GENERATION OF CERTAIN GROUPS BY THREE INVOLUTIONS, TWO OF WHICH COMMUTE.

by

MICHAEL BORIS Cherkassoff

M.Sc. (Mathematics) Moscow State University, 1988

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in

THE FACULTY OF GRADUATE STUDIES

Department of Mathematics

We accept this thesis as conforming to the required standard

THE UNIVERSITY OF BRITISH COLUMBIA

August 1998

© Michael Boris Cherkassoff, 1998
In presenting this thesis in partial fulfillment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the head of my department or by his or her representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Department of Mathematics
The University of British Columbia
Vancouver, Canada

Date Sept 30, 1998
Abstract

In this thesis the question of generating $PSL_n(q)$ with three involutions, two of which commute is completely settled. When such a generation is possible we explicitly supply the generators as well as all computations that would enable one to write any particular matrix in terms of these generators.

We also provide a complete classification (up to conjugacy) of embeddings of the Klein 4-group into $PSL_n(q)$ over finite fields of odd characteristic and explicitly list representatives of each embedding.
# Table of Contents

Abstract ........................................ ii

Table of Contents ................................ iii

List of Figures .................................. iv

Acknowledgements ................................ v

Chapter 1. Introduction. ......................... 1

Chapter 2. Preliminaries and Notation. ....... 5

Chapter 3. Embeddings of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ into $PSL_n(q)$ 10
  3.1 Statement of the Results .................. 10
  3.2 Enumeration of Classes of Involutions. ... 12
  3.3 Two Commuting Involutions ............... 14

Chapter 4. 3 by 3 matrices. ................... 20

Chapter 5. Positive answer for $n \geq 4$. .... 23
  5.1 Strategy .................................. 23
  5.2 Case of $4 \times 4$ matrices. .............. 26
  5.3 Case of $5 \times 5$ matrices. .............. 33
  5.4 Case of $(4k + 1) \times (4k + 1)$ matrices. ... 37
  5.5 Case of $(4k + 3) \times (4k + 3)$ matrices. ... 55
  5.6 Case of $4k \times 4k$ matrices. .......... 70
  5.7 Case of $(4k + 2) \times (4k + 2)$ matrices. ... 80

Bibliography .................................. 90

Appendix A. Maple V input for $4 \times 4$ case. 92

Appendix B. Maple V input for $5 \times 5$ case. 95

Appendix C. Maple V input for $(4k + 1) \times (4k + 1)$ case. 97

Appendix D. Maple V input for $(4k + 3) \times (4k + 3)$ case. 100

Appendix E. Maple V input for $4k \times 4k$ case. 103

Appendix F. Maple V input for $(4k + 2) \times (4k + 2)$ case. 106
List of Figures

5.1 First step of obtaining $U_{4k-2,2}(t), k > 2$. ................................................. 77
5.2 First step of obtaining second column. ................................................................. 78
5.3 Obtaining second column (whole block). ............................................................... 79
5.4 Obtaining transvections in $(4k+2) \times (4k+2)$ case. ............................................ 88
Acknowledgements

I would like to express my warmest gratitude to my supervisor Denis Sjerve for the all kinds of continued support he provided me throughout the years that it took to write this thesis. This piece of work would have not been possible if not for that support.

It would have been impossible for me to do this research without the assistance of a great program - GAP[15]. Although I use Maple V in demonstrations of the proofs, the real research has been done with GAP, and the answers were obtained first using it. My thanks to all people in Aachen and Saint Andrews who developed (and continue developing) it, but especially to Alexander Hulpke who provided me with some code to incorporate into my programs.

I would also like to thank Keith Orpen and Sandy Rutherford and many other people for assisting with TeX.
Chapter 1
Introduction.

The main task of this thesis is to completely answer, for the groups $PSL_n(q)$, the well known question first posed by V.D.Mazurov [10] (question 7.30): Which finite simple groups may be generated by three involutions, two of which commute?

This question has generated considerable interest and has been partially answered in many cases. For example, it has been answered by Ya.Nuzhin [11] for Chevalley groups over finite fields of characteristic 2. For odd characteristic the paper by M.C.Tamburini and P.Zucca [17] gives the (positive) answer for $PSL_n(q)$, $PSp_{2n}(q)$, $PSO_n(q)$, $PSU_n(q^2)$ provided the rank is sufficiently large. The paper by D.Sjerve and M.Cherkassoff [16] answers the question for $PSL_2(q)$, $PGL_2(q)$, alternating and symmetric groups ($A_n$ and $S_n$). Ya.Nuzhin [12] gave the same answer for $A_n$ independently, though it must be noted that his proof of impossibility of such generation for $A_6$ given in [11] is incorrect. Also in [3] M.Conder gives the positive answer for alternating and symmetric groups with rank sufficiently (and rather) high using a completely different approach. After this thesis had been completed the AMS Math Reviews published a review of two papers by Ya.Nuzhin [13, 14] where this question is settled for all Chevalley groups.

We formulate the complete answer to the problem of generating $PSL_n(q)$ by three involutions, two of which commute, as follows:

**Theorem 1.1.**  

\[ n = 1 \text{ - the problem is trivial.} \]

\[ n = 2 \text{ - } PSL_2(q) \text{ can be so generated, iff } q \neq 2, 3, 7, 9 ([16]) \]
Chapter 1. Introduction.

\[ n = 3 \] - \( PSL_3(q) \) cannot be so generated ([11] for even \( q \), Chapter 4 of this thesis for odd \( q \)).

\[ n = 4 \] - \( PSL_4(q) \) cannot be so generated, if \( q \) is even ([11]) and can be if \( q \) is odd (Section 5.2 of this thesis).

\[ n > 4 \] - \( PSL_n(q) \) can be so generated, ([11] for even \( q \), Sections 5.3–5.7 of this thesis for odd \( q \)).

As a semi-independent result we provide a complete classification of embeddings up to conjugacy of the Klein 4-group into \( PSL_n(q) \) with odd \( q \). A partial corollary of this classification, namely the fact that such an embedding into \( PSL_3(q) \) is unique, is crucial in proving the impossibility of generation of \( PSL_3(q) \) by three involutions two of which commute.

The motivation for the study of the question of generation of groups by three involutions two of which commute comes from different areas:

- It is known ([8]) that every finite simple non-abelian group other than \( PSU_3(3) \) is generated by three involutions. Therefore it is natural to restrict the conditions on the generators even further and ask for commutativity of two of the involutions. (We can't in fact ask for any further restrictions, since two involutions generate a dihedral group and if one of the three involutions commute with two others we get a direct product of the group of order 2 and a dihedral group).

- There is a famous conjecture of Lovász [7] that states that every vertex transitive graph, with just 4 exceptions, has a hamiltonian path. As D.Witte and J.A.Gallian [18] point out “We are nowhere near a proof” of this conjecture. However there is a considerable interest in proving it for certain classes of graphs. One obvious class of vertex transitive graphs is the class of Cayley graphs of presentations of groups. J.H.Conway, N.J.A.Sloane and A.R.Wilks [4] have shown that hamiltonian cycles exist in reflection groups. Their argument, in fact, applies to any group generated by involutions, such that its Dynkin diagram is a tree. Hence one of the corollaries of this thesis is the existence
Chapter 1. Introduction.

do a hamiltonian cycle in the Cayley graphs of $PSL_n(q)$ with odd $q$ and $n \geq 4$. We also note that the case of only three involutions is the hardest in the graph-theoretical sense (since every vertex has minimal valiance - 3) as well as in the group theoretical sense (we have the minimal possible number of generating involutions).

- The third source of interest comes from the study of regular polyhedra and algebraic curves over number fields. A. Grothendieck in his famous Esquisse d’un Programme [6] poses a question about finite quotients of the Cartographic group $C_2$,

$$C_2 = \langle r_1, r_2, r_3 | r_1^2 = r_2^2 = r_3^2 = (r_1r_2)^2 = 1 \rangle.$$ 

Therefore we show that $PSL_n(q)$ with $n \geq 4$, $q$- odd are examples of such quotients.

The thesis is organized into the following chapters.

This introduction is followed by a chapter where we collect necessary definitions, notation and other preliminary material.

Chapter 3 gives the complete classification of embeddings of the Klein 4-group into $PSL_n(q)$.

Chapter 4 answers negatively the main question of this thesis for the case of $3 \times 3$ matrices.

The core of this thesis is Chapter 5. There we prove that for any $n \geq 4$ it is possible to generate $PSL_n(q)$ by three involutions, two of which commute.

The strategy of the proof is described in detail in Section 5.1, but in brief it is quite simple. In the language of Chevalley groups, first we obtain one root element, then a root subgroup and then move it around to obtain more and more root subgroups until we exhaust the whole root system thus obtaining the whole group.

We would like to point out that the methods used in the proofs are elementary. Also our proofs are completely constructive – not only do we explicitly give generators, we also in most cases give a precise sequence of computations that leads to obtaining every transvection (or root) and therefore (by Gauss elimination) any matrix (representative of an element of the group). In other words we present an algorithm for writing any particular element of the group as a
word in the generators. We note that in Ya.Nuzhin's papers [11, 13, 14] such an algorithm is not given and in M.C.Tamburini–P.Zucca's paper [17] a considerable amount of effort is needed to deduce it.

All matrix computations found in this thesis have been verified by the Maple V program. The verification Maple V input files for the values of \( n = 4 \ldots 10 \) are attached in Appendices. Also they are available in 4 different formats (plain text, Maple V worksheet, HTML and \LaTeX sources) at http://www.math.ubc.ca/~mikec/thesis.html.
Chapter 2
Preliminaries and Notation.

In this chapter we introduce notation to be used throughout the thesis and state a few useful lemmas.

By \( \nu_2(n) \) we denote the highest power of 2 in \( n \). For example \( \nu_2(144) = 4 \), \( \nu_2(29) = 0 \).

In the definition of the following two functions we follow J. Arkin [2]:

\[
A(m,n) = \begin{cases} 
1 & \text{if } m \text{ divides } n, \\
0 & \text{otherwise,} 
\end{cases} \quad \text{where } m \in \mathbb{Z}_{>0}, n \in \mathbb{Z}_{\geq 0}.
\]

In particular \( A(m,0) = 1 \).

\( p_m(n) \) is the number of partitions of \( n \) into parts not exceeding \( m \). The generating function for \( p_m(n) \) is

\[
F_m(x) = \frac{1}{(1-x)(1-x^2)\ldots(1-x^m)} = \sum_{n=0}^{\infty} p_m(n)x^n
\]

The most important fact for us is that by Theorem 1.4 in [1], \( p_m(n) \) is equal to the number of partitions of \( n \) having at most \( m \) terms.
Chapter 2. Preliminaries and Notation.

Lemma 2.1. (Formulas (10), (17), and (18) in [2])

\[
P_2(n) = \frac{1}{2}(n + 1 + A(2,n)) = \left[\frac{n}{2}\right] + 1
\]

\[
P_3(n) = \frac{1}{24}(2n^2 + 12n + 13 + 3(-1)^n + 8A(3,n))
\]

\[
P_4(n) = \frac{1}{288}(2n^3 + 30n^2 + 135n + 125 + 9(n + 3)(-1)^n + 64A(3,n) + 32A(3,n + 2) + 72A(4,n))
\]

For block-diagonal matrices we will use direct sum notation. So, for instance, the matrix

\[
\begin{pmatrix}
A & 0 & 0 \\
0 & B & 0 \\
0 & 0 & C
\end{pmatrix}
\]

will be denoted by \( A \oplus B \oplus C \).

For even \( n \) matrices of the special form:

\[
\begin{pmatrix}
0 & 1 \\
\lambda & 0 \\
\vdots & \vdots \\
\lambda x^{-1} & 0
\end{pmatrix},
\]

where all 4 blocks are of the size \( n/2 \times n/2 \) will be denoted by \( R_n(\lambda, x) \).

The identity matrix will be denoted by \( I \).

The following matrices deserve special attention:

Definition 2.2. A transvection is a matrix that has 1's on the diagonal and only one non-zero off-diagonal entry.
Chapter 2. Preliminaries and Notation.

In other words a transvection is a matrix of the form \( I + tE_{ij} \), where \( t \) is element of \( \text{GF}(q) \), \( E_{ij} \) is an elementary matrix that has 1 in \((i, j)\) entry and 0 in any other entry. In the theory of Chevalley groups such elements are called root elements.

We will denote transvections by \( U_{ij}(t) \). Sometimes such a notation might lead to an ambiguity. In that cases we use comma to separate indices of the entry. Yet sometimes we use comma for completely different purpose - to indicate the dimension \( n \) of the group a transvection belongs to. If it might lead to an ambiguity we use parentheses such as for \( U_{(2,2k+1),n} \). On the other hand it should be clear from the context whether comma separates dimension or two indices.

We also need the following

**Definition 2.3.** A "double transvection" is a matrix that has 1's on the diagonal and two non-zero off-diagonal entries.

We don't reserve any special notation for "double transvections", when necessary we will write them as \( I + \alpha E_{ij} + \beta E_{i'j'} \).

Also it should be noted that all "double transvections" that we will use will have their non-zero off-diagonal entries either in the same row or in the same column.

Throughout the thesis the following letters will be used solely with the following meaning:

\[
\begin{align*}
n &= \text{dimension of the studied group } (PSl_n(q)), \\
q &= \text{the size of the underlying field } (q \text{ is always assumed odd}), \\
d &= \text{g. c. d.}(n, q - 1), \\
r &= \frac{q - 1}{d}, \\
s &= \frac{n}{d}, \\
\zeta &= \text{some (fixed) primitive root of unity in } GF(q).
\end{align*}
\]

The next lemma is obvious:

**Lemma 2.4.** The \( n^{th} \) roots of unity in \( GF(q) \) are \( \zeta^{ir} \), \( i = 1, \ldots, d \).
Chapter 2. Preliminaries and Notation.

We need the well-known criterion for conjugacy of matrices over a field (see, for example, [5] Theorem VI.5.7 or [9]):

**Theorem 2.5.** Two matrices $A$ and $B$ in $GL_n(q)$ are similar if and only if they have the same invariant polynomials or, what is the same, the same elementary divisors in the field $GF(q)$.

The following criterion determines when two conjugate matrices in $GL_n(q)$ are conjugate by an element of $SL_n(q)$:

**Lemma 2.6.** Suppose $A, B \in GL_n(q)$ and $A$ is conjugate to $B$ in $GL_n(q)$ by $C \in GL_n(q)$. Then $A$ and $B$ are conjugate by an element of $SL_n(q)$ if and only if there exists $X \in \text{Cent}_{GL_n(q)}(A)$ such that $\det X = \det C$.

**Proof.** Let $C^{-1}AC = B$, $C \in GL_n(q)$, and $D^{-1}AD = B$, $D \in SL_n(q)$. Then $DC^{-1}ACD^{-1} = A$, so $X = CD^{-1} \in \text{Cent}_{GL_n(q)}(A)$. Clearly $\det X = \det C$.

Conversely, let $X \in \text{Cent}_{GL_n(q)}(A)$ be such that $\det X = \det C$. Then $XAX^{-1} = A$ and $C^{-1}XAX^{-1}C = B$. Since $\det(X^{-1}C) = 1$, $A$ and $B$ are conjugate by an element of $SL_n(q)$. 

The following lemma shows that preimages of involutions of $PSL_n(q)$ always satisfy the criterion in lemma 2.6.

**Lemma 2.7.** Suppose $A \in GL_n(q)$, $A^2 = \lambda I$, and $B$ is conjugate to $A$. Then there exists an element $C \in SL_n(q)$, such that $B = C^{-1}AC$.

**Proof.** If $A^2 = \lambda I$, then the minimal polynomial of $A$ divides $f(x) = x^2 - \lambda$. If the minimal polynomial of $A$ is linear, then $A$ is scalar, lies in the center of $GL_n(q)$, so $B = A$ and the statement is trivially true.

If the minimal polynomial of $A$ is quadratic, it coincides with $f(x)$ and there are two cases to consider: $f(x)$ is reducible and $f(x)$ is irreducible, which correspond to $\lambda$ being square or non-square in $GF(q)$. Suppose $\lambda = \chi^2$, then $f(x) = (x - \chi)(x + \chi)$ and the elementary divisors
are \((x - \chi)\) and \((x + \chi)\). Hence \(A\) is similar to a diagonal matrix and its centralizer contains certain conjugates of all diagonal matrices and, in particular, of diag(1, \ldots, 1, \xi) for any \(\xi\). So the statement follows from lemma 2.6.

If \(f(x)\) is irreducible, then \(n\) is necessarily even, say \(n = 2k\) and the characteristic polynomial of \(A\) is \((f(x))^k\) and \(A\) must be similar to \(X = \bigoplus_{m=1}^{k} \begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix}\). Direct calculation shows that the matrices which lie in the centralizer of \(X\) have the following form:

\[
Y = \begin{pmatrix} v_1 \\ v_1X \\ \vdots \\ v_k \\ v_kX \end{pmatrix}
\]

where the \(v_i\) are row vectors in \(GF(q)^n\).

We set \(v_1 = (x, y, 0, \ldots, 0)\) and all other \(v_i\) to have 1 in the \((2i - 1)\)st entry and 0 in all other entries. Then the determinant of \(Y\) equals to \((x^2 - \lambda y^2)(-\lambda)^{k-1}\). Since the Diophantine equation \(x^2 - \lambda y^2 = s\) in any finite field has solutions in \(x, y\) for any non-zero \(\lambda\) and \(s\), we have matrices of any determinant in the centralizer of \(X\). \(\square\)
Chapter 3
Embeddings of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ into $PSL_n(q)$

In this chapter we enumerate conjugacy classes of involutions in the groups $PSL_n(q)$ for odd $q$ and determine up to conjugacy all possible embeddings of the Klein 4-group into $PSL_n(q)$. We will give explicit descriptions of the classes and representatives using elementary methods of linear algebra.

3.1 Statement of the Results

The conjugacy classes of one involution are described by the following

Theorem 3.1. The number of conjugacy classes of involutions in $PSL_n(q)$ is:

(i) $\frac{n-1}{2}$, if $n$ is odd;

(ii) $\frac{n}{2}$, if $1 \leq \nu_2(n) < \nu_2(q-1)$;

(iii) $\frac{n}{4} + 1$, if $\nu_2(n) > \nu_2(q-1)$;

(iv) $\frac{n-2}{4} + 1$, if $\nu_2(n) = \nu_2(q-1) = 1$;

(v) $\frac{n}{4}$, if $\nu_2(n) = \nu_2(q-1) > 1$.

The typical representatives of each class have the following forms (cases are as above):
Chapter 3. Embeddings of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ into $\text{PSL}_n(q)$

(i) $I_{n-l} \oplus -I_l$, with even $l$, $2 \leq l < n$

(ii) $I_{n-l} \oplus -I_l$, with even $l$, $2 \leq l \leq \frac{n}{2}$ and $\zeta I_{n-l} \oplus -\zeta I_l$
with odd $l$, $1 \leq l \leq \frac{n}{2}$.

(iii) and (iv) $I_{n-l} \oplus -I_l$, with even $l$, $2 \leq l \leq \frac{n}{2}$ and $X = \bigoplus_{m=1}^{k} \begin{pmatrix} 0 & 1 \\ \zeta^m & 0 \end{pmatrix}$ where $k = \frac{n}{2}$.

(v) $I_{n-l} \oplus -I_l$, with even $l$, $2 \leq l \leq \frac{n}{2}$.

The embeddings of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ into $\text{PSL}_n(q)$ are described by

**Theorem 3.2.** The number of embeddings of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ into $\text{PSL}_n(q)$ up to conjugacy is:

(i) $p_4(n) - p_2(n)$, if $n$ is odd;

(ii) $p_4(n) - p_2(n) + 2$, if $1 \leq \nu_2(n) < \nu_2(q-1)$;

(iii) $p_4 \left( \frac{n}{2} \right) - p_2 \left( \frac{n}{2} \right) + p_4 \left( \frac{n-4}{2} \right) + \frac{n}{2} + 4$, if $\nu_2(n) > \nu_2(q-1)$;

(iv) $p_4 \left( \frac{n}{2} \right) - p_2 \left( \frac{n}{2} \right) + p_4 \left( \frac{n-4}{2} \right) + \frac{n}{2}$, if $\nu_2(n) = \nu_2(q-1) = 1$;

(v) $p_4 \left( \frac{n}{2} \right) - p_2 \left( \frac{n}{2} \right) + p_4 \left( \frac{n-4}{2} \right) + 2$, if $\nu_2(n) = \nu_2(q-1) > 1$.

The typical embeddings are given by:

(a) Representatives are $R_1 = I_l \oplus -I_{n-l}$, $R_2 = I_{m_1} \oplus -I_{m_2} \oplus I_{m_3} \oplus -I_{m_4}$, $m_1 \leq m_2 \leq m_3 \leq m_4$, $m_1 + m_2 + m_3 + m_4 = n$, $m_2 \neq 0$, $m_1 + m_2 = l$. Also in cases (iii), (iv), and (v) all $m$'s have to be of the same parity. These embeddings amount to $p_4(n) - p_2(n)$ in cases (i) and (ii) and to $p_4 \left( \frac{n}{2} \right) - p_2 \left( \frac{n}{2} \right) + p_4 \left( \frac{n-4}{2} \right)$ in cases (iii), (iv), and (v).

(b) $R_1 = I_l \oplus -I_{n-l}$, $R_2 = \bigoplus_{m=1}^{k} \begin{pmatrix} 0 & 1 \\ \zeta^m & 0 \end{pmatrix}$, $k = \frac{n}{2}$, $l$ is even. These classes exist only in cases
(iii) and (iv) and there are only $\frac{n}{2}$ of them.

(c) $R_1 = I_{n/2} \oplus -I_{n/2}$, $R_2 = R_n(1, 1), R_n(1, \zeta), R_n(\zeta^r, 1)$ or $R_n(\zeta^r, \zeta)$ in case (iii) and $R_2 = R_n(1, 1)$ or $R_n(1, \zeta)$ in case (v).

### 3.2 Enumeration of Classes of Involutions.

Let an element $a$ be an involution in $PSL_n(q)$. This means that any preimage of $a$ in $SL_n(q)$, say $A$, satisfies the equation $x^2 - \lambda = 0$, where $\lambda$ is an $n^{th}$ root of unity in $GF(q)$. The minimal polynomial of $A$ must therefore divide $f(x) = x^2 - \lambda$. If the minimal polynomial of $A$ is linear, then $A$ is scalar and hence lies in the center of $SL_n(q)$, so $a$ is the identity in $PSL_n(q)$. Therefore if $a$ is an involution in $PSL_n(q)$, the minimal polynomial of $A$ is $x^2 - \lambda$.

We have two cases to consider - $f(x)$ is reducible or $f(x)$ is irreducible. If $\lambda = \zeta^i$, the cases are: $ir$ is even or odd.

Suppose $f(x)$ is reducible. Then $ir$ is even and the minimal polynomial of $A$ is $f(x) = (x - \chi)(x + \chi)$, where $\chi = \zeta^{ir/2}$. Therefore the elementary divisors are $(x - \chi)$ and $(x + \chi)$ and $A$ is similar to a diagonal matrix. The characteristic polynomial of $A$ is $g(x) = (x - \chi)^{l_1}(x + \chi)^{l_2}$, $l_1 + l_2 = n$.

In the case of an irreducible minimal polynomial, $ir$ is odd, hence both $i$ and $r$ are odd. It follows that $d$ is even and therefore $n$ is also even. Let $n = 2k$. Then the characteristic polynomial of $A$ is $g(x) = (x^2 - \lambda)^k$ and $A$ is similar to the matrix $\bigoplus_{m=1}^{k} \begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix}$.

By lemma 2.7 conjugacy classes of involutions stay the same, when we consider conjugation only by elements of $SL_n(q)$. Therefore we need to determine which conjugacy classes of involutions of $SL_n(q)$ fall into the same class after factorization. The next lemma gives a partial answer to this question.

**Lemma 3.3.** Let $A = \chi l_1 \oplus -\chi l_2$ be an element of $SL_n(q)$. Then $A$ represents in $PSL_n(q)$ the same element as $I_{l_1} \oplus -I_{l_2}$, if $l_2$ is even, and as $\zeta^{r/2} I_{l_1} \oplus -\zeta^{r/2} I_{l_2}$, if $l_2$ is odd. The latter can happen only if $r$ is even.
Chapter 3. Embeddings of \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \) into \( \text{PSL}_n(q) \)

**Proof.** We have \( \chi^n(-1)^{l_2} = 1 \). Hence if \( l_2 \) is even then \( \text{diag}(\chi, \ldots, \chi) \in Z(SL_n(q)) \) and we get the first part of the statement. Now suppose \( l_2 \) is odd. If \( y = \chi^2 \), then \( y^n = 1 \) and by lemma 2.4 \( y = \zeta^{ir} \) for some \( i \). Note that \( ir \) is even and \( \chi = \pm \zeta^{ir/2} \). In the case \( \chi = \zeta^{ir/2} \), \( \chi^n(-1)^{l_2} = 1 \) becomes \( \chi^{ir/2}(-1)^{l_2} = (-1)^{l_2} \zeta^{ir} = (-1)^{l_2} \zeta^{is} = 1 \). Since \( l_2 \) is odd, \( is \) is also odd. Therefore \( s \) is odd, \( i \) is odd and hence \( r \) is even. Now \( \zeta^{rn/2} = \zeta^{s(q-1)/2} = (-1)^s = -1 \), so \( \zeta^{r/2} I_1 \oplus -\zeta^{r/2} I_2 \) is in \( SL_n(q) \). Also, since \( \frac{1-i}{2} \) is an integer, \( z = \zeta^{(\frac{1+i}{2})r} \) is an \( n \)th root of unity in \( GF(q) \), so \( \text{diag}(z, \ldots, z) \in Z(SL_n(q)) \) and we have our statement for this case. In the case \( \chi = -\zeta^{ir/2} \), \( \chi^n(-1)^{l_2} = 1 \) and we get \( (-1)^{l_2+is} = 1 \). If \( n \) is even, the same argument shows that with \( z = -\zeta^{(\frac{1-i}{2})r} \), \( \text{diag}(z, \ldots, z) \in Z(SL_n(q)) \) and again we have the statement. And if \( n \) is odd, then both \( s \) and \( d \) are odd, hence \( r \) is even and \( i \) is also even. Now \( \left(-\zeta^{(\frac{1-i}{2})r}\right)^n = (-1)^n(-1)^i = (-1)^{i} \). Therefore, again with \( z = -\zeta^{(\frac{1-i}{2})r} \), \( \text{diag}(z, \ldots, z) \in Z(SL_n(q)) \) and the lemma is proven. \( \square \)

We are now ready to prove the reducible case of Theorem 3.1.

**Proposition 3.4.** The number of conjugacy classes of involutions in \( \text{PSL}_n(q) \) that have reducible minimal polynomial is

\[
\begin{cases}
p_2(n), & \text{if } r \text{ is even;} \\p_2\left(\frac{n}{2}\right), & \text{if } r \text{ is odd.}
\end{cases}
\]

**Proof.** By lemma 3.3 the conjugacy class of the matrix is determined by a pair \((l_1, l_2), l_1 + l_2 = n\). However, the conjugacy class of a pair \((l_1, l_2)\) is the same as that of the pair \((l_2, l_1)\). To see this, denote by \( A_1 \) the representative described in lemma 3.3 corresponding to \((l_1, l_2)\), and by \( A_2 \) the one corresponding to \((l_2, l_1)\).

If \( n \) is odd, then one of \( l \)’s (say \( l_1 \)) is even and the other is odd. Since \( (\zeta^{r/2})^n(-1)^{l_2} = 1 \), we have \( (-\zeta^{r/2})^n = 1 \) since both \( n \) and \( l_2 \) are odd. Therefore \( \text{diag}(-\zeta^{r/2}, \ldots, -\zeta^{r/2}) \) belongs to \( Z(SL_n(q)) \) and \( A_1 \) and \( A_2 \) represent conjugate elements.

If \( n \) is even, then since \( (-1)^n = 1 \), we have \( A_1 \sim -A_2 \).
Chapter 3. Embeddings of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ into $\text{PSL}_n(q)$

Therefore we have to count the number of pairs $(l_1, l_2), 1 \leq l_1 \leq l_2, l_1 + l_2 = n$, when $r$ is even, and the pairs $(l_1, l_2), 1 \leq l_1 \leq l_2, l_1 + l_2 = n, l_1 \equiv l_2 \equiv 0 \mod 2$, when $r$ is odd.

Clearly these are the numbers stated. \[\square\]

A similar proposition is true for the irreducible case of Theorem 3.1.

**Proposition 3.5.** The number of conjugacy classes of involutions in $\text{PSL}_n(q)$ that have irreducible minimal polynomial is equal to 1 in cases (iii) and (iv) of Theorem 3.1 and 0 otherwise.

**Proof.** We already know that the conjugacy class of such an involution in $\text{SL}_n(q)$ is determined only by a scalar $\lambda$. Two matrices $A = \bigoplus_{m=1}^{k} \begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix}$ and $B = \bigoplus_{m=1}^{k} \begin{pmatrix} 0 & 1 \\ \mu & 0 \end{pmatrix}$, where $\lambda = \zeta^{ir}, \mu = \zeta^{jr}$, with $r, i, j$ - odd, are conjugate in $\text{PSL}_n(q)$ if and only if $A$ is conjugate to $\eta B$ in $\text{SL}_n(q)$ for some $\eta$, such that $\eta^n = 1$. The elementary divisors of $A$ are $(x^2 - \lambda)$, and those of $\eta B$ are $(x^2 - \eta^2 \mu)$. Therefore taking $\eta = \left(\frac{\lambda}{\mu}\right)^{1/2} = \zeta^{\frac{i-j}{2}r}$ we see that all such involutions fall into the same conjugacy class (the condition on $\eta$ is automatically satisfied since $\frac{i-j}{2}$ is an integer.)

When does this class exist? Recall that since $\lambda$ is not a square, $ir$ is odd, so $r$ is odd and we are in one of the last three cases of the theorem 3.1. We also have

$$1 = (-\lambda)^k = (-1)^k \zeta^{ir/2} = (-1)^k \zeta^{ird/2} = (-1)^k \zeta^{is(q-1)/2} = (-1)^k \zeta^{is}.$$ 

Since $i$ is odd, $k$ and $s$ are of the same parity. When they are both even we have the case (iii) of the theorem 3.1, when they both are odd we have case (iv). \[\square\]

### 3.3 Two Commuting Involutions

In the section 3.2 we enumerated the conjugacy classes of a single involution in $\text{PSL}_n(q)$. This section enumerates conjugacy classes of two commuting involutions: All considerations are quite similar to those in section 3.2 thanks to the following

**Lemma 3.6.** For any embedding of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ into $\text{PSL}_n(q)$ one of the involutions is conjugate to a diagonal involution.
Chapter 3. Embeddings of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ into $PSL_n(q)$

**Proof.** An involution is conjugate to a diagonal involution if and only if it has minimal polynomial $x^2 - \lambda = 0$, where $\lambda$ is a square in $GF(q)$. So $\lambda = \zeta^k$, where $\zeta$ is a primitive root and $k$ is an even integer. If two involutions are not conjugate to a diagonal matrix then their product is, since the sum of two odd integers is even. 

Hence, without loss of generality, we can assume that the first involution is diagonal corresponding to a pair $(l_1, l_2)$.

Our strategy for determining conjugacy classes of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ inside $PSL_n(q)$ relies on the more general

**Proposition 3.7.** Let $V_1 = \{e, v_{11}, v_{12}, v_{13}\}$ and $V_2 = \{e, v_{21}, v_{22}, v_{23}\}$ be two subgroups of $G$ isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Then $V_1$ is conjugate to $V_2$ if and only if there exists $g \in G$, $h \in \text{Cent}_G(v_{11})$, $1 \leq i_1 \neq i_2 \leq 3$, such that $v_{11} = gv_{2i_1}g^{-1}, v_{12} = hgv_{2i_2}g^{-1}h^{-1}$

**Proof.** Suppose $V_1 \sim V_2$. Then there exists $a \in G$, such that $v_{11} = av_{2i_1}a^{-1}$ and $v_{12} = av_{2i_2}a^{-1}$ for some $i_1 \neq i_2$. Take any $b \in \text{Cent}_G(v_{11})$, then $v_{11} = bv_{11}b^{-1} = bav_{2i_1}a^{-1}b^{-1}$. Now take $g = ba, h = b^{-1}$ to get the statement.

For the converse note that $v_{11} = hv_{11}h^{-1} = hgv_{2i_1}g^{-1}h^{-1}$ and also

$v_{13} = v_{11}v_{12} = hgv_{2i_1}g^{-1}h^{-1}hgv_{2i_2}g^{-1}h^{-1} = hgv_{2i_1}v_{2i_2}g^{-1}h^{-1} = hgv_{2i_2}g^{-1}h^{-1}.$

Therefore $V_1$ is conjugated to $V_2$ by $hg$.

Hence the strategy for determining conjugacy classes is to bring one involution to (some) standard form and then, by conjugating by an element of the centralizer bring the second involution to (yet another) standard form.

The next lemma is similar to lemma 3.3:

**Lemma 3.8.** Let $A = \xi I_{m_1} \oplus -\xi I_{m_2} \oplus \xi I_{m_3} \oplus -\xi I_{m_4}$ be an element of $SL_n(q)$. Then $A$ represents in $PSL_n(q)$ the same element as $I_{m_1} \oplus -I_{m_2} \oplus I_{m_3} \oplus -I_{m_4}$, if $m_2 + m_4$ is even, and...
Chapter 3. Embeddings of \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \) into \( \text{PSL}_n(q) \)

as \( \zeta^{r/2}I_{m_1} \oplus -\zeta^{r/2}I_{m_2} \oplus \zeta^{r/2}I_{m_3} \oplus -\zeta^{r/2}I_{m_4} \), if \( m_2 + m_4 \) is odd. The latter can happen only if \( r \) is even.

**Proof.** The proof is a copy of the proof of lemma 3.3 with \( l_2 \) substituted by \( m_2 + m_4 \).

By lemma 3.6 we can assume that the first involution has the form \( I_{l_1} \oplus -I_{l_2} \) or \( \zeta I_{l_1} \oplus -\zeta I_{l_2} \).

In the case \( l_1 \neq l_2 \) matrices commuting with the first involution have the form \(
\begin{pmatrix}
A_{11} & 0 \\
0 & A_{22}
\end{pmatrix}
\),

where \( A_{11} \) is a \( l_1 \times l_1 \) matrix and \( A_{22} \) is a \( l_2 \times l_2 \) matrix.

In the case \( l_1 = l_2 \) the matrices in the centralizer of the first involution have the form \( \begin{pmatrix}
A_{11} & 0 \\
0 & A_{22}
\end{pmatrix} \)
or \( \begin{pmatrix}
0 & A_{12} \\
A_{21} & 0
\end{pmatrix} \).

We will call matrices of the form \( \begin{pmatrix}
A_{11} & 0 \\
0 & A_{22}
\end{pmatrix} \) matrices of the type I, and matrices of the form \( \begin{pmatrix}
0 & A_{12} \\
A_{21} & 0
\end{pmatrix} \) matrices of the type II.

**Proposition 3.9.** The number of conjugacy classes of possible embeddings of \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \) into \( \text{PSL}_n(q) \) such that the second matrix has the type I and reducible minimal polynomial is

\[
\begin{cases}
p_4(n) - p_2(n), & \text{if } r \text{ is even} \\
p_4\left(\frac{n}{2}\right) - p_2\left(\frac{n}{2}\right) + p_4\left(\frac{n - 4}{2}\right), & \text{if } r \text{ is odd.}
\end{cases}
\]

**Proof.** If a matrix of the type I is an involution we have \( A_{11}^2 = \lambda I_{l_1}, A_{22}^2 = \lambda I_{l_2} \) for some (but same) \( \lambda \). Also \( \det A_{11} \cdot \det A_{22} = 1 \). (Of course \( \lambda^n = 1 \)).

Since \( \lambda \) is a square, both \( A_{11} \) and \( A_{22} \) have reducible minimal polynomial, so they are both similar to diagonal matrices inside \( GL(l_1, q) \) and \( GL(l_2, q) \) correspondingly. According to lemma 2.6 these conjugations can be achieved by elements of \( SL(l_1, q) \) and \( SL(l_2, q) \).

Hence applying lemma 3.8 we see that the conjugacy class of the embedding of \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \) into \( \text{PSL}_n(q) \) is determined by a 4-tuple \( (m_1, m_2, m_3, m_4) \) with \( m_1 + m_2 + m_3 + m_4 = n \). (It is
understood also that \( l_1 \) and \( l_2 \) are found from the conditions \( l_1 = m_1 + m_2 \) and \( l_2 = m_3 + m_4 \).)

The last step is to determine which 4-tuples yield the same conjugacy class. The claim is that for any permutation of \((m_1, m_2, m_3, m_4)\) the conjugacy class of the embedding stays the same. Indeed, multiplication of the second matrix by a scalar matrix \((-I, \text{if } n \text{ is even, and } -\zeta^{r/2}I, \text{if } n \text{ is odd})\) induces the permutation \((m_2, m_1, m_4, m_3)\). Exchanging the first and second matrices gives \((m_1, m_3, m_2, m_4)\) and exchanging the second and third gives \((m_1, m_2, m_4, m_3)\). Since these 3 permutations generate \(S_4\), the conjugacy class of an embedding is determined by an unordered 4-tuple \((m_1, m_2, m_3, m_4)\).

Also when \( r \) is odd, by lemmas 3.3 and 3.8 only 4-tuples having all elements of the same parity are allowed.

Therefore the number of conjugacy classes of an embedding of \(\mathbb{Z}_2 \oplus \mathbb{Z}_2\) into \(\text{PSL}_n(q)\) is determined by the number of integer 4-tuples \(0 \leq m_1 \leq \cdots \leq m_4\) with \(m_1 + m_2 + m_3 + m_4 = n\). To avoid degenerate case we also demand \(m_2 \neq 0\). In the case of even \( r \) we count all such 4-tuples, in case of odd \( r \), only those of the same parity. Therefore the number of conjugacy classes is \(p_4(n) - p_2(n)\) if \( r \) is even, and \(p_4(n/2) - p_2(n/2) + p_4\left(\frac{n-4}{2}\right)\) if \( r \) is odd.

**Proposition 3.10.** The number of conjugacy classes of embeddings of \(\mathbb{Z}_2 \oplus \mathbb{Z}_2\) into \(\text{PSL}_n(q)\) such that the second matrix has irreducible minimal polynomial and type I is equal to

\[
\begin{cases}
\frac{n}{2} & \text{if } \nu_2(n) = \nu_2(q-1) = 1, \text{ or } \nu_2(n) > \nu_2(q-1); \\
0 & \text{otherwise.}
\end{cases}
\]

**Proof.** First note that there are no such embeddings if \( n \) is odd (there are no involutions with irreducible minimal polynomial by proposition 3.5). If \( n \) is even, then the characteristic polynomials of both \(A_{11}\) and \(A_{22}\) must be of even degrees since \((x^2 - \lambda)^k\) does not have factors of odd degrees. Hence both \(l_1\) and \(l_2\) are even. For each such pair the argument of the proof of the proposition 3.5 applies without change to show that there is only one class of such an embedding if the conditions of cases (iii) and (iv) of the Theorem 3.1 are satisfied and none otherwise. \(\square\)
Chapter 3. Embeddings of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ into $PSL_n(q)$

The embeddings with the second involution of the type II are described by the following proposition for both reducible and irreducible minimal polynomials.

**Proposition 3.11.** The number of conjugacy classes of embeddings of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ into $PSL_n(q)$ such that second involution is of the type II is

\[
\begin{cases} 
2 & \text{if } 1 \leq \nu_2(n) \leq \nu_2(q - 1); \\
4 & \text{if } \nu_2(n) > \nu_2(q - 1); \\
0 & \text{otherwise.}
\end{cases}
\]

**Proof.** This is the case when $l_1 = l_2 = k$ and the second (and therefore third) matrix has the form $R_2 = \begin{pmatrix} 0 & A \\ \lambda A^{-1} & 0 \end{pmatrix}$, where $A \in GL_k(q)$, $(-1)^k \lambda^k = 1$, $\lambda = \zeta^r$. Hence, as usual, we have the condition on $\lambda$: $is + k$ is even.

Note how a matrix of this form is changed by conjugation:

\[
\begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix} \begin{pmatrix} 0 & A \\ \lambda A^{-1} & 0 \end{pmatrix} \begin{pmatrix} X^{-1} & 0 \\ 0 & Y^{-1} \end{pmatrix} = \begin{pmatrix} 0 & XAY^{-1} \\ \lambda Y A^{-1} X^{-1} & 0 \end{pmatrix},
\]

and

\[
\begin{pmatrix} 0 & X \\ Y & 0 \end{pmatrix} \begin{pmatrix} 0 & A \\ \lambda A^{-1} & 0 \end{pmatrix} \begin{pmatrix} 0 & Y^{-1} \\ X^{-1} & 0 \end{pmatrix} = \begin{pmatrix} 0 & \lambda X A^{-1} Y^{-1} \\ YAX^{-1} & 0 \end{pmatrix}.
\]

We have $\det(X) \cdot \det(Y) = 1$ in the first case and $\det(X) \cdot \det(Y) = (-1)^k$ in the second.

It follows that the **parity** of the power of $\zeta$ in the determinant of $A_{12}$ is invariant under such conjugation.

Let $\det A = x^{-1}$. Then by conjugating $R_2$ by $\text{diag}(1, \ldots ,1,x) \oplus A$ we bring $R_2$ to the form $R_n(\lambda, x)$ (see section 2 for notation).

If $x = \zeta^t$, let $y = \zeta^{-[t/2]}$. Then conjugating the last matrix by

\[\text{diag}(1, \ldots ,1,y,1,\ldots,1,y^{-1})\]

we obtain $R_n(\lambda, \alpha)$ as a form for $R_2$, where $\alpha$ is 1 or $\zeta$ depending on parity of $t$. 

18
Now we need to decide for which $\lambda$ and $\alpha$, the corresponding $R_n(\lambda, \alpha)$ fall into the same conjugacy class.

$\lambda$ cannot be changed by conjugation, but, as in lemma 3.3, matrices with different $\lambda$'s fall into the same conjugacy class after factorization. More precisely: multiplication of a matrix by $\eta I$ such that $\eta^n = 1$ changes $\lambda$ to $\lambda \eta^2$. And, since $\eta$ is also of the form $\eta = \zeta^{ir}$, by a choice of an appropriate $\eta$, $\lambda$ can be made 1 or $\zeta^r$, depending on the parity of $i$ in the original $\lambda (= \zeta^{ir})$. We repeat the procedure of bringing multiplied matrix to the form $R_n(\lambda, \alpha)$ and end up with at most 4 conjugacy classes of this type in $\text{PSL}_n(q)$ corresponding to the second matrices having the forms $R_n(1,1)$, $R_n(1,\zeta)$, $R_n(\zeta^r,1)$ and $R_n(\zeta^r,\zeta)$.

The conjugacy classes of the embeddings corresponding to these 4 matrices are all distinct because of the difference of the elementary divisors or because of the difference in the parity of the power of $\zeta$ in the determinant of $A_{21}$. So we only need to check in which cases these matrices belong to $\text{SL}_n(q)$. We have $\det R_n(1,1) = \det R_n(1,\zeta) = (-1)^k$, $\det R_n(\zeta^r,1) = \det R_n(\zeta^r,\zeta) = (-1)^{k+s}$. Therefore, if $k$ is odd, $R_n(1,1)$ and $R_n(1,\zeta)$ do not belong to $\text{SL}_n(q)$ and we have only two classes of embeddings of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. (Note that since $i$ is odd, $s$ is odd and hence $R_n(\zeta^r,1)$ and $R_n(\zeta^r,\zeta)$ belong to $\text{SL}_n(q)$).

Finally, if $k$ is even, then if $s$ is even, we have all four classes, and if $s$ is odd, $R_n(\zeta^r,1)$ and $R_n(\zeta^r,\zeta)$ are not in $\text{SL}_n(q)$ and there are only two classes, corresponding to $R_n(1,1)$ and $R_n(1,\zeta)$.

Combining the results of the propositions in this section we obtain Theorem 3.2.
Chapter 4
3 by 3 matrices.

In this chapter we prove the following

**Theorem 4.1.** $PSL_3(q)$ cannot be generated by three involutions two of which commute.

**Proof.** According to Theorem 3.2 there is only one conjugacy class of embeddings of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ into $PSL_3(q)$. Therefore the first two (commuting) involutions can be chosen as

$$R_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \quad \text{and} \quad R_2 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

We let $R_3 = R_1 R_2$ and let $R_0$ denote identity matrix $I$. We will show that no third involution $X$ can be chosen so that $PSL_3(q) = \langle X, R_1, R_2 \rangle$ or, equivalently, that $SL_3(q)$ can not be generated by $X, R_1, R_2$ and scalar matrices.

For matrices $A, B \in SL_3(q)$ we use the notation $A \approx B$ to indicate that $A, B$ agree up to a scalar, that is $A = \lambda B$ for some $\lambda \in GF(q)$. Necessarily $\lambda^3 = 1$.

Now, fix an involution $X$ and let $G = \langle X, R_1, R_2 \rangle$.

By Theorem 3.1 there is only one conjugacy class of involutions in $PSL_3(q)$. So there exists a matrix $C \in SL_3(q)$ such that $X \approx CR_1 C^{-1}$. Let

$$C = \begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{bmatrix} \quad \text{and} \quad C^{-1} = \begin{bmatrix} \hat{c}_{11} & \hat{c}_{12} & \hat{c}_{13} \\ \hat{c}_{21} & \hat{c}_{22} & \hat{c}_{23} \\ \hat{c}_{31} & \hat{c}_{32} & \hat{c}_{33} \end{bmatrix}$$
Chapter 4. 3 by 3 matrices.

Since $CC^{-1} = I$, we have

\[ X \simeq CR_1C^{-1} \simeq C \begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} - I \simeq 2c\tilde{c} - I, \]

where $c = \begin{pmatrix} c_{11} \\ c_{21} \\ c_{31} \end{pmatrix}$ and $\tilde{c} = (\tilde{c}_{11}, \tilde{c}_{12}, \tilde{c}_{13})$ are the first column and first row of $C$ and $C^{-1}$ respectively.

If any one of $c_{11}, c_{21}, c_{31}, \tilde{c}_{11}, \tilde{c}_{12}, \tilde{c}_{13}$ is zero then each of $X, R_1, R_2$ have both off-diagonal entries in some row or column equal to zero. For example, if $\tilde{c}_{12} = 0$ then $X, R_1, R_2$ all have both $(1,2)$ and $(3,2)$ entries equal to 0. Since the matrices with such a property form a proper subgroup of $PSL_3(q)$, all elements of $G$ will have the form

\[ \begin{bmatrix} * & 0 & * \\ * & * & * \\ * & 0 & * \end{bmatrix} \]

and obviously $G \neq PSL_3(q)$.

Therefore, for $X, R_1, R_2$ to generate $PSL_3(q)$ none of $c_{11}, c_{21}, c_{31}, \tilde{c}_{11}, \tilde{c}_{12}, \tilde{c}_{13}$ can be equal to zero.

So from now on we assume this is the case.

Now suppose we have chosen $X$ such that $X \simeq 2c\tilde{c} - I$. Consider the group $D(X, R_1, R_2)D^{-1}$ where $D = \text{diag}(d_1, d_2, d_3)$ for some $d_1, d_2, d_3$. Obviously this group has the same number of elements as $G$ and will be all of $PSL_3(q)$ if, and only if, $G = PSL_3(q)$.

Since $D$ commutes with all $R_i$’s we have $D(X, R_1, R_2)D^{-1} = (DXD^{-1}, R_1, R_2)$, and therefore without loss of generality we can change $c$ to $Dc$ and $\tilde{c}$ to $\tilde{c}D^{-1}$.

Let $D = \text{diag}(c_{11}^{-1}, c_{21}^{-1}, c_{31}^{-1})$. Then

\[ X \simeq \begin{bmatrix} 2\alpha & 2\beta & 2\gamma \\ 2\alpha & 2\beta & 2\gamma \\ 2\alpha & 2\beta & 2\gamma \end{bmatrix} - I \]
Chapter 4. 3 by 3 matrices.

where $\alpha = c_{11}^{-1} \tilde{c}_{11}$, $\beta = c_{21}^{-1} \tilde{c}_{12}$, and $\gamma = c_{31}^{-1} \tilde{c}_{13}$.

Now let $F = \text{diag}(\alpha, \beta, \gamma)$. Then $FXF^{-1} = X^T$. Suppose $B$ is an element of $(X, R_1, R_2)$. Then $B \simeq R_iXR_jX \ldots XR_kXR_l$. Therefore

$$FBF^{-1} \simeq FR_iF^{-1}FXF^{-1} \ldots FXF^{-1}FR_iF^{-1} = R_iX^TR_jX^T \ldots X^TR_kX^TR_l = (R_iXR_kX \ldots XR_jXR_l)^T \simeq (R_i^{-1}X^{-1}R_k^{-1}X^{-1} \ldots X^{-1}R_j^{-1}X^{-1}R_i^{-1})^T = (B^{-1})^T$$

This means if $B$ is in $G$ then conjugating it by a diagonal matrix we get a scalar multiple of $(B^T)^{-1}$. Then obviously

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \notin G$$

This proves the negative part of Theorem 1.1.

In the Introduction we have mentioned that one possible motivation for the question of which groups can be generated by three involutions, two of which commute, is the problem of finding a Hamiltonian cycle in a Cayley graph of a group.

In the light of the negative answer to the question of such generation of $PSL_3(q)$ the following question can be posed: can $PSL_3(q)$ be generated by some number of involutions such that their Dynkin diagram is a tree? Unfortunately the answer to this, even more relaxed, question is still NO. This can be shown by considerations similar to those in this chapter. Again the key reason is that there is only one way to embed $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ into $PSL_3(q)$. 

22
Chapter 5
Positive answer for $n \geq 4$.

The purpose of this chapter is to prove

**Theorem 5.1.** $\text{PSL}_n(q)$, with $q$ odd, can be generated by three involutions, two of which commute, if $n \geq 4$.

**5.1 Strategy**

We are going to prove Theorem 5.1 by induction on the size of the matrices. Starting with the matrices of some size $n \times n$ we will show how to expand them to size $(n + 4) \times (n + 4)$ so that computations stay practically the same.

For each $n$ we will explicitly give three generators and demonstrate how to obtain all (off-diagonal) transvections, which are well-known to generate $\text{PSL}_n(q)$.

First we establish the result for $n = 4$ and $n = 5$ in sections 5.2 and 5.3. While the case $n = 4$ is completely distinct, the case $n = 5$ could have served as the base of the induction for the $n = 4k + 1$ case. However, although the generators are exactly the same (in terms of the Bar Operation introduced in definition 5.2) as in the general case, some computations in the proof are specific to the case $n = 5$ and cannot be extended for larger matrices. Hence we treat the case $n = 5$ in a separate section. Nevertheless we will point out the parts of the computation that are common to all of $n = 4k + 1$ and will use those when we prove the cases $n = 9, 13, 17, \ldots$.

Then in sections 5.4, 5.5, 5.6 and 5.7, we deal with the cases $n = 4k + 1$, $n = 4k + 3$, $n = 4k$, $n = 4k + 5$.
Chapter 5. Positive answer for \( n \geq 4 \).

and \( n = 4k + 2 \) respectively.

The method of proof in all cases is quite similar, consisting of the following Steps:

**Step 1.** Obtain a transvection in \( G \), thus getting a subgroup isomorphic to \( \mathbb{Z}/p\mathbb{Z} \).

**Step 2.** Obtain all transvections at some spot, thus getting a subgroup isomorphic to \( \text{GF}(q) \). Note that this step is redundant if \( q = p \).

**Step 3.** Obtain all off-diagonal transvections.

As we already mentioned, the completion of **Step 3** means the end of the proof. Since the precise sequence of computations necessary for completing each step varies from case to case, we will describe it in detail in the corresponding sections.

All computations were verified by a Maple V program. The input files for the cases \( n = 4, \ldots, 10 \) are provided in Appendices A–F and are also available at [http://www.math.ubc.ca/~mikec/thesis.html](http://www.math.ubc.ca/~mikec/thesis.html)

Here is the description of the process for increasing the matrix size by 4.

Let us call the matrix

\[
B_0 = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix},
\]

a block of type 0. Similarly

\[
B_1 = \begin{bmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{bmatrix},
\]

a block of type 1,

\[
B_2 = \begin{bmatrix}
1 & 1 & 0 & 0 \\
0 & -1 & 0 & 0 \\
0 & 0 & 1 & 1 \\
0 & 0 & 0 & -1
\end{bmatrix},
\]
Chapter 5. Positive answer for n \geq 4.

a block of type 2,

\[
B_3 = \begin{bmatrix} -1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix},
\]

a block of type 3,

\[
B_4 = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix},
\]

a block of type 4 and

\[
B_5 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix},
\]

a block of type 5.

**Definition 5.2.** If \( A \) is any matrix we denote by \( \overline{A[type,i]} \) the matrix obtained by an insertion of the block \( B_{type} \) after the \( i \)-th row and \( i \)-th column. We will call this the **Bar Operation**.

Here are some examples of this notation:

If \( A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \), then

\[
\overline{A[4,1]} = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ c & 0 & 0 & 0 & 0 & d \end{bmatrix},
\]

If \( B = \begin{bmatrix} a & b & c & d & e & f \\ d & e & f & g & h & i \end{bmatrix} \), then

\[
\overline{B[2,0]} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & a & b & c \\ 0 & 0 & 0 & d & e & f \\ 0 & 0 & 0 & g & h & i \end{bmatrix}
\]

The next lemma is obvious.
Chapter 5. Positive answer for $n \geq 4$.

Lemma 5.3. The Bar Operation has the following properties:

1. $A[k, i] \cdot B[k, i] = AB[0, i]$, if $k = 0, 1, 2, 3, 5$.

2. $B[k, i] \cdot A[0, i] \cdot B[k, i]^{-1} = BAB^{-1}[0, i]$, if $k = 0, \ldots, 5$.

3. $A[k, i] \cdot B[0, i] \cdot A[k, i]^{-1} \cdot B[0, i]^{-1} = ABA^{-1}B^{-1}[0, i]$, if $k = 0, \ldots, 5$.

In sections 5.4–5.7 we will give explicit generators for the base cases of the induction, that is $n \times n$, where $n = 9, 7, 8, 6$. Then the generators for higher dimensions are described inductively in terms of the Bar Operation. Most computations also are expressed in terms of the Bar Operation and easily verified by lemma 5.3.

5.2 Case of $4 \times 4$ matrices.

In this section we prove the following

Proposition 5.4. For any odd $q \geq 3$, $SL_4(q)$ can be generated by the following three matrices:

$R_1 = \begin{bmatrix} 1 & x & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & x & 0 & 1 \end{bmatrix}, \quad R_2 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ and $R_3 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$,

where $x = -1$, if $q = 3$, and if $q \geq 5$, then $x \in GF(q)$ is chosen so that $z = \frac{x}{1 - x}$ is a primitive root in $GF(q)$ (this in particular implies $x \neq 0, 4, 8$).

Corollary 5.5. $PSL_4(q)$ can be generated by three involutions two of which commute for any odd $q \geq 3$.

Proof. Simple computations show that $R_1^2 = R_2^2 = R_3^2 = (R_1R_2)^2 = I$.

We start with the following
Chapter 5. Positive answer for \( n \geq 4 \).

**Lemma 5.6.** Suppose \( q \geq 5 \). Let \( T = \begin{bmatrix} A & 0 \\ B & C \end{bmatrix} \) be the \( 4 \times 4 \) matrix, where \( A, B \) and \( C \) are the \( 2 \times 2 \) matrices: 
\[
A = \begin{bmatrix} -1 + \frac{x}{2} & x \\ \frac{1}{2} & -1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ \frac{x}{2} & x \end{bmatrix}, \quad C = \begin{bmatrix} 1 & \zeta \\ 0 & 1 \end{bmatrix}.
\]
Let \( x \neq 0, 8 \) and suppose \( A^m = I \). Then
\[
T^m = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ m\zeta z & 4m\zeta z & 1 & m\zeta \\ 0 & 0 & 0 & 1 \end{bmatrix},
\]
where \( z = \frac{x}{8-x} \).

**Proof.** By an easy induction \( T^k = \begin{bmatrix} A^k & 0 \\ B_k & C^k \end{bmatrix} \), where
\[
B_k = BA^{k-1} + CBA^{k-2} + \cdots + C^jBA^{k-1-j} + \cdots + C^{k-2}BA + C^{k-1}B.
\]
Our goal is to compute \( B_m = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \).

Now
\[
C^jB = \begin{bmatrix} 1 & l\zeta \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ \frac{x}{2} & x \end{bmatrix} = \begin{bmatrix} l\zeta \frac{x}{2} & l\zeta x \\ \frac{x}{2} & x \end{bmatrix},
\]
and
\[
(\alpha, \beta) = \left(\frac{x}{2}, x\right) \cdot \zeta \cdot (A^{m-2} + 2A^{m-3} + \cdots + (m-2)A + (m-1)I)
\]
\[
(\gamma, \delta) = \left(\frac{x}{2}, x\right) \cdot (A^{m-1} + A^{m-2} + \cdots + A + I)
\]
Since \( x \neq 8, A - I \) is invertible, so \( A^m - I = 0 \) is equivalent to \( A^{m-1} + A^{m-2} + \cdots + A + I = 0 \), and hence \((\gamma, \delta) = (0, 0)\).

Let
\[
X = A^{m-2} + 2A^{m-3} + \cdots + (m-2)A + (m-1)I
\]
and
\[
Y = (m-1)A^{m-1} + (m-2)A^{m-2} + \cdots + 2A^2 + A.
\]
Chapter 5. Positive answer for \( n \geq 4 \).

Then \( X = -Y \), since

\[
X + Y = (m - 1)(A^{m-1} + A^{m-2} + \cdots + A + I) = (m - 1) \cdot 0 = 0.
\]

To compute \( Y \), first assume \( A \) is diagonal, say \( A_d = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} \), \( \lambda^m = 1 \).

Let

\[
f(x) = (m - 1)x^{m-1} + (m - 2)x^{m-2} + \cdots + x^2 + x.
\]

Then \( Y_d = \begin{bmatrix} f(\lambda) & 0 \\ 0 & f(\lambda^{-1}) \end{bmatrix} \).

Write

\[
f(x) = x ((m - 1)x^{m-2} + (m - 2)x^{m-3} + \cdots + x + 1) = xg(x).
\]

Then

\[
\int g(x)dx = x^{m-1} + x^{m-2} + \cdots + x + C = \frac{x^{m-1}}{x - 1} + C,
\]

and therefore

\[
g(x) = \frac{m x^{m-1}(x - 1) - x^m + 1}{(x - 1)^2},
\]

So \( g(\lambda) = \frac{m \lambda^{m-1}}{\lambda - 1} \) and \( f(\lambda) = \frac{m}{\lambda - 1} \).

Thus

\[
Y_d = \begin{bmatrix} \frac{m}{\lambda - 1} & 0 \\ 0 & \frac{m}{\lambda^{-1} - 1} \end{bmatrix}.
\]

Now if \( E \) is such that \( A = E A_d E^{-1} \), then \( Y = E Y_d E^{-1} \). The characteristic polynomial of \( A \) is

\[
f(t) = t^2 - \left( \frac{x}{2} - 2 \right) t + 1,
\]

so since \( x \neq 0, 8 \), \( A \) is diagonalizable. We can take \( E \) to be the matrix having eigenvectors of \( A \) as columns. A choice of eigenvectors (from the second row of \( A \)) is

\[
e_\lambda = \begin{pmatrix} \lambda + 1 \\ 1 \\ -2 \end{pmatrix}, \quad \text{and} \quad e_{\lambda^{-1}} = \begin{pmatrix} \lambda^{-1} + 1 \\ 1 \\ -2 \end{pmatrix},
\]
Chapter 5. Positive answer for $n \geq 4$.

and so

$$E = \begin{bmatrix} \lambda + 1 & \lambda^{-1} + 1 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \quad \text{and} \quad E^{-1} = \frac{2}{\lambda - 1 - \lambda} \begin{bmatrix} -\frac{1}{2} & -\lambda^{-1} - 1 \\ \frac{1}{2} & \lambda + 1 \end{bmatrix}.$$

Therefore (using $\lambda + \lambda^{-1} = \frac{x}{2} - 2$) we have

$$Y = \frac{2m}{4-x/2} \begin{bmatrix} -1 & \frac{x}{4} & \frac{x}{2} \\ \frac{1}{4} & \frac{x/2 - 2}{2} \end{bmatrix}, \quad \text{and} \quad X = -\frac{4m}{8-x} \begin{bmatrix} -1 & \frac{x}{4} \\ \frac{1}{4} & \frac{x-4}{4} \end{bmatrix}.$$

Note that the entries of $A, Y$ and $E$ might not lie in $GF(q)$, but they are elements of $GF(q^2)$. Nevertheless $Y$ is an element of $SL_4(q)$. Finally

$$(\alpha, \beta) = -\frac{4m \zeta}{8 - x} \left( \frac{x}{4}, x \right) \begin{bmatrix} -1 & \frac{x}{4} \\ \frac{1}{4} & \frac{x-4}{4} \end{bmatrix} = m \zeta \cdot (1, 4),$$

and the lemma is proved. \hfill \Box

The analogue of this lemma for the case $q = 3$ is the following

**Lemma 5.7.** Let

$$T = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 1 \end{bmatrix}.$$ \hspace{1cm} Then $T^3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$

**Proof.** Computation \hfill \Box

Now we are ready to prove proposition 5.4.

**Proof.** Let $G = \langle R_1, R_2, R_3 \rangle$. We will go through the Steps described in section 5.1. For this particular case we will use lemmas 5.6 and 5.7 to get a transvection at the position $(3,1)$.

Step 2 is redundant for $q = 3$. We will repeatedly use lemma 5.6 to obtain all transvections at position $(3,1)$ for $q \geq 5$. Then in Step 3 we will easily obtain all transvections at the positions $(3,4), (2,4), (2,1)$ and $(2,4)$, and then after a few computations we will obtain the rest.
Chapter 5. Positive answer for \( n \geq 4 \).

See Appendix A for the Maple V input file to verify all computations.

By computation:

\[
(R_2R_3)^4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -2 & 1 & 4 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}
\]

Therefore for any integer \( s \)

\[
(R_2R_3)^{4s} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -2s & 1 & 4s & 2s \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}
\]

and

\[
R_3(R_2R_3)^{4s} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ -2s & 1 & 4s + 1 & 2s + \frac{1}{2} \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}
\]

Let \( s_0 = \begin{cases} \frac{p-1}{4}, & \text{if } p \equiv 1 \mod 4, \\ \frac{3p-1}{4}, & \text{if } p \equiv 3 \mod 4. \end{cases} \)

(\text{In other words } s_0 = -\frac{1}{4}). \) Then we put

\[
R_4 = R_3(R_2R_3)^{4s_0} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ \frac{1}{2} & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}
\]

and

\[
T = R_1R_4 = \begin{bmatrix} \frac{x}{2} - 1 & x & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ \frac{x}{2} & x & 0 & 1 \end{bmatrix}
\]

Now \( T \) satisfies the conditions of lemma 5.6 with \( \zeta = 1 \), if \( q \geq 5 \), or lemma 5.7, if \( q = 3 \). Hence

\[
T_m = T^m = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ mz & 4mz & 1 & m \\ 0 & 0 & 0 & 1 \end{bmatrix}, \tag{5.1}
\]

if \( q \geq 5 \), or

\[
T_m = T^3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},
\]

if \( q = 3 \). Note that in the first case \( z \neq 0 \), since \( x \neq 0 \), and \( m \neq 0 \), since \( m \) is a divisor of \( q - 1 \).

Put

\[
S = T_mR_2T_mR_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ mz - m & 0 & 1 & m - mz \\ 0 & 0 & 0 & 1 \end{bmatrix}, \tag{5.2}
\]

\[30\]
Chapter 5. Positive answer for $n \geq 4$.

if $q \geq 5$, or

$$S = T_m R_2 T_m R_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

if $q = 3$, and then

$$U_{31}(2m(z - 1)) = (T_m R_4 S)^2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2m z - 2m & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad (5.3)$$

if $q \geq 5$, or

$$U_{31}(1) = (T_m R_4 S)^2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

if $q = 3$.

Note that $U_{31}(2m(z - 1)) \neq I$ since $z \neq 1$, or equivalently $x \neq 4$. At this point we have completed Step 1 for $q \geq 5$. If $q = 3$, we have in fact completed Step 1 and Step 2.

Now we complete Step 2 of the proof for $q \geq 5$.

$U_{31}(2m(z - 1))$ generates a subgroup which contains all transvections at the (3,1) position with non-zero off-diagonal elements being multiples of $z - 1$, we denote them $U_{31}(k(z - 1))$. Putting

$$U_{34}(-m(z - 1)) = U_{31}(-m(z - 1))S \quad (5.4)$$

we obtain a similar subgroup at the (3,4) spot. Consequently

$$T_z = TU_{34}(z - 1) = \begin{bmatrix} x & -1 & x & 0 \\ 2 & -1 & x & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & 1 & z \\ x & x & 0 & 1 \end{bmatrix}, \quad (5.5)$$
Chapter 5. Positive answer for \( n \geq 4 \).

satisfies conditions of the lemma 5.6 with \( \zeta = z \). So by the lemma

\[
T_z^m = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
mz^2 & 4mz^2 & 1 & mz \\
0 & 0 & 0 & 1
\end{bmatrix}.
\] (5.6)

So repeating the computations 5.1–5.6 using \( T_z \) instead of \( T \) we get

\[
S_z = T_z^m R_2 T_z^m R_2
\]

and

\[
U_{31}(2m(z^2 -1)) = (T_z^m R_4 S_z)^2
\]

and

\[
U_{31}(2m(z^2 -z)) = U_{31}(2m(z^2 -z)) U_{31}(2m(z-1)).
\]

Note now that \( U_{31}(2m(z^2 -1)) \) generates the same subgroup as \( U_{31}(z^2 -1) \). As before we obtain \( U_{34}(z^2 -1) \) and set \( T_z^2 = T U_{34}(z^2 -1) \). Now we repeat the computations 5.1–5.6 with \( T_z^2 \) and inductively with all \( T_z^l, l \in \mathbb{N} \). Doing this we will run through all the elements of the form \( z^k -1 \), thus, if \( z \) is a primitive root, through all the elements of \( GF(q) \) except \(-1\).

Hence we obtain all the transvections \( U_{31}(t) \) and Step 2 is completed.

For Step 3 we do not distinguish cases \( q = 3 \) and \( q \geq 5 \), since we only use the Step 2 result which is the same for both cases.

Multiplying \( U_{31}(t) \) by the corresponding \( S \) we obtain all transvections \( U_{34}(t) \).

Now \( (R_3 U_{34}(t))^2 = U_{24}(t) \) and \( R_2 U_{24}(-t) R_2 = U_{21}(-t) \). Also \( (R_1 U_{31}(t))^2 = U_{32}(-tx) \).

So at this point we have obtained all transvections at spots \((3,1), (3,2), (3,4), (2,1), \) and \((2,4)\).

Now put

\[
R_5 = U_{32}(1) R_3 U_{34}(-1) U_{24}(1/2) U_{32}(1) = \begin{bmatrix}
-1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}.
\]

Then we have \( U_{23}(t) = R_5 U_{32}(t) R_5 \). Hence we have all transvections at the spot \((2,3)\). Since we also have all transvections at the spot \((3,2)\), our group contains the subgroup isomorphic to \( SL_2(q) \) at the entries \((2,2), (2,3), (3,2), \) and \((3,3)\). In particular, the matrix

\[
R_6 = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 \\
0 & 0 & -1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}.
\]
Now we need a few more computations to finish the proof. Put

\[ Q = R_5R_1R_3U_{23}(1) = \begin{bmatrix} 1 & x & 2x & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & x & 0 & 1 \end{bmatrix} \]

and

\[ P = U_{32}(t)U_{23}(-1)R_6Q = \begin{bmatrix} 1 & x & 2x & 0 \\ 0 & -1 & 0 & 0 \\ 0 & -t & -1 & 0 \\ 0 & x & 0 & 1 \end{bmatrix}, \]

Then \( P^2U_{32}(2t) = U_{12}(-2xt) \), and we obtain all transvections at the spot \((1,2)\). Finally

\[ \begin{align*} 
U_{13}(t) &= U_{12}(-t)U_{23}(-1)U_{12}(t)U_{23}(1) \\
U_{14}(t) &= U_{13}(-t)U_{34}(-1)U_{13}(t)U_{34}(1) \\
U_{43}(t) &= R_2U_{13}(-t)R_2 \\
U_{41}(t) &= R_2U_{14}(t)R_2 \\
U_{42}(t) &= R_2U_{12}(t)R_2 
\end{align*} \]

We have obtained all transvections, thus completing Step 3 and the proof of the proposition. \( \square \)

### 5.3 Case of 5 × 5 matrices.

In this section we go through Steps 1, 2 and 3 in the case of 5 by 5 matrices. Step 1 will be very easy and we’ll obtain \( U_{23}(1) \). To complete Step 2 we will first obtain \( U_{24}(1) \) and then all \( U_{24}(t), t \in GF(q) \). Step 3 will consist of three following substeps:

a) Obtain all \( U_{2i}(t) \)

b) Obtain all \( U_{j2}(t) \)

c) Obtain all \( U_{ij}(t) \)
Chapter 5. Positive answer for \( n > 4 \).

See Appendix B for the input Maple V file to verify computations.

We will enumerate some of the computations that we will use in the next section to prove inductively the case of \( n = 4k + 1 \).

As in the previous section the main result is the

**Proposition 5.8.** For any odd \( q > 3 \) \( SL_5(q) \) can be generated by the following three matrices:

\[
\begin{align*}
R_1 &= \begin{bmatrix}
1 & x & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & -x & 0 & 0 & 1
\end{bmatrix}, &
R_2 &= \begin{bmatrix}
0 & 0 & 0 & 0 & 1 \\
0 & -1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0
\end{bmatrix} &
\text{and } R_3 &= \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & -1
\end{bmatrix},
\end{align*}
\]

where \( x \) is a primitive root in \( GF(q) \).

There is an immediate

**Corollary 5.9.** \( PSL_5(q) \) can be generated by three involutions two of which commute for any odd \( q > 3 \).

**Proof.** As in the case of \( 4 \times 4 \) matrices simple computations show that \( R_1^2 = R_2^2 = R_3^2 = (R_1R_2)^2 = I \)

\( \Box \)

**Proof of the proposition 5.8.** We start with

\[
U_{23}(4) = (R_2R_3)^4 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 4 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{bmatrix}. \tag{5.7}
\]

Thus completing Step 1. At this point we have obtained all transvections \( U_{23}(l) \), where \( l \) is an integer.

Our next goal is to complete Step 2. We will do it by obtaining all transvections \( U_{24}(t) \), where \( t \) is an arbitrary element of \( GF(q) \). Computations to obtain \( U_{24}(1) \) are unique to the case \( q = 5 \).
Chapter 5. Positive answer for \( n \geq 4 \).

Let

\[
R_4 = R_3U_{23}(-1) = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & -1
\end{bmatrix}
\quad \text{and} \quad W = (R_1R_4)^4 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & -2x & 1 & 0 & 0 \\
0 & -2x & 0 & 1 & 0 \\
0 & 4x & 0 & 0 & 1
\end{bmatrix}.
\]

Also let

\[
S = WR_2WR_2 = \begin{bmatrix}
1 & -4x & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 4x & 0 & 0 & 1
\end{bmatrix}.
\]

Thus we have obtained all matrices with ones on the diagonal and having as the only off-diagonal entries the opposite integer multiples of \( x \) at the spots \((1,2)\) and \((5,2)\). In particular we have obtained the matrix

\[
T = \begin{bmatrix}
1 & x & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & -x & 0 & 0 & 1
\end{bmatrix}.
\]

Now if

\[
R_6 = R_1T^{-1} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1
\end{bmatrix}, \quad \text{then} \quad U_{24}(1) = R_6U_{23}(-1)R_6 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{bmatrix}.
\]

To finish Step 2 we need to produce all \( U_{24}(t) \) from \( U_{24}(1) \).

We proceed as follows: assume that we have obtained some \( U_{24}(a) \), then we can also obtain

\[
P = (R_1R_3R_1U_{24}(a))^2 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & x & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & -2x & 1
\end{bmatrix} \quad (5.8)
\]

35
Chapter 5. Positive answer for $n \geq 4$.

and

$$U_{24}(xa) = P^{-1}U_{23}(1)PU_{23}(-1) = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & xa & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{bmatrix}.$$  (5.9)

This means that starting with $U_{24}(1)$ we can successively obtain $U_{24}(x^l)$ for all integers $l$ hence all $U_{24}(t), t \in \text{GF}(q)$ since $x$ is a primitive root. This completes Step 2.

Now

- $U_{23}(t) = R_6 U_{24}(t) R_6$.  \hfill (5.10)
- $U_{25}(t) = R_3 U_{24}(t) R_3 U_{24}(-t)$. \hfill (5.11)
- $U_{21}(t) = R_2 U_{25}(-t) R_2$. \hfill (5.12)

We have just obtained all transvections with off-diagonal element in the second row thus completing substep a). The next series of computations obtains all transvections with off-diagonal element in the second column.

$$Q = R_1 U_{21} \left( \frac{1}{x} \right) R_1 U_{21} \left( -\frac{2}{x} \right) = \begin{bmatrix}
0 & x & 0 & 0 & 0 \\
-\frac{1}{x} & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
1 & -x & 0 & 0 & 1
\end{bmatrix}.$$ \hfill (5.13)

$$F_1 = \left( Q U_{21} \left( -\frac{2}{x^2} \right) Q \right)^2 = \begin{bmatrix}
1 & t & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & -t & 0 & 0 & 1
\end{bmatrix}.$$ \hfill (5.14)

$$F_2 = (U_{23}(1) R_3 F_1)^2 = \begin{bmatrix}
1 & 2t & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & -t & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{bmatrix}.$$ \hfill (5.15)
Chapter 5. Positive answer for \( n \geq 4 \).

\[
F_3 = R_6 F_2 R_6 = \begin{bmatrix}
1 & -2t & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & t & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}
\]  

(5.16)

So now

\begin{itemize}
  \item \( U_{12}(-4t) = (U_{23}(1)R_3 F_3)^2 \),
  \item \( U_{32}(t) = U_{12}(2t)F_3 \),
  \item \( U_{42}(t) = U_{12}(2t)F_2^{-1} \) and
  \item \( U_{52}(t) = U_{12}(t)F_1^{-1} \).
\end{itemize}

(5.17) (5.18) (5.19) (5.20)

We have obtained all transvections with off-diagonal entry in the second column thus completing substep b).

Now to finish Step 3 and the proof we observe that for \( i, j, 2 \) all distinct

\[
U_{ij}(t) = U_{i2}(1)U_{2j}(t)U_{i2}(-1)U_{2j}(-t)
\]

(5.21)

\[\square\]

5.4 Case of \((4k + 1) \times (4k + 1)\) matrices.

In this section we deal with the case \( n = 4k + 1, k \geq 2 \). We will use the Bar Operation(see Definition 5.2) to increase the size of the matrices inductively and we will use lemma 5.3 to verify that the same computations yield the same results for all sizes.

Precisely we want to prove the following

Proposition 5.10. Let \( R_1, R_2 \) and \( R_3 \) be the \( 5 \times 5 \) matrices defined in proposition 5.8. Define inductively:

\[
R_{1,5} = R_1, \quad R_{2,5} = R_2, \quad R_{3,5} = R_3
\]

and

\[
R_{1,n} = \overline{R_{1,n-4}[1, 2]}, \quad R_{2,n} = \overline{R_{2,n-4}[0, 2]}, \quad R_{3,n} = \overline{R_{3,n-4}[2, 3]}, \quad \text{for } n = 4k + 1, k \geq 2.
\]
Chapter 5. Positive answer for $n \geq 4$.

Then $SL_n(q) = \langle R_{1,n}, R_{2,n}, R_{3,n} \rangle$

As in the cases of $4 \times 4$ and $5 \times 5$ matrices we have an immediate

**Corollary 5.11.** $PSL_{4k+1}(q)$, $k \geq 2$ can be generated by three involutions two of which commute.

**Proof.** This follows immediately from the previous proposition, computations of corollary 5.9 and lemma 5.3

In essence the proof of proposition 5.10 follows from the following (trivial) key observation and lemma 5.3,

**Lemma 5.12.**

\[ a) \quad R_{1,n} = R_{1,n-4}[1, 2j], \quad 1 \leq j \leq 2k - 2, \]

\[ b) \quad R_{2,n} = R_{2,n-4}[0, j], \quad 2 \leq j \leq 4k - 4, \]

\[ c) \quad R_{3,n} = R_{3,n-4}[2, 2j + 1], \quad 1 \leq j \leq 2k - 2. \]

This means that we have considerable freedom where to choose the place for the Bar Operation. We will exploit this freedom to use lemma 5.3. That lemma justifies "expanded computation" only if the Bar Operation took place at the same position in matrices involved in the computation, therefore in the series of computations we will treat the same matrix for example sometimes as expanded at the (4,4) spot and sometimes at (5,5) spot. See computations 5.30–5.33 for examples of this treatment.

See Appendix C for the Maple V file containing the input for computations in $9 \times 9$ case.

The following three lemmas describe how the generators $R_{1,n}$, $R_{2,n}$, $R_{3,n}$ act on elementary matrices $E_{ij}$. (These lemmas can also be regarded as an alternate definition for $R_{1,n}$, $R_{2,n}$, $R_{3,n}$). The proofs are just elementary read-off of the rows and columns of the generators.

Left multiplication by the first generator is described by the following
Chapter 5. Positive answer for \( n \geq 4 \).

**Lemma 5.13. For any** \( 1 \leq j \leq 4k + 1 \)

\( a) \ R_{1,n}E_{1j} = E_{1j} \)

\( b) \ R_{1,n}E_{2j} = xE_{1j} - E_{2j} - xE_{4k+1,j} \)

\( c) \ R_{1,n}E_{2l+1,j} = E_{2l+2,j}, \ for \ 1 \leq l \leq 2k - 1 \)

\( d) \ R_{1,n}E_{2l+2,j} = E_{2l+1,j}, \ for \ 1 \leq l \leq 2k - 1 \)

\( e) \ R_{1,n}E_{4k+1,j} = E_{4k+1,j} \)

Right multiplication by the first generator is described by the following

**Lemma 5.14. For any** \( 1 \leq i \leq 4k + 1 \)

\( a) \ E_{i1}R_{1,n} = E_{i1} + xE_{i2} \)

\( b) \ E_{i2}R_{1,n} = -E_{i2} \)

\( c) \ E_{i2l+1}R_{1,n} = E_{i2l+2}, \ for \ 1 \leq l \leq 2k - 1 \)

\( d) \ E_{i2l+2}R_{1,n} = E_{i2l+1}, \ for \ 1 \leq l \leq 2k - 1 \)

\( e) \ E_{i4k+1}R_{1,n} = E_{i4k+1} - xE_{i2} \)

Similarly left multiplication by the second generator is described by the following

**Lemma 5.15. For any** \( 1 \leq j \leq 4k + 1 \)

\( a) \ R_{2,n}E_{1j} = E_{4k+1,j} \)

\( b) \ R_{2,n}E_{2j} = -E_{2j} \)

\( c) \ R_{2,n}E_{ij} = E_{ij}, \ for \ 3 \leq i \leq 4k \)

\( d) \ R_{2,n}E_{4k+1,j} = E_{1j} \)

And right multiplication by the second generator is described by the following
Chapter 5. Positive answer for $n \geq 4$.

Lemma 5.16. For any $1 \leq i \leq 4k + 1$

a) $E_{i1}R_{2,n} = E_{i,4k+1}$

b) $E_{i2}R_{2,n} = -E_{i2}$

c) $E_{ij}R_{2,n} = E_{ij}$, for $3 \leq i \leq 4k$

d) $E_{i,4k+1}R_{2,n} = E_{i1}$

Finally left multiplication by the third generator is described by the following

Lemma 5.17. For any $1 \leq j \leq 4k + 1$

a) $R_{3,n}E_{1j} = E_{1j}$

b) $R_{3,n}E_{2l,j} = E_{2l,j}$, for $1 \leq l \leq 2k$

c) $R_{3,n}E_{2l+1,j} = E_{2l,j} - E_{2l+1,j}$, for $1 \leq l \leq 2k$

And right multiplication by the third generator is described by the following

Lemma 5.18. For any $1 \leq i \leq 4k + 1$

a) $E_{i1}R_{3,n} = E_{i1}$

b) $E_{i,2l}R_{3,n} = E_{i,2l} + E_{i,2l+1}$, for $1 \leq l \leq 2k$

c) $E_{i,2l+1}R_{3,n} = -E_{i,2l+1}$, for $1 \leq l \leq 2k$

Now we are ready to prove proposition 5.10.

Proof of proposition 5.10. The steps in this case are similar to those for $5 \times 5$ matrices.

Step 1 will be very easy and we’ll obtain $U_{23}(1)$.

To complete Step 2 we will first obtain $U_{24}(1)$ and then all $U_{24}(t), t \in GF(q)$. We will do it by first obtaining $U_{2j}(1)$ for $4 \leq j \leq 4k - 1$, then having obtained $U_{2,4k-1}(1)$ we will use it to finish Step 2 by obtaining all $U_{24}(t)$ with $t \in GF(q)$. 40
Chapter 5. Positive answer for \( n \geq 4 \).

**Step 3** will consist of three following substeps:

a) Obtain all \( U_{2j}(t) \)

b) Obtain all \( U_{i2}(t) \)

c) Obtain all \( U_{ij}(t) \)

For **Step 1** we only need to note that \( R_{2,n} = \overline{R_{2,n-4}[0,3]} \) by lemma 5.12, hence by lemma 5.3 and computation 5.7 we have

\[
U_{23,n}(4) = U_{23,n-4}(4)[0,3] = (R_{2,n-4}[0,3] \cdot \overline{R_{3,n-4}[0,3]})^4
\]

Therefore we have just obtained all transvections \( U_{23,n}(l) \), where \( l \) is an integer.

We now proceed with **Step 2**. First we obtain \( U_{24,n}(l) \) and \( U_{25,n}(l) \) with \( l \) an integer. For the base of the induction \( (n = 9) \) we make the following computations:

\[
P_{1,9} = R_{1,9}U_{23,9}(1)R_{1,9} = \begin{bmatrix}
1 & 0 & 0 & x & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & -x & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 
\end{bmatrix} \tag{5.22}
\]

\[
P_{2,9} = R_{3,9}P_{1,9}R_{3,9} = \begin{bmatrix}
1 & 0 & 0 & x & x & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & -1 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & -x & -x & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & x & x & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 
\end{bmatrix} \tag{5.23}
\]
Chapter 5. Positive answer for \( n \geq 4 \).

\[
P_{3,9} = R_{2,9}P_{2,9}R_{2,9}P_{2,9}^{-1} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]  \hspace{1cm} (5.24)

and finally

\[
U_{24,9}(2) = R_{3,9}P_{3,9}R_{3,9} \quad \text{and} \quad U_{25,9}(2) = U_{24,9}(2)P_{3,9} \hspace{1cm} (5.25)
\]

\[
U_{26,9}(2) = R_{3,9}P_{3,9}R_{3,9} \quad \text{and} \quad U_{27,9}(2) = U_{26,9}(2)P_{3,9} \hspace{1cm} (5.26)
\]

We now will repeat computations 5.22–5.26 starting with \( U_{25}(1) \) instead of \( U_{23}(1) \) to obtain \( U_{26}(2) \) and \( U_{27}(2) \). In fact the same computations will work successively in the \( n \times n \) case and we will obtain all transvections in the second row but the last two. In other words in the \( n \times n \) case we can obtain all \( U_{2j}(1) \) for \( 3 \leq j \leq 4k - 1 \) thanks to the following

Claim 5.19. Let \( 1 \leq l \leq 2k - 2 \).

Set \( P_1 = R_{1,n}U_{2,2l+1}(\xi)R_{1,n}, P_2 = R_{3,n}P_1R_{3,n}, P_3 = R_{2,n}P_2R_{2,n}P_2^{-1} \). Then

a) \( U_{2,2l+2}(2\xi) = R_{3,n}P_3R_{3,n} \)

b) \( U_{2,2l+3}(2\xi) = U_{2,2l+2}^{-1}(2\xi)P_3 \)

Proof. Since \( U_{2,2l+1}(\xi) = I + \xi E_{2,2l+1} \) we have by lemmas 5.13 and 5.14

\[
P_1 = I + R_{1,n}\xi E_{2,2l+1}R_{1,n} = I + \xi(xE_{1,2l+1} - E_{2,2l+1} - xE_{4k+1,2l+1})R_{1,n}
\]

\[
= I + \xi xE_{1,2l+2} - \xi E_{2,2l+2} - \xi xE_{4k+1,2l+2}
\]

42
Chapter 5. Positive answer for \( n \geq 4 \).

Now by lemmas 5.17 and 5.18 we have

\[
P_2 = R_{3,n} P_1 R_{3,n} = R_{3,n} (I + \xi x E_{1,2l+2} - \xi E_{2,2l+2} - \xi E_{4k+1,2l+2}) R_{3,n}
= I + \xi x E_{1,2l+2} R_{3,n} - \xi E_{2,2l+2} R_{3,n} - \xi (E_{4k,2l+2} - E_{4k+1,2l+2}) R_{3,n}
= I + \xi x E_{1,2l+2} + \xi x E_{1,2l+3} - \xi E_{2,2l+2} - \xi E_{2,2l+3} - \xi E_{4k,2l+2}
- \xi x E_{4k,2l+3} + \xi x E_{4k+1,2l+2} + \xi x E_{4k+1,2l+3}
\]

Now write \( P_2 = I + Q \). Then since \( 2l + 2 > 2 \) and \( 2l + 3 \leq 2(2k - 1) + 3 = 4k - 1 < 4k \), \( Q^2 = 0 \) as every product of elementary matrices involved is equal to 0. Hence \( P_2^{-1} = I - Q \).

Also by lemmas 5.15 and 5.16 we have

\[
R_{2,n} P_2 R_{2,n} = R_{2,n} (I + \xi x E_{1,2l+2} + \xi x E_{1,2l+3} - \xi E_{2,2l+2} - \xi E_{2,2l+3}
- \xi x E_{4k,2l+2} - \xi x E_{4k,2l+3} + \xi x E_{4k+1,2l+2} + \xi x E_{4k+1,2l+3}) R_{2,n}
= I + \xi (x E_{4k+1,2l+2} + x E_{4k+1,2l+3} + E_{2,2l+2} + E_{2,2l+3}
- x E_{4k,2l+2} - x E_{4k,2l+3} + x E_{1,2l+2} + x E_{1,2l+3}) R_{2,n}
= I + \xi (x E_{4k+1,2l+2} + x E_{4k+1,2l+3} + E_{2,2l+2} + E_{2,2l+3}
- x E_{4k,2l+2} - x E_{4k,2l+3} + x E_{1,2l+2} + x E_{1,2l+3})
= I + Q'
\]

Again all the products of elementary matrices in the product of \( Q \) and \( Q' \) are 0. Hence

\[
P_3 = R_{2,n} P_2 R_{2,n} P_2^{-1} = (I + Q')(I - Q) = I + Q' - Q = I + 2\xi E_{2,2l+2} + 2\xi E_{2l+3}
\]

Finally by lemmas 5.17 and 5.18

\[
R_{3,n} P_3 R_{3,n} = R_{3,n} (I + 2\xi E_{2,2l+2} + 2\xi E_{2,2l+3}) R_{3,n} = I + \xi (2E_{2,2l+2} + 2E_{2,2l+3}) R_{3,n}
= I + 2\xi E_{2,2l+2} + 2\xi E_{2,2l+3} - 2\xi E_{2,2l+3} = U_{2,2l+2}(2\xi)
\]

and

\[
U_{2,2l+2}^{-1}(2\xi) P_3 = (I - 2\xi E_{2,2l+2})(I + 2\xi E_{2,2l+2} + 2\xi E_{2,2l+3})
= I + 2\xi E_{2,2l+2} + 2\xi E_{2,2l+3} - 2\xi E_{2,2l+2} = U_{2,2l+3}(2\xi)
\]

and the claim is proved.
Chapter 5. Positive answer for \( n \geq 4 \).

Therefore, using the claim with \( \xi = 1 \) we successively obtain \( U_{2j}(l) \), where \( l \) is an integer and \( 3 \leq j \leq 4k - 1 \).

To finish Step 2 we need to produce \( U_{24}(t) \) for all \( t \in \text{GF}(q) \). The computations are exactly the same as in the \( 5 \times 5 \) case (5.8–5.9) but we need to split them into smaller steps to show that they still hold in higher sizes. More precisely:

Claim 5.20. Let

\[
P_1 = R_{1,n}U_{24}(\xi)R_{1,n} \quad P_2 = R_{3,n}P_1R_{3,n} \quad P_3 = R_{1,n}P_2R_{1,n}.
\]

Then \( U_{24}(x^\xi) = P_3^{-1}U_{2,4k-1}(1)P_3U_{2,4k-1}(-1) \).

Proof. We compute these matrices in the case \( n = 9 \) and then use lemma 5.3 to prove the claim for all \( n = 4k + 1 \).

\[
P_{1,9} = R_{1,9}U_{24,9}(\xi)R_{1,9} = \begin{bmatrix}
1 & 0 & x^\xi & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -\xi & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & -x^\xi & 0 & 0 & 0 & 0 & 0 & 1 
\end{bmatrix}
\]

(5.27)

\[
P_{2,9} = R_{3,9}P_{1,9}R_{3,9} = \begin{bmatrix}
1 & 0 & -x^\xi & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & \xi & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & x^\xi & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & -x^\xi & 0 & 0 & 0 & 0 & 1 & 0 
\end{bmatrix}
\]

(5.28)
Chapter 5. Positive answer for \( n \geq 4 \).

\[
P_{3,9} = R_{1,9} P_{2,9} R_{1,9} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & -\xi & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & -2 \xi & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}
\]

(5.29)

Finally,

\[
U_{24,9}(x \xi) = P_{3,9}^{-1} U_{27,9}(1) P_{3,9} U_{27,9}(-1).
\]

For the bigger sizes we notice that \( U_{24,n}(\xi) = U_{24,n-4}[0, 4] \). Therefore by lemmas 5.3 and 5.12 we have

\[
P_{1,n} = P_{1,n-4}[0, 4] = R_{1,n-4} U_{24,n-4}(\xi) R_{1,n-4}[0, 4] = R_{1,n-4}[1, 4] \cdot U_{24,n-4}(\xi)[0, 4] \cdot R_{1,n-4}[1, 4]
\]

(5.30)

Observe that \( P_{1,n} \) can also be regarded as \( P_{1,n-4}[0, 5] \). Hence by lemmas 5.3 and 5.12

\[
P_{2,n} = P_{2,n-4}[0, 5] = R_{3,n-4} P_{1,n-4} R_{3,n-4}[0, 5] = R_{3,n-4}[2, 5] \cdot P_{1,n-4}[0, 5] \cdot R_{3,n-4}[2, 5]
\]

(5.31)

Regarding \( P_{2,n} \) as \( P_{2,n-4}[0, 4] \) we have

\[
P_{3,n} = P_{3,n-4}[0, 4] = R_{1,n-4} P_{2,n-4} R_{1,n-4}[0, 4] = R_{1,n-4}[1, 4] \cdot P_{2,n-4}[0, 4] \cdot R_{1,n-4}[1, 4]
\]

(5.32)

Finally we regard \( U_{(2,4k-1),n}(1) \) as \( U_{(2,4k-5),n-4}(1)[0, 4] \) and we obtain

\[
U_{24,n}(x \xi) = U_{24,n-4}(x \xi)[0, 4] = P_{3,n-4}^{-1} U_{(2,4k-5),n-4}(1) P_{3,n-4} U_{(2,4k-5),n-4}(-1)[0, 4] =
\]

\[
\frac{U_{24,n-4}(x \xi)[0, 4]}{P_{3,n-4}[0, 4]} \cdot U_{(2,4k-5),n-4}(1)[0, 4] \cdot P_{3,n-4}[0, 4] \cdot U_{(2,4k-5),n-4}(-1)[0, 4]
\]

(5.33)

And the claim is proved. \( \Box \)

Therefore starting with \( U_{24}(1) \) we can successively obtain all \( U_{24}(x^l) \) for any integer \( l \). Hence if \( x \) is a primitive root in \( GF(q) \) we obtain all \( U_{24}(t) \) for any \( t \in GF(q) \), thus completing Step 2.
Chapter 5. Positive answer for \( n \geq 4 \).

For substep \( a \) of Step 3 we first obtain \( U_{25}(t) \):

\[
U_{25,9}(t) = R_{3,9}U_{24,9}(t)R_{3,9}U_{24,9}(-t)
\]  

(5.34)

and

\[
U_{25,n}(t) = U_{25,n-4}(t)[0,5] = R_{3,n-4}U_{24,n-4}(t)R_{3,n-4}U_{24,n-4}(-t)[0,5]
\]

\[
= R_{3,n-4}[2,5] \cdot U_{24,n-4}(t)[0,5] \cdot R_{3,n-4}[2,5] \cdot U_{24,n-4}(-t)[0,5]
\]

Now use claim 5.19 with \( \xi = t \) to obtain successively all \( U_{2j}(t) \) with \( 5 \leq j \leq 4k - 1 \).

We have to work a little harder to obtain the last two transvections in the second row. This is achieved by the following computations (first we do them for \( n = 9 \)):

\[
P_{1,9} = R_{1,9}U_{25,9}(t)R_{1,9} =
\]

\[
\begin{bmatrix}
1 & 0 & 0 & 0 & x\tau & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & -\tau & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & -x\tau & 0 & 0 & 1
\end{bmatrix}
\]

\[
P_{2,9} = R_{3,9}P_{1,9}R_{3,9} =
\]

\[
\begin{bmatrix}
1 & 0 & 0 & 0 & x\tau & x\tau & 0 & 0 \\
0 & 1 & 0 & 0 & -\tau & -\tau & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & -x\tau & -x\tau & 0 & 1 \\
0 & 0 & 0 & 0 & x\tau & x\tau & 0 & 1
\end{bmatrix}
\]
Chapter 5. Positive answer for $n \geq 4$.

$$P_{3,9} = R_{1,9}P_{2,9}R_{1,9} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & t & 0 & 0 & t & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -xt & 0 & 1 & -xt & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2xt & 0 & 0 & 2xt & 1 \end{bmatrix}$$

$$P_{4,9} = U_{27,9}(1)P_{3,9}U_{27,9}(-1)P_{3,9}^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -tx & 0 & 0 & -tx & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Finally

$$U_{28,9}(-tx) = U_{25,9}(tx)P_{4,9}$$

and

$$U_{29,9}(-tx) = R_{3,9}U_{28,9}(-tx)R_{3,9}U_{28,9}(tx)$$

As $t$ runs through all elements of $GF(q)$ so does $-tx$, hence we have just obtained all $U_{28}(t)$ and $U_{29}(t)$ with $t \in GF(q)$ for $n = 9$.

By lemmas 5.3 and 5.12 we have

$$P_{1,n} = P_{1,n-4}[0,4] = R_{1,n-4}U_{(2,4k-7),n-4}(t)R_{1,n-4}[0,4] = R_{1,n-4}[1,4] \cdot U_{(2,4k-7),n-4}(t)[0,4] \cdot R_{1,n-4}[1,4],$$

$$P_{2,n} = P_{2,n-4}[0,3] = R_{3,n-4}P_{1,n-4}R_{3,n-4}[0,3] = R_{3,n-4}[2,3] \cdot P_{1,n-4}[0,3] \cdot R_{3,n-4}[2,3],$$

$$P_{3,n} = P_{3,n-4}[0,4] = R_{1,n-4}P_{2,n-4}R_{1,n-4}[0,4] = R_{1,n-4}[1,4] \cdot P_{2,n-4}[0,4] \cdot R_{1,n-4}[1,4],$$

47
Chapter 5. Positive answer for \( n \geq 4 \).

\[
P_{4,n} = P_{4,n-4}[0,4] = U_{(2,4k-5),n-4}(1)P_{3,n-4}U_{(2,4k-5),n-4}(-1)P_{3,n-4}^{-1}[0,4]
\]

\[
= U_{(2,4k-5),n-4}(1)[0,4] \cdot P_{3,n-4}[0,4] \cdot U_{(2,4k-5),n-4}(-1)[0,4] \cdot P_{3,n-4}^{-1}[0,4]
\]

Hence

\[
U_{(2,4k),n}(t) = U_{(2,4k-4),n-4}(t)[0,4] = U_{(2,4k-7),n-4}(-t)P_{4,9}[0,4]
\]

and

\[
U_{(2,4k+1),n}(t) = U_{(2,4k-3),n-4}(t)[0,5] = R_{3,n-4}U_{(2,4k),n-4}(t)R_{3,n-4}U_{(2,4k),n-4}(-t)[0,5]
\]

To finish substep a) of Step 3 we only need to obtain \( U_{21}(t) \) and \( U_{23}(t) \). The former is achieved by an easy computation using lemmas 5.15 and 5.16:

\[
R_{2,n}U_{2,4k+1}(-t)R_{2,n} = R_{2,n}(I - tE_{2,4k+1})R_{2,n} = I + tE_{2,4k+1}R_{2,n} = I + tE_{21} = U_{21}(t)
\]

and the latter by the following series of computations:

\[
P_{1,9} = R_{1,9}U_{24,9}(t)R_{1,9} = \begin{bmatrix}
1 & 0 & xt & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -t & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & -xt & 0 & 0 & 0 & 0 & 1 & 0
\end{bmatrix}
\]

\[
P_{2,9} = R_{3,9}P_{1,9}R_{3,9} = \begin{bmatrix}
1 & 0 & -xt & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & t & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & xt & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & -xt & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]
Chapter 5. Positive answer for $n \geq 4$.

$$P_{3,9} = P_{2,9}P_{1,9} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -2x & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$P_{4,9} = R_{2,9}P_{3,9}R_{2,9}P_{3,9} = \begin{bmatrix} 1 & 0 & -2x & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2x & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -2x & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Finally

$$U_{23,9}(-2t) = P_{4,9}P_{2,9}^{-2}.$$

For the $n \times n$ case these computations expand as follows:

$$P_{1,n} = \overline{P_{1,n-4}[0,4]} = \overline{R_{1,n-4}U_{24,n-4}(t)R_{1,n-4}[0,4]} = \overline{R_{1,n-4}[1,4] \cdot U_{24,n-4}(t)[0,4] \cdot R_{1,n-4}[1,4]}$$

$$P_{2,n} = \overline{P_{2,n-4}[0,5]} = \overline{R_{3,n-4}P_{1,n-4}R_{3,n-4}[0,5]} = \overline{R_{3,n-4}[2,5] \cdot P_{1,n-4}[0,5] \cdot R_{3,n-4}[2,5]}$$

$$P_{3,n} = \overline{P_{3,n-4}[0,5]} = \overline{P_{2,n-4}P_{1,n-4}[0,5]} = \overline{P_{2,n-4}[0,5] \cdot P_{1,n-4}[0,5]}$$

$$P_{4,n} = \overline{P_{4,n-4}[0,5]} = \overline{R_{2,n-4}P_{3,n-4}R_{2,n-4}[0,5]}$$

$$= \overline{R_{2,n-4}[0,5] \cdot P_{3,n-4}[0,5] \cdot R_{2,n-4}[0,5] \cdot P_{3,n-4}[0,5]}$$

Finally

$$U_{23,n}(-2t) = \overline{U_{23,n-4}[0,5]} = \overline{P_{4,n-4}P_{2,n-4}^{-2}[0,5]} = \overline{P_{4,n-4}[0,5] \cdot P_{2,n-4}[0,5]}^{-2}.$$
Chapter 5. Positive answer for \( n \geq 4 \).

This finishes substep a) of Step 3.

For substep b) we first obtain the “double transvection” \( Y = I + tE_{12} - tE_{n2} \), then through other “double transvections” we will obtain the transvection \( U_{12}(t) \) and then all transvections \( U_{12}(t) \).

The first part is achieved by the following computations:

\[
P_{1,9} = R_{1,9}U_{21,9} \left( \frac{1}{x} \right) R_{1,9} =
\begin{bmatrix}
2 & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{x} & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
-1 & -x & 0 & 0 & 0 & 0 & 0 & 0 & 1 
\end{bmatrix}
\]

\[
P_{2,9} = P_{1,9}U_{21,9} \left( \frac{-2}{x} \right) =
\begin{bmatrix}
0 & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{x} & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & -x & 0 & 0 & 0 & 0 & 0 & 0 & 1 
\end{bmatrix}
\]

\[
P_{3,9} = P_{3,9}U_{21,9} \left( \frac{-t}{2x^2} \right) P_{3,9} =
\begin{bmatrix}
-1 & -\frac{1}{2}t & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
2 & \frac{1}{2}t & 0 & 0 & 0 & 0 & 0 & 0 & 1 
\end{bmatrix}
\]
Chapter 5. Positive answer for $n \geq 4$.

Then

$$P_{4,9} = I + tE_{12} - tE_{92} = P_{3,9}^2.$$  

We easily expand these computations to the $n \times n$ case:

$$P_{1,n} = P_{1,n-4}[0,2] = R_{1,n-4}U_{21,n-4} \left( \frac{1}{x} \right) R_{1,n-4}[0,2]$$

$$= R_{1,n-4}[1,2] \cdot U_{21,n-4} \left( \frac{1}{x} \right)[0,2] \cdot R_{1,n-4}[1,2]$$

$$P_{2,n} = P_{2,n-4}[0,2] = P_{1,n-4}U_{21,n-4} \left( \frac{2}{x} \right)[0,2] = P_{1,n-4}[0,2] \cdot U_{21,n-4} \left( \frac{2}{x} \right)[0,2]$$

$$P_{3,n} = P_{3,n-4}[0,2] = P_{2,n-4}U_{21,n-4} \left( -\frac{t}{2x^2} \right) P_{2,n-4}[0,2]$$

$$= P_{2,n-4}[0,2] \cdot U_{21,n-4} \left( -\frac{t}{2x^2} \right)[0,2] \cdot P_{2,n-4}[0,2]$$

Then

$$P_{4,n} = I + tE_{12} - tE_{n2} = P_{4,n-4}[0,2] = P_{3,n-4}[0,2] = P_{3,n-4}[0,2]^2.$$  

In the subsequent computations we will refer to this $P_{4,n}$ as $T_n$.

We now obtain another involution using $t = x$ in $T_n$:

$$R_{4,n} = T_nR_{1,n}.$$  

To describe how it acts on the elementary matrices we state the following two lemmas which are analogues of lemmas 5.13-5.18. The proof again is trivial. For left multiplication by $R_{4,n}$ we have

**Lemma 5.21.** For any $1 \leq j \leq 4k + 1$

a) $R_{4,n}E_{1j} = E_{1j}$

b) $R_{4,n}E_{2j} = -E_{2j}$

c) $R_{1,n}E_{2l+1,j} = E_{2l+2,j},$ for $1 \leq l \leq 2k - 1$
Chapter 5. Positive answer for \( n \geq 4 \).

d) \( R_{i,n}E_{2l+2,j} = E_{2l+1,j} \), for \( 1 \leq l \leq 2k-1 \)

e) \( R_{i,n}E_{4k+1,j} = E_{4k+1,j} \)

And right multiplication by \( R_{4,n} \) is described by the following

**Lemma 5.22.** For any \( 1 \leq i \leq 4k+1 \)

a) \( E_{i1}R_{1,n} = E_{i1} \)

b) \( E_{i2}R_{1,n} = -E_{i2} \)

c) \( E_{i,2l+1}R_{1,n} = E_{i,2l+2}, \) for \( 1 \leq l \leq 2k-1 \)

d) \( E_{i,2l+2}R_{1,n} = E_{i,2l+1}, \) for \( 1 \leq l \leq 2k-1 \)

e) \( E_{i,4k+1}R_{1,n} = E_{i,4k+1} \)

Our next goal is to obtain all “double transvections” with non-zero off-diagonal entries at the spots \((1,2)\) and \((i,2)\) with \( 3 \leq i \leq 4k+1 \).

We demonstrate the computations that we will use by obtaining \( I + 2tE_{12} - tE_{32} \) and \( I - 2tE_{12} + tE_{72} \) in the case \( n = 9 \):

\[
P_{1,9} = (U_{23,9}(1)R_{3,9}T_{9})^2 = \begin{bmatrix}
1 & 2t & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & -t & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\] (5.35)
Chapter 5. Positive answer for \( n \geq 4 \).

\[
P_{2,9} = R_{4,9} P_{1,9} R_{4,9} = \\
\begin{bmatrix}
1 & -2t & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}
\]

(5.36)

Now we repeat computations 5.35–5.36 again starting with \( P_{2,9} \) instead of \( T_9 \), thus obtaining “double transvections” with non-zero entries at the spots (1,2) and (6,2) and also (1,2) and (5,2). In fact in general case we can repeat these computations to obtain “double transvections” all the way up to the spots (1,2) and (3,2) thanks to the following

Claim 5.23. Let \( T = I + \alpha E_{12} + \beta E_{2l+1,2} \) with \( 2 \leq l \leq 2k \).

Then \( (U_{23}(1)R_3T)^2 = I + 2\alpha E_{12} + \beta E_{2l,2} \) and \( R_4(I - 2\alpha E_{12} + \beta E_{2l,2})R_4 = I - 2\alpha E_{12} - \beta E_{2l-1,2} \)

Proof. Using lemmas 5.18 and 5.17 first compute

\[
(I + E_{23})R_3(I + \alpha E_{12} + \beta E_{2l+1,2}) \\
= (R_3 - E_{23})(I + \alpha E_{12} + \beta E_{2l+1,2}) \\
= R_3 - E_{23} + \alpha E_{12} + \beta E_{2l,2} - \beta E_{2l+1,2} \\
\]
Chapter 5. Positive answer for $n \geq 4$.

Now square it:

$$(R_3 - E_{23} + \alpha E_{12} + \beta E_{21,2} - \beta E_{21+1,2}) \cdot (R_3 - E_{23} + \alpha E_{12} + \beta E_{21,2} - \beta E_{21+1,2}) = I - E_{23} + \alpha E_{12} + \beta E_{21,2} - \beta(E_{21,2} - E_{21+1,2}) + E_{23} + \alpha(E_{12} + E_{13}) - \alpha E_{13} + \beta(E_{21,2} + E_{21,3}) - \beta E_{21,3} - \beta(E_{21+1,2} + E_{21+1,3}) + \beta E_{21+1,3} = I + 2\alpha E_{12} + \beta E_{21,2}$$

(5.38)

Also by lemmas 5.21 and 5.22

$$R_4(I + 2\alpha E_{12} + \beta E_{21,2})R_4 = I + 2\alpha E_{12}R_4 + \beta E_{21-1,2}R_4 = I - 2\alpha E_{12} - \beta E_{21-1,2}$$

(5.39)

From this claim it follows that starting with the previously obtained $T_n = I + tE_{12} - tE_{4k+1,2}$ we obtain after $2k - 1$ repetitions of the computations 5.35–5.36 a “double transvection” $I + 2^{2k-1} tE_{12} + tE_{32}$ along with all intermediate “double transvections”. We are finally ready to obtain all transvections $U_{12}(t)$. For $n = 9$:

$$U_{12}(-16t) = (U_{23}(1) R_3(I + 8tE_{12} + tE_{23}))^2 =$$

$$= \begin{bmatrix}
1 & -16t & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}$$

(5.40)
Chapter 5. Positive answer for $n \geq 4$.

And we extend computation 5.40 to an arbitrary $n$ by

$$U_{12,n}(-2^{2k}t) = U_{12,n-4}(-2^{2k}t)[0,3]$$

$$= (U_{23,n-4}(1)R_3(I + 2^{2k-1}tE_{12,n-4} + tE_{23,n-4}))^2[0,3]$$

$$= (U_{23,n-4}(1)R_3(I + 2^{2k-1}tE_{12,n-4} + tE_{23,n-4}))[0,3]^2$$

$$= \left( U_{23,n-4}(1)[0,3] \cdot R_{3,n-4}[2,3] \cdot (I + 2^{2k-1}tE_{12,n-4} + tE_{23,n-4})[0,3] \right)^2$$

(5.41)

Now to complete substep b) of Step 3 we note that we can obtain all transvections in the second row by just multiplying the “double transvections” previously obtained by an appropriate transvection $U_{12}(-2^l t)$.

Finally to finish Step 3 and thus the proof of the proposition we refer to computation 5.21. □

5.5 Case of $(4k + 3) \times (4k + 3)$ matrices.

In this section we deal with the case $n = 4k + 3$, $k \geq 1$. This case is almost an exact copy of the previous case ($n = 4k + 1$, $k \geq 2$). In fact all computations stay the same with the results differing by plus or minus sign here and there, which will not affect the argument.

We will use the Bar Operation (see Definition 5.2) to increase the size of the matrices inductively and we will use lemma 5.3 to verify that the same computations yield the same results for all sizes.

Precisely we want to prove the following

**Proposition 5.24.** Let

$$R_1 = \begin{bmatrix} -1 & x & 0 \\ 0 & 1 & 0 \\ 0 & -x & -1 \end{bmatrix}, \quad R_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad \text{and} \quad R_3 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 1 \end{bmatrix},$$

where $x$ is such that $-x$ is a primitive root in $GF(q)$. Define inductively:

$$R_{1,3} = R_1, \quad R_{2,3} = R_2, \quad R_{3,3} = R_3$$

and

$$R_{1,n} = R_{1,n-4}[1,2], \quad R_{2,n} = R_{2,n-4}[0,2], \quad R_{3,n} = R_{3,n-4}[3,3], \quad \text{for } n = 4k + 3, \ k \geq 1.$$
Chapter 5. Positive answer for \( n \geq 4 \).

Then \( SL_n(q) = \langle R_{1,n}, R_{2,n}, R_{3,n} \rangle \).

As in all previous cases we have an immediate

**Corollary 5.25.** \( PSL_{4k+3}(q), \ k \geq 2 \) can be generated by three involutions two of which commute.

**Proof.** This follows immediately from the previous proposition, easy computations to check that \( R_1, R_2, R_3 \) and \( R_1R_2 \) are indeed involutions and lemma 5.3

In essence the proof of proposition 5.24 follows from the following (trivial) key observation and lemma 5.3,

**Lemma 5.26.**

\[
\begin{align*}
\text{a) } & R_{1,n} = R_{1,n-4}[1,2j], & 1 \leq j \leq 2k-1, \\
\text{b) } & R_{2,n} = R_{2,n-4}[0,j], & 2 \leq j \leq 4k-2, \\
\text{c) } & R_{3,n} = R_{3,n-4}[3,2j+1], & 0 \leq j \leq 2k-1.
\end{align*}
\]

The comments to lemma 5.12 also apply here.

See Appendix D for the Maple V input file to verify computations.

The following three lemmas describe how the generators \( R_{1,n}, R_{2,n}, R_{3,n} \) act on elementary matrices \( E_{ij} \). (These lemmas can also be regarded as an alternate definition for \( R_{1,n}, R_{2,n}, R_{3,n} \).) The proofs are elementary.

Left multiplication by the first generator is described by the following

**Lemma 5.27.** For any \( 1 \leq j \leq 4k + 3 \)

\[
\begin{align*}
\text{a) } & R_{1,n}E_{1j} = -E_{1j} \\
\text{b) } & R_{1,n}E_{2j} = xE_{1j} + E_{2j} - xE_{4k+3,j}
\end{align*}
\]
Chapter 5. Positive answer for $n \geq 4$.

  c) $R_{1,n}E_{2l+1,j} = E_{2l+2,j}$, for $1 \leq l \leq 2k$

  d) $R_{1,n}E_{2l+2,j} = E_{2l+1,j}$, for $1 \leq l \leq 2k$

  e) $R_{1,n}E_{4k+3,j} = -E_{4k+3,j}$

Right multiplication by the first generator is described by the following

**Lemma 5.28.** For any $1 \leq i \leq 4k + 3$

  a) $E_{i1}R_{1,n} = -E_{i1} + xE_{i2}$

  b) $E_{i2}R_{1,n} = E_{i2}$

  c) $E_{i,2l+1}R_{1,n} = E_{i,2l+2}$, for $1 \leq l \leq 2k$

  d) $E_{i,2l+2}R_{1,n} = E_{i,2l+1}$, for $1 \leq l \leq 2k$

  e) $E_{i,4k+3}R_{1,n} = -E_{i,4k+3} - xE_{i2}$

Similarly left multiplication by the second generator is described by the following

**Lemma 5.29.** For any $1 \leq j \leq 4k + 3$

  a) $R_{2,n}E_{1j} = E_{4k+3,j}$

  b) $R_{2,n}E_{2j} = -E_{2j}$

  c) $R_{2,n}E_{ij} = E_{ij}$, for $3 \leq i \leq 4k + 2$

  d) $R_{2,n}E_{4k+3,j} = E_{1j}$

And right multiplication by the second generator is described by the following

**Lemma 5.30.** For any $1 \leq i \leq 4k + 3$

  a) $E_{i1}R_{2,n} = E_{i,4k+3}$

  b) $E_{i2}R_{2,n} = -E_{i2}$

57
Chapter 5. Positive answer for $n \geq 4$.

c) $E_{ij}R_{2,n} = E_{ij}$, for $3 \leq i \leq 4k + 2$

d) $E_{i,4k+3}R_{2,n} = E_{i1}$

Finally left multiplication by the third generator is described by the following

Lemma 5.31. For any $1 \leq j \leq 4k + 3$

a) $R_{3,n}E_{1j} = -E_{1j}$

b) $R_{3,n}E_{2l,j} = -E_{2l,j}$, for $1 \leq l \leq 2k + 1$

c) $R_{3,n}E_{2l+1,j} = E_{2l,j} + E_{2l+1,j}$, for $1 \leq l \leq 2k + 1$

And right multiplication by the third generator is described by the following

Lemma 5.32. For any $1 \leq i \leq 4k + 3$

a) $E_{i1}R_{3,n} = E_{i1}$

b) $E_{i,2l}R_{3,n} = -E_{i,2l} + E_{i,2l+1}$, for $1 \leq l \leq 2k + 1$

c) $E_{i,2l+1}R_{3,n} = E_{i,2l+1}$, for $1 \leq l \leq 2k + 1$

Now we are ready to prove proposition 5.24.

Proof of proposition 5.24. The steps in this case are exactly the same as in case $n = 4k + 1$.

Step 1 will be very easy and we'll obtain $U_{23}(1)$.

To complete Step 2 we will first obtain $U_{24}(1)$ and then all $U_{24}(t)$, $t \in GF(q)$. We will do it by first obtaining $U_{2j}(1)$ for $4 \leq j \leq 4k + 1$, then having obtained $U_{2,4k+1}(1)$ we will use it to finish Step 2 by obtaining all $U_{24}(t)$ with $t \in GF(q)$.

Step 3 will consist of three following substeps:

a) Obtain all $U_{2j}(t)$
Chapter 5. Positive answer for \( n \geq 4 \).

b) Obtain all \( U_{i2}(t) \)

c) Obtain all \( U_{ij}(t) \)

For Step 1 we compute:

\[
U_{23,7}(-4) = (R_{2,7}R_{3,7})^4 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -4 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}
\] (5.42)

and note that \( R_{2,n} = \overline{R_{2,n-4}[0,3]} \) by lemma 5.26, hence by lemma 5.3 and computation 5.42 we have

\[
U_{23,n}(-4) = U_{23,n-4}(-4)[0,3] = (R_{2,n-4}[0,3] \cdot \overline{R_{3,n-4}[3,3]})^4.
\]

Note that we are not able to start the computation from \( n = 3 \) since \( R_{2,7} \neq \overline{R_{2,3}[0,3]} \). But for all higher sizes we have just obtained all transvections \( U_{23,n}(l) \), where \( l \) is an integer.

We now proceed with Step 2. First we obtain \( U_{24,n}(l) \) and \( U_{25,n}(l) \) with \( l \) an integer. For the base of the induction \( (n = 7) \) we make the following computations:

\[
P_{1,7} = R_{1,7}U_{23,7}(1)R_{1,7} = \begin{bmatrix}
1 & 0 & 0 & x & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & -x & 0 & 1 \\
\end{bmatrix}
\] (5.43)

\[
P_{2,7} = R_{3,7}P_{1,7}R_{3,7} = \begin{bmatrix}
1 & 0 & 0 & x & -x & 0 \\
0 & 1 & 0 & 1 & -1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & x & -x & 1 \\
0 & 0 & 0 & x & -x & 0 \\
\end{bmatrix}
\] (5.44)
Chapter 5. Positive answer for $n \geq 4$.

\[
P_{3,7} = R_{2,7} P_{2,7} R_{2,7}^{-1} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & -2 & 2 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\] (5.45)

and finally

\[
U_{24,7}(-2) = R_{3,7} P_{3,7} R_{3,7} \quad \text{and} \quad (5.46)
\]
\[
U_{25,7}(2) = U_{24,7}(2) P_{3,7}
\] (5.47)

In sizes higher than 7 we will repeat computations 5.43-5.47 starting with $U_{25}(1)$ instead of $U_{23}(1)$ to obtain $U_{26}(2)$ and $U_{27}(2)$. In fact the same computations will work successively in the $n \times n$ case and we will obtain all transvections in the second row but the last two. (In the $7 \times 7$ case we’ve already done so). In other words in the $n \times n$ case we can obtain all $U_{23}(1)$ for $3 \leq j \leq 4k + 1$ thanks to the following

**Claim 5.33.** Let $1 \leq l \leq 2k - 1$.

Set $P_1 = R_{1,n} U_{2,2l+1}(\xi) R_{1,n}$, $P_2 = R_{3,n} P_1 R_{3,n}$, $P_3 = R_{2,n} P_2 R_{2,n} P_2^{-1}$. Then

a) $U_{2,2l+2}(-2\xi) = R_{3,n} P_3 R_{3,n}$

b) $U_{2,2l+3}(2\xi) = U_{2,2l+2}(2\xi) P_3$

**Proof.** Since $U_{2,2l+1}(\xi) = I + \xi E_{2,2l+1}$ we have by lemmas 5.27 and 5.28

\[
P_1 = I + R_{1,n} \xi E_{2,2l+1} R_{1,n} = I + \xi(\xi E_{1,2l+1} + E_{2,2l+1} - \xi E_{4k+3,2l+1}) R_{1,n}
\]

\[
= I + \xi \xi E_{1,2l+2} + \xi E_{2,2l+2} - \xi E_{4k+3,2l+2}
\]

Now by lemmas 5.31 and 5.32 we have

\[
P_2 = R_{3,n} P_1 R_{3,n} = R_{3,n}(I + \xi E_{1,2l+2} + \xi E_{2,2l+2} - \xi E_{4k+3,2l+2}) R_{3,n}
\]

\[
= I - \xi \xi E_{1,2l+2} R_{3,n} - \xi E_{2,2l+2} R_{3,n} - \xi(\xi E_{4k+2,2l+2} + E_{4k+3,2l+2}) R_{3,n}
\]

\[
= I + \xi E_{1,2l+2} - \xi(\xi E_{1,2l+3} + \xi E_{2,2l+2} - \xi E_{2,2l+3} + \xi E_{4k+2,2l+2}
\]

\[
- \xi E_{4k+2,2l+3} + \xi E_{4k+3,2l+2} - \xi E_{4k+3,2l+3}
\]

60
Chapter 5. Positive answer for \( n \geq 4 \).

Now write \( P_2 = I + Q \). Then since \( 2l + 2 > 2 \) and \( 2l + 3 \leq 2(2k - 1) + 3 = 4k + 1 < 4k + 2 \), \( Q^2 = 0 \) as every product of elementary matrices involved is equal to 0. Hence \( P_2^{-1} = I - Q \).

Also by lemmas 5.29 and 5.30 we have

\[
R_{2,n}P_2R_{2,n} = R_{2,n}(I + \xi x E_{1,2l+2} - \xi x E_{1,2l+3} + \xi E_{2,2l+2} - \xi E_{2,2l+3} \\
+ \xi x E_{4k+2,2l+2} - \xi x E_{4k+2,2l+3} + \xi x E_{4k+3,2l+2} - \xi x E_{4k+3,2l+3})R_{2,n} \\
= I + \xi(x E_{4k+3,2l+2} - x E_{4k+3,2l+3} - E_{2,2l+2} + E_{2,2l+3} \\
+ x E_{4k+3,2l+2} - x E_{4k+3,2l+3} + x E_{1,2l+2} - x E_{1,2l+3})R_{2,n} \\
= I + \xi(x E_{4k+3,2l+2} - x E_{4k+3,2l+3} - E_{2,2l+2} + E_{2,2l+3} \\
+ x E_{4k+3,2l+2} - x E_{4k+3,2l+3} + x E_{1,2l+2} - x E_{1,2l+3}) \\
= I + Q'
\]

Again all the products of elementary matrices in the product of \( Q \) and \( Q' \) are 0. Hence

\[
P_3 = R_{2,n}P_2R_{2,n}P_2^{-1} = (I + Q')(I - Q) = I + Q' - Q = I - 2\xi E_{2,2l+2} + 2\xi E_{2l+3}
\]

Finally by lemmas 5.31 and 5.32

\[
R_{3,n}P_3R_{3,n} = R_{3,n}(I - 2\xi E_{2,2l+2} + 2\xi E_{2,2l+3})R_{3,n} = I + \xi(2E_{2,2l+2} - 2E_{2,2l+3})R_{3,n} \\
= I - 2\xi E_{2,2l+2} + 2\xi E_{2,2l+3} - 2\xi E_{2,2l+3} = U_{2,2l+2}(-2\xi)
\]

and

\[
U_{2,2l+2}(2\xi)P_3 = (I + 2\xi E_{2,2l+2})(I - 2\xi E_{2,2l+2} + 2\xi E_{2,2l+3}) \\
= I - 2\xi E_{2,2l+2} + 2\xi E_{2,2l+3} + 2\xi E_{2,2l+2} = U_{2,2l+3}(2\xi)
\]

and the claim is proved. \( \square \)

Therefore, using the claim with \( \xi = 1 \) we successively obtain \( U_{2j}(l) \), where \( l \) is an integer and \( 3 \leq j \leq 4k + 1 \).

To finish Step 2 we need to produce \( U_{24}(t) \) for all \( t \in \text{GF}(q) \). The computations are exactly the same as in the \((4k + 1) \times (4k + 1)\) case (5.20–5.29). More precisely:
Chapter 5. Positive answer for \( n \geq 4 \).

Claim 5.34. Let

\[
P_1 = R_{1,n}U_{24}(\xi)R_{1,n} \quad P_2 = R_{3,n}P_1R_{3,n} \quad P_3 = R_{1,n}P_2R_{1,n}.
\]

Then \( U_{24}(-x\xi) = P_3^{-1}U_{2,4k+1}(1)P_3U_{2,4k+1}(-1) \).

Proof. We compute these matrices in the case \( n = 7 \) and then use lemma 5.3 to prove the claim for all \( n = 4k + 3 \).

\[
P_{1,7} = R_{1,7}U_{24,7}(\xi)R_{1,7} = \begin{bmatrix}
1 & 0 & x\xi & 0 & 0 & 0 & 0 \\
0 & 1 & \xi & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & -x\xi & 0 & 0 & 0 & 1 \\
0 & 0 & -x\xi & 0 & 0 & 0 & 1
\end{bmatrix}
\]

(5.48)

\[
P_{2,7} = R_{3,7}P_{1,7}R_{3,7} = \begin{bmatrix}
1 & 0 & -x\xi & 0 & 0 & 0 & 0 \\
0 & 1 & -\xi & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & -x\xi & 0 & 0 & 1 & 0 \\
0 & 0 & -x\xi & 0 & 0 & 0 & 1
\end{bmatrix}
\]

(5.49)

\[
P_{3,7} = R_{1,7}P_{2,7}R_{1,7} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & -\xi & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & -x\xi & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 2x\xi & 0 & 0 & 1
\end{bmatrix}
\]

(5.50)

Finally,

\[
U_{24,7}(-x\xi) = P_{3,7}^{-1}U_{25,7}(1)P_{3,7}U_{25,7}(-1).
\]

For the bigger sizes we notice that \( U_{24,n}(\xi) = U_{24,n-4}[0,4] \). Therefore by lemmas 5.3 and 5.26 we have

\[
P_{1,n} = P_{1,n-4}[0,4] = R_{1,n-4}U_{24,n-4}(\xi)R_{1,n-4}[0,4] = R_{1,n-4}[1,4] \cdot U_{24,n-4}(\xi)[0,4] \cdot R_{1,n-4}[1,4]
\]

(5.51)
Chapter 5. Positive answer for \( n \geq 4 \).

Observe that \( P_{1,n} \) can also be regarded as \( P_{1,n-4}[0,5] \). Hence by lemmas 5.3 and 5.26

\[
P_{2,n} = P_{2,n-4}[0,5] = R_{3,n-4}P_{1,n-4}R_{3,n-4}[0,5] = R_{3,n-4}[3,5] \cdot P_{1,n-4}[0,5] \cdot R_{3,n-4}[3,5]
\]  

(5.52)

Regarding \( P_{2,n} \) as \( P_{2,n-4}[0,4] \) we have

\[
P_{3,n} = P_{3,n-4}[0,4] = R_{1,n-4}P_{2,n-4}R_{1,n-4}[0,4] = R_{1,n-4}[1,4] \cdot P_{2,n-4}[0,4] \cdot R_{1,n-4}[1,4]
\]  

(5.53)

Finally we regard \( U_{(2,4k+1),n}^{(1)} \) as \( U_{(2,4k-3),n-4}^{(1)}[0,4] \) and we obtain

\[
U_{24,n}(-x \xi) = U_{24,n-4}(-x \xi)[0,4] = P_{3,n-4}^{-1}U_{(2,4k-3),n-4}^{(1)}P_{3,n-4}U_{(2,4k-3),n-4}^{(-1)}[0,4]
\]

\[
= P_{3,n-4}[0,4] \cdot U_{(2,4k-3),n-4}^{(1)}[0,4] \cdot P_{3,n-4}[0,4] \cdot U_{(2,4k-3),n-4}^{(-1)}[0,4]
\]  

(5.54)

And the claim is proved.

Therefore starting with \( U_{24}^{(1)} \) we can successively obtain all \( U_{24}^{((-x)^l)} \) for any integer \( l \). Hence if \(-x\) is a primitive root in GF\((q)\) we obtain all \( U_{24}^{(t)} \) for any \( t \in GF(q) \), thus completing Step 2.

For substep a) of Step 3 we first obtain \( U_{25}^{(-t)} \):

\[
U_{25,7}(-t) = R_{3,7}U_{24,7}(t)R_{3,7}U_{24,7}(-t)
\]  

(5.55)

and

\[
U_{25,n}(-t) = U_{25,n-4}(-t)[0,5] = R_{3,n-4}U_{24,n-4}(-t)\cdot 3,n-4U_{24,n-4}(-t)[0,5]
\]

\[
= R_{3,n-4}[3,5] \cdot U_{24,n-4}(t)[0,5] \cdot R_{3,n-4}[3,5] \cdot U_{24,n-4}(-t)[0,5]
\]

(5.56)

Now use claim 5.33 with \( \xi = t \) to obtain successively all \( U_{2j}(t) \) with \( 5 \leq j \leq 4k + 1 \).

We have previously obtained \( U_{23}^{(1)} \) but not \( U_{23}^{(t)} \). We now do just that using the matrix \( P_2 \) from Claim 5.34 (see computation 5.49):

\[
U_{23,7}(2 \xi) = R_{2,7}P_{2,7}R_{2,7}P_{2,7}^{(-1)} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2\xi & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]  

(5.56)
Chapter 5. Positive answer for \( n \geq 4 \).

Hence setting \( \xi = t \) we have all \( U_{23,7}(t) \). Now we expand computation 5.56 using the Bar Operation:

\[
U_{23,n}(2\xi) = U_{23,n-4}(2\xi)[0,4] = R_{2,7}P_{2,7}R_{2,7}P_{2,7}^{-1}[0,4]
\]

\[
= R_{2,7}[0,4] \cdot P_{2,7}[0,4] \cdot R_{2,7}[0,4] \cdot P_{2,7}^{-1}[0,4]
\]

To obtain \( U_{2,4k+2}(t) \) and \( U_{2,4k+3}(t) \) we make the following computations (first we do them for \( n = 7 \)):

\[
P_{1,7} = R_{1,7}U_{23,7}(t)R_{1,7} = \begin{bmatrix}
1 & 0 & 0 & xt & 0 & 0 & 0 \\
0 & 1 & 0 & t & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & -xt & 0 & 0 & 1
\end{bmatrix}
\]

\[
P_{2,7} = R_{3,7}P_{1,7}R_{3,7} = \begin{bmatrix}
1 & 0 & 0 & xt & -xt & 0 & 0 \\
0 & 1 & 0 & t & -t & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & xt & -xt & 1 & 0 \\
0 & 0 & 0 & xt & -xt & 0 & 1
\end{bmatrix}
\]

\[
P_{3,7} = R_{1,7}P_{2,7}R_{1,7} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & t & 0 & 0 & -t & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & xt & 0 & 1 & -xt & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & -2xt & 0 & 0 & 2xt & 1
\end{bmatrix}
\]

\[
P_{4,7} = U_{25,7}(-1)P_{3,7}U_{25,7}(1)P_{3,7}^{-1} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -xt & 0 & 0 & xt & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]
Chapter 5. Positive answer for \( n \geq 4 \).

Finally

\[ U_{26,7}(t x) = U_{23,7}(t x)P_{4,7} \]

and

\[ U_{27,7}(-t x) = R_{3,7}U_{26,7}(-t x)R_{3,7}U_{26,7}(t x) \]

As \( t \) runs through all elements of \( \text{GF}(q) \) so does \(-t x\), hence we have just obtained all \( U_{26}(t) \) and \( U_{27}(t) \) with \( t \in \text{GF}(q) \) for \( n = 7 \).

By lemmas 5.3 and 5.26 we have

\[ P_{1,n} = P_{1,n-4}[0,2] = R_{1,n-4}U_{(2,4k-5),n-4}(t)R_{1,n-4}[0,2] \]
\[ = R_{1,n-4}[1,2] \cdot U_{(2,4k-5),n-4}[0,2] \cdot R_{1,n-4}[1,2], \]
\[ P_{2,n} = P_{2,n-4}[0,3] = R_{3,n-4}P_{1,n-4}R_{3,n-4}[0,3] = R_{3,n-4}[3,3] \cdot P_{1,n-4}[0,3] \cdot R_{3,n-4}[3,3], \]
\[ P_{3,n} = P_{3,n-4}[0,2] = R_{1,n-4}P_{2,n-4}R_{1,n-4}[0,2] = R_{1,n-4}[1,2] \cdot P_{2,n-4}[0,2] \cdot R_{1,n-4}[1,2], \]
\[ P_{4,n} = P_{4,n-4}[0,2] = U_{(2,4k-3),n-4}(1)P_{3,n-4}U_{(2,4k-3),n-4}(-1)P_{3,n-4}^{-1}[0,2] \]
\[ = U_{(2,4k-3),n-4}(1)[0,2] \cdot P_{3,n-4}[0,2] \cdot U_{(2,4k-3),n-4}(-1)[0,2] \cdot P_{3,n-4}^{-1}[0,2] \]

Hence

\[ U_{(2,4k+2),n}(t x) = U_{(2,4k-2),n-4}(t x)[0,2] = U_{(2,4k-5),n-4}(t x)P_{4,7}[0,2] \]
\[ = U_{(2,4k-5),n-4}(t x)[0,2] \cdot P_{4,7}[0,2] \]

and

\[ U_{(2,4k+3),n}(t) = U_{(2,4k-1),n-4}(t)[0,3] = R_{3,n-4}U_{(2,4k+2),n-4}(t)R_{3,n-4}U_{(2,4k+2),n-4}(-t)[0,3] \]
\[ = R_{3,n-4}[2,3] \cdot U_{(2,4k+2),n-4}(t)[0,3] \cdot R_{3,n-4}[2,3] \cdot U_{(2,4k+2),n-4}(-t)[0,3] \]

To finish substep a) of Step 3 we only need to obtain \( U_{21}(t) \). This is achieved by an easy computation using lemmas 5.29 and 5.30:

\[ R_{2,n}U_{2,4k+3}(-t)R_{2,n} = R_{2,n}(I - tE_{2,4k+3})R_{2,n} = I + tE_{2,4k+3}R_{2,n} = I + tE_{21} = U_{21}(t). \]
Chapter 5. Positive answer for \( n \geq 4 \).

This finishes substep a) of Step 3.

For substep b) we first obtain the "double transvection" \( Y = I + tE_{12} - tE_{n2} \), then through other "double transvections" we will obtain the transvection \( U_{12}(t) \) and then all transvections \( U_{i2}(t) \).

The first part is achieved by the following computations:

\[
P_{1,7} = R_{1,7}U_{21,7}\left( \frac{1}{x} \right) R_{1,7} = \begin{bmatrix} 2 & -x & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ x & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & x & 0 & 0 & 0 & 1 \end{bmatrix}
\]

\[
P_{2,7} = P_{1,7}U_{21,7}\left( \frac{2}{x} \right) = \begin{bmatrix} 0 & -x & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ x & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & x & 0 & 0 & 0 & 1 \end{bmatrix}
\]

\[
P_{3,7} = P_{2,7}U_{21,7}\left( -\frac{t}{2x^2} \right) P_{2,7} = \begin{bmatrix} -1 & -\frac{1}{2}t & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 2 & \frac{1}{2}t & 0 & 0 & 0 & 1 \end{bmatrix}
\]

Then

\[
P_{4,7} = I + tE_{12} - tE_{72} = P_{3,7}^2.
\]
Chapter 5. Positive answer for \( n \geq 4 \).

We easily expand these computations to the \( n \times n \) case:

\[
P_{1,n} = R_{1,n-4}[0,2] = R_{1,n-4}U_{21,n-4}\left\{\frac{1}{x}\right\}R_{1,n-4}[0,2]
\]
\[
= R_{1,n-4}[1,2] \cdot U_{21,n-4}\left\{\frac{1}{x}\right\}[0,2] \cdot R_{1,n-4}[1,2]
\]

\[
P_{2,n} = P_{2,n-4}[0,2] = P_{1,n-4}U_{21,n-4}\left\{\frac{2}{x}\right\}[0,2] = P_{1,n-4}[0,2] \cdot U_{21,n-4}\left\{\frac{2}{x}\right\}[0,2]
\]

\[
P_{3,n} = P_{3,n-4}[0,2] = P_{2,n-4}U_{21,n-4}\left\{-\frac{t}{2x^2}\right\}P_{2,n-4}[0,2]
\]
\[
= P_{2,n-4}[0,2] \cdot U_{21,n-4}\left\{-\frac{t}{2x^2}\right\}[0,2] \cdot P_{2,n-4}[0,2]
\]

Then

\[
I + tE_{12} - tE_{n2} = P_{4,n-4}[0,2] = P_{3,n-4}[0,2] = P_{3,n-4}[0,2]^2.
\]

We will call this matrix \( T_n \).

We now obtain another involution using \( t = -x \) in \( T_n \):

\[
R_{4,n} = T_nR_{1,n}.
\]

To describe how it acts on the elementary matrices we state the following two lemmas which are analogues of lemmas 5.27–5.32. The proof again is trivial. For left multiplication by \( R_{4,n} \) we have

**Lemma 5.35.** For any \( 1 \leq j \leq 4k + 3 \)

a) \( R_{4,n}E_{1j} = -E_{1j} \)

b) \( R_{4,n}E_{2j} = E_{2j} \)

c) \( R_{4,n}E_{2l+1,j} = E_{2l+2,j}, \) for \( 1 \leq l \leq 2k \)

d) \( R_{4,n}E_{2l+2,j} = E_{2l+1,2}, \) for \( 1 \leq l \leq 2k \)

e) \( R_{4,n}E_{4k+3,j} = E_{4k+3,j} \)
Chapter 5. Positive answer for \( n \geq 4 \).

And right multiplication by \( R_{4,n} \) is described by the following

**Lemma 5.36.** For any \( 1 \leq i \leq 4k + 3 \)

\[ a) \ E_{i1}R_{4,n} = -E_{i1} \]

\[ b) \ E_{i2}R_{4,n} = E_{i2} \]

\[ c) \ E_{i,2l+1}R_{4,n} = E_{i,2l+2}, \ for \ 1 \leq l \leq 2k \]

\[ d) \ E_{i,2l+2}R_{4,n} = E_{i,2l+1}, \ for \ 1 \leq l \leq 2k \]

\[ e) \ E_{i,4k+3}R_{4,n} = -E_{i,4k+3} \]

Our next goal is to obtain all “double transvections” with non-zero off-diagonal entries at the spots (1,2) and (i,2) with \( 3 \leq i \leq 4k + 3 \).

We demonstrate the computations that we will use by obtaining \( I + 2tE_{12} + tE_{52} \) and \( I - 2tE_{12} + tE_{52} \) in the case \( n = 7 \):

\[
P_{1,7} = (U_{23,7}(-1)R_{3,7}T_7)^2 = \begin{bmatrix} 1 & 2t & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (5.57)
\]

\[
P_{2,7} = R_{4,7}P_{1,7}R_{4,7} = \begin{bmatrix} 1 & -2t & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & t & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad (5.58)
\]

Now we repeat computations 5.57–5.58 again starting with \( P_{2,7} \) instead of \( T_7 \), thus obtaining “double transvections” with non-zero entries at the spots (1,2) and (4,2) as well as (1,2) and (3,2). In fact, in the general case we can repeat these computations to obtain “double transvections” all the way up to the spots (1,2) and (3,2) thanks to the following.
Chapter 5. Positive answer for $n \geq 4$.

Claim 5.37. Let $T = I + \alpha E_{12} + \beta E_{2l+1,2}$ with $2 \leq l \leq 2k + 1$.

Then $(U_{23}(-1)R_3T)^2 = I + 2\alpha E_{12} - \beta E_{2l,2}$ and $R_4(I + 2\alpha E_{12} - \beta E_{2l,2})R_4 = I - 2\alpha E_{12} - \beta E_{2l-1,2}$

Proof. Using lemmas 5.32 and 5.31 first compute

$$
(I - E_{23})R_3(I + \alpha E_{12} + \beta E_{2l+1,2}) = (R_3 - E_{23})(I + \alpha E_{12} + \beta E_{2l+1,2})
$$

$$
= R_3 - E_{23}
$$

$$
- \alpha E_{12}
$$

$$
+ \beta E_{2l,2} + \beta E_{2l+1,2}
$$

(5.59)

Now square it:

$$
(R_3 - E_{23} - \alpha E_{12} + \beta E_{2l,2} + \beta E_{2l+1,2}) \cdot (R_3 - E_{23} - \alpha E_{12} + \beta E_{2l,2} + \beta E_{2l+1,2})
$$

$$
= I + E_{23} + \alpha E_{12} - \beta E_{2l,2} + \beta(E_{2l,2} + E_{2l+1,2})
$$

$$
- E_{23}
$$

$$
- \alpha(-E_{12} + E_{13}) + \alpha E_{13}
$$

$$
+ \beta(-E_{2l,2} + E_{2l,3}) - \beta E_{2l,3}
$$

$$
+ \beta(-E_{2l+1,2} + E_{2l+1,3}) - \beta E_{2l+1,3}
$$

$$
= I + 2\alpha E_{12} - \beta E_{2l,2}
$$

(5.60)

Also by lemmas 5.35 and 5.36

$$
R_4(I + 2\alpha E_{12} - \beta E_{2l,2})R_4 = I - 2\alpha E_{12}R_4 - \beta E_{2l-1,2}R_4 = I - 2\alpha E_{12} - \beta E_{2l-1,2}
$$

(5.61)

From this claim it follows that starting with the previously obtained $T_n = I + tE_{12} - tE_{4k+3,2}$ we obtain after $2k$ repetitions of the computations 5.57–5.58 a “double transvection" $I + 2^ktE_{12} - tE_{32}$ along with all intermediate “double transvections". We are finally ready to obtain all
transvections $U_{12}(t)$. For $n = 7$:

$$U_{12}(8t) = (U_{23}(-1)R_3(I + 4tE_{12} + tE_{23}))^2 = \begin{bmatrix}
1 & 8t & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}$$

And we extend computation 5.62 to an arbitrary $n$ by

$$U_{12,n}(2^{2k+1}t) = U_{12,n-4}(2^{2k+1}t)[0,3]
= (U_{23,n-4}(-1)R_3(I + 2^{2k}tE_{12,n-4} - tE_{23,n-4}))^2[0,3]
= (U_{23,n-4}(-1)R_3(I + 2^{2k}tE_{12,n-4} - tE_{23,n-4}))^2[0,3]^2
= \left(U_{23,n-4}(-1)[0,3] \cdot R_{3,n-4}[3,3] \cdot (I + 2^{2k}tE_{12,n-4} - tE_{23,n-4})[0,3]\right)^2
$$

Now to complete substep b) of Step 3 we note that we can obtain all transvections in the second column by just multiplying “double transvections” previously obtained by an appropriate transvection $U_{12}(-2^t t)$.

Finally to finish Step 3 and thus the proof of the proposition we refer to computation 5.21. □

5.6 Case of $4k \times 4k$ matrices.

In this section we prove the possibility of generation of $PSl_{4k}(q)$ with $k \geq 2$.

Precisely we prove

**Proposition 5.38.** Let

$$R_1 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
[x] & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
\end{bmatrix}, \quad R_2 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
\end{bmatrix}, \quad \text{and}
$$
Chapter 5. Positive answer for \( n \geq 4 \).

\[
R_3 = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{bmatrix},
\]

where \( x \) is a primitive root in \( GF(q) \). Define inductively:

\[
R_{1,8} = R_1, \quad R_{2,8} = R_2, \quad R_{3,8} = R_3
\]

and

\[
R_{1,n} = R_{1,n-4}[0,2], \quad R_{2,n} = R_{1,n-4}[1,1], \quad R_{1,n} = R_{1,n-4}[1,0], \quad \text{for } n = 4k, \ k \geq 3.
\]

Then \( SL_n(q) = \langle R_{1,n}, R_{2,n}, R_{3,n} \rangle \).

An immediate corollary of this proposition is

**Corollary 5.39.** \( PSL_{4k}(q), k \geq 2 \) can be generated by three involutions two of which commute.

The proof is a routine check that the matrices are indeed involutions and that the first two commute (this is done exactly the same way as in corollaries 5.11 and 5.25)

Before starting the proof of Proposition 5.38 we, as in earlier cases, observe the following trivial facts:

**Lemma 5.40.**

\[a) \ R_{1,n} = R_{1,n-4}[0,j], \quad 0 \leq j \leq 4k - 7, \]
\[b) \ R_{2,n} = R_{2,n-4}[1,2j + 1], \quad 0 \leq j \leq 2k - 4, \]
\[c) \ R_{3,n} = R_{3,n-4}[1,2j], \quad 0 \leq j \leq 2k - 3. \]

The proof of Proposition 5.38 contains far fewer matrix computations than the proofs of propositions 5.10 and 5.24. Mostly we deal with permutation matrices and thus have to do only
Chapter 5. Positive answer for $n \geq 4$.

much simpler permutation computations. We also provide diagrams to help with some of the computations.

In Appendix E though we provide the full Maple V input files including even those simple but crucial computations.

Proof of Proposition 5.38. We are going to complete the same Steps described in Section 5.1.

Step 1 is relatively easy (especially when characteristic $p$ does not divide $4k - 2$). In fact this is the only step in the proof that involves heavy matrix computations similar to those in Sections 5.2–5.5. We obtain $U_{4k-1,2}(x)$ during this step.

Step 2 is also quite simple and we obtain $U_{4k-2,2}(t)$ and (as can be easily seen) $U_{4k-1,2}(t)$ together with $U_{23}(t)$ for all $t \in \text{GF}(q)$.

And in Step 3 we first aim for getting transvections in the second column but in fact we obtain all transvections in the upper-left $(4k - 2) \times (4k - 2)$ block. After that the proof is easy to finish.

We first compute $(R_2 R_3)^{4k-2}$. (Here we include the computation for $k = 2$).

\[
(R_2 R_3)^6 = \begin{bmatrix}
-1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 6 \\
0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]

Note that in the general case the matrix $(R_2 R_3)^{4k-2}$ has $(4k - 2) \times (4k - 2)$ block equal to $-I$ and $2 \times 2$ block-transvection $I + (4k - 2)E_{12}$. This follows from the fact that both $R_2$ and $R_3$ are block-diagonal matrices with blocks of the sizes $(4k - 2) \times (4k - 2)$ and $2 \times 2$. The first block is a sign-permutation matrix with a single $-1$ at the end in $R_2$ and a permutation matrix in $R_3$. The product of these two permutations is a $(4k - 2)$-cycle. The product of $2 \times 2$ matrices is the negative of the simple transvection $I + E_{12}$.  

72
Chapter 5. Positive answer for \( n \geq 4 \).

Now the following sequence of computations will produce a transvection Let

\[
P_{1,8} = \begin{bmatrix}
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & a \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix},
\]

\( (5.64) \)

\[
P_{2,8} = (R_3 R_1 P_{1,8} R_3)^4 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & -2a x & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & -4 x & 0 & 0 & 0 & 0 & 1 & 0 \\
\end{bmatrix},
\]

\( (5.65) \)

\[
P_{3,8} = P_{1,8}^2 P_{2,8} P_{1,8}^{-2} P_{2,8} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & -8a x & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix},
\]

\( (5.66) \)

This gives transvections \( U_{72}(m x) \) with \( m \) an integer if characteristic \( p \) does not divide \( 4k - 2 \). The computations \( 5.64-5.66 \) are easily expanded by the Bar Operation to obtain \( U_{4k-1,2}(m x) \) with \( m \) an integer for this case:

\[
P_{2,n} = \overline{P_{2,n-4}[0,2]} = (R_{3,n-4} R_{1,n-4} P_{1,n-4} R_{3,n-4})^4[0,2] = (R_{3,n-4}[1,2] \cdot R_{1,n-4}[0,2] \cdot P_{1,n-4}[5,2] \cdot R_{3,n-4}[1,2])^4
\]

\( (5.67) \)

\[
P_{3,n} = \overline{P_{3,n-4}[0,2]} = P_{2,n}^2 P_{2,n-4} P_{2,n-4}^{-2} P_{2,n-4}[0,2]
\]

\( (5.69) \)

\[
P_{3,n} = P_{2,n}^2 \overline{P_{2,n}[0,2]} P_{2,n-4}[5,2] P_{2,n-4}[0,2] P_{2,n-4}[0,2]
\]

\( (5.70) \)

73
Chapter 5. Positive answer for $n \geq 4$.

In case the characteristic $p$ divides $4k - 2$ we obtain transvections $U_{4k,1}(mx)$ with $m$ an integer using the following computations:

$$P_{1,8} = \begin{bmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

And expand this by

$$P_{2,8} = (P_{1,8}R_{1,8})^4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ -4x & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

This completes Step 1 of the proof.

We make a couple more computations to obtain $U_{4k-1,2}(mx)$ in case the characteristic $p$ divides $4k - 2$ to uniformize the consequent considerations.

$$P_{3,8} = R_{3,8}P_{2,8}R_{3,8} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -4x & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 4x & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$
Chapter 5. Positive answer for $n \geq 4$.

$$P_{4,8} = R_{1,8}P_{3,8}R_{1,8} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & -4x & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & -4x & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}$$

$$P_{5,8} = P_{4,8}P_{1,8}P_{4,8}^{-1}P_{1,8} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -8x & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}$$

$$P_{6,8} = P_{3,8}^2P_{5,8} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 8x & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}$$

Each of these computations is easily expanded by the Bar Operation at the spot (2,2) in exactly the same manner as it has been done in expansions 5.67–5.71.

For Step 2 we first note that $U_{4k-2,2}(x) = R_1U_{4k-1,2}(x)R_1$. From now till the end of Step 2 we will use only $R_2$ and $R_3$ to obtain new transvections. Since both are just sign-permutation matrices in the block $(4k-2) \times (4k-2)$ we will obtain only transvections (in that block) by conjugating transvections from that block. Also it is obvious that from a transvection $U_{ij}(\alpha)$ we can obtain only transvections $U_{i'j'}(\pm \alpha)$. Since $U_{ij}(\alpha)$ is just the inverse of $U_{ij}(-\alpha)$ we can without loss of generality assume that non-diagonal entry stays the same under any conjugation by these two generators. Therefore we only need to follow the position of the non-diagonal entry.
Chapter 5. Positive answer for \( n \geq 4 \).

The permutation corresponding to \( R_2 \) is \( p_2 = (2,3)(4,5) \ldots (4k - 4,4k - 3) \). The permutation corresponding to \( R_3 \) is \( p_3 = (1,2)(3,4) \ldots (4k - 3,4k - 2) \).

Therefore any index of the non-diagonal entry is changed by \( \pm 1 \) depending on parity and the generator that is used for conjugation (except when the index is 1 or \( 4k - 2 \) and the conjugator is \( R_2 \), in which case the index does not change).

Hence starting with \( U_{4k-2,2}(x) \) and conjugating alternately by \( R_3 \) and \( R_2 \) we successively obtain starting with \( R_3 \) positions: \( (4k - 3,1), (4k - 4,1), (4k - 5,2), (4k - 6,3), \ldots , (2k,2k - 3), (2k - 1,2k - 2) \) and starting with \( R_2 \) we successively obtain positions: \( (4k - 2,3), (4k - 3,4), \ldots , (2k + 3,2k - 2), (2k + 2,2k - 1) \).

Thus if \( n = 8 \) \( (k = 2) \) we can obtain \( U_{23}(x) \). Now, the commutator of \( U_{62}(x) \) and \( U_{23}(x) \) is \( U_{63}(x^2) \). We then obtain \( U_{62}(x^2) \) by conjugating by \( R_2 \) and again bring the non-diagonal entry (this time \( x^2 \)) to the position \( (2,3) \). The commutator of \( U_{62}(x) \) and \( U_{23}(x^2) \) is \( U_{63}(x^3) \).

Repeating this process we obtain all powers of \( x \) as non-diagonal entry at the position \( (6,2) \). Thus if \( x \) is a primitive root in \( \text{GF}(q) \) we obtain all transvections at this position. This completes Step 2 in the case \( n = 8 \).

For the general case we need a little extra work. Having obtained \( U_{2k+2,2k-1}(x) \) and \( U_{2k-1,2k-2}(x) \) we obtain \( U_{2k+2,2k-2}(x^2) \) by taking their commutator.

By conjugating successively by \( R_3 \) and \( R_2 \) starting with \( R_3 \) we move this entry from position \( (2k + 2,2k - 2) \) through \( (2k + 1,2k - 3), \ldots , (5,1), (4,1), (3,2) \) to position \( (2,3) \).

See figure 5.1 to for the details of trajectories of the non-diagonal entry under conjugation.

Now the commutator of \( U_{4k-2,2}(x) \) and \( U_{23}(x^2) \) is \( U_{4k-2,2}(x^3) \). Hence by repeating the process we can obtain all odd powers of \( x \) at the position \( (4k - 2,2) \). But since every element of \( \text{GF}(q) \) can be written as a sum of (two) odd powers of a primitive root, taking \( x \) to be primitive root gives us all transvections at the position \( (4k - 2,2) \) thus completing Step 2.

For Step 3 we assume that we have obtained all transvections \( U_{4k-1,2}(t) \) and \( U_{23}(t), t \in \text{GF}(q) \).
Chapter 5. Positive answer for $n \geq 4$.

Figure 5.1: First step of obtaining $U_{4k-2,2}(t)$, $k > 2$.
(Curved arrows denote commutators.)

(They can be obtained from $U_{4k-2,2}(t)$ by conjugation by $R_1$ or a sequence of conjugations by $R_3$ and $R_2$.)

We will now concentrate on obtaining transvections in the second column. First from $U_{4k-2,2}(t)$ through conjugation by $R_3$, $R_2$ and $R_3$ we obtain $U_{4k-5,2}(t)$. Now take the commutator of $U_{4k-5,2}(t)$ and $U_{23}(1)$ to get $U_{4k-5,3}(t)$ and then take the conjugate of the latter by $R_2$ to obtain $U_{4k-6,2}(t)$. We repeat the process conjugating by $R_3$, $R_2$ and $R_3$ to get $U_{4k-9,2}(t)$, then taking the commutator with $U_{23}(1)$ to get $U_{4k-9,3}(t)$ and conjugating by $R_2$ to get $U_{4k-10,2}(t)$ etc. This stops once we have obtained $U_{62}(t)$.
Chapter 5. Positive answer for $n \geq 4$.

At this moment we have obtained all transvections $U_{i2}(t)$ with $i = 4j - 1$ and $i = 4j + 2$ for $1 \leq j \leq k - 1$. (See figure 5.2).

Now successively conjugating $U_{j-1,1}(t)$ by $R_3$ we obtain $U_{j-1,1}(t)$, then conjugating by $R_1$ we get $U_{j-1,1}(t)$, then using $R_3$ again we get $U_{j-1,1}(t)$.

Now we again repeatedly do the following starting with $j = 4k - 3$:

Take a commutator of $U_{j+2}(t)$ and $U_{23}(1)$ to get $U_{j+3}(t)$.

Conjugate $U_{j+3}(t)$ by $R_2$, to get $U_{j+1,2}(t)$.

Conjugate $U_{j+1,2}(t)$ by $R_3$, $R_2$ and $R_3$ to obtain $U_{j+4,2}(t)$.

Figure 5.2: First step of obtaining second column.
(Curved arrows denote commutators.)
Chapter 5. Positive answer for $n \geq 4$.

This way we get all the transvections $U_{i2}(t)$ with $i = 4j - 3$ and $i = 4j$ with $1 \leq j \leq k - 1$.

![Figure 5.3: Obtaining second column (whole block). (Curved arrows denote commutators.)](image)

In fact we have obtained much more than that. Once we have all transvections in the second column of the block $(4k - 2) \times (4k - 2)$ we in fact have all transvections in this block which we obtain only by conjugating by a series of $R_3$’s and $R_2$’s. (See figure 5.3 – the last fact outlined by dotted lines).

Finally we note that since we have $U_{4k-1,2}(t)$ we can (taking appropriate commutators) obtain the whole $4k - 1$st row except the last entry. Also since $U_{2,4k-1}(t) = R_1 U_{2,4k-2}(t) R_1$ we also obtain all $4k - 1$st column without the last entry.
Chapter 5. Positive answer for $n \geq 4$.

Two of the last necessary transvections are obtained as follows:

$$U_{1,4k}(t) = R_3 U_{2,4k-1}(t) R_3 U_{1,4k-1}(-t), \quad \text{and} \quad U_{4k,2}(t) = R_1 U_{12}(t/x) R_1 U_{12}(-t/x).$$

We now can obtain the rest of transvections using appropriate commutators. □

5.7 Case of $(4k + 2) \times (4k + 2)$ matrices.

This is the last section. We prove here the case of $(4k + 2) \times (4k + 2)$ matrices. This section’s main result is the following two propositions:

**Proposition 5.41.** Let

$$R_1 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
x & 0 & 0 & 0 & 0 & -1
\end{bmatrix}, \quad R_2 = \begin{bmatrix}
-1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -1
\end{bmatrix}
$$

and

$$R_3 = \begin{bmatrix}
0 & -1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 0 & 0 & 1 & 0
\end{bmatrix},$$

where $x$ is a primitive root in $GF(q)$. Then $SL_6(q) = \langle R_1, R_2, R_3 \rangle$.

**Proposition 5.42.** Let

$$R_1 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
x & 0 & 0 & 0 & 0 & -1
\end{bmatrix}, \quad R_2 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}$$
Chapter 5. Positive answer for $n \geq 4$

and

$$R_3 = \begin{bmatrix} 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$

where the choice of $x$ is discussed on page 87. Define inductively

$$R_{1,6} = R_1, \quad R_{2,6} = R_2, \quad R_{3,6} = R_3$$

and

$$R_{1,n} = R_{1,n-4}[0,1], \quad R_{2,n} = R_{2,n-4}[1,2], \quad R_{3,n} = R_{3,n-4}[4,2],$$

for $n = 4k + 2, k \geq 2$.

Then $SL_n(q) = \langle R_{1,n}, R_{2,n}, R_{3,n} \rangle$.

The immediate corollary is

**Corollary 5.43.** $PSL_{4k+2}(q), k \geq 2$ can be generated by three involutions, two of which commute.

**Remark 1.** Note the difference of this case from all previous. $R_3$ is not an involution in $SL_n(q)$ but its image in $PSL_n(q)$ is.

The difference between $n = 6$ and $n = 4k + 2$ with $k \geq 2$ is very small (and is notable only in Step 1), so we will use the same computations almost everywhere in both cases. Thus we combine the proofs into one proof.

As in previous section we note how the Bar Operation works on our generators:

**Lemma 5.44.**

a) $R_{1,n} = \overline{R_{1,n-4}[0,j]}, \quad 1 \leq j \leq 4k - 1,$

b) $R_{2,n} = \overline{R_{2,n-4}[1,2j + 1]}, \quad 0 \leq j \leq 2k,$

c) $R_{3,n} = \overline{R_{3,n-4}[4,2j]}, \quad 0 \leq j \leq 2k + 1.$

81
Chapter 5. Positive answer for \( n \geq 4 \).

**Proof of propositions 5.41 and 5.42.** Step 1 is the most difficult step in this proof. We obtain a transvection at the spot \((6,2)\) if \( n = 6 \) and at the spot \((4k - 2, 1)\) if \( n \geq 10 \). Step 2 is relatively simple and Step 3 looks very much like Step 3 in Section 5.6.

We first make computations for \( n = 6 \):

\[
P_1 = (R_1R_3)^4 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
-x & 0 & -1 & 0 & 0 & 0 \\
0 & -x & 0 & -1 & 0 & 0 \\
0 & -x & 0 & 0 & -1 & 0 \\
x & 0 & 0 & 0 & 0 & -1
\end{bmatrix}, \tag{5.72}
\]

\[
P_2 = R_2P_1R_2 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
x & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & -x & -1 & 0 & 0 \\
0 & 0 & -x & 0 & -1 & 0 \\
x & 0 & 0 & 0 & 0 & -1
\end{bmatrix}, \tag{5.73}
\]

\[
P_3 = (P_2P_1)^2 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
2x^2 & 0 & 0 & 1 & 0 & 0 \\
2x^2 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}, \tag{5.74}
\]

\[
P_4 = R_3P_3R_3 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & -2x^2 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 2x^2 & 0 & 0 & 0 & 1
\end{bmatrix}, \tag{5.75}
\]

and finally

\[
U_{62}(4x^2) = P_4R_1P_4^{-1}R_1 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 4x^2 & 0 & 0 & 0 & 1
\end{bmatrix}, \tag{5.76}
\]
Chapter 5. Positive answer for \( n \geq 4 \).

In the higher dimensions cases the first computations are the same but unfortunately they only lead to a “double transvection”, not a transvection so we have to continue. The analogue of computations 5.72–5.76 for the case \( n = 10 \) is the following:

\[
P_1 = (R_1R_3)^4 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
-x & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & -x & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & -x & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
\end{bmatrix},
\tag{5.77}
\]

\[
P_2 = R_2P_1R_2 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
-x & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & -x & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & -x & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
\end{bmatrix},
\tag{5.78}
\]

\[
P_3 = (P_2P_1)^2 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 2x & -2x & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 2x & -2x & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix},
\tag{5.79}
\]
Chapter 5. Positive answer for \( n \geq 4 \).

\[
R_4 = R_3 R_3 R_3 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
2x & 0 & 0 & 2x & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
2x & 0 & -2x & 0 & 0 & 0 & 0 & 0
\end{bmatrix} \quad (5.80)
\]

and

\[
P_5^2 = P_4 R_4 P_4^{-1} R_1 = R_5 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
4x & 0 & 0 & 4x & 0 & 0 & 0 & 1 \\
\end{bmatrix} \quad (5.81)
\]

The computations 5.77–5.81 expand using the Bar Operation and Lemma 5.44 as follows:

\[
P_{1,n} = 
\bar{P}_{1,n-4}^{[0,2]} = (R_{1,n-4} R_{3,n-4})^{4}[0,2] = (R_{1,n-4}^{[0,2]} \cdot R_{3,n-4}^{[4,2]})^{4}, \quad (5.82)
\]

\[
P_{2,n} = 
\bar{P}_{2,n-4}^{[0,3]} = R_{2,n-4}^{[1,3]} P_{1,n-4}^{[0,3]} \cdot R_{3,n-4}^{[0,3]} \cdot R_{2,n-4}^{[0,3]}, \quad (5.83)
\]

\[
P_{3,n} = 
\bar{P}_{3,n-4}^{[0,3]} = (P_{2,n-4}^{[0,3]} P_{1,n-4}^{[0,4]})^{2}[0,3] = (\bar{P}_{2,n-4}^{[0,3]} \cdot \bar{P}_{1,n-4}^{[0,4]})^{4}, \quad (5.84)
\]

\[
P_{4,n} = 
\bar{P}_{4,n-4}^{[0,4]} = R_{3,n-4}^{[0,4]} P_{3,n-4}^{[0,4]} R_{3,n-4}^{[0,4]} \cdot R_{3,n-4}^{[0,4]} \cdot R_{3,n-4}^{[0,4]} \cdot R_{3,n-4}^{[0,4]}, \quad (5.85)
\]

and

\[
P_{5,n} = 
\bar{P}_{5,n-4}^{[0,4]} = P_{4,n-4} R_{1,n-4}^{[0,4]} P_{4,n-4} - 1) R_{1,n-4}^{[0,4]} = P_{4,n-4}^{[0,4]} \cdot R_{1,n-4}^{[0,4]} \cdot P_{4,n-4}^{[0,4]} \cdot R_{1,n-4}^{[0,4]}, \quad (5.86)
\]

\[
= P_{4,n-4}^{[0,4]} \cdot R_{1,n-4}^{[0,4]} \cdot P_{4,n-4}^{[0,4]} \cdot R_{1,n-4}^{[0,4]} \quad (5.87)
\]
Chapter 5. Positive answer for \( n \geq 4 \).

Now \( R_2 \) is a permutation matrix and \( R_3 \) is a sign permutation matrix. The permutations corresponding to them are \( p_2 = (2, 3)(4, 5) \ldots (4k, 4k+1) \) and \( p_3 = (1, 2)(3, 4) \ldots (4k+1, 4k+2) \).

We now conjugate \( P_{5,n} \) successively by \( R_2 \) and \( R_3 \) to bring the \((4k+2, 4)\) entry to the \((5, 4k+2)\) position. The \((4k+2, 1)\) entry will go to the \((5, 4k - 2)\) position at the same time. (In other words we conjugate \( P_{5,n} \) by \((R_2R_3)^{2k-1}\). When we do this the sign of the \((4k+2, 4)\) entry might change, but it does not matter since we can take an inverse of the "double transvection" we obtain in the end. We call this "double transvection" \( P_{6,n} \). Now

\[
P_6 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & a & 0 & 0 & b \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]

(5.88)

where \( a \) and \( b \) are equal to \( \pm 4x \).

\[
P_7 = R_1P_6R_1P_6^{-1} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]

(5.89)

Now consider \( R_4 = (R_2R_3)^{(2k+1)} \). From the permutation multiplication it follows that \( R_4 \) is the matrix that has only entries equal to \( \pm 1 \) along the big non-main diagonal and zeroes everywhere
Chapter 5. Positive answer for \( n \geq 4 \).

else. In particular conjugation by it swaps first and last row as well as first and last column with possible multiplication by \(-1\)

So to finish **Step 1** we need to make following computations.

\[
P_8 = R_4 P_7 R_4 =
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]  \quad (5.90)

and finally

\[
U_{4k-2,1} = (R_1 P_8)^2 =
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
\epsilon_1 4 b + \epsilon_2 b x^2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
= (5.91)
\]

where \( \epsilon_1, \epsilon_2 = \pm 1 \).

The only possible source of trouble, i.e. not obtaining a transvection, can arise if \( x^2 \pm 4 = 0 \). We will address this issue at the end of **Step 2**, when we discuss the choice of \( x \).

The computations 5.89–5.91 are easily expanded by the Bar Operation at the position (5,5) by identity blocks.

This completes **Step 1**.

For **Step 2** we again divide the cases of \( n = 6 \) and \( n \geq 10 \) although the computations are the
Chapter 5. Positive answer for \( n \geq 4 \).

same.

We proceed very similarly to Step 2 in the proofs of previous sections. Let \( n = 6 \). Suppose we have a transvection \( U_{62}(a) \). Then \( U_{51}(a) = R_3 U_{62}(a) R_3 \) and \( U_{26}(a) = R_4 U_{51}(a) R_4 \). Now \( U_{21}(a x) = (R_1 U_{26}(a))^2 \). In the same way \( U_{56}(-a x) = R_4 U_{21}(a x) R_4 \) and \( U_{46}(a x) = R_2 U_{56}(-a x) R_2 \). Finally \( U_{51}(a x^2) = R_1 U_{46}(a x) R_1 U_{56}(a x) \). This means that having started with \( U_{51}(a) \) we are able to obtain \( U_{51}(a x^2) \) and since any element of the field can be obtained as a sum of (two) even powers, we can obtain all \( U_{51}(t) \) with \( t \in GF(q) \) by choosing \( x \) to be a primitive root.

This completes Step 2 in the case \( n = 6 \).

We do similar computations in case \( n \geq 10 \).

We start with \( U_{4k-2,1}(a) \). \( U_{5,4k+2}(\pm a) = R_4 U_{4k-2,1}(a) R_4 \). \( U_{5,1}(\pm a x) = (R_1 U_{5,4k+2}(a))^2 \). In the same way \( U_{4k-2,4k+2}(\pm a x) = R_4 U_{5,1}(a x) R_4 \) and \( U_{4k-2,1}(\pm a x^2) = (R_1 U_{4k-2,4k+2}(\pm a x))^2 \). So similarly to case \( n = 6 \) we obtain all \( U_{4k-2,1}(t) \), \( t \in GF(q) \).

It should be noted here that Step 2 is redundant if \( q = p \) and thus we don't need \( x \) to be primitive root to obtain all transvections. This means that if \( q = p \) we choose \( x \) such that \( x^2 + 4 \neq 0 \) or \( x^2 - 4 \neq 0 \) depending on the dimension (the sign depends on \( R_4 = (R_2 R_3)^{(2k+1)} \)). If \( q = 9 \) then any primitive root satisfies \( x^2 \pm 4 \neq 0 \) and we choose it for \( x \). And if \( q \geq 25 \) then there are plenty (more than 4) primitive roots to choose from and we always can satisfy this condition.

Appendix F provides the input in case \( n = 10 \) and note that it trivially expands at the spot \((2k + 1, 2k + 1)\) by the Bar Operation using the identity block.

This completes Step 2.

Now for Step 3 we are going to use only \( R_2 \) and \( R_3 \) in a way similar to the \( 4k \times 4k \) case.

First we note that each transvection spot we obtain yields immediately \( 2n \) new spots that are
Chapter 5. Positive answer for $n \geq 4$.

obtained by conjugation by $R_2$ and $R_3$. We get two transvections in each row this way (also two transvections in each column). If we have a transvection $U$ in the first row (but not in columns $4k$ and $4k + 1$) or a transvection in the last column (but not in rows $4k$ and $4k + 1$), then computing $(R_1 U)^2$ will yield yet another transvection in the last row and the same column or the first column and the same row. We will call it flipping. The $2n$ new transvections then will have positions symmetrical to $2n$ positions of the original transvection. See figure 5.4 for the details.

Figure 5.4: Obtaining transvections in $(4k + 2) \times (4k + 2)$ case.

The rest of the proof is easy. We start with the $(4k - 1, 1)$ position and obtain the $(4k + 1, 3)$ position by $R_3$ and $R_2$. We also obtain the $(2, 4k)$ position by applying $R_2 R_3$ to the $(4k + 1, 3)$.
Chapter 5. Positive answer for $n \geq 4$.

position. Now we flip the $(2,4k)$ position to the symmetric position which is $(2,3)$. After that we proceed exactly as in the first half of obtaining second column in the proof of Proposition 5.38. (compare Figures 5.2 and 5.4). After obtaining half of the transvections we just use $R_1$ to flip to symmetric positions.

This gives us all the transvections except those on the big non-main diagonal. They are easily obtained as commutators.

\[\square\]
Bibliography


Bibliography


Appendix A
Maple V input for $4 \times 4$ case.

```plaintext
> with(linalg):
> em:= mat -> map(simplify,evalm(mat)):
> tr:= proc(i,j,val)
> local res;
> res := matrix(4,4,0);
> res[i,j] := val;
> evalm(res+l);
> end:
> c:= proc(a,b)
> em(a*b*a^(-1)*b^(-1));
> end:
> co:= proc(a,b)
> em(a^(-1)*b*a);
> end:
> r1:=array(1..4,1..4,[[1,x,0,0],[0,-1,0,0],[0,0,-1,0],[0,x,0,1]]);
> r2:=array(1..4,1..4,[[0,0,0,1],[0,1,0,0],[0,0,-1,0],[1,0,0,0]]);
> r3:=array(1..4,1..4,[[1,0,0,0],[0,1,1,1/2],[0,0,-1,-1],[0,0,0,1]]);
> em(r1^2);
> em(r2^2);
> em(r3^2);
> em((r1*r2)^2);
> det(r1);
> det(r2);
```
Appendix A.  Maple V input for 4 x 4 case.

> det(r3);
> t3:=array(1..4,1..4,[[0,-1,0,0],[1,-1,0,0],[0,0,1,1],[1,-1,0,1]]);
> em(t3^3);
> em((r2&r3)^4);
> r3xr2r3_4s:=em(r3&*tr(2,1,-2*s)&*tr(2,3,4*s)&*tr(2,4,2*s)));
> r4:=subs(s=-1/4,em(r3xr2r3_4s));
> T:=em(r1*r4);
> t33:=array(1..4,1..4,[[1,0,0,0],[0,1,0,0],[1,1,1,0],[0,0,0,1]]);
> s3:=em(t3*r2*t3*r2);
> u3_31:=em((t3*r4*s3)^2);
> tm:=array(1..4,1..4,[[1,0,0,0],[0,1,0,0],[m*z,4*m*z,1,m],[0,0,0,1]]);
> t:=em(tm^r2*tm^r2);
> u31:=em((tm^r4*s)^2);
> u31m:=tr(3,1,-m*(z-1));
> u34:=em(u31m*s);
> u34z:=tr(3,4,z-1);
> tz:=em(T*u34z);
> tmz:=array(1..4,1..4,[[1,0,0,0],[0,1,0,0],[m*z^2,4*m*z^2,1,mz],[0,0,0,1]]);
> sz:=em(tmz^r2*tmz^r2);
> u31z:=em((tmz^r4*sz)^2);
> u34t:=tr(3,4,t);
> u31t:=tr(3,1,t);
> u24t:=em((r3*u34t)^2);
> u21t:=em(r2*u24t*r2);
> u32:=em((r1*u31t)^2);
> r5:=em(tr(3,2,1)*r3*tr(3,4,-1)*tr(2,4,1/2)*tr(3,2,-1));
> u32t:=tr(3,2,t);
> u23t:=evalm(r5*u32t*r5);
> r6:=array(1..4,1..4,[[1,0,0,0],[0,-1,0,0],[0,0,-1,0],[0,0,0,1]]);
> q:=em(r5*r1*r5*r1*tr(2,3,1));
> p:=em(u32t*tr(2,3,-1)*r6*q);
> u12:=em(p^2*tr(3,2,-2*t));
Appendix A. Maple V input for $4 \times 4$ case.

> u13t:=em(tr(1,2,-t)&*tr(2,3,-1)&*tr(1,2,t)&*tr(2,3,1));
> u14t:=em(u13t^(-1)&*tr(3,4,-1)&*u13t&*tr(3,4,1));
> u43t:=em(r2&*u13t&*r2);
> u41t:=em(r2&*u14t&*r2);
> u42:=em(r2&*tr(1,2,t)&*r2);
Appendix B
Maple V input for $5 \times 5$ case.

```maple
> with(linalg):
> em:=mat -> map(simplify,evalm(mat)):
> tr:= proc(i,j,val)
> local res;
> res := matrix(5,5,0); res[i,j]:= val; evalm(res+1);
> end:
> rl:=array(l..5,1..5, 
[[l,x,0,0,0],
[0,-1,0,0,0],
[0,0,0,1,0],
[0,0,1,0,0],
[0,-x,0,0,1]]);
> r2:=array(l..5,1..5, 
[[0,0,0,0,1],
[0,-1,0,0,0],
[0,0,1,0,0],
[0,0,0,1,0],
[1,0,0,0,0]]);
> r3:=array(l..5,1..5, 
[[1,0,0,0,0],
[0,1,1,0,0],
[0,0,-1,0,0],
[0,0,0,1,1],
[0,0,0,0,-1]]);
> em(rl&*rl),em(r2&*r2),evalm(rl&*r2&*rl&*r2),evalm(r3*r3);
> det(rl),det(r2),det(r3);
> r2r3_4:=em((r2&*r3)~4);
> u23:=tr(2,3,l);
> r4:=em(r3*u23^(-1));
> w:=evalm((r1&*r4)^4);
> s:=evalm(w&*r2&*w&*r2);
> T:=em(tr(1,2,x)&*tr(5,2,-x));
> r6:=evalm(r1&*T^(-1));
> u24:=evalm(r6&t23^(-1)&*r6);
> u24a:=tr(2,4,a);
```
Appendix B. Maple V input for $5 \times 5$ case.

\begin{verbatim}
> p := em((r1*r3*r1*u24a)^2);
> u24xa := em(p^(-1)*r23*p^t23^(-1));
> u24t := tr(2, 4, t);
> u25t := em(r3*u24t*r3*u24t^(-1));
> u21t := em(r2*u25t^(-1)*r2);
> q := em(r1*tr(2, 1, 1/x)*r1*tr(2, 1, -2/x));
> f1 := em((q*tr(2, 1, -t/(2*x^2))*r2)^2);
> f2 := em((u23*r3*f1)^2);
> f3 := em(r6*f2*r6);
> u12 := em((u23*r3*f3)^2);
> u32 := em(tr(1, 2, 2*t)*f3);
> u42 := em(tr(1, 2, 2*t)*f2^(-1));
> u52 := em(tr(1, 2, t)*f1^(-1));
\end{verbatim}
Appendix C
Maple V input for \((4k + 1) \times (4k + 1)\) case.

```maple
> with(linalg):
> em:= mat -> map(simplify,evalm(mat)):
> tr:= proc(i,j,val)
> local res;
> res := matrix(9,9,0);
> res[i,j] := val;
> evalm(res+l);
> end:
> rl:=matrix([[l,x,0,0,0,0,0,0,0],[0,-1,0,0,0,0,0,0,0] ,[0,0,0,1,0,0,0,0,0],
[0,0,1,0,0,0,0,0,0],[0,0,0,0,1,0,0,0,0],[0,0,0,0,1,0,0,0,0],[0,0,0,0,0,1,0,0,0],
[0,0,0,0,0,1,0,0,0],[0,0,0,0,0,0,1,0,0],[0,-x,0,0,0,0,0,0,1]]);
> em(rl&*rl);
> r2:=matrix([[0,0,0,0,0,0,0,0,1],[0,-1,0,0,0,0,0,0,0],
[0,0,1,0,0,0,0,0,0],[0,0,0,1,0,0,0,0,0],[0,0,0,0,1,0,0,0,0],[0,0,0,0,1,0,0,0,0],
[0,0,0,0,0,1,0,0,0],[0,0,0,0,0,0,1,0,0],[0,0,0,0,0,0,0,1,0],[1,0,0,0,0,0,0,0,0]]);
> evalm(rl&*r2&*rl&*r2);
> r3:=matrix([[1,0,0,0,0,0,0,0,0],[0,1,1,0,0,0,0,0,0],[0,0,-1,0,0,0,0,0,0],[0,0,0,1,1,0,0,0,0],
[0,0,0,0,1,1,0,0,0],[0,0,0,0,-1,0,0,0,0],[0,0,0,0,0,1,1,0,0],[0,0,0,0,0,0,-1,0,0],[0,0,0,0,0,0,0,1,1],[0,0,0,0,0,0,0,0,-1]]);
> em(r3*r3);
> det(r1),det(r2),det(r3);
> r2r3_4:=em((r2&*r3)^4);
```

97
Appendix C. Maple V input for \((4k + 1) \times (4k + 1)\) case.

\[
\begin{align*}
> & \quad u_{23} := \text{tr}(2,3,1); \\
> & \quad p_1 := \text{em}(r1 * u_{23} * r1); \\
> & \quad p_2 := \text{em}(r3 * p1 * r3); \\
> & \quad p_3 := \text{em}(r2 * p2 * r2 * p2^(-1)); \\
> & \quad u_{24.2} := \text{em}(r3 * p3 * r3); \\
> & \quad \text{em}(u_{24.2}^(-1) * p3); \\
> & \quad p_{11} := \text{em}(r1 * \text{tr}(2,5,1) * r1); \\
> & \quad p_{21} := \text{em}(r3 * p_{11} * r3); \\
> & \quad p_{31} := \text{em}(r2 * p_{21} * r2 * p_{21}^(-1)); \\
> & \quad u_{26.2} := \text{em}(r3 * p_{31} * r3); \\
> & \quad \text{em}(u_{26.2}^(-1) * p_{31}); \\
> & \quad u_{23} := \text{tr}(2,3,1); \\
> & \quad u_{24} := \text{tr}(2,4,1); \\
> & \quad u_{25} := \text{tr}(2,5,1); \\
> & \quad u_{26} := \text{tr}(2,6,1); \\
> & \quad u_{27} := \text{tr}(2,7,1); \\
> & \quad u_{24a} := \text{tr}(2,4,a); \\
> & \quad p_{19} := \text{em}(r1 * u_{24a} * r1); \\
> & \quad p_{29} := \text{em}(r3 * p_{19} * r3); \\
> & \quad p_{39} := \text{em}(r1 * p_{29} * r1); \\
> & \quad u_{24ax} := \text{em}(p_{39}^(-1) * u_{27} * p_{39} * u_{27}^(-1)); \\
> & \quad u_{25t} := \text{tr}(2,5,t); \\
> & \quad p_{19.1} := \text{em}(r1 * u_{25t} * r1); \\
> & \quad p_{29.1} := \text{em}(r3 * p_{19.1} * r3); \\
> & \quad p_{39.1} := \text{em}(r1 * p_{29.1} * r1); \\
> & \quad p_{49.1} := \text{em}(u_{27} * p_{39.1} * u_{27}^(-1) * p_{39.1}^(-1)); \\
> & \quad u_{28tx} := \text{em}(\text{tr}(2,5,t*x) * p_{49.1}); \\
> & \quad u_{29tx} := \text{em}(r3 * u_{28tx} * r3 * u_{28tx}^(-1)); \\
> & \quad u_{21t} := \text{em}(r2 * \text{tr}(2,9, -t) * r2); \\
> & \quad p_{1.1} := \text{em}(r1 * \text{tr}(2,4, t) * r1); \\
> & \quad p_{2.1} := \text{em}(r3 * p_{1.1} * r3); \\
> & \quad p_{3.1} := \text{em}(p_{2.1} * p_{1.1});
\end{align*}
\]
Appendix C. Maple V input for \((4k + 1) \times (4k + 1)\) case.

\[
\begin{align*}
\text{> } p4_1 &:= \text{em}(r2 \ast p3.1 \ast r2 \ast p3.1); \\
\text{> } u23t &:= \text{em}(p4.1 \ast p2.1^\sim(-2)); \\
\text{> } p1_2 &:= \text{em}(r1 \ast tr(2,1,1/x) \ast r1); \\
\text{> } p2_2 &:= \text{em}(p1.2 \ast tr(2,1,-2/x)); \\
\text{> } p3_2 &:= \text{em}(p2.2 \ast tr(2,1,-t/(2*x*x)) \ast p2.2); \\
\text{> } tn &:= \text{em}(p3.2^\sim 2); \\
\text{> } r4 &:= \text{subs}(t=x, \text{em}(tn \ast r1)); \\
\text{> } p1_3 &:= \text{em}((u23 \ast r3 \ast tn)^\sim 2); \\
\text{> } p2_3 &:= \text{em}(r4 \ast p1.3 \ast r4); \\
\text{> } p1_4 &:= \text{em}((u23 \ast r3 \ast p2.3)^\sim 2); \\
\text{> } p2_4 &:= \text{em}(r4 \ast p1.4 \ast r4); \\
\text{> } p1_5 &:= \text{em}((u23 \ast r3 \ast p2.4)^\sim 2); \\
\text{> } p2_5 &:= \text{em}(r4 \ast p1.5 \ast r4); \\
\text{> } u12t &:= \text{em}((u23 \ast r3 \ast (tr(1,2,-8*t) \ast tr(3,2,t)))^\sim 2);
\end{align*}
\]
Appendix D
Maple V input for \((4k + 3) \times (4k + 3)\) case.

> with(linalg):
> em := mat -> map(simplify, evalm(mat)):
> tr := proc(i,j,val)
> local res;
> res := matrix(7,7,0);
> res[i,j] := val;
> evalm(res+1);
> end:
> rl := matrix([[l,0,0,0,0,0,0], [0,1,0,0,0,0,0], [0,0,0,0,1,0,0],
> [0,0,0,0,0,0,1], [0,0,0,0,0,-x,0], [0,0,0,0,-x,0,0],
> [0,-x,0,0,0,0,-x]])
> em(rl*rl);
> det(rl);
> r2 := matrix([[0,0,0,0,0,0,1], [0,-1,0,0,0,0,0], [0,0,1,0,0,0,0],
> [0,0,0,1,0,0,0], [0,0,0,0,1,0,0], [0,0,0,0,0,1,0], [1,0,0,0,0,0,0]])
> det(r2);
> evalm(rl*r2*rl*r2);
> evalm(r2&r2);
> r3 := matrix([[1,0,0,0,0,0,0], [0,-1,1,0,0,0,0], [0,0,1,0,0,0,0],
> [0,0,0,1,0,0,0], [0,0,0,0,1,0,0], [0,0,0,0,0,1,0], [0,0,0,0,0,0,1]])
> em(r3*r3);
> det(r3);
> u23 := em((r2*r3)^4);
> u23 := tr(2,3,1);
Appendix D. Maple V input for \((4k + 3) \times (4k + 3)\) case.

```maple
> p1:=em(r1*u23*r1);
p2:=em(r3*p1*r3);
p3:=em(r2*p2*r2*p2*(-1));
u24.2:=em(r3*p3*r3);
u252:=em(u24.2*(-1)*p3);
u24:=tr(2,4,1):
u25:=tr(2,5,1):
u24a:=tr(2,4,a):
p17:=em(r1*u24a*r1);
p27:=em(r3*p17*r3);
em(r2*p27*r2*p27*(-1));
p37:=em(r1*p27*r1);
u24ax:=em(p37*(-1)*u25*p37*u25*(-1));
u24t:=tr(2,4,t):
u25t:=em(r3*u24t*r3*u24t*(-1));
u23t:=tr(2,3,t);
p.1:=em(r1*u23t*r1);
p.2:=em(r3*p.1*r3);
p.3:=em(r1*p.2*r1);
p.4:=em(u25*(-1)*p.3*u25*p.3*(-1));
u26tx:=em(tr(2,3,t*x)*p.4);
u27tx:=em(r3*u26tx*(-1)*r3*u26tx);
u27t:=tr(2,7,t);
p11:=em(r1*tr(2,1,-1/x)*r1);
p21:=em(p11*tr(2,1,2/x));
p31:=em(p21*tr(2,1,-t/(2*x^2))*p21);
p41:=em(p31^2);
r4:=subs(t=-x,em(p41*r1));
p1.1:=em((u23*(-1)*r3*p41)^2);
p2.1:=em(r4*p1.1*r4);
p1.2:=em((u23*(-1)*r3*p2.1)^2);
```

101
Appendix D. Maple V input for $(4k+3) \times (4k+3)$ case.

> p2_2:=em(r4*p1_2*r4);
> u12t:=em((u23^(-1)*r3*p2_2)^2);
Appendix E
Maple V input for $4k \times 4k$ case.

```maple
> with(linalg):
> em:= mat -> map(simplify,evalm(mat)):
> tr:= proc(i,j,val)
> local res;
> res := matrix(8,8,0);
> res[i,j] := val;
> evalm(res+1);
> end:
> c:= proc(a,b)
> em(a&*b&*a^-1&*b^-1));
> end:
> mp:= proc(a,b)
> mulperms(a,b);
> end:
> co:= proc(a,b)
> em(a^-1&*b&a);
> end:
> r1:=matrix([[1,0,0,0,0,0,0,0],[0,1,0,0,0,0,0,0],[0,0,1,0,0,0,0,0],
[0,0,0,1,0,0,0,0],[0,0,0,0,1,0,0,0],[0,0,0,0,0,1,0,0],[0,0,0,0,0,0,1,0],
[x,0,0,0,0,0,0,-1]]);
> em(r1*r1);
> det(r1):
> r2:=matrix([[1,0,0,0,0,0,0,0],[0,0,1,0,0,0,0,0],[0,1,0,0,0,0,0,0],
[0,0,0,1,0,0,0,0],[0,0,0,0,1,0,0,0],[0,0,0,0,0,1,0,0],[0,0,0,0,0,0,1,0],
[x,0,0,0,0,0,0,-1]]);
> em(r1*r1);
> det(r1);
```
Appendix E. Maple V input for $4k \times 4k$ case.

\[
\begin{bmatrix}
0,0,0,0,1,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0
\end{bmatrix};
\]

\[
> \text{det}(r2);
\]

\[
> \text{c}(r1,r2);
\]

\[
> \text{evalm}(r2*r2);
\]

\[
> r3:=\text{matrix}\left(\begin{array}{cccccccc}
0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
\end{array}\right);
\]

\[
> \text{em}(r3*r3);
\]

\[
> \text{det}(r3);
\]

\[
> t1:=\text{em}\left(\left(r2*r3\right)^{-6}\right);
\]

\[
> p1:=\text{em}\left(t1*\text{tr}(7,8,a-6)\right);
\]

\[
> p2:=\text{em}\left((r3*r1*ta*r3)^{-4}\right);
\]

\[
> p3:=\text{c}(ta^2,ta2);
\]

\[
> p18:=\text{em}\left(t1*\text{tr}(7,8,-6)\right);
\]

\[
> p28:=\text{em}\left((p18*r1)^{-4}\right);
\]

\[
> p38:=\text{co}(r3,p28);
\]

\[
> p48:=\text{co}(r1,p38);
\]

\[
> p58:=\text{em}\left(p48*p18*p48^{-1}\right);\]

\[
> p68:=\text{em}\left(p38^2*p58\right);
\]

\[
> u72:=\text{tr}(7,2,a);
\]

\[
> u62:=\text{co}(r1,u72);
\]

\[
> u51:=\text{co}(r3,u62);
\]

\[
> u41:=\text{co}(r2,u51);
\]

\[
> u32:=\text{co}(r3,u41);
\]

\[
> u23:=\text{co}(r2,u32);
\]

\[
> u73:=\text{c}(u72,u23);
\]

\[
> u72a2:=\text{co}(r2,u73);
\]

\[
> c(u72a2,u23);
\]

\[
> u26:=\text{tr}(2,6,a);
\]

\[
> u27:=\text{co}(r1,u26);
\]

\[
> \text{em}(r3*u27*r3*\text{tr}(1,7,-a));
\]
Appendix E. Maple V input for $4k \times 4k$ case.

> em(r1&*tr(1,2,a/x)&*r1&*tr(1,2,-a/x));
>
Appendix F
Maple V input for \((4k + 2) \times (4k + 2)\) case.

The 6 \times 6 input file:
\[
\begin{verbatim}
> with(linalg):
> em:= mat -> map(simplify, evalm(mat)):
> tr:= proc(i,j,val)
> local res;
> res := matrix(6,6,0);
> res[i,j] := val;
> evalm(res+l);
> end:
> c:= proc(a,b)
> em(a*b&*a~(-1)&*b~(-1));
> end:
> co:= proc(a,b)
> em(a~(-1)&*b&*a);
> end:
> rl:=matrix([[l,0,0,0,0,0], [0,1,0,0,0,0], [0,0,1,0,0,0], [0,0,0,0,1,0],
[0,0,0,1,0,0], [x,0,0,0,0,-l]]);
> em(rl&*rl);
> det(rl);
> r2:=matrix([[-1,0,0,0,0,0], [0,0,1,0,0,0], [0,1,0,0,0,0], [0,0,0,0,1,0],
[0,0,0,1,0,0], [0,0,0,0,0,-1]]);
> det(r2);
> c(r1,r2);
\end{verbatim}
\[
\]
Appendix F. Maple V input for \((4k + 2) \times (4k + 2)\) case.

\[
> \text{evalm}(r2*r2);
> r3:=\text{matrix}([[0,-1,0,0,0,0],[1,0,0,0,0,0],[0,0,0,-1,0,0],[0,0,1,0,0,0],
[0,0,0,0,-1],[0,0,0,0,1,0]]);
> \text{em}(r3*r3);
> \text{det}(r3);
> r4:=\text{em}((r2*r3)^3);
> p1:=\text{em}((r1*r3)^4);
> p2:=\text{co}(r2,p1);
> p3:=\text{em}((p2*p1)^2);
> p4:=\text{co}(r3,p3);
> c(p4,r1);
> u62:=\text{tr}(6,2,a);
> u51:=\text{co}(r3,u62);
> u26:=\text{co}(r4,u51);
> u21x:=\text{em}((r1*u26)^2);
> u56x:=\text{co}(r4,u21x);
> u46x:=\text{co}(r2,u56x);
> \text{em}(r1*u46x*r1*u56x^(-1));
>
\]  

The 10 \times 10 input file.

\[
> \text{with(linalg)}:
> \text{em}:= \text{mat} \rightarrow \text{map(simplify,evalm(mat))}:
> \text{tr}:= \text{proc}(i,j,\text{val})
> \text{local res;}
> \text{res} := \text{matrix}(10,10,0);
> \text{res}[i,j] := \text{val};
> \text{evalm(res+1)};
> \end:
> \text{c}:= \text{proc}(a,b)
> \text{em}(a*b*b^(-1)+a^(-1)*b^(-1));
> \end:
> \text{co}:= \text{proc}(a,b)
\]
Appendix F. Maple V input for $(4k + 2) \times (4k + 2)$ case.

> em(a^(-1)*b*a);
> end:
> r1:=matrix([[1,0,0,0,0,0,0,0,0,0],[0,1,0,0,0,0,0,0,0,0],
              [0,0,1,0,0,0,0,0,0,0],[0,0,0,1,0,0,0,0,0,0],
              [0,0,0,0,1,0,0,0,0,0],[0,0,0,0,0,1,0,0,0,0],
              [0,0,0,0,0,0,1,0,0,0],[0,0,0,0,0,0,0,1,0,0],
              [0,0,0,0,0,0,0,0,1,0],[x,0,0,0,0,0,0,0,0,-1]]);
> em(r1*r1);
> det(r1);
> r2:=matrix([[1,0,0,0,0,0,0,0,0,0],[0,0,1,0,0,0,0,0,0,0],
              [0,1,0,0,0,0,0,0,0,0],[0,0,0,1,0,0,0,0,0,0],
              [0,0,0,0,1,0,0,0,0,0],[0,0,0,0,0,1,0,0,0,0],
              [0,0,0,0,0,0,1,0,0,0],[0,0,0,0,0,0,0,1,0,0],
              [0,0,0,0,0,0,0,0,1,0],[0,0,0,0,0,0,0,0,0,1]]);
> det(r2);
> c(r1,r2);
> evalm(r2*r2);
> r3:=matrix([[0,-1,0,0,0,0,0,0,0,0],[1,0,0,0,0,0,0,0,0,0],
              [0,0,0,-1,0,0,0,0,0,0],[0,0,1,0,0,0,0,0,0,0],
              [0,0,0,0,1,0,0,0,0,0],[0,0,0,0,0,1,0,0,0,0],
              [0,0,0,0,0,0,-1,0,0,0],[0,0,0,0,0,0,0,1,0,0],
              [0,0,0,0,0,0,0,0,-1],[0,0,0,0,0,0,0,0,1,0]]);
> em(r3*r3);
> det(r3);
> r4:=em((r2*r3)^5);
> p1:=em((r1*r3)^4);
> p2:=co(r2,p1);
> p3:=em((p2*p1)^2);
> p4:=co(r3,p3);
> p5:=em(p4*r1*p4^(-1)*r1);
> p6:=co(em((r2*r3)^3),p5);
> p6ab:=em(tr(5,6,a)*tr(5,10,b));
> p7b:=c(r1,p6ab);
> p7pm:=em(tr(6,1,eps1*b*x)*tr(6,10,eps2*2*b));
> p8:=co(r4,p7pm);
Appendix F. Maple V input for \((4k + 2) \times (4k + 2)\) case.

```maple
> p82pm:=em((r1*p8)^2);
> t61:=tr(6,1,a);
> t510:=co(t,61);
> t51x:=em((r1*t510)^2);
> t610x:=co(t,51x);
> t61x2:=em((r1*t610x)^2);
> 
```
Chapter 5. Positive answer for \( n \geq 4 \).

Now \( R_2 \) is a permutation matrix and \( R_3 \) is a sign permutation matrix. The permutations corresponding to them are \( p_2 = (2, 3)(4, 5) \ldots (4k, 4k+1) \) and \( p_3 = (1, 2)(3, 4) \ldots (4k+1, 4k+2) \).

We now conjugate \( P_{5,n} \) successively by \( R_2 \) and \( R_3 \) to bring the \((4k+2, 4)\) entry to the \((5, 4k+2)\) position. The \((4k+2, 1)\) entry will go to the \((5, 4k-2)\) position at the same time. (In other words we conjugate \( P_{5,n} \) by \( (R_2 R_3)^{(2k-1)} \). When we do this the sign of the \((4k+2, 4)\) entry might change, but it does not matter since we can take an inverse of the “double transvection” we obtain in the end. We call this “double transvection” \( P_{6,n} \). Now

\[
P_6 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & a & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}, \quad (5.88)
\]

where \( a \) and \( b \) are equal to \( \pm 4x \).

\[
P_7 = R_1 P_6 R_1 P_6^{-1} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
\text{b}x & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix} \quad (5.89)
\]

Now consider \( R_4 = (R_2 R_3)^{(2k+1)} \). From the permutation multiplication it follows that \( R_4 \) is the matrix that has only entries equal to \( \pm 1 \) along the big non-main diagonal and zeroes everywhere

85