfrak{f}}(G, \mathrm{D}_{2n})$ corresponding to the regular embedding of G in $\mathrm{Hol}(\mathrm{D}_{2n})$. Take $M = \langle r \rangle \subseteq \mathrm{D}_{2n}$, which is a characteristic subgroup of D_{2n}. Then the pair $(\mathfrak{g}^{-1}M, \mathbb{Z}_n)$ is realizable. Hence we have that $\mathfrak{g}^{-1}M \cong \mathbb{Z}_l \rtimes \mathbb{Z}_k$ for some $(k, l) = 1, kl = 2n$. Since $\mathfrak{g}^{-1}M$ is a subgroup of index 2, the result follows. □

Chapter 9

Further plans

In this part, we have mentioned results on skew braces such that one of the additive or the circle group is isomorphic to $\mathbb{Z}_n \rtimes \mathbb{Z}_2$ for the case of n being odd. In the future we would like to extend our work for the other case, i.e. n being even. We will be hoping to solve a more intricate question which is as follows.

Question 7. *Let $G = \mathbb{Z}_n \rtimes \mathbb{Z}_p$ where p is a prime. Classify all the groups H of order np such that (G, H) is realizable or (H, G) is realizable.*

Index

Bibliography

[ArPa22a] Arvind, N.; Panja, S. *'On $\mathbb{Z}_n \rtimes \mathbb{Z}_2$-Hopf-Galois structures'*, Journal of Algebra,Volume 596,2022, Pages 37-52.,

[ArPa22b] Arvind, N.; Panja, S. *'Hopf-Galois Realizability of $\mathbb{Z}_n \rtimes \mathbb{Z}_2$'*, https://arxiv.org/abs/2201.10862, To appear in Journal of Pure and Applied Algebra

[By04] Byott, N. P. *'Hopf-Galois structures on field extensions with simple Galois groups.'* Bull. London Math. Soc. 36 (2004), no. 1, 23-29.

[Bl74] Blum, J. *'Enumeration of the square permutations in S_n.'*, Journal of Combinatorial Theory, Series A 17, no. 2 (1974): 156-161.

[Bo83] Borel, A. *'On free subgroups of semisimple groups.'* Enseign. Math. (2), 29(1-2):151164, 1983.

[BoGl80] Bolker, Ethan D.; Gleason, Andrew M. *'Counting permutations.'*, Journal of Combinatorial Theory, Series A 29.2 (1980): 236-242.

[BoAnDe00] Bona, M.; Andrew M.; Dennis W.,*Permutations with roots'*, Random Structures & Algorithms 17, no. 2 (2000): 157-167

[Ba71] Baxter, R. J. *'Eight-vertex model in lattice statistics'*, Phys. Rev. Lett. 26(1971), 832833.

[By96] Byott, N. P. *'Uniqueness of Hopf Galois structure of separable field extensions'*, Comm. Algebra 24 (1996), 3217-3228.

[BaCeJe16] Bachiller D., Ced F., Jespers E. *'Solutions of the Yang-Baxter equation associated with a left brace'*, J. Algebra 463 (2016), 80-102.

[BaFeJe16] Bachiller, D.;Ferran, C.; Jespers, E, *'Solutions of the Yang-Baxter equation associated with a left brace.'* J. Algebra, 463:80102,2016.

[Be+Go89] Bertram, Edward A.; Gordon, B.*'Counting special permutations'*, European Journal of Combinatorics 10.3 (1989): 221-226.

[BuGi16] Burness, T., Giudici, M. (2016). *'Classical Groups, Derangements and Primes'* (Australian Mathematical Society Lecture Series). Cambridge: Cambridge University Press. doi:10.1017/CBO9781139059060

[Bu1905] Burnside, W.*'On finite groups in which all the Sylow subgroups are cylical'*, Messenger Math. 35 (1905), 46-50.

[But55] Butler, M. C. R.,*'The irreducible factors of $f(x^m)$ over a finite field'*, J. London Math. Soc. 30 (1955), 480-482

[Ch19] Childs, L. N. *'Bi-skew braces and Hopf Galois structures'.* New York J. Math. 25 (2019), 574-588.

[Ca85] Carter, R. W.; *'Simple groups of Lie type.'* Reprint of the 1972 original. Wiley Classics Library. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989. x+335 pp. ISBN: 0-471-50683-4

[Ca72] Carter, R., *'Simple groups of lie type.'* John Wiley and Sons, 1972.

[CaCaDe20] Campedel, E.; Caranti, A.; Del Corso, I. *'Hopf-Galois structures on extensions of degree p^2q and skew braces of order p^2q: the cyclic Sylow p-subgroup case.'* J. Algebra 556 (020), 1165-1210.

[Ch00] Childs L. N.*'Taming wild extensions: Hopf algebras and local Galois module theory'*, Mathematical Surveys and Monographs, 80. American Mathematical Society, Providence, RI, 2000. viii+215 pp. ISBN: 0-8218-2131-8.

[CeJeOk14] Ced F., Jespers E., Okniski J.*'Braces and the Yang-Baxter equation'*, Comm. Math. Phys. 327 (2014), no. 1, 101-116.

[Wa91] Waring, E., *'Meditationes algebraicae.* Translated from the Latin, edited and with a foreword by Dennis Weeks. With an appendix by Franz X. Mayer, translated from the German by Weeks American Mathematical Society, Providence, RI, 1991. lx+459 pp. ISBN: 0-8218-0169-4

[Fu99] Fulman, J. (1999). *'Cycle indices for the finite classical groups'*, Journal of Group Theory, 2(3), 251-289.

[Fu97] Fulman, J. (1997). *"Probability in the Classical Groups over Finite Fields: Symmetric Functions, Stochastic Algorithms, and Cycle Indices"*, Ph.D. thesis

[FuNePr05] Fulman, J.; Neumann, P. M.; Praeger, C. E., *'A generating function approach to the enumeration of matrices in classical groups over finite fields'*, Mem. Amer. Math. Soc. 176 (2005), no. 830, vi+90 pp.

[GoLiBr] Samuel Gonshaw, Martin W. Liebeck and E.A. OBrien*' Unipotent class representatives for finite classical groups'*. J. Group Theory 20 (2017), no. 3, 505525.

[GrPa87] Greither C., Pareigis B.,*Hopf Galois theory for separable field extensions*, Journal of Algebra, Volume 106, Issue 1,1987,Pages 239-258.

[GuVe17] Guarnieri L.; Vendramin L. *'Skew braces and the Yang-Baxter equation.'* Math. Comp., 86(307):25192534, 2017.

[HoKu71] Hoffman, Kenneth; Kunze, Ray *'Linear algebra.'* Second edition Prentice-Hall, Inc., Englewood Cliffs, N.J. 1971 viii+407 pp.

[HuLaSh15] Hui, C. Y.; Larsen, M.; Shalev, A. *'The Waring problem for Lie groups and Chevalley groups.'* Israel J. Math. 210 (2015), no. 1, 81100.

[Hu72] Humphreys, James E. *'Introduction to Lie algebras and representation theory.'* Graduate Texts in Mathematics, Vol. 9. Springer-Verlag, New York-Berlin, 1972. xii+169 pp.

[Hu75] Humphreys, James E. *'Linear algebraic groups.'* Graduate Texts in Mathematics, No. 21. Springer-Verlag, New York-Heidelberg, 1975. xiv+247 pp.

[Ku81] Kung, J., *'The cycle structure of a linear transformation over a finite field'*, Linear Algebra Appl. 36 (1981), 141-155.

[KuKuSi21] Kulshrestha, Amit, Kundu, Rijubrata and Singh, Anupam. *'Asymptotics of the powers in finite reductive groups'*Journal of Group Theory, vol. , no. , 2021, pp.00001015152020020

[KuMo22] Kundu, Rijubrata; Mondal, Sudipa *'Powers in the wreath product of G with Sn'*,arXiv:2010.04954, To appear in Journal of group theory

[KuSi22] Kundu R., Singh A. *'Generating functions for the powers in $GL(n;q)$'* arXiv preprint arXiv:2003.14057, to appear in Israel Journal of Mathematics

[La02] Larry C. Grove (2002),*'Classical Groups and Geometric Algebra'* American Mathematical Society, pp 169 Series: Graduate Studies in Mathematics 39 ISBN: 978-0-8218-2019-3

[LiNi97] R. Lidl and H. Niederreiter, *'Finite Fields, Encyclopedia of Mathematics and its Applications 20*, 2nd Ed. Cambridge University Press, 1997.

[LiBrShTi10] Liebeck, Martin W.; O'Brien, E. A.; Shalev, Aner; Tiep, Pham Huu *'The Ore conjecture.'* J. Eur. Math. Soc. (JEMS) 12 (2010), no. 4, 9391008.

[LiBrShTi12] Liebeck, Martin W.; O'Brien, E. A.; Shalev, Aner; Tiep, Pham Huu *'Products of squares in finite simple groups.'* Proc. Amer. Math. Soc. 140 (2012), no. 1, 2133.

[LiShTi11] Larsen, Michael; Shalev, Aner; Tiep, Pham Huu *'The Waring problem for finite simple groups.'* Ann. of Math. (2) 174 (2011), no. 3, 18851950.

[LiShTi13] Larsen, Michael; Shalev, Aner; Tiep, Pham Huu *'Waring problem for finite quasisimple groups.'* Int. Math. Res. Not. IMRN 2013, no. 10, 23232348.

[LiShTi19] Larsen, Michael; Shalev, Aner; Tiep, Pham Huu *'Probabilistic Waring problems for finite simple groups.'* Ann. of Math. (2) 190 (2019), no. 2, 561608.

[MeGo90] Meyn, Helmut; Gotz, Werner *'Self-reciprocal polynomials over finite fields.'* Sminaire Lotharingien de Combinatoire (Oberfranken, 1990), 8290, Publ. Inst. Rech. Math. Av., 413, Univ. Louis Pasteur, Strasbourg, 1990.

[MeGo90] H. Meyn, W. Gtz*'Self-reciprocal Polynomials Over Finite Fields'*, vol. 413/S-21, Publ. I.R.M.A, Strasbourg, 1990, pp. 8290

[Mi69] Milnor, J. (1969). *'On Isometries of Inner Product Spaces'*, Inventiones Mathematicae 8 (1969): 83-97.

[NePr95] Neumann, Peter M.; Praeger, Cheryl E. *'Cyclic matrices over finite fields.'* J. London Math. Soc. (2) 52 (1995), no. 2, 263284.

[PaSi22] Panja S., Singh A. *'Powers in finite orthogonal and symplectic groups: A generating function approach'* arXiv preprint arXiv:2202.11513

[PoRe87] G. Polya and R. C. Read. *'Combinatorial enumeration of groups, graphs, and chemical compounds'* (Springer-Verlag, 1987)

[Ru07] Wolfgang Rump. *'Braces, radical rings, and the quantum Yang-Baxter equation.'* J. Algebra, 307(1):153170, 2007.

[Ru19] Rump, W. *'Classification of cyclic braces, II'.* Trans. Amer. Math. Soc. 372 (2019), no. 1, 305-328.

[St88] Stong, R., *'Some asymptotic results on finite vector spaces'*, Advances in Applied Mathematics 9, 167-199 (1988)

[Sh09] Shalev, Aner *'Word maps, conjugacy classes, and a noncommutative Waring-type theorem.'* Ann. of Math. (2) 170 (2009), no. 3, 13831416.

[Sh13] Aner Shalev, *'Some results and problems in the theory of word maps'*, Erds centennial, Bolyai Soc. Math. Stud., vol. 25, Jnos Bolyai Math.Soc., Budapest, 2013, pp. 611649.

[Sh80] K. Shinoda. *'The characters of Weil representations associated to finite fields'* J. Algebra, 66(1):251280, 1980

[Sp09] Springer, T. A. *'Linear algebraic groups.'* Reprint of the 1998 second edition. Modern Birkhuser Classics. Birkhuser Boston, Inc., Boston, MA, 2009. xvi+334 pp. ISBN: 978-0-8176-4839-8https://www.maths.usyd.edu.au/u/don/code/Magma/GOConjugacy.pdf

[Sw68] Sweedler, Moss E. *'The Hopf algebra of an algebra applied to field theory'.* J. Algebra 8 (1968), 262276.

[St68] R. Steinberg, *'Endomorphisms of Linear Algebraic Groups'.* Memoirs Amer. Math. Soc.,80(1968).

[SmVe18] Smoktunowicz, Agata; Vendramin, Leandro *'On skew braces (with an appendix by N. Byott and L. Vendramin)'*. J. Comb. Algebra 2 (2018), no. 1, 4786.

[SmVe18] Smoktunowicz A., Vendramin L.*'On skew braces (with an appendix by N. Byott and L. Vendramin)'*, J. Comb. Algebra 2 (2018), no. 1, 47-86.

[Ts19] Tsang, C. *'Non-existence of Hopf-Galois structures and bijective crossed homomorphisms.'* J. Pure Appl. Algebra 223 (2019), no. 7, 2804-2821.

[Ts21] Tsang, C. *'Hopf-Galois structures on finite extensions with quasisimple Galois group.'* Bull. Lond. Math. Soc. 53 (2021), no. 1, 148-160.

[Ts20] Tsang, C. ; Qin, C. *'On the solvability of regular subgroups in the holomorph of a finite solvable group'*, Internat. J. Algebra Comput. 30 (2020), no. 2, 253265.

[Ts20] Tsang, C. *'Hopf-Galois structures on finite extensions with almost simple Galois group'*, Journal of Number Theory, Volume 214, 2020, Pages 286-311,

[Cr21] Crespo, T. *'Hopf Galois structures on field extensions of degree twice an odd prime square and their associated skew left braces'*, Journal of Algebra, Volume 565,2021, Pages 282-308,

[Ta1] D. E. Taylor*'Conjugacy Classes in Finite Symplectic Groups'*, online notes, available at https://www.maths.usyd.edu.au/u/don/code/Magma/SpConjugacy.pdf

[Ta2] D. E. Taylor*'Conjugacy Classes in Finite Orthogonal Groups'*, online notes, available at https://www.maths.usyd.edu.au/u/don/code/Magma/GOConjugacy.pdf

[MaTe11] Malle, Gunter; Testerman, Donna *'Linear algebraic groups and finite groups of Lie type.'* Cambridge Studies in Advanced Mathematics, 133. Cambridge University Press, Cambridge, 2011. xiv+309 pp. ISBN: 978-1-107-00854-0

[Ts22] Tsang, C.*'Hopf-Galois structures on cyclic extensions and skew braces with cyclic multiplicative group'*, preprint (https://arxiv.org/abs/2112.08894)

[Wi17] de Graaf, Willem Adriaan *'Computation with linear algebraic groups.'* Monographs and Research Notes in Mathematics. CRC Press, Boca Raton, FL, 2017. xiv+327 pp. ISBN: 978-1-4987-2290-2

[Wa63] Wall, G. E.. *'On the conjugacy classes in the unitary, symplectic, and orthogonal groups'*, J. Austral. Math. Sot. 3 (1963), 1-62

[Ya67] C.N. Yang, *'Some exact results for the many-body problem in one dimension with repulsive delta-function interaction'*, Phys. Rev. Lett. 19 (1967), 13121315.

[Ze18] Zenouz N. K. *'On Hopf-Galois Structures and Skew Braces of Order p^3'*, Ph.D. thesis, The University of Exeter, UK, (2018).