An Examination of Pre-Bloch Groups over Finite Fields with Elementary Techniques

Adam Ryan

September 1, 2017

1 Abstract

I prove the linear independence of $\frac{q-3}{2}$ relations of the pre-Bloch group over a field $\mathbb{F}_q$ with $\mathrm{Char}(\mathbb{F}_q) \neq 2$ using only elementary methods. It is known for a pre-Bloch group over a finite field that $q-2$ relations are linearly independent, however this result has previously been shown using techniques which originate from Homology and K-Theory. This result places a lower bound on the number of linearly independent relations, and may serve as a stepping-stone towards an elementary proof that the pre-Bloch group over a finite field is itself finite.

Contents

2 Introduction

It has been shown by Hutchinson [6] that the pre-Bloch group of a finite field of order q is isomorphic to a cyclic group of order $q + 1$. This fact tells us that the pre-Bloch group of a finite field is finite and thus a presentation matrix of the pre-Bloch group must have maximal rank. The motivating questions for this study are the following:

It has been shown that the presentation matrix of a pre-Bloch group over a finite field has maximal rank.

- Is it possible to systematically find an explict list of $q-2$ relations of the total $(q-2) \cdot (q-3)$ relations which are linearly independent?
- Furthermore, can it be shown that the pre-Bloch group is cyclic via explicit means?
- If we can show that the pre-Bloch group is cyclic, can we explicitly find a generator?
- Are there any explicit identities amongst the relations which can be systematically found?

In this section we will introduce the pre-Bloch group over a finite field, provide a motivation for its study, and provide some known results. As the structure of the pre-Bloch group is fundamentally tied to the arithmetic of the underlying field, we will review what we mean by a field and detail some essential results which will prove necessary to our study of the pre-Bloch group. Finally, as the concept of free modules and presentation matrices are intrinsically linked to our exploration of the pre-Bloch group over a finite field, we will provide a brief revision of these topics.

2.1 Review of Fields

In this section, we will review what we mean by a finite field, and we will explore the key results which are required to examine the pre-Bloch group. As the underlying arithmetic of the finite field is largely responsible for the structure of the pre-Bloch group over that field, it is essential that the reader is deeply familiar with these results and the notation associated with finite fields. We present these well-known results without proof so that the reader may recall them. The exposition here is based on [1].

Definition: Field
We say that a commutative ring $(R, +, \cdot, 0_R, 1_R)$ in which every non-zero element has a multiplicative inverse is a field, denoted $\mathbb{F}$. We denote the multiplicative group of a field $\mathbb{F}^*$.

Definition: Finite Field and Infinite Field.
We say that a field with a finite number of elements is a finite field. We call the number of elements in a finite field the order of the field. If a field is not finite, we say it is an infinite field.

Proposition:
The commutative ring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a field if and only if $n = p$ is prime. This is the unique field with p elements. We denote $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$

Theorem:
For every finite field $|\mathbb{F}_q| = q = p^n$ with $p \in \mathbb{N}$ prime, and $n \in \mathbb{N}$.

Definition: Multiplicative order
Let $r \in \mathbb{F}_q$. We call the multiplicative order of r, denoted $\text{ord}(r)$, the smallest $a \in \mathbb{N}$ such that $r^a = 1_{\mathbb{F}_q}$.

Definition: The Prime Subfield of a Field
We call the smallest subset P of $\mathbb{F}$ which is itself a field the prime subfield of F.

Proposition:
For p prime and $\text{Char}(\mathbb{F}_q) = p$, the prime subfield P of $\mathbb{F}_{p^n}$ is isomorphic to $\mathbb{F}_p$.

Definition: Generator
For $r \in \mathbb{F}$ such that $< r >= \{r^1, r^2, r^3, \ldots, r^{q-2}, r^{q-1} = 1\} = (\mathbb{F}_q^*, \cdot, 1_\mathbb{F})$ then we call r the generator of $\mathbb{F}^*$. Here, r is a primitive root of $\mathbb{F}$.

Lemma:
For every finite field, there exists at least one generator.

Proposition:
There exists a field $\forall q = p^n$ such that $\mathbb{F}_q$ is a field. Furthermore, if $\mathbb{F}$ and $\mathbb{G}$ are finite fields such that $|\mathbb{F}| = |\mathbb{G}| = q$, then $\mathbb{F} \cong \mathbb{G}$

Question:

We know that fields of the form p^n are possible, but how do we construct fields where $n > 1$?

Answer:
We will demonstrate that this can be done by adjoining a root of an irreducible polynomial of degree d to $\mathbb{F}_p[x]$. This new field is an 'extension' of $\mathbb{F}_p$ and contains p^d elements.

Example:
Construct the field $\mathbb{F}_4$.

Solution to Example:
First, we take the field $\mathbb{F}_2 = \{0, 1\}$, and examine the polynomial ring $\mathbb{F}_2[X]$. We define $S := \{p(x) : p(x) \in \mathbb{F}_2[X] \text{ and } \deg(p(x)) \leq 2\}$. Then:

$$S = \{0,\ 1,\ x + 0,\ x + 1,\ x^2 + 1,\ x^2 + 0,\ x^2 + x + 0,\ x^2 + x + 1\}$$

Secondly, we observe that the polynomial $x^2 + x + 1$ is the only irreducible polynomial in $F_2[X]$ with $\deg(p(x)) \leq 2$ and neither 0 nor 1 is a root of the polynomial. We will call i the root of the polynomial

By taking $\mathbb{F}_2[X]/ < x^2 + x + 1 >$ we see that the elements are:

$$\mathbb{F}_2[X]/ < x + 2 + x + 1 >= \{0, 1, i, 1 + i\}$$

We can verify that this is indeed a field, that this field has four elements, and we see that this field has characteristic 2 with a prime subfield of $\mathbb{F}_2$

2.2 Free Modules, Presentation Matrices, and Group Generators

In this section we will examine free modules and presentation matrices. These topics will be essential in justifying our analysis of the pre-Bloch group over a finite field. This will also allow us to justify our usage of linear algebraic techniques to identify identities and to attempt to determine the size of this group by examining the properties of certain matrices. The exposition in this section is based on Chapter 14 of [1]. Throughout this section we will go with the convention that unless otherwise stated, R refers to a non-zero ring.

Definition: Free Module
Let R be a ring. Let M be an R-Module. We say that M is a free module if there exists a basis, with the usual definition which we will explicity give below, of M.

Example:
Let R be a ring. Then R is a free module as any unit of R is a basis, and thus the module is of rank 1.

Definition: Span and Generator:
Let R be a ring, and let M be an R-module. We say that for $m_1, \ldots m_n \in M$, the span of $m_1, \ldots, m_n$ is the set:

$$\text{Span}(m_1, \ldots, m_n) := \{r_1 m_1 + \ldots + r_n m_n : r_1, \ldots, r_n \in R\}$$

If $\exists m_1, \ldots, m_n \in M$ such that $\text{Span}(m_1, \ldots, m_n) = M$, then we say that $m_1, \ldots, m_n$ are generators of M, and that M is finitely generated.

Definition: Linear Independance
Let R be a ring, and let M be an R-module. We say that $m_1, \ldots, m_n \in M$ are linearly independent if given $r_1, \ldots r_n \in R$:

$$r_1 m_1 + r_2 m_2 + \ldots r_{n-1} m_{n-1} + r_n m_n = 0 \implies r_1 = \ldots = r_n = 0$$

Definition: Basis
Let R be a ring, and let M be an R-module. We say that

$$B := \{m_1, m_2, \ldots, m_n : m_i \in M \ \forall i \leq n\}$$

is a basis of M if the follow criteria are met:

- $Span(B) = M$
- The elements of B are linearly independent.

Definition: Relation
Let M be an R-module. Let $B = \{m_1, m_2, \ldots, m_n\} \subseteq M$, we can associate B with a homomorphism of modules, ϕ_B, as :

$$\phi_B : R^n \to M$$

$$\phi_B(r_1, \ldots, r_n) = (r_1, r_2, \ldots, r_n) \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \sum_{i=1}^{n} r_i m_i$$

We say that $(r_1, \ldots, r_n) \in \mathrm{Ker}(\phi_B)$ is a relation.

Note:
B is a basis of an R-module M if and only if the homomorphism ϕ_B (as defined above) is isomorphic.

Definition: Complete Set of Relations
Let M be an R-Module. Let B be a set such that $\mathrm{Span}(B) = M$. Let ϕ_B be the homomorphism previously defined. We say that a set of relations S is a complete set of relations if:

$$\mathrm{Span}(S) = \mathrm{Ker}(\phi_B)$$

Theorem:
If A is an integer matrix, then there are elementary integer matrices Q and P, which originate from row and column operations, such that:

$$A' = Q^{-1} \cdot A \cdot P$$

where A' is of the form:

$$A' = \begin{pmatrix} \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_k \end{bmatrix} & \\ & 0 \end{pmatrix}$$

with $d_1 | d_2 | d_3 | \ldots | d_k$ and $k \leq n$

Proof:
The proof shall be omitted, but may be found in [1] as the Proof of Theorem 14.4.6

Note:
When diagonalising integer matrices, as we do not have inverses $\forall z \in \mathbb{Z}$, the row and column operations we can do are restricted. As highlighted in [1] (page 418) row and column operations are restricted to the following:

- Multiply a column or row by -1
- Add an integer multiple of a row to another, or an integer multiple of a column to another.
- Swap the position of two rows or columns

Example:
We will diagonalise the following integer matrix:

$$M = \begin{pmatrix} 3 & 0 & -1 & 1 & 0 & -1 \\ -2 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & -2 & 0 & 2 \end{pmatrix}$$

We will add the second and third row to the first row.

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ -2 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & -2 & 0 & 2 \end{pmatrix}$$

We will subtract the first column from the remaining columns.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ -2 & 3 & 2 & 4 & 3 & 2 \\ 0 & 0 & 2 & -2 & 0 & 2 \end{pmatrix}$$

We will add twice the first row to the second row.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 2 & 4 & 3 & 2 \\ 0 & 0 & 2 & -2 & 0 & 2 \end{pmatrix}$$

We will rearrange the columns so that the values in the second row are ordered.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 3 & 3 & 4 \\ 0 & 2 & 2 & 0 & 0 & -2 \end{pmatrix}$$

We will subtract the highest multiple of $a_{2,2} \leq a_{2,j}$ times the second column from column j

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 1 & 0 \\ 0 & 2 & 0 & -2 & -2 & -6 \end{pmatrix}$$

We will reorder the columns such that the second row is ordered.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & -6 & -2 & -2 & 2 \end{pmatrix}$$

We will subtract the highest multiple of $a_{2,4} \leq a_{2,j}$ times the fourth column from column j.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -6 & -2 & 0 & 6 \end{pmatrix}$$

We'll subtract the highest multiple of $a_{2,4} \leq a_{i,4}$ from row i.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -6 & 0 & 0 & 6 \end{pmatrix}$$

We'll rearrange to place zero columns in the final columns of the matrix and 1 in $a_{2,2}$.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -6 & 6 & 0 & 0 \end{pmatrix}$$

We multiply all columns containing a negative value by -1 and subtract the third column from the fourth column to arrive at our final answer

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 \end{pmatrix}$$

Note:
We note that when we are dealing with rings, not all modules are free. There are modules which simply do not have a basis. To describe some of these modules we will use matrices referred to as "Presentation Matrices". These matrices shall be fundamental in our examination of the pre-Bloch group over a finite field.

Definition: Presentation Matrix
Let A denote an $m \times n$ R-matrix. Then A defines a homomorphism of R-Modules:

$$A : R^n \to R^m$$

$$A \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = (x_1, x_2, \ldots, x_m)$$

We note that the image of this map is all linear combinations of the columns in A with coefficients in R, and thus we denote $\mathrm{Im}(A)$ by $A \cdot R^n$.

The quotient module $R^m/\mathrm{Im}(A) = R^m/A \cdot R^n$ is then "presented" by the matrix A, and we call A a presentation matrix of M. More formally, we state:

If $\exists f : R^m/A \cdot R^n \to M$ such that f is an isomorphism, and A is an $m \times n$ matrix, we call f a presentation of the module M, and say that A is a presentation matrix of M.

Example:
What is a presentation matrix of C_5 and C_7?

We note that $C_5 \cong \mathbb{Z}/5\mathbb{Z}$ with $5 \in \mathbb{Z}$, and likewise $C_7 \cong \mathbb{Z}/7\mathbb{Z}$ with $7 \in \mathbb{Z}$. Hence the matrix [5] presents C_5 and the matrix [7] presents C_7.

Note:
As the concept of relations is one which will be essential to the study of the pre-Bloch group, we will provide an example.

Example:
Consider the $\mathbb{Z}$-module generated by $\{x_1, x_2, x_3\}$ with the relations:

- $x_1 + x_2 + x_3 = 0$
- $2x_1 + -1x_2 + 3x_3 = 0$
- $-2x_1 + 4x_2 + x_3 = 0$

This is then presented by the matrix with the coefficients of the relations in the columns:

$$A = \begin{pmatrix} 1 & 2 & -2 \\ 1 & -1 & 4 \\ 1 & 3 & 1 \end{pmatrix}$$

Theorem:
Let A be a matrix associated with the homomorphism:

$$\phi_A : \mathbb{Z}^n \to \mathbb{Z}^m$$

Then the following conditions are equivalent

- $\exists n$ linearly independent columns of A
- $\text{rank}(A) = n$
- $\mathbb{Z}^m / A \cdot \mathbb{Z}^n$ is finite.

Proof:
To begin, we note that simply by the definition, the first two conditions are equivalent. So we need to show:

$$\text{rank}(A) = n \iff Z^m / A \cdot Z^n \text{(the cokernel of A) is finite.}$$

We recall our theorem previously mentioned theorem that if A is an integer matrix, then there are elementary integer matrices Q and P, which originate from row and column operations, such that:

$$A' = Q^{-1} \cdot A \cdot P$$

where A' is of the form:

$$A' = \begin{pmatrix} \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_k \end{bmatrix} & \\ & 0 \end{pmatrix}$$

with $d_1 | d_2 | d_3 | \ldots | d_k$ and $k \leq n$

Hence we can assume that A has been already diagonalised, as if not it is possible to find row and column operations to diagonalise it. Therefore A is of the form A' in the above recollection of the diagonalisation theorem.

Hence by the structure theorem we can write:

$$\mathbb{Z}^m / A\mathbb{Z}^n \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z}/d_{k+1}\mathbb{Z}/ \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$$

$\rightarrow$ If $\text{rank}(A) = n$ then the cokernel is isomorphic to the direct sum of finite sets, and is therefore finite.

$\leftarrow$ If $\mathbb{Z}^m / A\mathbb{Z}^n$ is finite, then as A can be diagonalised, we have:

$$\mathbb{Z}^m / A\mathbb{Z}^n \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z}/d_{k+1}\mathbb{Z}/ \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$$

If $\text{rank}(A) = k < n$ then,

$$\mathbb{Z}^m / A\mathbb{Z}^n \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z}/0\mathbb{Z}$$

And thus $\text{coker}(A)$ is isomorphic to an infinite set, and thus is not finite, so we must have that $\text{rank}(A) = n$.

Note:

It is this result which shall play a crucial role in our examination of the pre-Bloch group, and allow us to justify whether the pre-Bloch group is finite by examination of a matrix which presents it. This connection shall be further outlined in the next section.

2.3 Pre-Bloch Group

The relations of the pre-Bloch group over a Finite Field is the main topic of study in this paper. Inff this section we will give a brief overview of the pre-Bloch group, motivate its study, and provide some results which serve as the basis for our investigation. The study of pre-Bloch group stems from its intricate relation with hyperbolic geometry, in particular its relation to ideal tetrahedra and the dilogarithm function. An exposition on these connections may be found in: [2] and [13].

Definition: The pre-Bloch group, $\mathcal{P}(\mathbb{F})$.
Let $R(x, y)$, such that $x, y \in \mathbb{F}\backslash\{0, 1\}$ and $x \neq y$, be an element in $\mathbb{Z}[\mathbb{F}\backslash\{0, 1\}]$ such that:

$$R(x, y) = [x] - [y] + [\frac{y}{x}] - [\frac{1 - x^{-1}}{1 - y^{-1}}] + [\frac{1 - x}{1 - y}]$$

We will call this the "five term relation", where the terms are those of the dilogarithm function in [13].

The pre-Bloch group $\mathcal{P}(\mathbb{F})$ is the abelian group generated by the symbols $[x]$, with $x \in \mathbb{F}\backslash\{0, 1\}$, subject to the relation $R(x, y) = 0$ [3].

The Bloch Group, $\mathcal{B}(\mathbb{F})$ is then taken to be the kernel of the map:

$$f : \mathcal{P}(\mathbb{F}) \to \mathbb{F}^* \wedge \mathbb{F}^*$$

$$f([z]) = z \wedge (1 - z)$$

Note:
We note that $\mathcal{P}(\mathbb{F})$ is a finitely generated $\mathbb{Z}$-module when $\mathbb{F} = \mathbb{F}_q$, with a finite set of relations (of size $(q-2)\cdot(q-3)$ as $x \neq y$). Therefore $\mathcal{P}(\mathbb{F})$ has a presentation matrix which we can use to analyse $\mathcal{P}(\mathbb{F})$. It is this approach that shall form the basis of this study. We will start by giving an example.

Example:
Let us consider the relations for $\mathbb{F}_5$. We have the following list of relations:

$$R(2, 3) = [2] - [3] + [\frac{3}{2}] - [\frac{1 - 2^{-1}}{1 - 3^{-1}}] + [\frac{1 - 2}{1 - 3}] = 0[2] + 0[3] + 1[4]$$

$$R(2, 4) = [2] - [4] + [\frac{4}{2}] - [\frac{1 - 2^{-1}}{1 - 4^{-1}}] + [\frac{1 - 2}{1 - 4}] = 3[2] + 0[3] - 2[4] + 0[3]$$

$$R(3, 2) = [3] - [2] + [\frac{2}{3}] - [\frac{1 - 3^{-1}}{1 - 2^{-1}}] + [\frac{1 - 3}{1 - 2}] = 0[2] + 0[3] + 1[4]$$

$$R(3, 4) = [3] - [4] + [\frac{4}{3}] - [\frac{1 - 3^{-1}}{1 - 4^{-1}}] + [\frac{1 - 3}{1 - 4}] = -1[2] + 2[3] + 0[4]$$

$$R(4, 2) = [4] - [2] + [\frac{2}{4}] - [\frac{1 - 4^{-1}}{1 - 2^{-1}}] + [\frac{1 - 4}{1 - 2}] = -1[2] + 2[3] + 0[4]$$

$$R(4, 3) = [4] - [3] + [\frac{3}{4}] - [\frac{1 - 4^{-1}}{1 - 3^{-1}}] + [\frac{1 - 4}{1 - 3}] = 1[2] - 2[3] + 2[4]$$

Thus the presentation matrix of $\mathcal{P}(\mathbb{F}_5)$ is:

$$M = \begin{pmatrix} 0 & 3 & 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & 2 & 2 & -2 \\ 1 & -2 & 1 & 0 & 0 & 2 \end{pmatrix}$$

Note:
As $\mathbb{F}_q^*$ is generated by some $r \in \mathbb{F}_q^*$, we can rewrite the function as powers of some primitive root r as:

$$R(r^i, r^j) = [r^i] - [r^j] + [r^{j-i}] - [\frac{1-r^{-i}}{1-r^{-j}}] + [\frac{1-r^i}{1-r^j}]$$

This allows us to enumerate the elements as powers of a primitive element $r \in \mathbb{F}_q^*$.

Example: We observe that $< 2 > = \{2, 4, 3, 1\} = \mathbb{F}_5^*$. So the list of relations for $\mathbb{F}_5$, as seen before (now in terms of a generator), are:

$$R(r^1, r^2) = [r^1] - [r^2] + [r^{2-1}] - [\frac{1-r^{-1}}{1-r^{-2}}] + [\frac{1-r^1}{1-r^2}] = 3[r^1] - 2[r^2] + 0[r^3] = \{3, -2, 0\}$$

$$R(r^1, r^3) = [r^1] - [r^3] + [r^{3-1}] - [\frac{1-r^{-1}}{1-r^{-3}}] + [\frac{1-r^1}{1-r^3}] = 0[r^1] + 1[r^2] + 0[r^3] = \{0, 1, 0\}$$

$$R(r^2, r^1) = [r^2] - [r^1] + [r^{2-1}] - [\frac{1-r^{-2}}{1-r^{-1}}] + [\frac{1-r^2}{1-r^1}] = -1[r^1] + 0[r^2] + 2[r^3] = \{-1, 0, 2\}$$

$$R(r^2, r^3) = [r^2] - [r^3] + [r^{2-3}] - [\frac{1-r^{-2}}{1-r^{-3}}] + [\frac{1-r^2}{1-r^3}] = 1[r^1] + 2[r^2] + -2[r^3] = \{1, 2, -2\}$$

$$R(r^3, r^1) = [r^3] - [r^1] + [r^{3-1}] - [\frac{1-r^{-3}}{1-r^{-1}}] + [\frac{1-r^3}{1-r^1}] = 0[r^1] + 1[r^2] + 0[r^3] = \{0, 1, 0\}$$

$$R(r^3, r^2) = [r^3] - [r^2] + [r^{3-2}] - [\frac{1-r^{-3}}{1-r^{-2}}] + [\frac{1-r^3}{1-r^2}] = -1[r^1] + 0[r^2] + 2[r^3] = \{-1, 0, 2\}$$

and thus our presentation matrix, now with re-ordered rows and columns, is:

$$M = \begin{pmatrix} 3 & 0 & -1 & 1 & 0 & -1 \\ -2 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & -2 & 0 & 2 \end{pmatrix}$$

Definition: $\{x\}$
For $x \in \mathbb{F}^*$, we define:

$$\{x\} := \begin{cases} [x] + [x^{-1}] \text{ if } x \neq 1 \\ 0 \text{ if } x = 1 \end{cases} \in \mathcal{P}(\mathbb{F})$$

Note:
Through an abuse of notation, we will later use this same notation to refer to an element in $\mathbb{Z}[\mathbb{F}\backslash\{0,1\}]$. We will explicitly note when we are working in $\mathbb{Z}[\mathbb{F}\backslash\{0,1\}]$.

Proposition:
It is a well-known result of Suslin [8] that the map $f : x \to \{x\}$ is a homomorphism from $\mathbb{F}^*$ to the

elements of order dividing 2 in $\mathcal{P}(\mathbb{F})$.

Proof:
We note that in the group $\mathcal{P}(\mathbb{F})$ we have the following identities:

$$R(x,y) = [x] - [y] + [\frac{y}{x}] - [\frac{1-x^{-1}}{1-y^{-1}}] + [\frac{1-x}{1-y}] = 0$$

$$R(x^{-1},y^{-1}) = [x^{-1}] - [y^{-1}] + [\frac{y^{-1}}{x^{-1}}] - [\frac{1-x^{1}}{1-y^{1}}] + [\frac{1-x^{-1}}{1-y^{-1}}] = 0$$

By adding these equations we see:

$$R(x,y)+R(x^{-1},y^{-1}) = [x]-[y]+[\frac{y}{x}]-[\frac{1-x^{-1}}{1-y^{-1}}]+[\frac{1-x}{1-y}]+[x^{-1}]-[y^{-1}]+[\frac{y^{-1}}{x^{-1}}]-[\frac{1-x^{1}}{1-y^{1}}]+[\frac{1-x^{-1}}{1-y^{-1}}] = 0$$

and by rearranging and simplifying we get:

$$R(x,y) + R(x^{-1},y^{-1}) = ([x] + [x^{-1}]) - ([y] + [y^{-1}]) + ([\frac{y}{x}] + [\frac{x}{y}]) = 0$$

and by using our definition of $\{x\}$ we get:

$$R(x,y) + R(x^{-1},y^{-1}) = \{x\} - \{y\} + \{z\} = 0$$

However, now observe that we can also interchange x and y to get the relation:

$$R(y,x) + R(y^{-1},x^{-1}) = \{y\} - \{x\} + \{z^{-1}\} = 0$$

And by adding both relations we get:

$$2\{z\} = 0$$

We thus verify that $2\{x\} = 0$ $\forall x \in \mathbb{F}_q^*$

Corollary:
From the above, we also see that the relation $\{x\} + \{\frac{y}{x}\} = \{y\}$ holds. This is valid as if $x = y$, $x = 1$, the relation is trivial. If $y = 1$ then as $\{x\} = \{x^{-1}\}$ we retrieve the relation $2\{x\} = 0$.

Proposition:
It is also well-known result of Suslin [8] that in $\mathcal{P}(\mathbb{F})$, $c_{\mathbb{F}} = [x] + [1-x]$ is constant $\forall x \in \mathbb{F}\backslash\{0,1\}$.

Proof:
We note that in the group $\mathcal{P}(\mathbb{F})$ we have the following identities:

$$R(x,y) = [x] - [y] + [\frac{y}{x}] - [\frac{1-x^{-1}}{1-y^{-1}}] + [\frac{1-x}{1-y}] = 0$$

$$R(1-y,1-x) = [1-y] - [1-x] + [\frac{1-x}{1-y}] - [\frac{1-(1-y)^{-1}}{1-(1-x)^{-1}}] + [\frac{1-(1-y)}{1-(1-x)}] = 0$$

By subtracting the two relations, we see:

$$R(x,y) - R(1-y,1-x) = [x] + [1-x] - ([y] + [1-y]) = 0$$

and thus we get our desired equality that

$$[x] + [1 - x] = [y] + [1 - y]$$

Corollary:
$3c_{\mathbb{F}} = \{-1\}$

Proof:
We have from the above:

$$3c_{\mathbb{F}} = [x] + [1 - x] + [x^{-1}] + [1 - x^{-1}] + [(1 - x)^{-1}] + [1 - (1 - x)^{-1}]$$

$$3c_{\mathbb{F}} = \{x\} + \{1 - x\} + \{1 - x^{-1}\} = \{-(1 - x)^2\} = \{-1\}$$

Corollary:

$$6c_{\mathbb{F}} = 0$$

Proof:
Recall we have:

$$3c_{\mathbb{F}} = \{-1\}$$

Thus:

$$6c_{\mathbb{F}} = \{-1\} + \{-1\} = 2\{-1\}$$

And as $2\{x\} = 0$ we have our result that:

$$6c_{\mathbb{F}} = \{-1\} + \{-1\} = 0$$

Proposition:
$\mathcal{P}(\mathbb{F}) \cong C_{q+1}$ and thus, because this is finite, the rank of the presentation matrix of $\mathcal{P}(\mathbb{F})$ is maximal.

Proof:
This was proved by Hutchinson [6].

Note:
This proof is what shall form the basis of our research. The proof is based primarily on techniques from homological algebra. It is highly desirable to find a more direct proof of this result so we can get to the essence of the pre-Bloch group to try and determine what precisely is responsible for its structure. In particular, this proof also tell us that the pre-Bloch group over a finite field is itself finite, and thus of maximal rank. This tells us that out of the total $(q - 2) \cdot (q - 3)$ relations for a finite field $\mathbb{F}_q$, there are in fact $q - 2$ of these which are linearly independent. It would be quite interesting to determine which relations, and why, are the linearly independent relations, as these are going to determine the entire pre-Bloch group.

3 Main Body

We recall our motivating question for this study:

Question: Is it possible to explicitly and systematically describe $q-2$ relations of the total $(q-2)\cdot(q-3)$ which are linearly independent as q varies?

There are a number of challenges, detailed below, which make this question difficult to answer.

Challenge 1: The first immediate difficulty one encounters is that the number of relations for a finite field $\mathbb{F}_q$ is $(q-2)\cdot(q-3)$. As the the size of the field increases, the total number of relations grows quadratically, while the number of elements in $\mathbb{F}_q$ grows linearly. Even when the field contains only 13 elements, there are already a total of 110 relations, and of these we are looking for 10 linearly independent relations. As we wish to find a consistent set of relations which are linearly independent regardless of the field, it is necessary to be able to examine a set of relations across a number of fields, to try and identify any pattern which may arise in which relations are linearly independent to one another. As the total number of relations increases very quickly, the size of the matrix becomes very large (as it has dimensions $(q-2)\times(q-2)\cdot(q-3)$), and it quickly becomes inefficient to compute all relations by hand, the first step in our study was to write a programme to automate this process.

Challenge 2: The second difficulty which arises is how we should try to choose which relations to select. Ideally, we would like to arrange our presentation matrix such that the first $q-2$ columns (which correspond to a relation) are linearly independent, and the remaining columns are those which are linearly dependant (and thus may be removed).There are two obvious methods which can be used to order elements of a finite field. The first method consists of a simple lexographic ordering. The second method consists of considering the elements in finite field as powers of a generator of the multiplicative group of the finite field, and ordering them according to the power of this generator. We need to determine some way to choose which elements of the finite field to select for our relations, and this is something which is non-obvious.

Challenge 3: The third challenge which presents itself is the lack of information we have about the connection between addition and multiplication in a finite field. This proves to be an important point as determing what the terms

$$[\frac{1-x^{-1}}{1-y^{-1}}] \text{ and } [\frac{1-x}{1-y}]$$

from the five term relation will be as a power of a generator in the field is important to determing what the coefficient is of each element of the field for a given relation. These terms are highly variable to what elements in the field we choose for the relation. Finding identities that allow us to restrict what these terms can be, and impose further conditions on the relations will be particularly important. Because of how variable a relation is depending on which elements of the field are selected, it is entirely possible that there may not be a consistent set of relations which are linearly independent in every field; it may simply depend entirely on the field that we choose.

Challenge 4: The fourth and final difficulty which presents itself is that while we know the entire group is generated by a single element, we do not have a description as to what this element is. This problem is comparable to determining what element of a finite field is a generator, a problem for which we currently have no general solution for.

Various methods of attacking this problem were tried over the course of this study. We will provide details on the main results which we achieved, including a lower bound on the rank of the presentation matrix, and the main techniques which were used below.

3.1 Program to Calculate the Pre-Bloch Group

As the number of relations grows very quickly with the size of the field, the beginning of this investigation necessitated the creation of a computer program which would allow the underlying relations of the pre-Bloch group of a finite field to be quickly determined.

To accomplish this, I used Mathematica, a computational program based on the programming language known as ”Wolfram Language”, which is designed to ’automate away’ some of the ’lower level structure’ of other programming languages [12]. The main motivators for using Mathematica over other computational programs was the support for ”Finite Fields” through the ”Finite Fields Package” [11], and the author’s own familiarity with the program. The author is confident that similar computational programs which support finite fields, such as ”Sage Math” or ”Matlab”, could implement a similar algorithm. Similarly, the program has not been optimised for efficiency as its primary purpose was to simply allow for the quick calculation of the presentation matrix. It is very likely that there are a number of optimisations which could be made to this program.

Our program is as follows. We will supply and explain each piece of the code individually, and we will then at the end provide the program in its entirety

Code Input:

```
Needs["FiniteFields‘"]
Needs["IntegerSmithNormalForm‘"]
```

Code Output:

```
-Not Applicable-
```

Explanation: The first package loaded allows for the manipulation of finite fields. The second package provides an implementation which allows matrices to be put in Smith Normal Form using only the row and column manipulations which are allowed to be used for an integer matrix. This pacakage was written by Dr. Jabon and is available at (http : // library.wolfram.com/infocenter/MathSource/682/).

Code Input:

```
 FieldPowers[m_] := PowerList[GF[m]]
 Table[PowerListQ[GF[Prime[i]]] = True, {i, 80}]
 PowerListQ[GF[5]]
 Table[PowerListQ[GF[Prime[i]^2]] = True, {i, 20}]
 Table[PowerListQ[GF[Prime[i]^3]] = True, {i, 15}]
 Table[PowerListQ[GF[Prime[i]^4]] = True, {i, 10}]
```

Code Output:

```
 {Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, \
 Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, \
 Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, \
 Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, \
 Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, \
 Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, \
 Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, \
 Null, Null, Null}

 True

 {Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, \
 Null, Null, Null, Null, Null, Null, Null, Null, Null}

 {Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, Null, \
 Null, Null, Null, Null}

 {Null, Null, Null, Null, Null, Null, Null, Null, Null, Null}
```

Explanation: We start by defining a function called "FieldPowers[m]", where m refers to the order of the field. This function outputs the result as a vector whose length corresponds to the degree of the polynomial used to generate the elements of the field. This function outputs the elements of a given field by determining a generator of the field and returning the element as powers of that generator, where the first element corresponds to r^{q-1}, the second element corresponds to r^1, etc. Further details on which polynomials and generators Mathematica uses to generate these elements may be found in the documentation of the finite fields package [11]. The convention Mathematica uses is that a vector $\{v_0, v_1, v_2\}$ corresponds to the polynomial $v_0 + v_1x^1 + v_2x^2$.

We next begin by enabling the ability to take the discrete logarithm of an element of a given field. This must be manually enabled for every field. To take "Table[PowerListQ[GF[Prime[i]]] = True, i, 80]" as an example, this enables the ability to take the discrete logarithm of the fields $\mathbb{F}_p$ where p is one of the first 80 prime numbers. Subsequent instances enable the ability to take the discrete logarithm of extensions of a set number of fields. This function is computationally heavy, but it can easily be adjusted to enable the discrete logarithm for as many fields as one is interested in by increasing the bound of each line to include the desired number of fields.

Code Input:

```
FieldPowers[4]
Print["The above is the list of F4"]
FieldPowers[5]
Print["The above is the list of F5"]
FieldPowers[7]
Print["The above is the list of F7"]
```

Code Output:

```
{{1, 0}, {0, 1}, {1, 1}}

The above is the list of F4
```

```
 {{1}, {2}, {4}, {3}}

The above is the list of F5

{{1}, {3}, {2}, {6}, {4}, {5}}

The above is the list of F7
```

Explanation: Here we see examples to verify that the function ”FieldPowers[x]” correctly returns the vectors associated with the elements in the field $\mathbb{F}_x$. One important point here is that these vectors are not returned as elements in the field. This means addition between two vectors, say 3 and 4 in ”FieldPowers[5]” will return 7, rather than the desired 2. We verify that these are indeed the elements of the fields $\mathbb{F}_4$,$\mathbb{F}_5$, and $\mathbb{F}_7$.

Code Input:

```
Id[x_] := First[FieldPowers[x]]

Id[4]
Id[5]
Id[7]
```

Code Output:

```
 {1, 0}

 {1}

 {1}
```

Explanation: This defines a new function called ”Id[x]” which takes as an input the order of our field, and returns as an output the identity of that field by taking the first element of our function ”FieldPowers[x]” (which recall is ordered such that the first element is the identity, the generator of the field is the second element, and subsequent elements are successive powers of the generator). We verify that this correctly returns the identity element for each of $\mathbb{F}_4$,$\mathbb{F}_5$, and $\mathbb{F}_7$.

Code Input:

```
FL1[x_] := DeleteCases[FieldPowers[x], Id[x]]

FL1[4]
FL1[5]
FL1[7]
```

Code Output:

```
 {{0, 1}, {1, 1}}

 {{2}, {4}, {3}}

 {{3}, {2}, {6}, {4}, {5}}
```

Explanation: We define a new function "FL1[x]" which takes the order of a field as an input, and returns the elements in $\mathbb{F}_x \backslash \{1\}$. This is ordered according to powers of a generator, where the generator is the first element. We verify that $FL1[4]$, $FL1[5]$, and $FL[7]$ return the correct values.

Code Input:

```
G[p_, a_] :=
If[Mod[a, p - 1] != 0, Part[FL1[p], Mod[a, p - 1]], Id[p]]
(*This is going to give the element of the field which corresponds to \
power a of a generator in a field p*)



G[5, 2]
G[5, 3]
G[5, 4] == Id[5]
```

Code Output:

```
{4}

{3}

True
```

Explanation: We define a new function $G[p, a]$ which takes the order of the field as p and the power of a generator of that field as a, and then outputs the vector which corresponds to r^a. It does this by first determing if r^a is the identity. If it is the identity, it returns the identity. If it is not the identity, it takes the element in FL1[p] which corresponds to the power of the generator given. It takes this modulo $p - 1$ to ensure powers higher than this return correct answers. We see examples that verify this is working correctly by examining the field $\mathbb{F}_5$

Code Input:

```
FY[p_, a_] := GF[p][G[p, a]]
Field[p_] := Table[FY[p, i], {i, 1, p - 2}]
FOne[p_] := GF[p][Id[p]]
FY[5, 1]
FY[5, 2]
```

```
FY[5, 3]
FY[5, 4]
FY[4, 1]
FY[4, 2]
FY[4, 3]
FY[7, 1]
FY[(Prime[10])^2, 17]
```

Code Output:

$\{2\}_5$
$\{4\}_5$
$\{3\}_5$
$\{1\}_5$
$\{0, 1\}_2$
$\{1, 0\}_2$
$\{3\}_7$
$\{8, 26\}_{29}$

Explanation: Here we define ”FY[p,x]” to place the element into the field and allow arithmetic to be done inside that field. In Mathematica, this is accomplished using the function ”GF[p][v]”, where ”v” corresponds to the vector of the element in that field. Here, we substituted our function ”G[p,a]” for ”v” as this function returns the vector of the element associated with r^a in the field $\mathbb{F}_p$ (where p in this case is a prime or a power of a prime). FY[p,a] therefore outputs the element r^a when considered as an elment in the field.

The function ”Field[p]” outputs every element in a field $\mathbb{F}_p$,where p is the order of the field (prime, or a power of a prime), considered by Mathematica as an element of the field.

The function ”FOne[p]” outputs the identity in the field as an element in the field.

We compute a number of examples to verify that our function ”FY[p,a]” does indeed give us the answers which we expect, and one can verify that the output is correct.

We now have the means of selecting every element of any field, by selecting the order of the field, and choosing every possible power of a generator to provide every element in the field (as Field[p] does). We will use this to define the five term relation.

Code Input:

```
R[p_, a_, b_] :=
g[FY[p, a]] - g[FY[p, b]] + g[FY[p, b]/FY[p, a]] -
g[(FY[p, b]/
FY[p, a])*((FOne[p] - FY[p, a])/(FOne[p] - FY[p, b]))] +
g[(FOne[p] - FY[p, a])/(FOne[p] - FY[p, b])]

See[p_, a_, b_] :=
Print[g[FY[p, a]], " - ", g[FY[p, b]], " + ", g[FY[p, b]/FY[p, a]],
" - ", g[(FY[p, b]/
FY[p, a])*((FOne[p] - FY[p, a])/(FOne[p] - FY[p, b]))], " + ",
g[(FOne[p] - FY[p, a])/(FOne[p] - FY[p, b])]]
```

Code Output:

```
 -Not Applicable-
```

Explanation: Here we define the five term relation as R[p,a,b].

We define this function first by recalling that as powers of a generator of a finite field $\mathbb{F}_q$, it can be written as:

$$R(r^i, r^j) = [r^i] - [r^j] + [r^{j-i}] - [\frac{1-r^{-i}}{1-r^{-j}}] + [\frac{1-r^i}{1-r^j}]$$

We replace ”[x]” where $x \in \mathbb{F}_q$ with an undefined function named ”g(x)”, noting that in Mathematica functions are described using square brackets, to give us:

$$R(r^a, r^b) = g[r^a] - g[r^b] + g[r^{b-a}] - g[\frac{1-r^{-a}}{1-r^{-b}}] + g[\frac{1-r^a}{1-r^b}]$$

This function ’g’ exists such that in Mathematica, only terms with the same element from the finite field add together. Without the undefined function ’g’ inputted, Mathematica will default to adding the terms inside the finite field and only a single element of the finite field will be outputted. With this function, we can avoid this situation occuring.

We then translate that function into Mathematica, using ”FY[p,a]” to input ”$r^a \in \mathbb{F}_p$”, ”FY[p,b]” to input ”$r^b \in \mathbb{F}_p$”, and ”FOne[p]” to input $1_{\mathbb{F}_p}$.

Hence ”R[p,a,b]” allows us to find the relation corresponding to $R(r^a, r^b)$ for the field $\mathbb{F}_p$ where p is a prime or a power of a prime.

We also define the function ”See[p,a,b]” which allows us to see the calculation term-by-term to allow for easy troubleshooting if needed.

Code Input:

```
R[5, 1, 3]
See[5, 1, 3]
R[4, 1, 1]
R[4, 1, 2]
R[4, 2, 1]
R[4, 2, 2]
```

Code Output:

$g[\{4\}_5]]$
$g[\{2\}_5] - g[\{3\}_5] + g[\{4\}_5] - g[\{2\}_5] + g[\{3\}_5]$

$g[\{1,0\}_2]$
$3g[\{0,1\}_2] - 2g[\{1,1\}_2]]$
$-2g[\{0,1\}_2] + 3g[\{1,1\}_2]$
$g[\{1,0\}_2]$

Explanation: We calculate a few examples relations to verify this is working correctly. We manually verify that:

$$R(5,1,3) = R(2^1,2^3) = R(2,3) = g[2]-g[3]+g[\frac{3}{2}]-g[\frac{1-2^{-1}}{1-3^{-1}}]+g[\frac{1-2}{1-3}] = g[2]-g[3]+g[4]-g[2]+g[3] = g[4]$$

which is correct

$$R(4,1,1) = R(x,x) = g[x] - g[x] + g[\frac{x}{x}] - g[\frac{1-x^{-1}}{1-x^{-1}}] + g[\frac{1-x}{1-x}] = g[1]$$

which is not a valid relation as we do not take equal terms, but is correct in $\mathbb{F}_4$

$$R(4,1,2) = R(x,x^2) = g[x]-g[1+x]+g[\frac{1+x}{x}]-g[\frac{1-(x)^{-1}}{1-(1+x)^{-1}}]+g[\frac{1-(x)}{1-(1+x)}] = 3g[x]-2g[1+x]$$

which is correct in $\mathbb{F}_4$

$$R(4,2,1) = R(x^2,x^1) = g[1+x]-g[x]+g[\frac{x}{1+x}]-g[\frac{1-(1+x)^{-1}}{1-(x)^{-1}}]+g[\frac{1-(1+x)}{1-(x)}] = -2g[x]-3g[1+x]$$

which is correct in $\mathbb{F}_4$

$$R(4,2,2) = R(x^2,x^2) = g[1+x] - g[1+x] + g[\frac{1+x}{1+x}] - g[\frac{1-(1+x)^{-1}}{1-(1+x)^{-1}}] + g[\frac{1-(1+x)}{1-(1+x)}] = g[1]$$

which is not a valid relation as we do not take equal terms, but is correct in $\mathbb{F}_4$.

And thus is returning correct values for our relations, except for those in which we have $R(r^x, r^x)$.

Code Input:

```
AllRR[p_] := Flatten[Table[R[p, i, j], {i, 1, p - 2}, {j, 1, p - 2}]]

AllRR[4]
AllRR[5]
AllRR[7]
```

Code Output:

$\{g[\{1,0\}_2], 3g[\{0,1\}_2] - 2g[\{1,1\}_2], -2g[\{0,1\}_2] + 3g[\{1,1\}_2], g[\{1,0\}_2]\}$
$\{g[\{1\}_5], 3g[\{2\}_5]-2g[\{4\}_5], g[\{4\}_5], -g[\{2\}_5]+2g[\{3\}_5], g[\{1\}_5], g[\{2\}_5]-2g[\{3\}_5]+2g[\{4\}_5], g[\{4\}_5], -g[\{2\}_5]+2g[\{3\}_5], g[\{1\}_5]\}$
$\{g[\{1\}_7], 2g[\{3\}_7] - g[\{6\}_7], g[\{2\}_7] + g[\{3\}_7] - g[\{5\}_7], 2g[\{3\}_7] - 2g[\{4\}_7] + g[\{6\}_7], -g[\{2\}_7] + g[\{3\}_7]+2g[\{4\}_7]-g[\{5\}_7], g[\{2\}_7]-g[\{3\}_7]+g[\{4\}_7]+g[\{5\}_7]-g[\{6\}_7], g[\{1\}_7], 2g[\{3\}_7]-g[\{6\}_7], 2g[\{2\}_7]- g[\{3\}_7] - g[\{4\}_7] + g[\{5\}_7], 2g[\{2\}_7] - 2g[\{5\}_7] + g[\{6\}_7], -2g[\{3\}_7] + g[\{4\}_7] + 2g[\{6\}_7], -g[\{2\}_7] -$

$g[\{4\}_7]+2g[\{5\}_7]+g[\{6\}_7], g[\{1\}_7], g[\{3\}_7]-g[\{5\}_7]+g[\{6\}_7], g[\{2\}_7]+g[\{3\}_7]-g[\{5\}_7], -g[\{2\}_7]-g[\{3\}_7]+g[\{4\}_7]+g[\{5\}_7]+g[\{6\}_7], -g[\{2\}_7]+g[\{3\}_7]+2g[\{4\}_7]]-g[\{5\}_7], g[\{2\}_7]-g[\{3\}_7]+g[\{4\}_7]+g[\{5\}_7]-g[\{6\}_7], g[\{1\}_7], g[\{3\}_7]-g[[\{5\}_7]]+g[\{6\}_7], 2g[\{2\}_7]-g[\{3\}_7]-g[\{4\}_7]+g[\{5\}_7], -g[\{2\}_7]-g[\{3\}_7]+g[\{4\}_7]+g[\{5\}_7]+g[\{6\}_7], g[\{4\}_7]+2g[\{5\}_7]-2g[\{6\}_7], -g[\{2\}_7]-g[\{4\}_7]+2g[\{5\}_7]+g[\{6\}_7], g[\{1\}_7]\}$

Explanation: We define a function "AllRR[p] which uses our "R[p,a,b]" and iterates over all possible values of r^a and r^b excluding where $r^a = 1$ or $r^b = 1$, to output all possible relations associated with a certain field, including those relations where $a = b$ which will be the only relations to result in the (invalid) output "g[1]". We also verify with examples that "AllRR[p]" outputs the correct relations (and the invalid relations which produce "g[1]"). We use the function "Flatten[]" so that the output of AllRR[p] is a vector, with each term of the vector corresponding to a relation.

Code Input:

```
AR[p_] :=
DeleteCases[AllRR[p],
g[FOne[p]]](*all the relations except when a=b ones*)

DescriptionOfRelations[p_] := {AR[p],
Print["\n The number of Relations:Unique Relations in F", p,
" is: ", Length[AR[p]], " : ",
Length[DeleteDuplicates[Flatten[AR[p]]]]]}

DescriptionOfRelations[4]
DescriptionOfRelations[5]
```

Code Output:

The number of Relations:Unique Relations in F4 is: 2 : 2

$\{\{3g[\{0,1\}_2]-2g[\{1,1\}_2], -2g[\{0,1\}_2]+3g[\{1,1\}_2]\}, Null\}$

The number of Relations:Unique Relations in F5 is: 6 : 4

$\{\{3g[\{2\}_5]-2g[\{4\}_5], g[\{4\}_5], -g[\{2\}_5]+2g[\{3\}_5], g[\{2\}_5]-2g[\{3\}_5]+2g[\{4\}_5], g[\{4\}_5], -g[\{2\}_5]+2g[\{3\}_5]\}, Null\}$

Explanation: First, we define the function "AR[p]" to be all of the relations, except those where we are taking the relation of two identical elements, which correspond to the result "g[1]"). This function "AR[p]" outputs all of the relations for a field $\mathbb{F}_p$. Secondly, we define DescriptionOfRelations[p]. This allows us to identify gow many relations there are in total for a field, how many of these relations are unique (which is to say, it deletes all duplicate relations), and it outputs all relations. It must be noted that in "DescriptionOfRelations", the final entry "Null" is outputted where "g[1]" has been expelled from the list of relations. This "Null" does not appear in AR[p], and does not affect the count of the number of unique or total relations. It can be removed by deleting null cases from "DescriptionOfRelations", but has been left simply because it does not affect the function which is only designed to get a description of the relations for certain fields. We can compute a number of examples and we can verify that these do indeed correspond to what we are expecting, and that the count of the relations, and the unique relations, are accurate as they should be.

Code Input:

```
g[x_] := f[FieldInd[x]]
AR[5]
```

Code Output:

```
{3 f[1] - 2 f[2], f[2], -f[1] + 2 f[3], f[1] + 2 f[2] - 2 f[3],
f[2], -f[1] + 2 f[3]}
```

Explanation: We now define our function ”g[x]” by setting it to be another undefined function ”f” and by taking the discrete logarithm of ”x”. This is necessary because up until now, the elements are still considered to be elements in the field. By taking the discrete logarithm of each element we convert it back into an integer where ”f[1]” now corresponds to ”g[r^1]”, 'f[2]” corresponds to ”g[r^2]” etc.

Code Input:

```
PresentationMatrixOf[q_] :=
Transpose[D[AR[q], {g /@ Field[q]}]] // MatrixForm
Answer[p_] :=
Transpose[D[AR[p], {g /@ Field[p]}]] // SmithForm // MatrixForm
FinalAnswer[p_] := {Transpose[D[AR[p], {g /@ Field[p]}]] // MatrixForm ,
Transpose[D[AR[p], {g /@ Field[p]}]] // MatrixRank ,
Transpose[D[AR[p], {g /@ Field[p]}]] // SmithForm // MatrixForm}
```

Code Output:

```
-Not Applicable-
```

Explanation: Finally, we define the function ”PresentationMatrixOf[q]” which outputs the matrix:

$$M_q := \begin{pmatrix} \uparrow & \cdots & \uparrow & \uparrow & \cdots & \uparrow & \cdots & \uparrow & \cdots & \uparrow \\ R(r^1, r^2) & \dots & R(r^1, r^{q-2}) & R(r^2, r^1) & \dots & R(r^2, r^{q-2}) & \dots & R(r^{q-2}, r^1) & \dots & R(r^{q-2}, r^{q-3}) \\ \downarrow & \cdots & \downarrow & \downarrow & \cdots & \downarrow & \cdots & \downarrow & \cdots & \downarrow \end{pmatrix}$$

where $a_{s,j} = a_s[r^s]$ in the Relation R corresponding to column j, for the field $\mathbb{F}_q$.

Here, the function ”D” is a differential operator, and using this we can extract the coefficient for ”f”. In order to use the function ”D”, it is necessary that we are no longer considering the elements as finite field elements. It is for this reason that it is essential that we took the discrete logarithm of this element previously. We also define ”Answer[p]” which puts the presentation matrix into Smith Normal Form (using the function ”SmithForm” from the package we loaded), and the ”FinalAnswer[p]” function which outputs a vector containing the presentation matrix, the rank of the matrix, and the Smith Normal Form of the matrix.

We make the observation that it appears for small values the Smith Normal Form appears to always be of the form:

$$M_q = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & q+1 \end{pmatrix}$$

However we note that we have very limited evidence of this and thus one should be very cautious as our program is only able to efficiently calculate the presentation matrix, and the Smith Normal Form of the presentation matrix, for very small values and thus our evidence is limited.

Conclusion: Our final program is thus:

Code Input 1: Load Packages

```
Needs["FiniteFields‘"]
Needs["IntegerSmithNormalForm‘"]
```

Code Input 2: Define the relations in terms of an undefined function ’g’

```
FieldPowers[m_] := PowerList[GF[m]]

Table[PowerListQ[GF[Prime[i]]] = True, {i, 80}]
Table[PowerListQ[GF[Prime[i]^2]] = True, {i, 20}]
Table[PowerListQ[GF[Prime[i]^3]] = True, {i, 15}]
Table[PowerListQ[GF[Prime[i]^4]] = True, {i, 10}]

Id[x_] := First[FieldPowers[x]]
FL1[x_] := DeleteCases[FieldPowers[x], Id[x]]

G[p_, a_] :=
If[Mod[a, p - 1] != 0, Part[FL1[p], Mod[a, p - 1]], Id[p]]

FY[p_, a_] := GF[p][G[p, a]]

Field[p_] := Table[FY[p, i], {i, 1, p - 2}]

FOne[p_] := GF[p][Id[p]]

R[p_, a_, b_] :=
g[FY[p, a]] - g[FY[p, b]] + g[FY[p, b]/FY[p, a]] -
g[(FY[p, b]/FY[p, a])*((FOne[p] - FY[p, a])/(FOne[p] - FY[p, b]))] +
g[(FOne[p] - FY[p, a])/(FOne[p] - FY[p, b])]
```

```
See[p_, a_, b_] := Print[g[FY[p, a]], " - ", g[FY[p, b]], " + ", g[FY[p, b]/FY[p, a]], " - ",
 g[(FY[p, b]/FY[p, a])*((FOne[p] - FY[p, a])/(FOne[p] - FY[p, b]))], " + ",
g[(FOne[p] - FY[p, a])/(FOne[p] - FY[p, b])]]

AllRR[p_] := Flatten[Table[R[p, i, j], {i, 1, p - 2}, {j, 1, p - 2}]]

AR[p_] :=  DeleteCases[AllRR[p], g[FOne[p]]]

DescriptionOfRelations[p_] := {AR[p],
Print["\n The number of Relations:Unique Relations in F", p,
" is: ", Length[AR[p]], " : ",
Length[DeleteDuplicates[Flatten[AR[p]]]]]}
```

Code Input 3: Define 'g' and the presentation matrix.

```
g[x_] := f[FieldInd[x]]

PresentationMatrixOf[q_] :=  Transpose[D[AR[q], {g /@ Field[q]}]] // MatrixForm

Answer[p_] :=  Transpose[D[AR[p], {g /@ Field[p]}]] // SmithForm // MatrixForm

FinalAnswer[p_] := {Transpose[D[AR[p], {g /@ Field[p]}]] // MatrixForm ,
Transpose[D[AR[p], {g /@ Field[p]}]] // MatrixRank ,
Transpose[D[AR[p], {g /@ Field[p]}]] // SmithForm // MatrixForm}
```

3.2 Relation Identities

With the Mathematica program complete, it becomes possible to look for patterns among the relations to try and see if anything can be gleaned which we can use to leverage a proof that the rank of our matrix is maximal. As it is difficult to tell in advance what coefficients we will get from a relation, or a set of relations, it becomes useful to look at identities of relations, using our program to try and assist in finding these. We will outline two identities which were uncovered in this section.

Recall our five term equation:

$$R(x,y) = [x] - [y] + [\frac{y}{x}] - [\frac{1-x^{-1}}{1-y^{-1}}] + [\frac{1-x}{1-y}]$$

which can also be written as

$$R(r^i, r^j) = [r^i] - [r^j] + [r^{j-i}] - [\frac{1-r^{-i}}{1-r^{-j}}] + [\frac{1-r^i}{1-r^j}]$$

and also recall our presentation matrix M_q has the form:

$$M_q := \begin{pmatrix} \uparrow & \cdots & \uparrow & \uparrow & \cdots & \uparrow & \cdots & \uparrow & \cdots & \uparrow \\ R(r^1,r^2) & \dots & R(r^1,r^{q-2}) & R(r^2,r^1) & \dots & R(r^2,r^{q-2}) & \dots & R(r^{q-2},r^1) & \dots & R(r^{q-2},r^{q-3}) \\ \downarrow & \cdots & \downarrow & \downarrow & \cdots & \downarrow & \cdots & \downarrow & \cdots & \downarrow \end{pmatrix}$$

where $a_{s,j} = a_s[r^s]$ in the Relation R corresponding to column j.

We are looking for patterns among these matrices as q varies. We will motivate one of these identities with some examples, but first we will make an important note.

<u>**Note**</u>:
First, observe that:

$$R(r^i, r^j) = \sum_{n=1}^{q-2} a(i,j)_n [r^n] \text{ with } a(i,j)_n \in \mathbb{Z}$$

We will, when the meaning is unambiguous, simply refer to $a(i,j)_n$ as a_n for convenience.

By defining the homomorphism:

$$\varepsilon : \mathbb{Z}[\mathbb{F}_q \backslash \{0,1\}] \to \mathbb{Z}$$

$$\varepsilon(\sum_{n=1}^{q-2} a_n [r^n]) = \sum_{n=1}^{q-2} a_n$$

We observing that as there are three positive and two negative terms in our five term relation that

$$\varepsilon(R(r^i, r^j)) = \sum_{n=1}^{q-2} a(i,j)_n = 1 \text{ with } -2 \leq \varepsilon(a(i,j)_n) \leq 3$$

These results will prove to be essential to one of our identities.

Using these results, we will begin with some examples to motivate our main result.

Example:
Take $\mathbb{F}_4\backslash\{0,1\}$. We observe that $< x > = \{x, 1+x, 1\} = \mathbb{F}_4^*$. So the relations for $\mathbb{F}_4$ are

$$R(r,r^2) = [r] - [r^2] + [r^{2-1}] - [\frac{1-(r)^{-1}}{1-(r)^{-2}}] + [\frac{1-(r)}{1-(r^2)}] = 3[r^1] - 2[r^2]$$
$$R(r^2,r^1) = [r^2] - [r^1] + [r^{1-2}] - [\frac{1-(r)^{-2}}{1-(r)^{-1}}] + [\frac{1-(r^2)}{1-(r^1)}] = -2[r^1] + 3[r^2]$$

and thus:

$$M_4 = \begin{pmatrix} 3 & -2 \\ -2 & 3 \end{pmatrix}$$

Observe:
In M_4:

$$((3)+(-2))[r^1] = (1)[r^1]$$
$$((-2)+(3))[r^2] = (1)[r^2]$$

So $\sum_{i=1}^{(4-2)}(\sum_{j=1,j\neq i}^{(4-2)} R(r^i,r^j)) = \sum_{i=1}^{(4-2)}(4-3)[r^i]$.

Example:
Take $\mathbb{F}_5\backslash\{0,1\}$. Recall as we've seen that:

$$M_5 = \begin{pmatrix} 3 & 0 & -1 & 1 & 0 & -1 \\ -2 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & -2 & 0 & 2 \end{pmatrix}$$

Thus In M_5:

$$((3+0)+(-1+1)+(0-1))[r^1] = (2)[r^1]$$

$$((-2+1)+(0+2)+(1+0))[r^2] = (2)[r^2]$$

$$((0+0)+(2-2)+(0+2))[r^3] = (2)[r^3]$$

So $\sum_{i=1}^{(5-2)}(\sum_{j=1,j\neq i}^{(5-2)} R(r^i,r^j)) = \sum_{i=1}^{(5-2)}(5-3)[r^i]$.

We may observe that if we try for $\mathbb{F}_7$ that the sum of a row is $(7-3)$, if we try for $\mathbb{F}_8$ that the sum of a row is $(8-3)$, and for $\mathbb{F}_9$ the sum of a row is $(9-3)$. It becomes natural to ask if this pattern continues in general.

Theorem:
Let F_q be a field. Let $r \in \mathbb{F}_q$ be an element such that $< r >= X_{\mathbb{F}_q}$. Then:

$$\sum_{i=1}^{(q-2)}(\sum_{j=1,j\neq i}^{(q-2)} R(r^i,r^j)) = \sum_{i=1}^{(q-2)}(q-3)[r^i] \tag{1}$$

Proof:
We start by recalling:

$$R(r^i, r^j) = \sum_{n=1}^{(q-2)} a_n \cdot [r^n]$$

We observe that for a fixed s such that $0 < s < q-1$ we have:

$$\sum_{j=1, j\neq s}^{(q-2)} R(r^s, r^j) = \sum_{g=1}^{(q-2)} c_g^{(s)} \cdot [r^g] = \sum_{j=1, j\neq s}^{(q-2)} ([r^s] - [r^j] + [r^{j-s}] - [\frac{1-r^{-s}}{1-r^{-j}}] + [\frac{1-r^s}{1-r^j}])$$

We note that s is invariant and thus we have:

$$\sum_{j=1, j\neq s}^{(q-2)} R(r^s, r^j) = \sum_{g=1}^{(q-2)} c_g^{(s)} \cdot [r^g] = (q-3)[r^s] + \sum_{j=1, j\neq s}^{(q-2)} (-[r^j] + [r^{j-s}] - [\frac{1-r^{-s}}{1-r^{-j}}] + [\frac{1-r^s}{1-r^j}])$$

We also note that:

$$\sum_{j=1, j\neq s}^{(q-2)} (-[r^j] + [r^{j-s}] - [\frac{1-r^{-s}}{1-r^{-j}}] + [\frac{1-r^s}{1-r^j}]) = \sum_{t=1}^{(q-2)} b_t^{(s)} \cdot [r^t]$$

and by applying ε we have:

$$\sum_{t=1}^{(q-2)} b_t^{(s)} = 0$$

We therefore note that:

$$\sum_{j=1, j\neq s}^{(q-2)} R(r^s, r^j) = \sum_{g=1}^{(q-2)} c_g^{(s)} \cdot [r^g] = (q-3)[r^s] + \sum_{t=1}^{(q-2)} b_t^{(s)} \cdot [r^t]$$

Aside: We know that the sum of $(q-3)$ relations should add to $(q-3)$. We verify:

$$\sum_{g=1}^{(q-2)} c_g^{(s)} = (q-3) + \sum_{t=1}^{(q-2)} b_t^{(s)} = q - 3 + 0 = q - 3$$

By equating coefficients we see that:

$$c_i^{(s)} = \begin{cases} b_i^{(s)} & i \neq s \\ (q-3) + b_i^{(s)} & i = s \end{cases}$$

Next we add all of the relations together, noting that:

$$\sum_{s=1}^{(q-2)} (\sum_{j=1, j\neq s}^{(q-2)} R(r^s, r^j)) = \sum_{i=1}^{(q-2)} (d_i)[r^i] = \sum_{s=1}^{(q-2)} (c_g^{(s)} \cdot [r^g]) = \sum_{s=1}^{(q-2)} ((q-3)[r^s] + \sum_{t=1}^{(q-2)} b_t^{(s)} \cdot [r^t])$$

So:

$$\sum_{i=1}^{(q-2)} (d_i)[r^i] = \sum_{s=1}^{(q-2)} ((q-3)[r^s] + \sum_{t=1}^{(q-2)} b_t^{(s)} \cdot [r^t])$$

Therefore, if we expand this explicitly we observe:

$$\sum_{i=1}^{(q-2)} (d_i)[r^i] = ((q{-}3{+}b_1^{(1)})[r^1]{+}(b_2^{(1)})[r^2]{+}\ldots{+}(b_{q-2}^{(1)})[r^1]){+}\ldots{+}(((b_1^{(q-2)})[r^1]{+}(b_2^{(q-2)})[r^2]{+}\ldots{+}((q{-}3{+}b_{q-2}^{(1)})[r^1]))$$

and by rearranging to match powers of r we have:

$$\sum_{i=1}^{(q-2)} (d_i)[r^i] = \sum_{i=1}^{(q-2)} ((q-3)[r^i]) + \sum_{i=1}^{(q-2)} (\sum_{s=1}^{(q-2)} b_i^{(s)} \cdot [r^i])$$

and hence:

$$\sum_{i=1}^{(q-2)} (d_i)[r^i] = \sum_{i=1}^{(q-2)} ((q-3)[r^i]) + \sum_{s=1}^{(q-2)} (\sum_{i=1}^{(q-2)} b_i^{(s)} \cdot [r^i])$$

and likewise:

$$d_i = (q-3) + \sum_{s=1}^{(q-2)} b_i^{(s)}$$

So to prove our claim we want to show:

$$\sum_{s=1}^{(q-2)} b_i^{(s)} = 0$$

Aside: We have summed $(q-2) \cdot (q-3)$ relations together. Hence we expect that the sum of the coefficients should be $(q-2) \cdot (q-3)$. We verify that:

$$\sum_{i=1}^{(q-2)} (d_i) = \sum_{i=1}^{(q-2)} ((q-3) + \sum_{i=1}^{(q-2)} (\sum_{s=1}^{(q-2)} b_i^{(s)}) = (q-2) \cdot (q-3) + \sum_{i=1}^{(q-2)} (\sum_{s=1}^{(q-2)} b_i^{(s)})$$

So:

$$\sum_{i=1}^{(q-2)} (d_i) = (q-2) \cdot (q-3) + \sum_{i=1}^{(q-2)} (\sum_{s=1}^{(q-2)} b_i^{(s)}) = (q-2) \cdot (q-3) + \sum_{s=1}^{(q-2)} (\sum_{i=1}^{(q-2)} b_i^{(s)}) = (q-2) \cdot (q-3)$$

So now our problem is equivalent to showing:

$$\sum_{s=1}^{(q-2)} b_i^{(s)} = 0 \text{ and equivalently } \sum_{i=1}^{(q-2)} (\sum_{s=1}^{(q-2)} b_i^{(s)}[r^i]) = 0$$

We'll focus on the latter. Note that by definition of $b_i^{(s)}$ we get:

$$\sum_{s=1}^{(q-2)}(\sum_{i=1}^{(q-2)} b_i^{(s)}\cdot[r^i]) = \sum_{s=1}^{(q-2)}(\sum_{j=1,j\neq s}^{(q-2)}(-[r^j]+[r^{j-s}]-[\frac{1-r^{-s}}{1-r^{-j}}]+[\frac{1-r^s}{1-r^j}])$$

So now we can break this sum into four separate components:

$$\sum_{s=1}^{(q-2)}(\sum_{i=1}^{(q-2)} b_i^{(s)}\cdot[r^i]) = \sum_{s=1}^{(q-2)}(\sum_{j=1,j\neq s}^{(q-2)}(-[r^j])+\sum_{s=1}^{(q-2)}(\sum_{j=1,j\neq s}^{(q-2)}([r^{j-s}])+\sum_{s=1}^{(q-2)}(\sum_{j=1,j\neq s}^{(q-2)}(-[\tfrac{1-r^{-s}}{1-r^{-j}}])+\sum_{s=1}^{(q-2)}(\sum_{j=1,j\neq s}^{(q-2)}([\tfrac{1-r^s}{1-r^j}])$$

And with this we focus on each term, and pair them off to show that this equals zero.

Observe that in the first term, that because for a fixed s we get every term in our $\mathbb{F}_q\backslash\{0,1\}$ except the term where $s=j$, and we have $(q-2)$ of these sums, we have:

$$\sum_{s=1}^{(q-2)}(\sum_{j=1,j\neq s}^{(q-2)}(-[r^j]) = -\sum_{j=1}^{(q-2)}((q-3)[r^j])$$

Likewise that in the second term, that because for a fixed s we get every term in our $\mathbb{F}_q\backslash\{0,1\}$ except the term where $s=j$, and we have $(q-2)$ of these sums, we have:

$$\sum_{s=1}^{(q-2)}(\sum_{j=1,j\neq i}^{(q-2)}([r^{j-s}]) = \sum_{j=1}^{(q-2)}((q-3)[r^j])$$

Similarly that in the third term, for the same reason we have:

$$\sum_{s=1}^{(q-2)}(\sum_{j=1,j\neq i}^{(q-2)}(-[\frac{1-r^{-s}}{1-r^{-j}}]) = -\sum_{j=1}^{(q-2)}((q-3)[r^j])$$

And finally, in the fourth and final term, for the same reason we have:

$$\sum_{s=1}^{(q-2)}(\sum_{j=1,j\neq i}^{(q-2)}([\frac{1-r^s}{1-r^j}]) = \sum_{j=1}^{(q-2)}((q-3)[r^j])$$

Now we note that:

$$\sum_{s=1}^{(q-2)}(\sum_{i=1}^{(q-2)} b_i^{(s)}\cdot[r^i]) = \sum_{j=1}^{(q-2)}(q-3)[r^j] - \sum_{j=1}^{(q-2)}(q-3)[r^j] + \sum_{j=1}^{(q-2)}(q-3)[r^j] - \sum_{j=1}^{(q-2)}(q-3)[r^j] = 0$$

And therefore:

$$\sum_{i=1}^{(q-2)}(d_i)[r^i] = \sum_{i=1}^{(q-2)}((q-3)[r^i]) + \sum_{s=1}^{(q-2)}(0) = \sum_{i=1}^{(q-2)}((q-3)[r^i])$$

And thus:

$$\sum_{i=1}^{(q-2)} (d_i)[r^i] = \sum_{i=1}^{(q-2)} (q-3)[r^i]$$

And therefore as claimed:

$$\sum_{i=1}^{(q-2)} (\sum_{j=1, j\neq i}^{(q-2)} R(r^i, r^j)) = \sum_{i=1}^{(q-2)} (q-3)[r^i]$$

which ends our proof of the theorem, and provides our first identity.

For a second identity among relations, we will consider the square terms in F_q. To start, we will need some quick results

Lemma:
Take a field $\mathbb{F}_q$. Let $x \in \mathbb{F}_q \backslash \{0, -1, 1\}$. Then:

$$\frac{1-x^1}{1-x^2} = \frac{1}{1+x}$$

Proof:

$$\frac{1-x^1}{1-x^2} = \frac{1-x^1}{(1-x)(1+x)} = \frac{1}{1+x}$$

Lemma:
Take a field $\mathbb{F}_q$. Let $x \in \mathbb{F}_q \backslash \{0, -1, 1\}$. Then:

$$\frac{1-x^{-1}}{1-x^{-2}} = \frac{x}{1+x}$$

Proof:

$$\frac{1-x^{-1}}{1-x^{-2}} = \frac{1-\frac{1}{x}}{1-\frac{1}{x^2}} = (\frac{x-1}{x})(\frac{x^2-1}{x^2})^{-1} = (\frac{x-1}{x})(\frac{x^2}{(x-1)(x+1)}) = \frac{x}{1+x}$$

Corollary: Take a field $\mathbb{F}_q$. Let $x \in \mathbb{F}_q \backslash \{0, -1, 1\}$. Then:

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

Proof:

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

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

Corollary:

Take a field $\mathbb{F}_q$. Let $x \in \mathbb{F}_q \backslash \{0, -1, 1\}$. Then:

$$R(x, x^2) + R(x^{-1}, x^{-2}) = 2([x] + [x^{-1}]) - ([x^2] + [x^{-2}])$$

Proof:

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

Theorem:

Take a field $\mathbb{F}_q$. Let $x \in \mathbb{F}_q \backslash \{0, -1, 1\}$. Then:

$$\sum_{x \in T} R(x^1, x^2) = \begin{cases} \sum\limits_{x \in T \backslash (\mathbb{F}_q^*)^2} 2[x] - 2[-1] \text{ if } q = 1 \pmod 4 \\ \sum\limits_{x \in T \backslash (\mathbb{F}_q^*)^2} 2[x] \text{ if } q = 3 \pmod 4 \\ \sum\limits_{x \in T} [x] \text{ if } q = 0 \pmod 2 \end{cases} \tag{2}$$

where:

$$T = \mathbb{F}_q \backslash \{0, 1, -1\} / x^1 \sim x^{-1}$$

Proof:

Let $\mathbb{F}_q$ be a field. Let $x \in \mathbb{F}_q \backslash \{0, -1, 1\}$. Then:

$$\sum_{x \in T} R(x^1, x^2) = \sum_{x \in T} (2[x] - [x^2] - [\frac{x}{1+x}] + [\frac{1}{1+x}])$$

So term-by-term:

$$\sum_{x \in T} R(x^1, x^2) = \sum_{x \in T} (2[x]) - \sum_{x \in T} ([x^2]) - \sum_{x \in T} ([\frac{x}{1+x}]) + \sum_{x \in T} ([\frac{1}{1+x}])$$

Now, we define the following for $q = 2k$ or $q = 2k + 1$:

$$N_1 := \{r^1, r^2, \ldots, r^{k-1} : r^n \in T \text{ and such that } <r>= \mathbb{F}^*\}$$

$$N_2 := \{r^{k+1}, r^{k+2}, \ldots, r^{2k-1} : r^n \in T \text{ and such that } <r>= \mathbb{F}^*\}$$

Note that:

$$T = N_1 \cup N_2 \text{ and } N_1 \cap N_2 = \emptyset$$

Furthermore, we observe:

$$\exists f : N_1 \to N_2 : \text{f is bijective, given by} f(x) = x^{-1}$$

Hence we can split the sum into sums of those in N_1 and N_2.

$$\sum_{x\in T} R(x^1, x^2) = \sum_{x\in T}(2[x]) - \sum_{x\in T}([x^2]) - \sum_{x\in N_1}([\frac{x}{1+x}]) - \sum_{x\in N_2}([\frac{x}{1+x}]) + \sum_{x\in N_1}([\frac{1}{1+x}]) + \sum_{x\in N_2}([\frac{1}{1+x}])$$

So by our lemmas, and sending $x \in N_2$ to $x \in N_1$ by recalling that all elements in N_2 can be written as x^{-1} with $x \in N_1$:

$$\sum_{x\in T} R(x^1, x^2) = \sum_{x\in T}(2[x]) - \sum_{x\in T}([x^2]) - \sum_{x\in N_1}([\frac{x}{1+x}]) - \sum_{x\in N_1}([\frac{1}{1+x}]) + \sum_{x\in N_1}([\frac{1}{1+x}]) + \sum_{x\in N_1}([\frac{x}{1+x}])$$

So by simplifying and cancelling like-terms.

$$\sum_{x\in T} R(x^1, x^2) = \sum_{x\in T}(2[x]) - \sum_{x\in T}([x^2])$$

Now we split T into square terms, and non-square terms.

$$\sum_{x\in T} R(x^1, x^2) = \sum_{x\in T\setminus(\mathbb{F}_q^*)^2}(2[x]) + \sum_{x\in T\cap(\mathbb{F}_q^*)^2}(2[x]) - \sum_{x\in T}([x^2])$$

Case 1: $q = 1\ (mod\ 4)$.

If $q = 1\ (mod\ 4)$, $r^{4k} = 1$ and thus $(r^k)^2 = -1$. So

$$\sum_{x\in T} R(x^1, x^2) = \sum_{x\in T\setminus(\mathbb{F}_q^*)^2}(2[x]) + \sum_{x\in T\cap(\mathbb{F}_q^*)^2}(2[x]) - \sum_{x\in T\cap(\mathbb{F}_q^*)^2}(2[x]) - (2[-1])$$

and by simplifying we get:

$$\sum_{x\in T} R(x^1, x^2) = \sum_{x\in T\setminus(\mathbb{F}_q^*)^2} 2[x] - 2[-1]$$

Case 2: $q = 3\ (mod\ 4)$.

If $q = 3\ (mod\ 4)$, $r^{4k+2} = 1$ and thus $r^{k+1} = -1$. We note that as Char($\mathbb{F}$) $\neq 2$, $\nexists r^k : (r^k)^2 = -1$. Hence:

$$\sum_{x\in T} R(x^1, x^2) = \sum_{x\in T\setminus(\mathbb{F}_q^*)^2}(2[x]) + \sum_{x\in T\cap(\mathbb{F}_q^*)^2}(2[x]) - \sum_{x\in T\cap(\mathbb{F}_q^*)^2}(2[x])$$

and by simplifying we get:

$$\sum_{x\in T} R(x^1, x^2) = \sum_{x\in T\setminus(\mathbb{F}_q^*)^2} 2[x]$$

Case 3: $q = 0\ (mod\ 2)$.

We note that for Char($\mathbb{F}$) = 2:

$$f : \mathbb{F}_q \to \mathbb{F}_q$$
$$f(x) = x^2$$

is bijective. Thus:

$$\sum_{x \in T} R(x^1, x^2) = \sum_{x \in T} 2[x] - \sum_{x \in T} [x^2] = \sum_{x \in T} 2[x] - \sum_{x \in T} [x]$$

And by simplifying:

$$\sum_{x \in T} R(x^1, x^2) = \sum_{x \in T} [x]$$

3.3 Linearly Independant Relations

We now turn our attention towards trying to find $q-2$ linearly independent relations. The relations which we will consider are largely motivated from our previous exploration of identities amongst the relations. While we have successfully explicitly found a set of $\frac{q-3}{2}$ relations which are linearly independent, I have been unable to achieve better than this result which holds over any field. We will also provide counterexamples to a number of sets of relations which may initially seem promising.

Theorem:
Suppose $\mathrm{Char}(\mathbb{F}_q) \neq 2$. Then:

$$B = \{R(x, x^2) + R(x^{-1}, x^{-2}) : x \in \mathbb{F}_q^* \backslash \{-1, 1\}\} \subseteq \mathbb{Z}[\mathbb{F}_q \backslash \{0, 1\}]$$

is a set of linearly independent elements. We note that the cardinality of B is $\frac{q-3}{2}$.

Proof:
First, we note we are working in $\mathbb{Z}[F_q^* \backslash \{1\}]$.

We will use the following notations throughout

$$q := 2k + 1$$

$$r := r \in \mathbb{F}_q :< r >= (\mathbb{F}_q^*, \cdot, 1_{\mathbb{F}})$$
$$T := \mathbb{F}_q^* \backslash \{-1, 1\}$$
$$\{x\} := [x] + [x^{-1}] = \{x^{-1}\} \in \mathbb{Z}[\mathbb{F}_q \backslash \{0, 1\}]$$
$$L := \{r^1, r^2, r^3, \ldots, r^{k-1}\}$$
$$L^{-1} := \{r^{2k-1}, r^{2k-2}, r^{2k-3}, \ldots, r^{k+1}\}$$

We note from these that:
$$T = L \cup L^{-1} \text{ and } L \cap L^{-1} = \emptyset$$

and that the following map is a bijection:

$$f : L \to L^{-1}$$

$$f(x) = x^{-1}$$

We also note
$$\{\{x\}_{x \in L}\}$$
are linearly independent when we take $\{x\} \in \mathbb{Z}[\mathbb{F}_q \backslash \{0, 1\}]$.

We will also recall the quick results which will prove essential to our results:

$$\frac{1 - x^1}{1 - x^2} = \frac{1}{1 + x}$$

$$\frac{1 - x^{-1}}{1 - x^{-2}} = \frac{x}{1 + x}$$

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

Then:

$$\sum_{b\in B} \lambda_b b = \sum_{x\in T} \lambda_x (R(x,x^2) + R(x^{-1},x^{-2}))$$

and by our results:

$$\sum_{x\in T} \lambda_x (R(x,x^2) + R(x^{-1},x^{-2})) = \sum_{x\in T} \lambda_x 2([x]+[x^{-1}]) - ([x^2]+[x^{-2}]) = \sum_{x\in T} \lambda_x (2\{x\} - \{x^2\})$$

So now we wish to show:

$$\sum_{x\in T} \lambda_x (2\{x\} - \{x^2\}) = 0 \implies \lambda_x = 0 \ \forall x \in T$$

Comment: We observe that the second term here contains all square terms of T, whereas the first term contains all terms in T.

Now we define:

$$L^{(0)} := L,\ L^{(1)} := L \cap (\mathbb{F}_q^*)^{2^1},\ L^{(2)} := L \cap (\mathbb{F}_q^*)^{2^2},\ L^{(3)} := L \cap (\mathbb{F}_q^*)^{2^3} \dots$$

Comment: We see that $L^{(0)}$ is all terms in L. We see that $L^{(1)}$ is all square terms, etc. We care for these terms as equality of $\{x\}$ and $\{t^2\}$ can only occur when $x = t^2$ or $x = t^{-2}$ for some $t \in L$. Hereafter, we will consider $x \sim x^{-1}$.

Note that:

$$T = (L \backslash L^{(i)}) \cup L^{(i)} \text{ and that } (L \backslash L^{(i)}) \cap L^{(i)} = \emptyset$$

Now, we split our sum according to which square values they contain.

$$\sum_{x\in T} \lambda_x (2\{x\} - \{x^2\}) = \sum_{x\in L\backslash L^{(i)}} \lambda_x (2\{x\} - \{x^2\}) + \sum_{x\in L^{(i)}} \lambda_x (2\{x\} - \{x^2\})$$

and by splitting this term-by-term and rearranging:

$$\sum_{x\in T} \lambda_x (2\{x\} - \{x^2\}) = \sum_{x\in L\backslash L^{(i)}} \lambda_x 2\{x\} - \sum_{x\in L\backslash L^{(i)}} \lambda_x \{x^2\} + \sum_{x\in L^{(i)}} \lambda_x 2\{x\} - \sum_{x\in L^{(i)}} \lambda_x \{x^2\} = 0$$

We will prove using induction on i that $\lambda_x = 0$ for $x \in L \backslash L^{(i)}$.

Proof by Induction: By induction on i, we will show that $\lambda_x = 0$ for $x \in L \backslash L^{(i)}$.

Base Case: For $i = 1$, we have that.

$$\sum_{x\in T} \lambda_x (2\{x\} - \{x^2\}) = \sum_{x\in L\backslash L^{(1)}} \lambda_x 2\{x\} - \sum_{x\in L\backslash L^{(1)}} \lambda_x \{x^2\} + \sum_{x\in L^{(1)}} \lambda_x 2\{x\} - \sum_{x\in L^{(1)}} \lambda_x \{x^2\} = 0$$

However, we note that none of the terms in $\{x\}$ with $L\backslash L^{(1)}$ can occur in any of the other terms in our sum. Thus we have that:

$$\sum_{x\in L\backslash L^{(1)}} \lambda_x 2\{x\} = 0 \implies \lambda_x = 0 \ \forall x \in L\backslash L^{(1)} \text{ as } \{x\}_{x\in L} \text{ is linearly independent.}$$

Hence we have that:

$$\lambda_x = 0 \ \forall x \in L\backslash L^{(1)}$$

as claimed, and our base case is true.

Assumption: We assume it is true for i that $\lambda_x = 0 \ \forall x \in L\backslash L^{(i)}$

Proof for Successor: We will now prove it is true that by assuming:

$$\lambda_x = 0 \ \forall x \in L\backslash L^{(i)}$$

that it is true that:

$$\lambda_x = 0 \ \forall x \in L\backslash L^{(i+1)}$$

We have that:

$$\sum_{x\in T} \lambda_x(2\{x\} - \{x^2\}) = \sum_{x\in L\backslash L^{(i)}} \lambda_x 2\{x\} - \sum_{x\in L\backslash L^{(i)}} \lambda_x\{x^2\} + \sum_{x\in L^{(i)}} \lambda_x 2\{x\} - \sum_{x\in L^{(i)}} \lambda_x\{x^2\} = 0$$

And therefore:

$$\sum_{x\in T} \lambda_x(2\{x\} - \{x^2\}) = \sum_{x\in L^{(i)}} \lambda_x 2\{x\} - \sum_{x\in L^{(i)}} \lambda_x\{x^2\} = 0$$

Now we note that either $x \in L^{(i)}\backslash L^{(i+1)}$ or $x \in L^{(i+1)}$. Hence we can split out sum as:

$$\sum_{x\in T} \lambda_x(2\{x\} - \{x^2\}) = \sum_{x\in L^{(i+1)}} \lambda_x 2\{x\} - \sum_{x\in L^{(i)}} \lambda_x\{x^2\} + \sum_{x\in L^{(i)}\backslash L^{(i+1)}} \lambda_x 2\{x\} = 0$$

And thus as $x^2 \in L^{(i+1)}$ for $x \in L^{(i)}$, we therefore have:

$$\sum_{x\in L^{(i)}\backslash L^{(i+1)}} \lambda_x 2\{x\} = 0 \implies \lambda_x = 0 \ \forall x \in L^{(i)}\backslash L^{(i+1)} \implies \lambda_x = 0 \ \forall x \in L\backslash L^{(i+1)}$$

Hence our proof by induction is complete, and we have that

$$\lambda_x = 0 \ \forall x \in L\backslash L^{(i)} \ \forall i \in \mathbb{N}$$

With this result, our sum now becomes:

$$\sum_{x\in T} \lambda_x(2\{x\} - \{x^2\}) = \sum_{x\in L^{(i)}} \lambda_x 2\{x\} - \sum_{x\in L^{(i)}} \lambda_x\{x^2\} = 0$$

However we note that:

$$L = L^{(0)} \supseteq L^{(1)} \supseteq L^{(2)} \supseteq L^{(3)} \supseteq \dots$$

and thus, as L is finite and thus Noetherian, there must be some g in $\mathbb{N}$ such that:

$$L = L^{(0)} \supseteq L^{(1)} \supseteq L^{(2)} \supseteq L^{(3)} \supseteq \dots \supseteq L^{(g)} = L^{(g+1)} = L^{(g+2)} = L^{(g+3)} = \dots$$

Hence as $\lambda_x = 0 \; \forall x \in L \backslash L^{(g)}$ our sum becomes:

$$\sum_{x \in T} \lambda_x (2\{x\} - \{x^2\}) = \sum_{x \in L^{(g)}} \lambda_x 2\{x\} - \sum_{x \in L^{(g)}} \lambda_x \{x^2\} = 0$$

Observe that at this point:

$$f : L^{(g)} \to L^{(g+1)}$$
$$f(x) = x^2$$

is in fact a bijection, as $L^{(g+1)} = L^{(g)}$. Hence we can rewrite our sum in terms of elements in $L^{(g)}$ with:

$$\sum_{x \in T} \lambda_x (2\{x\} - \{x^2\}) = \sum_{x \in L^{(g)}} \lambda_{x^2} 2\{x^2\} - \sum_{x \in L^{(g)}} \lambda_x \{x^2\} = \sum_{x \in L^{(g)}} (2\lambda_{x^2} - \lambda_x)\{x^2\} = 0$$

However, note that $\{x^2\}_{x \in L}$ is linearly independent, and thus we have that:

$$\sum_{x \in L^{(g)}} (2\lambda_{x^2} - \lambda_x)\{x^2\} = 0 \implies (2\lambda_{x^2} - \lambda_x) = 0 \; \forall x \in L^{(g)}$$

Hence we have, $\forall x \in L^{(g)}$ that:

$$\lambda_x = 2\lambda_{x^2} = 4\lambda_{x^4} = 8\lambda_{x^8} = \dots$$

However, note that because $L^{(g)}$ is finite, and because squaring is a bijection, we must at some stage acquire:

$$\lambda_x = 2\lambda_{x^2} = 4\lambda_{x^4} = 8\lambda_{x^8} = \dots = 2^n \lambda_x \implies \lambda_x = 0$$

As this holds $\forall x \in L^{(g)}$, we have that

$$\lambda_x = 0 \; \forall x \in L^{(g)} \text{ and also } \lambda_x = 0 \; \forall x \in L \backslash L^{(g)}$$

And thus as :

$$\sum_{x \in T} \lambda_x (2\{x\} - \{x^2\}) = \sum_{x \in L^{(g)}} \lambda_x (2\{x\} - \{x^2\}) = 0 \implies \lambda_x = 0 \; \forall x \in L^{(g)}$$

Thus:

$$\sum_{x \in T} \lambda_x (2\{x\} - \{x^2\}) = 0 \implies \lambda_x = 0 \; \forall x \in T$$

Which proves our claim that for

$$B := \{R(x, x^2) + R(x^{-1}, x^{-2}) : x \in \mathbb{F}_q^* \backslash \{-1, 1\}, \mathrm{Char}(\mathbb{F}_q) \neq 2\}$$

Then:

$$\sum_{b \in B} \lambda_b b = 0 \implies \lambda_b = 0 \; \forall b \in B \text{ and } |B| = \frac{q-3}{2}$$

<u>**Note:**</u>
It is quite natural for us to now ask, can we do better than this set, and can we find a larger set of linearly independent relations? One set of relations which one may suspect to try is to simply take the first $q-2$, or $q-3$ (and then attempt to find one relation among the rest which is linearly

independent to each of those relations for a total of $q-2$ linearly independent relations) relations, when the relations are ordered lexographically or by the power of a generator.

Question:
If we let

$$S := \{R(r^1, r^j) : r \in \mathbb{F}_q \text{ such that } <r>= X_{\mathbb{F}},\ 2 \leq j \leq q-2\}$$

is it true that:

$$\sum_{a \in S} \lambda_a a = 0 \implies \lambda_a = 0\ \forall a \in S$$

Answer:
No. This set contains a counter example for $\mathbb{F}_{13}$, as the set is not maximal. Similarly, at $\mathbb{F}_{19}$ we find a counterexample.

Question:
If we order the relations lexographically, are the first $q-2$ linearly independent?

Answer:
No, we get an immediate counter example. Consider $\mathbb{F}_5$. If we order it lexographically, our first 3 relations are:

$$R(2,3) = 0[2] + 0[3] + 1[4]$$

$$R(2,4) = 3[2] + 0[3] - 2[4]$$

$$R(3,1) = 0[2] + 0[3] + 1[4]$$

and we have that $R(2,3) = R(3,2)$.

Note:
This eliminates the two most 'obvious' or immediate sets to consider. However, we can weaken our initial question.

Question:
Let

$$S_s := \{R(r^s, r^j) : r \in \mathbb{F}_q \text{ such that } <r>= \mathbb{F}^*,\ j \leq q-2 \text{ and } j \neq s\}$$

Is it true that $\exists g : 1 \leq g \leq q-2$ such that:

$$\sum_{a \in S_g} \lambda_a a = 0 \implies \lambda_a = 0\ \forall a \in S_g$$

Answer:
This is uncertain.

While I have been unable to find a counterexample, and one might suspect that this would indicate it is true, the program which was developed for this search is quite inefficient. Similarly, as this search was conducted on a relatively weak computer, and time was an important factor, it was only possible to check for relatively small fields and our evidence is very limited. One thing which makes this a particularly tricky question to answer is that there are a very large amount of variable factors which have a significant influence. For example, it is not immediately clear how one would even begin to choose such an s. Even if one could find such an s, it is not immediately obvious how one should go about proving linear independence, as our five term relation is highly dependant on the arithmetic of the underlying field, and thus it is not immediately obvious which terms will be equal as we vary j.

The idea would be to somehow prove that this is true (or find a counterexample), and to then find some additional relaton (as $|S_s| = q-3$), say P which will consistently be linearly independent to those in S_s, and to then take $S_s \cup P$ which will consist of $q-2$ linearly independent relations and prove that the rank of the presentation matrix is thus maximal, but it is not clear to me how one would approach this or if indeed it will hold for very large fields.

This approach suggests another way to tackle the problem of finding $q-2$ linearly independent relations. One could gradually build a set B by first starting with $B = \emptyset$. One could find some relation which is linearly independent to all the others, and take the union of this relation and B. One could then repeat this process until we have $q-2$ linearly independent relations. Alternatively, we could repeatedly find sets of relations which are linearly independent to one another, and then gradually take the union of these sets.

Ultimately, there is to the author no clear or obvious way to try and find which $q-2$ relations are linearly independent.

3.4 The Matrix $\mathbf{MT}_q$

Motivated by the difficulty in finding $q-2$ linearly independent relations for the pre-Bloch group over a finite field $\mathbb{F}_q$, I began to look at:

$$MT_q := M_q \cdot (M_q)^T$$

where

$$M_q := \begin{pmatrix} \uparrow & \dots & \uparrow & \uparrow & \dots & \uparrow & \dots & \uparrow & \dots & \uparrow \\ R(r^1, r^2) & \dots & R(r^1, r^{q-2}) & R(r^2, r^1) & \dots & R(r^2, r^{q-2}) & \dots & R(r^{q-2}, r^1) & \dots & R(r^{q-2}, r^{q-3}) \\ \downarrow & \dots & \downarrow & \downarrow & \dots & \downarrow & \dots & \downarrow & \dots & \downarrow \end{pmatrix}$$

for some field $\mathbb{F}_q$.

While this matrix MT_q (named to indicate "The Matrix M_q times its Transpose") was initially examined because its dimension is $q-2 \times q-2$ and thus one only needs to prove either the rows or columns are linearly independent, a number of very interesting and highly unexpected (conjectured) properties quickly became apparent. While these properties hold for small fields, and thus our evidence that these properties (which this section will explain in detail, in addition to a number of experiments which were conducted) hold in general is weak, they are of significant interest to the author and certainly warrant further study.

I will detail my work thus far, and cautiously provide some conjectured properties of MT_q below. To begin, and justify the exploration of this matrix, we will need the following result:

Theorem:
Let A be a real-valued $m \times n$ matrix. Then

$$\text{rank}(A) = \text{rank}(A \cdot A^T)$$

Proof:
We will use the rank-nullity theorem.

First, observe that for a vector $x \in R^m$:

$$(A^T)x = 0 \implies (A \cdot A^T)x = 0$$

Thus $\text{Ker}(A \cdot A^T) \supseteq \text{Ker}(A^T)$. ($\circledcirc$)

Next, note that if we have $x \in \text{Ker}(A \cdot A^T)$:

$$(A \cdot A^T)x = 0$$

Then:

$$x^T (A \cdot A^T)x = 0$$

Then we can rewrite this as:

$$(A^T x)^T \cdot (A^T x) = 0$$

Thus as A is real-valued:

$$(A^T x) = 0$$

And hence we have $\mathrm{Ker}(A \cdot A^T) \subseteq \mathrm{Ker}(A^T)$. $(\star)$

Therefore by $(\circledcirc)$ and $(\star)$, we get $\mathrm{Ker}(A \cdot A^T) = \mathrm{Ker}(A^T)$

The rank-nullity theorem states that:

$$m = \mathrm{rank}(A^T) + \mathrm{nul}(A^T)$$

By recalling the well-known result that $\mathrm{rank}(A) = \mathrm{rank}(A^T)$ we get:

$$m = \mathrm{rank}(A) + \mathrm{nul}(A^T)$$

We note that $A \cdot A^T$ is an $(m \times n) \times (n \times m) = m \times m$ matrix and therefore

$$m = \mathrm{rank}(A \cdot A^T) + \mathrm{nul}(A \cdot A^T)$$

Hence by combining both results we have:

$$\mathrm{rank}(A) + \mathrm{nul}(A^T) = m = \mathrm{rank}(A \cdot A^T) + \mathrm{nul}(A \cdot A^T)$$

Finally, as $\mathrm{Ker}(A \cdot A^T) = \mathrm{Ker}(A^T)$, we get that $\mathrm{nul}(A^T) = \mathrm{nul}(A \cdot A^T)$. We denote $\mathrm{nul}(A^T) = h$. Thus:

$$\mathrm{rank}(A) = m - h = \mathrm{rank}(A \cdot A^T)$$

And hence conclude with our result that

$$\mathrm{rank}(A) = \mathrm{rank}(A \cdot A^T)$$

<u>Notation:</u> For this section, we will define $v := (q-2)(q-3)$ for convenience.

<u>Definition:</u> MT_q

Let $\mathbb{F}_q$ be a field. Let M_q be the matrix defined as:

$$M_q := \begin{pmatrix} \uparrow & \dots & \uparrow & \uparrow & \dots & \uparrow & \dots & \uparrow & \dots & \uparrow \\ R(r^1, r^2) & \dots & R(r^1, r^{q-2}) & R(r^2, r^1) & \dots & R(r^2, r^{q-2}) & \dots & R(r^{q-2}, r^1) & \dots & R(r^{q-2}, r^{q-3}) \\ \downarrow & \dots & \downarrow & \downarrow & \dots & \downarrow & \dots & \downarrow & \dots & \downarrow \end{pmatrix}$$

for some field $\mathbb{F}_q$ where $a_{s,j}$ corresponds to $a_s[r^s]$ in the relation given by column j, where:

$$R(r^i, r^j) = [r^i] - [r^j] + [r^{j-i}] - [\frac{1 - r^{-i}}{1 - r^{-j}}] + [\frac{1 - r^i}{1 - r^j}]$$

Then:

$$MT_q := M_q \cdot (M_q)^T$$

<u>Note:</u>

It is clear that $MT_q \in M_{q-2}(\mathbb{Z})$ and that MT_q is a symmetric matrix.

Note:

Explicitly, we have:

$$MT_q = \begin{pmatrix} \sum\limits_{j=1}^{v}(a_{1,j})^2 & \sum\limits_{j=1}^{v} a_{1,j}a_{2,j} & \cdots & \sum\limits_{j=1}^{v} a_{1,j}a_{q-2,j} \\ \sum\limits_{j=1}^{v} a_{2,j}a_{1,j} & \sum\limits_{j=1}^{v}(a_{2,j})^2 & \cdots & \sum\limits_{j=1}^{v} a_{2,j}a_{q-2,j} \\ \vdots & \vdots & \ddots & \vdots \\ \sum\limits_{j=1}^{v} a_{q-2,j}a_{1,j} & \sum\limits_{j=1}^{v} a_{q-2,j}a_{2,j} & \cdots & \sum\limits_{j=1}^{v}(a_{q-2,j})^2 \end{pmatrix}$$

which can also be written as a Gramian Matrix [9] as:

$$MT_q = \begin{pmatrix} < a_{1,j}, a_{1,j} > & < a_{1,j}, a_{2,j} > & \cdots & < a_{1,j}, a_{q-2,j} > \\ < a_{2,j}, a_{1,j} > & < a_{2,j}, a_{2,j} > & \cdots & < a_{2,j}, a_{q-2,j} > \\ \vdots & \vdots & \ddots & \vdots \\ < a_{q-2,j}, a_{1,j} > & < a_{q-2,j}, a_{2,j} > & \cdots & < a_{q-2,j}, a_{q-2,j} > \end{pmatrix}$$

Notation:

For this section, to avoid confusion, we will use the following conventions:
$m_{i,j}$ will refer to the entry of the matrix MT_q in row i and column j.
$a_{i,j}$ will refer to the entry of the matrix M_q in row i and column j.

Example:

We will compute MT_5:

$$MT_5 = \begin{pmatrix} 3 & 0 & -1 & 1 & 0 & -1 \\ -2 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & -2 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 3 & -2 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 2 \\ 1 & 2 & -2 \\ 0 & 1 & 0 \\ -1 & 0 & 2 \end{pmatrix}$$

And thus, written somewhat suggestively:

$$m_{1,1} = (3 \cdot 3 + 0 \cdot 0) + ((-1) \cdot (-1) + 1 \cdot 1) + (0 \cdot 0 + (-1) \cdot (-1)) = 9 + 2 + 1 = 12$$

$$m_{1,2} = (3 \cdot (-2) + 0 \cdot 1) + ((-1) \cdot (0) + 1 \cdot 2) + (0 \cdot 1 + (-1) \cdot (0)) = -6 + 2 + 0 = -4$$

$$m_{1,3} = (3 \cdot (0) + 0 \cdot 0) + ((-1) \cdot (2) + 1 \cdot (-2)) + (0 \cdot 0 + (-1) \cdot (2)) = 0 - 4 - 2 = -6$$

$$m_{2,1} = ((-2) \cdot (3) + (1) \cdot (0)) + ((0) \cdot (-1) + (2) \cdot (1)) + ((1) \cdot (0) + (0) \cdot (-1)) = -6 + 2 + 0 = -4$$

$$m_{2,2} = ((-2) \cdot (-2) + (1) \cdot (1)) + ((0) \cdot (0) + (2) \cdot (2)) + ((1) \cdot (1) + (0) \cdot (0)) = 5 + 4 + 1 = 10$$

$$m_{2,3} = ((-2)\cdot(0) + (1)\cdot(0)) + ((0)\cdot(2) + (2)\cdot(-2)) + ((1)\cdot(0) + (0)\cdot(2)) = 0 - 4 + 0 = -4$$

$$m_{3,1} = ((0)\cdot(3) + (0)\cdot(0)) + ((2)\cdot(-1) + (-2)\cdot(1)) + ((0)\cdot(0) + (2)\cdot(-1)) = 0 - 4 - 2 = -6$$

$$m_{3,2} = ((0)\cdot(-2) + (0)\cdot(1)) + ((2)\cdot(0) + (-2)\cdot(2)) + ((0)\cdot(1) + (2)\cdot(0)) = 0 - 4 + 0 = -4$$

$$m_{3,3} = ((0)\cdot(0) + (0)\cdot(0)) + ((2)\cdot(2) + (-2)\cdot(-2)) + ((0)\cdot(0) + (2)\cdot(2)) = 0 + 8 + 4 = 12$$

To give:

$$MT_5 = \begin{pmatrix} 12 & -4 & -6 \\ -4 & 10 & -4 \\ -6 & -4 & 12 \end{pmatrix}$$

Example:
We will leave it to the reader to verify MT_4:

$$\begin{pmatrix} 13 & -12 \\ -12 & 13 \end{pmatrix}$$

Example:
We will leave it to the reader to verify MT_7:

$$\begin{pmatrix} 28 & -4 & -4 & -4 & -12 \\ -4 & 22 & -4 & -6 & -4 \\ -4 & -4 & 20 & -4 & -4 \\ -4 & -6 & -4 & 22 & -4 \\ -12 & -4 & -4 & -4 & 28 \end{pmatrix}$$

Example:
We will leave it to the reader to verify MT_8:

$$\begin{pmatrix} 29 & -2 & -6 & -2 & -6 & -8 \\ -2 & 29 & -6 & -2 & -8 & -6 \\ -6 & -6 & 29 & -8 & -2 & -2 \\ -2 & -2 & -8 & 29 & -6 & -6 \\ -6 & -8 & -2 & -6 & 29 & -2 \\ -8 & -6 & -2 & -6 & -2 & 29 \end{pmatrix}$$

Example:

We will leave it to the reader to verify MT_9:

$$\begin{pmatrix}
34 & -6 & -6 & -4 & -2 & -2 & -8 \\
-6 & 34 & -2 & -4 & -6 & -8 & -2 \\
-6 & -2 & 34 & -4 & -8 & -6 & -2 \\
-4 & -4 & -4 & 30 & -4 & -4 & -4 \\
-2 & -6 & -8 & -4 & 34 & -2 & -6 \\
-2 & -8 & -6 & -4 & -2 & 34 & -6 \\
-8 & -2 & -2 & -4 & -6 & -6 & 34
\end{pmatrix}$$

Example:
We will leave it to the reader to verify MT_{11}:

$$\begin{pmatrix}
42 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -6 \\
-4 & 44 & -6 & -6 & -4 & -2 & -2 & -8 & -4 \\
-4 & -6 & 44 & -2 & -4 & -6 & -8 & -2 & -4 \\
-4 & -6 & -2 & 44 & -4 & -8 & -6 & -2 & -4 \\
-4 & -4 & -4 & -4 & 40 & -4 & -4 & -4 & -4 \\
-4 & -2 & -6 & -8 & -4 & 44 & -2 & -6 & -4 \\
-4 & -2 & -8 & -6 & -4 & -2 & 44 & -6 & -4 \\
-4 & -8 & -2 & -2 & -4 & -6 & -6 & 44 & -4 \\
-6 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & 42
\end{pmatrix}$$

Example:
We will compute MT_{13}:

$$\begin{pmatrix}
52 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -6 \\
-4 & 58 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -12 & -4 \\
-4 & -4 & 54 & -6 & -6 & -4 & -2 & -2 & -8 & -4 & -4 \\
-4 & -4 & -6 & 54 & -2 & -4 & -6 & -8 & -2 & -4 & -4 \\
-4 & -4 & -6 & -2 & 54 & -4 & -8 & -6 & -2 & -4 & -4 \\
-4 & -4 & -4 & -4 & -4 & 50 & -4 & -4 & -4 & -4 & -4 \\
-4 & -4 & -2 & -6 & -8 & -4 & 54 & -2 & -6 & -4 & -4 \\
-4 & -4 & -2 & -8 & -6 & -4 & -2 & 54 & -6 & -4 & -4 \\
-4 & -4 & -8 & -2 & -2 & -4 & -6 & -6 & 54 & -4 & -4 \\
-4 & -12 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & 58 & -4 \\
-6 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & 52
\end{pmatrix}$$

Example:

We will leave it to the reader to verify MT_{16}:

$$\begin{pmatrix}
69 & -4 & -2 & -6 & -4 & -4 & -4 & -4 & -4 & -4 & -2 & -6 & -4 & -8 \\
-4 & 69 & -4 & -4 & -4 & -2 & -2 & -6 & -6 & -4 & -4 & -4 & -8 & -4 \\
-2 & -4 & 69 & -6 & -4 & -4 & -4 & -4 & -4 & -4 & -2 & -8 & -4 & -6 \\
-6 & -4 & -6 & 69 & -4 & -4 & -4 & -4 & -4 & -4 & -8 & -2 & -4 & -2 \\
-4 & -4 & -4 & -4 & 73 & -4 & -4 & -4 & -4 & -12 & -4 & -4 & -4 & -4 \\
-4 & -2 & -4 & -4 & -4 & 69 & -2 & -6 & -8 & -4 & -4 & -4 & -6 & -4 \\
-4 & -2 & -4 & -4 & -4 & -2 & 69 & -8 & -6 & -4 & -4 & -4 & -6 & -4 \\
-4 & -6 & -4 & -4 & -4 & -6 & -8 & 69 & -2 & -4 & -4 & -4 & -2 & -4 \\
-4 & -6 & -4 & -4 & -4 & -8 & -6 & -2 & 69 & -4 & -4 & -4 & -2 & -4 \\
-4 & -4 & -4 & -4 & -12 & -4 & -4 & -4 & -4 & 73 & -4 & -4 & -4 & -4 \\
-2 & -4 & -2 & -8 & -4 & -4 & -4 & -4 & -4 & -4 & 69 & -6 & -4 & -6 \\
-6 & -4 & -8 & -2 & -4 & -4 & -4 & -4 & -4 & -4 & -6 & 69 & -4 & -2 \\
-4 & -8 & -4 & -4 & -4 & -6 & -6 & -2 & -2 & -4 & -4 & -4 & 69 & -4 \\
-8 & -4 & -6 & -2 & -4 & -4 & -4 & -4 & -4 & -4 & -6 & -2 & -4 & 69
\end{pmatrix}$$

Example:
We will leave it to the reader to verify MT_{17}:

$$\begin{pmatrix}
74 & -4 & -6 & -4 & -4 & -6 & -4 & -4 & -4 & -2 & -4 & -4 & -2 & -4 & -8 \\
-4 & 72 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -6 & -4 \\
-6 & -4 & 74 & -4 & -4 & -2 & -4 & -4 & -4 & -6 & -4 & -4 & -8 & -4 & -2 \\
-4 & -4 & -4 & 74 & -6 & -4 & -6 & -4 & -2 & -4 & -2 & -8 & -4 & -4 & -4 \\
-4 & -4 & -4 & -6 & 74 & -4 & -2 & -4 & -6 & -4 & -8 & -2 & -4 & -4 & -4 \\
-6 & -4 & -2 & -4 & -4 & 74 & -4 & -4 & -4 & -8 & -4 & -4 & -6 & -4 & -2 \\
-4 & -4 & -4 & -6 & -2 & -4 & 74 & -4 & -8 & -4 & -6 & -2 & -4 & -4 & -4 \\
-4 & -4 & -4 & -4 & -4 & -4 & -4 & 70 & -4 & -4 & -4 & -4 & -4 & -4 & -4 \\
-4 & -4 & -4 & -2 & -6 & -4 & -8 & -4 & 74 & -4 & -2 & -6 & -4 & -4 & -4 \\
-2 & -4 & -6 & -4 & -4 & -8 & -4 & -4 & -4 & 74 & -4 & -4 & -2 & -4 & -6 \\
-4 & -4 & -4 & -2 & -8 & -4 & -6 & -4 & -2 & -4 & 74 & -6 & -4 & -4 & -4 \\
-4 & -4 & -4 & -8 & -2 & -4 & -2 & -4 & -6 & -4 & -6 & 74 & -4 & -4 & -4 \\
-2 & -4 & -8 & -4 & -4 & -6 & -4 & -4 & -4 & -2 & -4 & -4 & 74 & -4 & -6 \\
-4 & -6 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & 72 & -4 \\
-8 & -4 & -2 & -4 & -4 & -2 & -4 & -4 & -4 & -6 & -4 & -4 & -6 & -4 & 74
\end{pmatrix}$$

Conjecture:
One may observe that in each of our matrices above, some very strong patterns may be found. In particular, one may note that the following holds for all the matrices above. We conjecture that these hold in general:

- $\sum\limits_{i=1}^{q-2} m_{i,j} = \sum\limits_{j=1}^{q-2} m_{i,j} = \sum\limits_{i=1}^{q-2} (\sum\limits_{j=1}^{v} a_{s,j} a_{i,j}) = q-3$ for a fixed s.

- $\operatorname{rank}(MT_q) = q-2$ (Maximal rank) $\iff$ $\det(MT_q) \neq 0$ (Invertible matrix)

- $x^T(MT_q)x > 0 \; \forall x \in \mathbb{R}^{q-3}$ (Positive-definite matrix)

- For $E_q := \{\lambda : \lambda \text{ is an eigenvalue of } MT_q\}$, $min(E_q) = q - 3$
- $m_{i,j} = \sum\limits_{p=1}^{v} a_{i,p}a_{j,p} \begin{cases} > 0 \text{ if } i = j \\ < 0 \text{ if } i \neq j \end{cases}$ (note it is trivial that the diagonal entries are positive)
- $2|\sum\limits_{j=1}^{v}(a_{s,j})^2| > \sum\limits_{i=1}^{q-2}|(\sum\limits_{j=1}^{v} a_{s,j}a_{i,j})|$ (Strictly diagonally dominant matrix)
- $|\sum\limits_{j=1}^{v}(a_{s,j})^2| - \sum\limits_{i=1}^{q-2}|(\sum\limits_{j=1}^{v} a_{s,j}a_{i,j})| = q - 3$
- MT_q is bisymmetric (we know it's symmetric, so we need to show it's antisymmetric).

While this is very limited evidence, we naturally ask do these properties hold in general?

For the remainder of this section, we will begin working on proving these claims. Before we do, we note that some of these properties are very strong.

We note that if the minimal eigenvalue is $q - 3$, that our matrix is positive definite. We note that if it's positive definite, our matrix has maximum rank. We also note that if our matrix is strictly diagonally dominant, that the matrix is positive definite. As such, proving some of these results could serve as an effective way of showing that the rank of M_q is maximal using only elementary means.

Proposition:
For $m_{i,j}$ in MT_q, $a_{i,j}$ in M_q, and a fixed s:

$$\sum_{i=1}^{q-2} m_{i,j} = \sum_{j=1}^{q-2} m_{i,j} = \sum_{i=1}^{q-2}(\sum_{j=1}^{v} a_{s,j}a_{i,j}) = q - 3$$

Proof:
Let $m_{i,j}$ in MT_q, $a_{i,j}$ in M_q, and take a fixed s. Then:

$$\sum_{i=1}^{q-2} m_{i,j} = \sum_{i=1}^{q-2}(\sum_{j=1}^{v} a_{s,j}a_{i,j})$$

But

$$\sum_{i=1}^{q-2}(\sum_{j=1}^{v} a_{s,j}a_{i,j}) = \sum_{j=1}^{v}(\sum_{i=1}^{q-2} a_{s,j}a_{i,j})$$

But $a_{s,j}$ is invariant to i so:

$$\sum_{i=1}^{q-2}(\sum_{j=1}^{v} a_{s,j}a_{i,j}) = \sum_{j=1}^{v}(a_{s,j}(\sum_{i=1}^{q-2} a_{i,j}))$$

However we know the sum of the coefficients of a relation is 1. Thus:

$$\sum_{i=1}^{q-2}(\sum_{j=1}^{v} a_{s,j}a_{i,j}) = \sum_{j=1}^{v} a_{s,j}$$

And we've shown that the sum of the coefficients of a row vector is $q-3$

$$\sum_{j=1}^{v} a_{s,j} = q-3$$

So by symmetry we get our claim that:

$$\sum_{i=1}^{q-2} m_{i,j} = \sum_{j=1}^{q-2} m_{i,j} = q-3$$

This corresponds to the fact that the vector $\{1,1,1,\dots,1\} \in \mathbb{Z}^{q-3}$ is an eigenvector of MT_q, with an eigenvalue of $q-3$.

Definition: s-Submatrix of M_q

Let $\mathbb{F}_q$ be a field. Let M_q be as previously defined. We will call the "s-Submatrix of M_q", which we will denote by $SM_{s,q}$ the matrix:

$$SM_{s,q} := \left(\begin{array}{cccccc} \uparrow & \dots & \uparrow & \uparrow & \dots & \uparrow \\ R(r^s, r^1) & \dots & R(r^s, r^{s-1}) & R(r^s, r^{s+1}) & \dots & R(r^s, r^{q-2}) \\ \downarrow & \dots & \downarrow & \downarrow & \dots & \downarrow \end{array} \right)$$

Example:

For $\mathbb{F}_5$

$$SM_{1,5} := \begin{pmatrix} 3 & 0 \\ -2 & 1 \\ 0 & 0 \end{pmatrix}$$

$$SM_{2,5} := \begin{pmatrix} -1 & 1 \\ 0 & 2 \\ 2 & -2 \end{pmatrix}$$

$$SM_{3,5} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \\ 0 & 2 \end{pmatrix}$$

Definition: s-Submatrix of M_q Times its Transpose

Let $\mathbb{F}_q$ be a field. Let M_q be as previously defined. Let $SM_{s,q}$ as previously defined. Then we call the "s-Submatrix of M_q Times its Transpose", denoted $SMT_{s,q}$, the matrix:

$$SMT_{s,q} := (SM_{s,q}) \cdot (SM_{s,q})^T$$

Proposition:

$MT_q = \sum\limits_{s=1}^{q-2} SMT_{s,q}$

Proof:
This follows quite trivially from the definition of MT_q and $SM_{s,q}$

Observe that:

$$MT_q = \begin{pmatrix} SM_{1,q} & SM_{2,q} & \cdots & SM_{q-2,q} \end{pmatrix} \cdot \begin{pmatrix} (SM_{1,q})^T \\ (SM_{2,q})^T \\ \vdots \\ (SM_{q-2,q})^T \end{pmatrix} = \sum_{s=1}^{q-2} (SM_{s,q}) \cdot (SM_{s,q})^T = \sum_{s=1}^{q-2} (SMT_{s,q})$$

as claimed.

Definition: Extended s-Submatrix of M$_q$
Let $\mathbb{F}_q$ be a field. Let M_q be as previously defined. We will call the "Extended s-Submatrix of M_q", which we will denote by $ESM_{s,q}$ the $(q-2) \times (q-2) \cdot (q-3)$ matrix:

$$ESM_{s,q} := \begin{pmatrix} \uparrow & \cdots & \uparrow & \uparrow & \cdots & \uparrow & \uparrow & \cdots & \uparrow & \uparrow & \cdots & \uparrow \\ 0 & \cdots & 0 & R(r^s, r^1) & \ldots & R(r^s, r^{s-1}) & R(r^s, r^{s+1}) & \ldots & R(r^s, r^{q-2}) & 0 & \cdots & 0 \\ \downarrow & \ldots & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \ldots & \downarrow \end{pmatrix}$$

Proposition:

$$ESM_{s,q} \cdot (ESM_{s,q})^T = SMT_{s,q}$$

Proof:
The proof trivially follows from the definition of $ESM_{s,q}$ and $SMT_{s,q}$, and follows the proof that $MT_q = \sum\limits_{s=1}^{q-2} SMT_{s,q}$.

Proposition:

$$\text{rank}(M) \leq \sum_{s=1}^{q-2} SMT_{s,q}$$

Proof:

$$\text{rank}(M) = \text{rank}(M_q \cdot (M_q)^T)$$

$$M_q \cdot (M_q)^T = \sum_{s=1}^{q-2} SMT_{s,q}$$

$$\text{rank}(M_q \cdot (M_q)^T) \leq \sum_{s=1}^{q-2} \text{rank}(SMT_{s,q})$$

$$\text{rank}(M_q) \leq \sum_{s=1}^{q-2} \text{rank}(SMT_{s,q})$$

Proposition:

$$\text{rank}(M) \geq SM_{s,q} \ \forall s \leq q-2$$

Proof:
We have that $SM_{s,q}$ is a submatrix of M_q of dimension $(q-2) \times (q-3)$. Hence

$$\text{rank}(M) = a \leq q-2 \text{ and } \text{rank}(SM_{s,q}) = b \leq q-3$$

If $b > a$ then there are b linearly independent columns of $SM_{s,q}$. But this is a submatrix of M_q, hence there are at least b linearly independent columns of M_q. But then $a \geq b$, contradicting that $b > a$. Hence our claim is proven.

Note:
This is very much related to our question of whether there always exists some s such that rank$(SM_{s,q})$ is maximal, and if we can show via elementary means that the matrix M_q has maximum rank (as we know it does). If we can show (i.e. if it's true) that rank$(M) >$ rank$(SM_{s,q})$, and if we can show (i.e. if it is true) that there always exists some s such that rank$(SM_{s,q}) = q-3$, then we would have proven that rank$(M) = q-2$. From this point forward, we will assume this result to show that the matrix MT_q is indeed positive definite. The author would much prefer if this result could be shown either via elementary means, or if the result that the rank is maximal could first be shown via elementary means.

We also wish to note that if one could prove strict diagonal dominance via elementary means, this automatically implies the matrix is positive definite and thus has maximum rank. This is a consequence of the Gershgorin Circle Theorem.

Theorem: The Gershgorin Circle Theorem
The Gershgorin Circle Theorem is a well known result by Gershgorin originating in 1931 [4] and [10] which states if

$$R_i = \sum_{j=1, j\neq i}^{n} |a_{i,j}|$$

then all eigenvalues of an $n \times n$ complex-valued matrix A lie in at least one of the disks:

$$D_i = \{z : |z - a_{i,i}| \leq R_i\}$$

Proof: Omitted, but the proof of this well-known result may be found at [4]

Theorem: All eigenvalues of a Hermitian (or symmetric) matrix are strictly positive if and only if the matrix is positive definite

Proof: Omitted, but this proof may be found in chapter seven of [5]

Note: Observe if $0 \in D_i$ for some $i \in \mathbb{N}$, then

$$\exists D_i : 0 \in D_i = \{z : |z - a_{i,i}| \leq R_i\}$$

and hence

$$|0 - a_{i,i}| = |-a_{i,i}| = |a_{i,i}| \leq \sum_{j=1, j\neq i}^{n} |a_{i,j}|$$

If $0 \notin D_i$ for any $i \in \mathbb{N}$ then:

$$|a_{i,i}| > \sum_{j=1, j\neq i}^{n} |a_{i,j}|$$

and thus all eigenvalues are strictly positive, and thus the matrix is positive definite.

Proposition:

$$\text{rank}(MT_q) = q - 2$$

Proof:
Hutchinson [6] has shown $\text{rank}(M_q) = q - 2$. We also have $\text{rank}(M) = \text{rank}(M_q \cdot (M_q)^T)$. Thus $\text{rank}(MT_q) = q - 2$

Theorem:
MT_q is positive semi-definite.

Proof:
From [7] we have "Theorem 12.10. All Gram matrices are positive semi-definite." Here, we note that $MT_q = M \cdot M^T$ is a Gram Matrix and hence is positive semidefinite.

Theorem:
MT_q is positive definite.

Proof:
From [5] we have "Corollary 7.1.7. A positive semidefinite matrix is positive definite if and only if it is nonsingular.". From the above, we have that MT_q is positive semi-definite. We know from Hutchinson [6] that the rank is maximal. We know a square matrix has maximal rank if and only if it is nonsingular. We know the matrix is symmetric. Hence we have that MT_q is positive definite.

Note:
It remains to be shown

- $m_{i,j} = \sum\limits_{p=1}^{v} a_{i,p}a_{j,p} \begin{cases} > 0 \text{ if } i = j \\ < 0 \text{ if } i \neq j \end{cases}$
- $2|\sum\limits_{j=1}^{v} (a_{s,j})^2| > \sum\limits_{i=1}^{q-2} |(\sum\limits_{j=1}^{v} a_{s,j}a_{i,j})|$
- For $E_q := \{\lambda : \lambda \text{ is an eigenvalue of } MT_q\}$, $min(E_q) = q - 3$
- MT_q is bisymmetric (we know it's symmetric, so we need to show it's antisymmetric).

Proving or disproving these properties remain open. We note in particular that by our identity:

$$\sum_{i=1}^{q-2} m_{i,j} = \sum_{j=1}^{q-2} m_{i,j} = q - 3$$

if one could prove via only elementary means that the off-diagonal entries were negative, one would prove as a corollary that the matrix is diagonally dominant (since $m_{i,i} + \sum_{j=1, j\neq i}^{q-2} m_{i,j} = q - 3 > 0$ and the off-diagonals are negative), and therefore is positive definite, and hence has maximum rank. This would therefore be a highly desirable result.

4 Conclusion

While we were unable to prove using only elementary means that the rank of the presentation matrix of a pre-Bloch-group over a finite field is maximal using only elementary means, we have placed a lower bound on the rank. While it seems unlikely that there may be a consistent and explicit set of $q-2$ linearly independent relations, the possibility remains open that more sophisticated searches for linearly independent relations may be fruitful. An explicit set of $q-2$ linearly independent relations remains highly desirable.

We have also proven a number of identities which may aid in a complete description of the pre-Bloch group over a finite field. While we are skeptical that these are significant, and believe that they most likely are only minor results, it is possible that they may serve as stepping-stones to something more impactful.

Finally, we have uncovered some very intriguing patterns in the matrix which we have defined as MT_q. This matrix is one which we believe to be quite interesting, and as such is a strong candidate for further study.

We sumarise our main results below:

Recall the five term relation:

$$R(x,y) = [x] - [y] + [\frac{y}{x}] - [\frac{1-x^{-1}}{1-y^{-1}}] + [\frac{1-x}{1-y}]$$

Theorem:
Let F_q be a field. Let $r \in \mathbb{F}_q$ be a primitive element. Then:

$$\sum_{i=1}^{(q-2)} (\sum_{j=1, j\neq i}^{(q-2)} R(r^i, r^j)) = \sum_{i=1}^{(q-2)} (q-3)[r^i] \text{ in } \mathbb{Z}[\mathbb{F}\backslash\{0,1\}]$$

Theorem:
Let $\mathbb{F}_q$ be a field with. Let $x \in \mathbb{F}_q\backslash\{0,1,-1\}$. Then:

$$\sum_{x\in T} R(x^1, x^2) = \begin{cases} \sum\limits_{x\in T\backslash(\mathbb{F}_q^*)^2} 2[x] - 2[-1] \text{ if } q = 1 \pmod 4 \\ \sum\limits_{x\in T\backslash(\mathbb{F}_q^*)^2} 2[x] \text{ if } q = 3 \pmod 4 \\ \sum\limits_{x\in T} [x] \text{ if } q = 0 \pmod 2 \end{cases} \qquad \text{in } \mathbb{Z}[\mathbb{F}\backslash\{0,1\}]$$

Theorem:
Suppose $\text{Char}(\mathbb{F}_q) \neq 2$. Let:

$$B = \{R(x,x^2) + R(x^{-1}, x^{-2}) : x \in \mathbb{F}_q^*\backslash\{-1,1\}\} \subseteq \mathbb{Z}[\mathbb{F}\backslash\{0,1\}]$$

Then the elements of B are linearly independent to one another.

Theorem:
MT_q is positive definite.

5 Further Study

As we were unable to find $q-2$ linearly independent relations, it warrants further investigation as to whether it is indeed possible to show that the rank is maximal by finding an explicit set of $q-2$ linearly independent relations through a systematic means.

We feel that the question of whether there must always exist some s for $\mathbb{F}_q$ such that the set:

$$S_s = \{R(r^s, r^j) : r \in \mathbb{F}_q \text{ such that } <r>= \mathbb{F}_q^*,\, j \leq q-2 \text{ and } j \neq s\}$$

is linearly independent also to be something worth exploring. This question is one which also has ties to our exploration of the matrix MT_q and if it is true, it may serve as a means to prove using only elementary means that the rank of M_q is maximal, a question which is equivalent to whether it can be shown through elementary means that rank$(MT_q) = q-2$.

Finally, the matrix MT_q is particularly interesting due to the number of very strong patterns and conditions which we have observed via experimental evidence. We believe there is sufficient here to warrant further investigation, to either prove or disprove whether certain conditions hold in general.

We summarise some of the most interesting questions left to explore below:

Question:
Let

$$S_s := \{R(r^s, r^j) : r \in \mathbb{F}_q \text{ such that } <r>= \mathbb{F}_q^*,\, j \leq q-2 \text{ and } j \neq s\}$$

Is it true that $\exists g : 1 \leq g \leq q-2$ such that:

$$\sum_{a \in S_g} \lambda_a a = 0 \implies \lambda_a = 0 \;\forall a \in S_g$$

i.e.

$$\text{rank}(SM_{g,q}) = q-3$$

Question:
Let $\mathbb{F}_q$ be a field. Let M_q be the matrix as previously defined. Let MT_q as previously defined. Is it true and can it be shown via only elementary means that the following properties are satisfied

- rank$(MT_q) = q-2$ (Maximal rank) via only elementary means.
- $x^T(MT_q)x > 0 \;\forall x \in \mathbb{R}^{q-3}$ (Positive-definite matrix)
- $m_{i,j} = \sum\limits_{p=1}^{v} a_{i,p}a_{j,p} \begin{cases} > 0 \text{ if } i = j \\ < 0 \text{ if } i \neq j \end{cases}$
- $2|\sum\limits_{j=1}^{v}(a_{s,j})^2| > \sum\limits_{i=1}^{q-2} |(\sum\limits_{j=1}^{v} a_{s,j}a_{i,j})|$
- For $E_q := \{\lambda : \lambda \text{ is an eigenvalue of } MT_q\}$, $min(E_q) = q-3$

- MT_q is bisymmetric (we know it's symmetric, so we need to show it's antisymmetric).

Recall that a proof that MT_q is strictly diagonally dominant via elementary means would subsequently prove that the matrix is positive definite and thus has maximal rank. Similarly, proving that the minimal eigenvalue is $q-3$ would suffice to show the matrix is positive definite and has maximal rank as desired. Finally, if one can show that the off-diagonal terms are negative, by our identity concerning the sum of row-entries, one would show strict diagonal dominance.

6 Acknowledgements

The author would like to thank University College Dublin for providing the funding to allow this work to take place, and for facilitating this research. The author would like to provide considerable thanks to Dr. Kevin Hutchinson of University College Dublin for supervising this research project, for the many hours spent reviewing and discussing the work, and for providing innumerable suggestions to improve and verify all of the results obtained. Similarly, the author wishes to express his gratitude to Dr. Robert Osburn of University College Dublin for his role in organising the ”Undergraduate Research Projects” program, and for the guidance he provided in promoting student participation in the program.

References

[1] Michael Artin. *Algebra, Second Edition.* Pearson, 2011.

[2] Alan W. Reid Colin Maclachlan. *The Arithmetic of Hyperbolic 3-Manifolds*, volume 219 of *Graduate Texts in Mathematics.* Springer-Verlag New York, 1 edition, 2003.

[3] Johan L. Dupont and Chih-Han Sah. Scissors congruences, ii. *Journal of Pure and Applied Algebra*, 25(2):159 – 195, 1982.

[4] S. Gerschgorin. Uber die abgrenzung der eigenwerte einer matrix. *Bulletin de l'Académie des Sciences de l'URSS. Classe des sciences mathématiques et na*, pages 749–754, 1931.

[5] Roger A. Horn and Charles R. Johnson. *Matrix Analysis.* Cambridge University Press, New York, NY, USA, 2nd edition, 2012.

[6] Kevin Hutchinson. A bloch-wigner complex for sl_2. 2011.

[7] Peter J Olver. Numerical analysis lecture notes, 2008.

[8] Andrei Suslin. K3 of a field and the bloch group. pages 217 – 239, 1991.

[9] Prof. L. Vandenberghe. Ee133a - applied numerical computing (spring quarter 2017), chapter 4, matrix inverses.

[10] Eric W Weisstein. Gershgorin circle theorem.

[11] Wolfram. Finite fields package. http://reference.wolfram.com/language/FiniteFields/tutorial/FiniteFields.htm

[12] Stephen Wolfram. *An Elementary Introduction to the Wolfram Language.* Second edition edition, 2016.

[13] Don Zagier. *The Dilogarithm Function*, pages 3–65. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

7 Notation Reference:

$$\mathbb{F}_q := \text{ a field of order } q$$

$$\mathbb{F}^* := \text{ the multiplicative group of a field.}$$

$$r := r \in \mathbb{F}_q :< r >= \mathbb{F}^*$$

$$R(x,y) := [x] - [y] + [\frac{y}{x}] - [\frac{1-x^{-1}}{1-y^{-1}}] + [\frac{1-x}{1-y}]$$

$$R(r^i,r^j) = [r^i] - [r^j] + [r^{j-i}] - [\frac{1-r^{-i}}{1-r^{-j}}] + [\frac{1-r^i}{1-r^j}]$$

$$M_q := \begin{pmatrix} \uparrow & \dots & \uparrow & \uparrow & \dots & \uparrow & \dots & \uparrow & \dots & \uparrow \\ R(r^1,r^2) & \dots & R(r^1,r^{q-2}) & R(r^2,r^1) & \dots & R(r^2,r^{q-2}) & \dots & R(r^{q-2},r^1) & \dots & R(r^{q-2},r^{q-3}) \\ \downarrow & \dots & \downarrow & \downarrow & \dots & \downarrow & \dots & \downarrow & \dots & \downarrow \end{pmatrix}$$

$$MT_q := M_q \cdot (M_q)^T$$

$$SM_{s,q} := \begin{pmatrix} \uparrow & \dots & \uparrow & \uparrow & \dots & \uparrow \\ R(r^s,r^1) & \dots & R(r^s,r^{s-1}) & R(r^s,r^{s+1}) & \dots & R(r^s,r^{q-2}) \\ \downarrow & \dots & \downarrow & \downarrow & \dots & \downarrow \end{pmatrix}$$

$$SMT_{s,q} := (SM_{s,q}) \cdot (SM_{s,q})^T$$

$$ESM_{s,q} := \begin{pmatrix} \uparrow & \dots & \uparrow & \uparrow & \dots & \uparrow & \uparrow & \dots & \uparrow & \uparrow & \dots & \uparrow \\ 0 & \cdots & 0 & R(r^s,r^1) & \dots & R(r^s,r^{s-1}) & R(r^s,r^{s+1}) & \dots & R(r^s,r^{q-2}) & 0 & \cdots & 0 \\ \downarrow & \dots & \downarrow & \downarrow & \dots & \downarrow & \downarrow & \dots & \downarrow & \downarrow & \dots & \downarrow \end{pmatrix}$$