The MDS Conjecture and related questions in finite geometry

A Thesis

submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

by

Dhameliya Hiren Jayantibhai

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

April, 2019

Supervisor: Dr. Krishna Kaipa

Certificate

This is to certify that this dissertation entitled The MDS Conjecture and related questions in finite geometry towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents study/work carried out by Dhameliya Hiren Jayantibhai at Indian Institute of Science Education and Research under the supervision of Dr. Krishna Kaipa, Assistant Professor, Department of Mathematics, during the academic year 2018-2019.

K.V

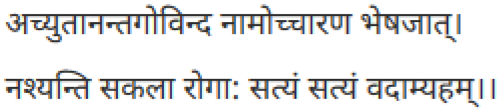
Dr. Krishna Kaipa

Committee:

Dr. Krishna Kaipa

Dr. Vivek Mallick

This thesis is dedicated to *Rushi* Dhanvantari,
who revealed the following truth to the world:



अच्युतानन्तगोविन्द नामोच्चारण भेषजात्।
नश्यन्ति सकला रोगा: सत्यं सत्यं वदाम्यहम्।।

Declaration

I hereby declare that the matter embodied in the report entitled The MDS Conjecture and related questions in finite geometry are the results of the work carried out by me at the Department of Mathematics, Indian Institute of Science Education and Research, Pune, under the supervision of Dr. Krishna Kaipa and the same has not been submitted elsewhere for any other degree.

Dhameliya Hiren Jayantibhai

Acknowledgments

I would like to express my sincere gratitude towards my supervisor Dr. Krishna Kaipa. He was always there whenever I had a problem, talking to him was very encouraging and motivating. I thank Dr. Vivek Mallick for his frequent feedback of the project. I would like to thank Department of Mathematics, IISER Pune for giving me this research opportunity.

I would like to thank my friends for helpful discussions. I have been cheerful around them and interactions with them have provided timely breaks to keep me energized for the project.

Without them I would have not been on this beautiful earth; I sincerely thank my parents for everything I have. I am grateful to my sister and brother for their support throughout the year. Finally, I would like to say, I can not repay the guidance given by my Guru Sri Bharati Shriji in recent years.

Abstract

The MDS conjecture is a long-standing problem in coding theory, first posed by Beniamino Segre in 1955. There is a simple case of the MDS conjecture which is known as rational normal curve (RNC) conjecture. There is a more general conjecture, that we call the Main-conjecture, which states that MDS code of length $q+1$ extending a Reed-Solomon (RS) code of length q is itself a RS code except when q is even and $k \in \{3, q-2\}$. The Main-conjecture is a special case of the more general problem which we call the Main-problem. The Main-problem is to find a condition on k, q and n such that MDS code of length $n+1$, extending a RS code of length n is itself a RS code. First part of the thesis is to study the Main-problem. The most general answer to the Main-problem was given by Ron Roth and Gadiel Seroussi [7] in 1986. In this thesis, we present a new proof of Roth and Seroussi's result given by K. Kaipa [3], using combinatorial nullstellensatz of Noga Alon [1]. One of the applications of Roth and Seroussi's result is that we can find the covering radius of Projective Reed-Solomon (PRS) codes (Reed-Solomon codes of maximum possible length $q+1$) in some cases, which leads to an important problem of determining deep holes (words at the covering radius distance from the code) of PRS codes. In particular, we classify deep holes of PRS codes of dimensions $q-3$ [9] and $q-4$ [4].

Contents

Introduction

The maximal distance separable (MDS) conjecture is a long-standing problem in coding theory and finite geometry. It was implicit in the questions posed by Beniamino Segre [6] in 1955. MDS conjecture states that, for $1 < k < q$ the maximum possible length of a k-dimensional MDS code over finite field $\mathbb{F}_q$ is $q+1$ except when q is even and $k \in \{3, q-1\}$ then it is $q+2$.

There is a simple case of the MDS conjecture which is known as rational normal curve (RNC) conjecture which is implied by the MDS conjecture. RNC conjecture states that there is no MDS code of length $q+2$ and dimension k extending a Reed Solomon (RS) code of length $q+1$ and dimension k except when q is even and $k \in \{3, q-1\}$. There is a more general conjecture which we call the Main-conjecture. The Main-conjecture states that MDS code of length $q+1$ and dimension k extending a Reed-Solomon code of length q and dimension k is itself a RS code except when q is even and $k \in \{3, q-2\}$. The Main-conjecture is a special case of the more general problem which is known as Main-problem. The Main-problem is to find a condition on $k,\ q$ and n such that MDS code of length $n+1$, extending a RS code of length n, is itself a RS code. The first part of the thesis is to study the Main-problem. The most general answer to the Main-problem was given by Ron Roth and Gadiel Seroussi [7] in 1986. In this thesis we study the new proof of their result given by K. Kaipa, using combinatorial nullstellensatz of Noga Alon [1]. This gives much simple proof to the result of Roth and Seroussi. In chapter 1, we present details of code, MDS conjecture and Main-problem. Chapter 2 is about the new proof of the result of Roth and Seroussi.

The result of Roth and Seroussi has applications in finite geometry and coding theory. Here we study the problem which is to determine the deep holes of projective Reed Solomon codes (Reed-Solomon codes of the maximum possible length $q+1$). Deep holes of the code are the words which are at the farthest distance from the code. Since there is a bijective correspondence between the equivalence classes of deep holes and the set of their projective syndromes [3], we focus on determining the projective syndromes of deep holes of projective Reed Solomon code.

Let G_k denote the generator matrix of the projective Reed Solomon code of dimension k ($PRS(q,k)$). For $1 < k < q$ (except $k \in \{3, q-1\}$ if q even), RNC conjecture holds for dimension k, then any $v \in \mathbb{F}_q^k$ is in linear span of some $k-1$ columns of G_k. We divide $\mathbb{F}_q^k$ in the disjoint sets $S_1,\ S_2, \cdots,\ S_{k-1}$, where S_r is the set of vectors of $\mathbb{F}_q^k$ such that it is in the span of some r columns of G_k but not in the span of any $r-1$ columns of G_k. In terms of coding theory, sets $S_1, \cdots, S_{k-1}$ divides received words in their distance from the code. We are interested in determining vectors in the set S_{k-1} because they are the syndromes of deep holes of $PRS(q, q+1-k)$. Chapter 3 of the thesis is the detail about the deep holes of the code.

K. Kaipa gave analysis for the deep holes of $PRS(q, q-2)$ in his work [3]. Then classification of deep holes of $PRS(q, q-3)$ is the recent work by K. Kaipa, J. Zhang and D. Wan [9]. Details of this work, deep holes of $PRS(q, q-3)$, has been given in chapter 3 of the thesis. Our recent work is the deep holes of $PRS(q, q-4)$. The work done so far has been explained in chapter 4 of the thesis.

Chapter 1

Preliminaries

1.1 Code

Messages are transmitted through a transmission channel. Due to noise in the transmission channel message gets corrupted and the receiver gets a wrong message, and we need a system such that it can detect the error and give a correct message. So, we first encode a message in a large space such that it is easy for a decoder to detect the error.

An encoder is a one-one map from $\mathcal{M} \rightarrow \mathcal{F}^n$, where $\mathcal{M}$ is a set of messages and $\mathcal{F}$ is a set of alphabets, and image of this map is called a code. Error correcting code $\mathcal{C}$ of length n over a set of alphabet $\mathcal{F}$ is a subset of $\mathcal{F}^n$. Elements in $\mathcal{F}^n$ are called words The words which are in the code are called codewords. Size of a code $|\mathcal{C}|$ is a number of codewords. When transmitted codeword c get corrupted, and the receiver receives corrupted word c', the role of the decoder is to give the best estimate for what c could have been. Let the c be a codeword sent and c' be a word received. Then with respect to some metric $d(x, y)$ on $\mathcal{F}^n$ where $x, y \in \mathcal{F}^n$, there is a number $d(\mathcal{C})$ such that any two codewords are at least $d(\mathcal{C})$ distance apart.If $d(c, c') \leq \lfloor \frac{d(\mathcal{C})-1}{2} \rfloor$ then decoder has no trouble in correcting a codeword.

Hamming metric is a commonly used metric. Hamming distance between two words x and y is the number of coordinates where x and y differ and is denoted by $d(x, y)$. Here we give definition of the parameter $d(\mathcal{C})$ which has described above.

Definition 1.1.1. *The minimum distance of a code $\mathcal{C}$ is $d(\mathcal{C}) = min\{d(x,y) : x, y \in \mathcal{C}, x \neq y\}$.*

1.2 Linear code

For a linear code, $\mathcal{F}$ is a finite field of order q, which we denote by $\mathbb{F}_q$, and $\mathcal{C}$ is a k dimensional linear subspace of $\mathbb{F}_q^n$. Linear code of dimension k and length n over $\mathbb{F}_q$ is denoted by $[n,k]_q$. It has a generator matrix $G_{k\times n}$ whose rows are the basis of the code. So, $\mathcal{C} = \{xG_{k\times n}, x \in \mathbb{F}_q^k$. Since the matrix $G_{k\times n}$ has rank k, we find some k linearly independent columns of G. Let this columns make a matrix $Q_{k\times k}$. Let $Q^{-1}G = G'$. If x is a message and $c = xG'$ be an associated codeword to x, then x is embedded in c on k positions which were chosen for Q. Since Q is an invertible matrix, G' generates same code as G(basis of the code does not change). Then we can multiply G' with suitable monomial matrix A on right hand side to get matrix $G'' = G'A$ which is of the form $G'' = [I_{k\times k}|B]$ for some $B_{k\times(n-k)}$ matrix. Matrix G'' generates different code as G but has same property as G.

Now, we define a dual of the code. Dual code, denoted with $\mathcal{C}^\perp$, of the code $\mathcal{C}$ is $\mathcal{C}^\perp = \{x \in \mathcal{F}^n : \sum_{i=1}^{k} x_i c_i = 0, \text{ for all } c \in \mathcal{C}\}$. It is easy to see that if $\mathcal{C}$ is linear code, then $\mathcal{C}^\perp = ker(G) = \{x \in \mathbb{F}_q^n : Gx = 0\}$ and $\mathcal{C}^\perp$ is also a subspace of $\mathbb{F}_q^n$. Rank nullity theorem implies that $dim(ker(G)) = n - k$ given $rank(G) = k$. So, $\mathcal{C}^\perp$ is a linear code of length n and dimension $n - k$.

Definition 1.2.1. *Generator matrix of $\mathcal{C}^\perp$ is called parity check matrix of $\mathcal{C}$. It is denoted with H and satisfies $GH^t = 0$.*

G and H are related as follows: If G is of the form as given above, , $G = [I_{k\times k}|B]$ for some $B_{k\times(n-k)}$ matrix, then $H = [-B^t|I_{n-k}]$.

For $c \in \mathcal{C}$, we define $wt(c)$ to be the number of non-zero positions of c.

Proposition 1.2.1. $d(\mathcal{C}) = min\{wt(c) : c \in \mathcal{C}, c{\neq}0\}$

Proof. Let $d = min\{wt(c) : c \in \mathcal{C}, c{\neq}0\}$. Suppose x, y and z be the codewords such that

$d(x,y) = d(\mathcal{C})$ and $d = wt(z)$.

$$d(\mathcal{C}) \leq d(z,0) = wt(z) = d \leq wt(x-y) = d(x,y) = d(\mathcal{C})$$

So, $d(\mathcal{C})$ $=d$. □

Linear code $[n,k]_q$ with minimum distance d is denoted by $[n,k,d]_q$.

1.3 MDS Code

Let the minimum distance of the code $\mathcal{C}$ is d, that implies any two codewords have maximum $n-d$ coordinates same. Then if we choose any $n-d+1$ coordinates of any two codewords of $\mathcal{C}$, they differ at minimum one position. So, $\mathcal{C}$ satisfy the equation $|\mathcal{C}| \leq q^{n-d+1}$. For linear code we get,

$$k \leq n-d+1. \tag{1.1}$$

If $\mathcal{C}$ attain equality in equation 1.1, $k = n-d+1$, then it is called a maximum distance separable(MDS) code. As the name suggest for given size and length of a code, codewords of an MDS code are separated with a maximum distance possible. Example, Reed-Solomon codes are MDS codes. This code has many application, like data storage.

We will use one easy result in the next proposition that, elementary row operation on G does not change the basis of the code and, hence the code. We call a matrix an MDS matrix if only if it generates an MDS code.

Proposition 1.3.1. *G is an MDS matrix if and only if its all the $k \times k$ minors are non zero.*

Proof. Let G_k be a $k \times k$ sub-matrix of G generated by any k columns of G. We want to show that G_k has full rank. Suppose G_k has rank less than k. Then its rows are linearly dependent. By elementary row operation we get matrix G'_k such that its one row has all zeros. With same elementary row operation on matrix G, we get G' such that in one row it has at least k zeros. So, by Proposition 1.2.1, we get $d(\mathcal{C}) \leq n-k$ which contradicts the fact that G is an MDS matrix and $d(\mathcal{C}) = n-k+1$. Thus G_k has full rank and it is a non-singular matrix.

Now, suppose all the $k \times k$ minors of G are non-zero. So, on any row we have max $k-1$ zeros by some elementary row operations on G because if it has k or more zeros then we take k columns according to these zeros and determinant of matrix generated by these columns is zero which contradicts to our assumption. Now, we show that there exist a codewod having $k-1$ zeros. G having a row rank k, it has some k columns which are linearly independent. Let these k columns form matrix Q. Then matrix $Q^{-1}G$ has a identity matrix when we choose its k columns which were used to form Q. So, there is a row of $Q^{-1}G$ having $k-1$ zeros. Since Q is an invertible matrix, $Q^{-1}G$ generates same code as G. So got a codeword having $k-1$ zeros. Hence $n - d(\mathcal{C}) = k-1$, which implies G is an MDS matrix. □

Proposition 1.3.2. *Dual of an MDS code is an MDS code.*

Proof. From equation 1.1, we get $d(\mathcal{C}^{\perp}) \leq k+1$. Suppose $d(\mathcal{C}^{\perp}) = t$ and $t < k+1$. So, there exit a codeword $u \in \mathcal{C}^{\perp}$ such that $wt(u) = t$. Since $Gu = 0$, we can see that, the t columns according to the non-zero entries of u are linealrly dependent. $t < k+1$ implies that $rank(G) < k$ which contradicts to the fact that $rank(G) = k$. So, $d(\mathcal{C}^{\perp}) = k+1$ and $\mathcal{C}^{\perp}$ is also an MDS code. □

Next, we prove a proposition for MDS code which we will use later.

Shortening of a code : Let $\mathcal{C}$ be a $[n,k,d]_q$ code. Now, for each $a \in \mathbb{F}_q$ consider the code $\mathcal{C}' = \{x \in \mathbb{F}_q^{n-1} : (x,a) \in \mathcal{C}\}$. Then $\mathcal{C}'$ is called shortened code of $\mathcal{C}$. As a special case consider $a = 0$, then shortened code $\mathcal{C}'$ is a linear code of length $n-1$ and minimum distance $d(\mathcal{C}') \geq d(\mathcal{C})$.

Proposition 1.3.3. *Shortening of an MDS code with respect to $a = 0$ is an MDS code.*

Proof. Let $\mathcal{C}'$ be a shortened code of an $[n,k,d]_q$ MDS code $\mathcal{C}$. Then $d(\mathcal{C}') \geq d(\mathcal{C})$. We can write generator matrix of $\mathcal{C}$ as $G = [I_k|A]$. Without loss of generality assume that we shortened $\mathcal{C}$ on the first coordinate with respect to $a = 0$. It is easy to see that all the linear combination of rows of G, except the first, the codewords of the shortened code $\mathcal{C}'$. So we get that $\mathcal{C}'$ has dimension $k-1$ and by removing first column and first row of G, we get generator matrix of $\mathcal{C}'$. So, $\mathcal{C}'$ has length $n-1$ and dimension $k-1$. Now, $d(\mathcal{C}) = n-k+1$ and $d(\mathcal{C}') \leq (n-1)-(k-1)+1$ implies $d(\mathcal{C}') = n-k+1$(since $d(\mathcal{C}') \geq d(\mathcal{C})$). □

1.4 Generalized Reed-Solomon(GRS) code

GRS code is a linear MDS code. It's generator matrix is determined by n distinct points $\{x_1, x_2, \cdots, x_n\}$ of the set $\{\mathbb{F}_q \cup \{\infty\}\}$.

We define $c_k(x)$ as following,

$$c_k(x) = \begin{cases} (1, x, x^2, \cdots, x^{k-1})^T & \text{if } x \in \mathbb{F}_q \\ (0, 0, \cdots, 1)^T & \text{if } x = \infty \end{cases}$$

Generator matrix of the GRS code is

$$G_k(\vec{x}, \vec{\nu}) = [c_k(x_1)|c_k(x_2)|\cdots|c_k(x_n)] \ diag[\nu_1, \nu_2, \cdots, \nu_n], \text{ where } \nu_i \in \mathbb{F}_q^\times \ \forall \text{ i.}$$

The GRS code generated by this matrix is

$$C_k(\vec{x}, \vec{\nu}) = \{(\nu_1 f(x_1), \nu_2 f(x_2), \cdots, \nu_n f(x_n)) : deg(f) \leq k-1\}.$$

When all $\nu_i = 1$, we call Generalized Reed-Solomon code as Reed-solomon Code.

Dual of the a GRS code is also a GRS code [2].

Definition 1.4.1. *$k-1$ dimensional projective space over $\mathbb{F}_q$ is the set of equivalences classes of $\mathbb{F}_q^k/\{0\}$ under the equivalence relation $v \sim \lambda v$ for $v \in \mathbb{F}_q^k \setminus \{0\}$ and $\lambda \in \mathbb{F}_q^\times$. It is denoted by $\mathbb{P}^{k-1}(\mathbb{F}_q)$.*

Definition 1.4.2. *n-arc in a projective space $\mathbb{P}^{k-1}(\mathbb{F}_q)$ is a set of n points $\{[V_1], [V_2], \cdots, [V_n]\}$ of a projective space $\mathbb{P}^{k-1}(\mathbb{F}_q)$ such that matrix formed by the representative of these points $[V_1 \mid V_2 \mid \cdots \mid V_n]$ has all the $k \times k$ minors non-zero. RNC of $\mathbb{P}^{k-1}(\mathbb{F}_q)$ is a set of $q+1$ points $\{c_k(x) : x \in \{\mathbb{F}_q \cup \{\infty\}\}\}$.*

RNC in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ can also be defined as below.

Definition 1.4.3. *RNC in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ is a image of the map $\phi : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^{k-1}(\mathbb{F}_q)$ defined as $[x, y] \mapsto [x^{k-1}, x^{k-2}y, \cdots, y^{k-1}]$.*

In the context of finite geometry, columns of the generator matrix of $[n,k]_q$ RS codes are the vectors representing n-arcs which contained in the normal rational curve(abbreviated RNC) of $k-1$ dimensional projective space $\mathbb{P}^{k-1}(\mathbb{F}_q)$.

Let $\mathcal{A}$ be a set of n points $[V_1], \cdots, [V_n]$ of $\mathbb{P}^{k-1}(\mathbb{F}_q)$ and $G = [v_1|\cdots|v_n]$ be a $k \times n$ matrix, where $v_1, \cdots, v_n$ are representative of points $[V_1], \cdots, [V_n]$. It is easy to see from definition of $n - arc$ that $\mathcal{A}$ is an $n - arc$ if and only if G is an MDS matrix.

1.5 MDS Conjecture

Let $k < q$. Then the maximum length $m_k(q)$ of the k-dimensional MDS code over $\mathbb{F}_q$ –equivalently the maximum size $m_k(q)$ of an arc in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ is given by:

$$m_k(q) = \begin{cases} q+2 & \text{if } q \text{ is even and } k = 3, q-1 \\ q+1 & \text{otherwise} \end{cases}$$

The conjecture was implicit in the first of the three questions posed by Beniamino Segre in 1955([8]).

1. Determine $m_k(q)$ and $[m_k(q), k]_q$ MDS codes –equivalently determine $m_k(q)$ and $m_k(q)$-arcs in $\mathbb{P}^{k-1}(\mathbb{F}_q)$.

2. For which values of k and q is every $[q+1, k]_q$ MDS code is a RS code? –equivalently for which values of k and q is every $q+1$-arc of $\mathbb{P}^{k-1}(\mathbb{F}_q)$ is a RNC?

3. Determine values of $n \leq q$ such that every $[n,k]_q$ MDS code is a RS code –equivalently determine values of $n \leq q$ such that every n-arc contained in a RNC.

1.6 Main-Problem

Our interest is to study the Main-problem which is closely related to the third question of Segre.

Main-Problem : Find conditions on k, q and n such that $[n+1,k]_q$ MDS code, extending a $[n,k]_q$ RS code is itself a RS code.

The special case of the Main-problem is Main-conjecture.

Main-Conjecture : For $2 \leq k \leq q-2$, every $[q+1,k]_q$ MDS code, extending a $[q,k]_q$ RS code, is itself a RS code except when q is even and $k = 3, q-2$.

If Main-conjecture holds in dimension $k-1$, then there is RNC-conjecture which holds in dimension k. See Proposition 1.6.1.

RNC-Conjecture : There is no $[q+2,k]_q$ MDS code by extending a $[q+1,k]_q$ RS code except when q is even and $k = 3, q-1$.

Proposition 1.6.1. *[5] Let $3 \leq k \leq q-1$ and assume $k \notin \{3, q-1\}$ if q is even. If the Main-conjecture holds in dimension $k-1$ then the RNC-conjecture holds in dimension k.*

Proof. Let $G = [G_k(\mathbb{F}_q \cup \infty)|a]$, where $a = [a_1, \cdots, a_k]^T$, be a generator matrix of $[q+2,k]_q$ MDS code extending a $[q+1,k]_q$ RS code. Without loss of generality we can assume that $c_k(\infty)$ be a first column of $G_k(\mathbb{F}_q \cup \infty)$. Now, shortening G on the first column we get $[q+1,k-1]_q$ MDS code whose generator matrix $G' = [G_{k-1}(\mathbb{F}_q)|a']$ has $a' = [a_1, \cdots, a_{k-1}]^T$ as a last column. If the Main-conjecture holds in dimension $k-1$ then $a' = c_{k-1}(\infty)$ and we get $a = [0, \cdots, 1, \lambda]$. MDS condition on G imply that λ can not be written as a sum of $k-1$ distinct points of $\mathbb{F}_q$ which is not possible for the values of k which we have considered(Lemma 1.6.2). □

For $k = 3$ and q odd, Main-conjecture is equivalent to Segre's fundamental theorem[6] that any $[q+1,3]_q$ MDS code is a RS code. That is the one proved case of the Main-conjecture. By duality of MDS and RS code, we prove that Main-conjecture also holds for $k = q-2$ when q is odd. The most general answer to the Main-problem was given by Roth and Seroussi which we will see later, in chapter 2.

Here is the Lemma which was used in the proof of Proposition 1.6.1.

Lemma 1.6.2. *Let $1 \leq l \leq q-2$. Assume $l \notin \{2, q-2\}$ if q is even. Then $T_l = \{x_1 + \cdots + x_l :$ where $x_1, \cdots, x_l$ are distinct elements of $\mathbb{F}_q\}$ is all of $\mathbb{F}_q$.*

Proof. If $l = 1$, then it is clear that $T_l = \mathbb{F}_q$. So let $2 \leq l \leq q-2$. Consider the map $\phi : \mathbb{F}_q \to \mathbb{F}_q$ given as $\phi(x) = ax+b$ where $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$. It is easy to check that ϕ is a bijective transformation of $\mathbb{F}_q$. So, it does not change T_l. Therefore $T_l = aT_l + lb$.

If we change x_l with keeping $x_1, \cdots, x_{l-1}$ fix, we see that T_l has at least $q-l+1 \geq 3$ elements(because $l \leq q-2$). In particular it has a non-zero element. Consider $b=0$ and $a \in \mathbb{F}_q^\times$, we get that $\mathbb{F}_q^\times \subset T_l$. So, we only need to find l such that $0 \in T_l$.

Considering the fact that sum of any two element of the field $\mathbb{F}_q$ is nonzero when q is even, we can say $0 \notin T_2$ when q is even. We see that $T_2 = T_{q-2}$ because sum of the all the elements of $\mathbb{F}_q$ is zero. So, $0 \notin T_{q-2}$ when q is even. Thus $T_2 = T_{q-2} = \mathbb{F}_q^\times$, when q is even.

Now we show that $0 \in T_l$ for $2 \leq l \leq q-2$ when q is odd and for $3 \leq l \leq q-3$ when q is even. If q is odd then we can write $\mathbb{F}_q^\times$ as an union of pairs of the form $\{x, -x\}$. Then taking elements of $\lfloor \frac{l}{2} \rfloor$ such pairs (with 0 when l is odd), we see that their sum is zero and total elements are l. So, $0 \in T_l$ when q is odd.

Now for q even, consider $l \equiv \pm\ 1\ mod\ 4$. Then taking $a=1$ in above transformation, we get that $T_l = T_l + \mathbb{F}_q$. From the fact that $l \in T_l$ and $-l \in \mathbb{F}_q$, we get that $0 \in T_l$. Now, consider $l \equiv 0\ mod\ 4$ when q is even. In this case we write $\mathbb{F}_q$ as union of pairs of the form $\{x, 1+x\}$. Taking $\frac{l}{2}$ such pairs, their sum is zero with total l elements of $\mathbb{F}_q$. Hence $0 \in T_l$ in this case.

Now, we are left with $l \equiv 2\ mod\ 4$ when q is even. Let $q = 2^m$. Since $T_l = T_{q-l}$ we take $l \geq q/2$. Consider the binomial expansion of $l = 2^{\nu_1} + 2^{\nu_2} + \cdots 2^{\nu_r}$ with $1 = \nu_1 < \nu_2 < \cdots < \nu_r = m-1$(since $l \equiv 2\ mod\ 4$ and $l \geq 2^{m-1}$). Let $\{b_1, \cdots, b_m\}$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_2$. The zero element of $\mathbb{F}_q$ is represented by the zero vector. Let $\mathbb{A}_i$ be the set of 2^i vectors as given below,

$$\mathbb{A}_i = \{b_{m-i} + \sum_{j=1}^{i} c_j b_{m-i+j} : c_1, \cdots, c_i \in \mathbb{F}_2\}$$

Sum of all the vectors in $\mathbb{A}_i$ is zero for $i \geq 2$ and is b_m for $i = 1$. Then the sum of the vectors of the set

$$\{0\} \cup \{b_{m-\nu_2} + b_{m-\nu_1, b_{m-\nu_1}}\} \cup (\mathbb{A}_{\nu_2} \setminus \{b_{m-\nu_2}\}) \cup \mathbb{A}_{\nu_3} \cup \cdots \cup \mathbb{A}_{\nu_r}$$

is zero and the set has size l. □

Chapter 2

Polynomial method for the Main-Problem

2.1 Introduction

In this chapter, we formulate the Main-problem as a problem in polynomials, and we try to solve it using polynomial methods, especially combinatorial nullstellensatz.

Let $\mathcal{D} = \{x_1, x_2, \cdots, x_n\}$ a set of n distinct points of $\mathbb{F}_q \cup \infty$. Let for $x \in \mathcal{D}$, $c_k(x)$ as defined above in 1.4. Then, the generator matrix of a $[n,k]_q$ RS code with evaluation set $\mathcal{D}$ is

$$G_k(\mathcal{D}) = [c_k(x_1)|c_k(x_2) \cdots |c_k(x_n)].$$

Main-problem can be rewritten as

Main-Problem $(restated)$**[5]:** Let $a = (a_0, \cdots, a_{k-1})^T$. Find condition on k, q and n such that $[G_k(\mathcal{D})|a]$ generates a $[n+1,k]_q$ MDS code if and only if $a = c_k(t)$ for some $t \in \{\mathbb{F}_q \ \cup \ \{\infty\}\} \setminus \mathcal{D}$.

We define polynomials V, f and g over $\mathbb{F}_q$ as follows:

$$V(X_1, \cdots, X_k) = \det[c_k(X_1)|c_k(X_2)| \cdots |c_k(X_k)] \in \mathbb{F}_q[X_1, X_2 \cdots, X_k].$$

Let s_i be the following polynomial identity in $\mathbb{F}_q[X_1, \cdots, X_{k-2}][T]$,

$$\prod_{i=1}^{k-2}(1 - TX_i) = \sum_{i=0}^{k-2} s_i(X_1, \cdots, X_{k-2})T^i.$$

We define f and g as;

$$\begin{aligned} f(X_1, \cdots, X_{k-2}) &= a_0 s_{k-2} + a_1 s_{k-3} + \cdots + a_{k-2} s_0 \\ g(X_1, \cdots, X_{k-2}) &= a_1 s_{k-2} + a_2 s_{k-3} + \cdots + a_{k-1} s_0. \end{aligned}$$

Now, we get a polynomial $h \in \mathbb{F}_q[X_1, X_2, \cdots, X_{k-2}]$ such that some condition on h implies matrix $[G_k(\mathcal{D})|a]$ generates $[n+1, k]_q$ MDS code. This condition is given in the next theorem.

Theorem 2.1.1. *[5] The matrix $[G_k(\mathcal{D})|a]$ generates $[n+1, k]_q$ MDS code if and only if the polynomial*

$$h = V(X_1, X_2, \cdots, X_{k-2}) f \prod_{i=1}^{k-2}(X_i f - g) \prod_{y \in \mathbb{F}_q \setminus \mathcal{D}} (yf - g) \tag{2.1}$$

vanishes on $\mathcal{D} \times \cdots \times \mathcal{D}$.

Proof. The matrix $[G_k(\mathcal{D})|a]$ generates $[n+1, k]_q$ MDS code if its all the $k \times k$ minor are non-zero. It is enough to check for distinct elements $x_1, \cdots, x_{k-1}$ of $\mathcal{D}$, when

$$det([c_k(x_1)| \cdots |c_k(x_{k-1})|a]) \neq 0.$$

Let the polynomial

$$\varphi(X_1, \cdots, X_{k-1}) = \frac{det([c_k(X_1)| \cdots |c_k(X_{k-1})|a])}{V(X_1, \cdots, X_{k-1})}$$

If $X_i = X_j$, for any i, j, then $det([c_k(X_1)| \cdots |c_k(X_{k-1})|a]) = 0$. So, $\varphi(X_1, \cdots, X_{k-1})$ is divisible by $(X_i - X_j)$, for all i, j, and hence divisible by $V(X_1, \cdots, X_{k-1})$. So, $\varphi \in \mathbb{F}_q[X_1, \cdots, X_{k-1}]$. Now, degree of X_i in numerator of φ is $\leq k-1$ and degree of X_i in denominator is $k-2$. So, $deg_{X_i}(\varphi) \leq 1$ for each $i \in \{1, \cdots, k-1\}$. So, we can write $\varphi = X_{k-1}\alpha + \beta$ for some $\alpha, \beta \in \mathbb{F}_q[X_1, \cdots, X_{k-2}]$.

Now we take determinant in denominator with respect to last column and we get,

$$\varphi(X_1, \cdots, X_{k-1}) = \sum_{i=1}^{k} a_{i-1} s_{k-i}(X_1, \cdots, X_{k-1}).$$

Since we can write $s_l(X_1, \cdots, X_{k-1}) = -X_{k-1} s_{l-1}(X_1, \cdots, X_{k-2}) + s_l(X_1, \cdots, X_{k-2})$, we conclude that $\alpha = -f$and $\beta = g$.

So, $det([c_k(X_1)| \cdots |c_k(X_{k-2})|a]) = V(X_1, \cdots, X_{k-1})(-X_{k-1}f + g)$.

For different points $x_1, \cdots, x_{k-2}$ of $\mathcal{D}$, we want $det([c_k(x_1)| \cdots |c_k(x_{k-1})|a]) \neq 0$. This is possible if $f(x_1, \cdots, x_{k-2}) = 0$ or if $f(x_1, \cdots, x_{k-2}) \neq 0$ then $\frac{g}{f}(x_1, \cdots, x_{k-2}) \neq x_{k-1}$ implies $\frac{g}{f}(x_1, \cdots, x_{k-2}) \notin \mathcal{D} \setminus \{x_1, \cdots, x_{k-2}\}$. So, either $f(x_1, \cdots, x_{k-2}) = 0$ or $\frac{g}{f}(x_1, \cdots, x_{k-2}) \in \{x_1, \cdots, x_{k-2}\} \cup \mathbb{F}_q \setminus \mathcal{D}$.

For any $(x_1, \cdots, x_{k-2})$ in $\mathcal{D}^{k-2}$, either x_i repeat for some i or all $x_1, \cdots, x_{k-2}$ are distinct. If x_i repeat for some i, then $V = 0$ and if all x_i distinct, then either $f = 0$ or $\frac{g}{f} \in \{x_1, \cdots, x_{k-2}\} \cup \mathbb{F}_q \setminus \mathcal{D}$. In both cases equation 2.1,

$$h = V(X_1, X_2, \cdots, X_{k-2}) f \prod_{i=1}^{k-2}(X_i f - g) \prod_{y \in \mathbb{F}_q \setminus \mathcal{D}} (yf - g),$$

vanishes.

□

2.2 The result of Roth and Seroussi

The most general answer to the Main-problem was given by Roth and Seroussi([7]). Their result was, one condition for Main-problem is $n \geq k + \lfloor (q-1)/2 \rfloor$ except when q is even and $k = 3$.

We use following elementary lemma to prove Roth-Seroussi's result.

Lemma 2.2.1. *[5] Let $F[X_1, X_2, \cdots, X_l]$ be a polynomial ring in l variables over a arbitrary field F. Let $S \subset F$ is a finite set of size n. Suppose $H \in F[X_1, X_2, \cdots, X_l]$ vanishes on $S \times \cdots \times S$.*

If $deg_{X_i}(H) < n$ for each $1 \leq i \leq l$, then $H = 0$ in $F[X_1, \cdots, X_l]$.

Using Theorem 2.1.1 and Lemma 2.2.1([1],Lemma 2.1), the proof of Roth-Seroussi's result becomes very short and simple. This proof uses a very weak form of combinatorial nullstellensatz, so our target is to use the full form of the nullstellensatz to get better result of the Main-problem.

Theorem 2.2.2. *Result of Roth and Seroussi[7][5] : When $n \geq k + \lfloor (q-1)/2 \rfloor$, matrix $[G_k(\mathcal{D})|a]$ is an MDS code if and only if $a = c_k(x)$ where $x \in \{\mathbb{F}_q \cup \{\infty\}\} \setminus \mathcal{D}$ except when char$(\mathbb{F}_q)$ is 2 then for $k = 3$, $a = [0\ 1\ 0]$ is also possible.*

Proof. $deg_{X_i}(h) \leq 2k-3+q-n$. Now, from Lemma 2.2.1 when h vanishes on $D \times D \times \cdots D$ and

$$deg_{X_i}(h) < n \Leftrightarrow 2k - 3 + q - n < n \Leftrightarrow n \geq k + \lfloor (q-1)/2 \rfloor,$$

then $h \equiv 0$.
Now, polynomial ring $\mathbb{F}_q[X_1, \cdots, X_{k-2}]$ is an integral domain. This gives three cases for value of a.

1. $f \equiv 0$. So, $f = a_0 s_{k-2} + a_1 s_{k-3} + \cdots + a_{k-2} s_0 \equiv 0$ which is possible if and only if $a_i = 0$ for all $i \in \{1, \cdots, k-1\}$(because $deg(s_i) = i$). Hence, in this case $a = c_k(\infty)$
2. $\prod_{y \in \mathbb{F}_q \setminus \mathcal{D}} (yf - g) \equiv 0$. Since $\mathbb{F}_q[X_1, \cdots, X_{k-2}]$ is an integral domain, $yf - g \equiv 0$ for some $y \in \mathbb{F}_q \setminus \mathcal{D}$. So we get $(ya_0 - a_1)s_{k-2} + \cdots + (ya_{k-2} - a_{k-1})s_0 \equiv 0$ which implies $a_i = ya_{i-1}$ for all $i \in \{1, \cdots, k-1\}$. So, $a = a_0 c_k(y)$. Hence, in this case $a = c_k(y)$ for some $y \in \mathbb{F}_q \setminus \mathcal{D}$.
3. $\prod_{i=1}^{k-2} (X_i f - g) \equiv 0$. Without loss of generality assume $X_1 f - g \equiv 0$. So, $X_1 = g/f$. We apply $\sigma \in S_{k-2}$ on $X_1 = g/f$ and get that $X_{\sigma(1)} = g/f = X_1$($f$ and g are symmetric polynomials). So, we get $X_{\sigma(1)} = X_1$ for all $\sigma \in S_{k-2}$ which is possible if and only if S_{k-2} is trivial, only when $k = 3$.
   Let $k = 3$. Then we have $s_1 = -X_1$(let $X_1 = X$) and $s_0 = 1$. So, we get $a_0 X^2 + a_2 = 2a_1 X$. It has only non-zero solution $a = [0\ 1\ 0]$, if q even. □

Condition in Roth-Seroussi's result is $n \geq k + \lfloor (q-1)/2 \rfloor$. Now, we want to study the Main-problem in case $n < k + \lfloor (q-1)/2 \rfloor$. In this case using combinatorial Nullstellensatz of Noga Alon([1]) and develop the following variant of Combinatorial Nullstellensatz.

For $\nu, \mu \in \mathbb{Z}^l$ we say $\mu \geq \nu$ if $\mu_i \geq \nu_i$ for each i, and we say $\mu > \nu$ if $\mu \neq \nu$ and $\mu \geq \nu$. We denote $\nu_1 + \nu_2 + \cdots + \nu_l$ as $|\nu|$.

Theorem 2.2.3. *[5] Let H be as in Lemma 2.2.1. Then, H can be written uniquely as:*

$$H = \sum_{\nu > 0} \chi(X_1)^{\nu_1} \cdots \chi(X_l)^{\nu_l} H_\nu$$

with $deg_{X_i}(H_\nu) < n$ for each i,
moreover $deg(H_\nu) \leq deg(H) - |\nu|n$ and $deg_{X_i}(H_\nu) \leq deg_{X_i}(H) - \nu_i n$ for each i.

Proof. Let $\chi(T) = \prod_{x \in \mathcal{D}}(T - x)$, where $\mathcal{D} \in \mathbb{F}_q$ be a set of size n.
For H being as in Lemma 2.2.1, we can write

$$H = \sum_{i=1}^{k-2} \chi(X_i)_i H_i$$

with $deg(H_i) \leq deg(H) - n$(check, [1, Theorem 1.1]).

Now we do, if possible, repeated long division of H_i with $\chi(X_j)$ for all i, j. Thus we get H in the following form.

$$H = \sum_{\nu > 0} \chi(X_1)^{\nu_1} \cdots \chi(X_{k-2})^{\nu_{k-2}} H_\nu, \text{where } \nu \in \mathbb{Z}^{k-2}.$$

Consider $S_H = \{\nu : H_\nu \neq 0\}$. Since $deg(H) \geq |\nu|n + deg(H_\nu)$, polynomial $H_\nu = 0$ when $|\nu| > deg(H)/n$. Thus S_H is a finite set. Suppose

$$H = \sum_{\nu > 0} \chi(X_1)^{\nu_1} \cdots \chi(X_{k-2})^{\nu_{k-2}} H'_\nu$$

is a different expression for H. Let $S_{H'} = \{\nu : H'_\nu \neq 0\}$ and it's also a finite set as above.

Now, consider $g_\nu = H_\nu - H'_\nu$. Let $S_g = \{\nu : g_\nu \neq 0\}$ which is also finite because $S_g \subset S_H \cup S_{H'}$. If S_g is not empty, take the maximal element μ of S_g. Consider the monomial $X_1^{m_1} \cdots X_{k-2}^{m_{k-2}}$ with $n\mu_i \leq m_i < n(\mu_i + 1)$ for each i. Since $deg_{X_i}(g_\nu) < n$ for all ν, such polynomial can appear in $\chi(X_1)^{\nu_1} \cdots \chi(X_{k-2})^{\nu_{k-2}} g_\nu$ if and only if $\nu \geq \mu$, i.e. only for $\nu = \mu$(since μ is an maximal element of S_g). Since $g_\mu \neq 0$, such monomial does exist in $\chi(X_1)^{\mu_1} \cdots \chi(X_{k-2})^{\mu_{k-2}} g_\mu$ and its coefficient in the expression $\sum_{\nu>0} \chi(X_1)^{\nu_1} \cdots \chi(X_{k-2})^{\nu_{k-2}} g_\nu$ is non-zero which contradicts the fact that $\sum_{\nu>0} \chi(X_1)^{\nu_1} \cdots \chi(X_{k-2})^{\nu_{k-2}} g_\nu = 0$. Hence S_g is empty and $H_\nu = H'_\nu$ for every ν.

Suppose $deg(H_\nu) > deg(H) - |\nu|n$ for some ν. So, $deg(\chi(X_1)^{\nu_1} \cdots \chi(X_{k-2})^{\nu_{k-2}} H_\nu) > deg(H)$. Consider the highest degree monomial $X_1^{t_1} \cdots X_{k-2}^{t_{k-2}}$ of H_ν where $t_i < n$ for each i. Then $X_1^{n\nu_1+t_1} \cdots X_{k-2}^{n\nu_{k-2}+t_{k-2}}$ is a top degree monomial of $\chi(X_1)^{\nu_1} \cdots \chi(X_{k-2})^{\nu_{k-2}} H_\nu$. Since the coefficient of this monomial, $X_1^{n\nu_1+t_1} \cdots X_{k-2}^{n\nu_{k-2}+t_{k-2}}$, in H is zero, it has non-zero coefficient in $\chi(X_1)^{\mu_1} \cdots \chi(X_{k-2})^{\mu_{k-2}} H_\mu$ for some $\mu \neq \nu$ and $deg(\chi(X_1)^{\mu_1} \cdots \chi(X_{k-2})^{\mu_{k-2}} H_\mu) > deg(H)$. This is possible only if $n\nu_i + t_i < n(\mu_i + 1)$ for each i which implies $\nu < \mu$. Then passing to μ and repeating we can assume ν is a maximal element of S_H with monomial $X_1^{n\nu_1+t_1} \cdots X_{k-2}^{n\nu_{k-2}+t_{k-2}}$, having non-zero coefficient in H and having degree higher than $deg(H)$. This contradiction proves that $deg(H_\nu) \leq deg(H) - |\nu|n$ for all ν.

Suppose $deg_{X_i}(H_\nu) > deg_{X_i}(H) - \nu_i n$ for some $i \in \{1, \cdots, k-2\}$. Consider the top degree monomial ${X_1}^{t_1} \cdots {X_{k-2}}^{t_{k-2}}$ of H_ν, this implies $t_i + \nu_i n > deg_{X_i}(H)$ where $t_i = deg_{X_i}(H_\nu)$. Since coefficient of the monomial ${X_1}^{n\nu_1+t_1} \cdots {X_{k-2}}^{n\nu_{k-2}+t_{k-2}}$ in H is zero, it has non-zero coefficient in $\chi(X_1)^{\mu_1} \cdots \chi(X_{k-2})^{\mu_{k-2}} H_\mu$ for some $\mu \neq \nu$. This implies $deg_{X_i}(H) < n\nu_i + t_i \leq n\mu_i + t'_i$ where $t'_i = deg_{X_i}(H_\mu)$. This is possible only if $\mu > \nu$ and particularly ν can not be a maximal element of S_H. Then passing to μ and repeating we can assume ν is a maximal element of S_H with monomial ${X_1}^{n\nu_1+t_1} \cdots {X_{k-2}}^{n\nu_{k-2}+t_{k-2}}$ having non-zero coefficient in H. This contradiction proves the result. $\square$

Chapter 3

Deep holes of the Reed-Solomon code

3.1 What is a deep hole?

Let $\mathcal{C}$ be a $[n,k,d]_q$ linear code. Let G be a generator matrix and H a parity check matrix of $\mathcal{C}$. We can see that $syn(x) = 0$ if and only if $x \in \mathcal{C}$.

Definition 3.1.1. *For any word $u \in \mathbb{F}_q^n$, define its syndrome to be $syn(u) = Hu \in \mathbb{F}_q^{n-k}$. So, $syn(x) = 0$ if and only if $x \in \mathcal{C}$.*

Definition 3.1.2. *Covering radius of a code $\mathcal{C}$, is the smallest integer $\rho(\mathcal{C})$ such that balls of radius $\rho(\mathcal{C})$ around all the codewords exhaust $\mathbb{F}_q^n$.*
The distance of word u from the code $\mathcal{C}$ is $d(u,\mathcal{C}) = min\{d(u,c) : c \in \mathcal{C}\} = min\{wt(u-c) : c \in \mathcal{C}\}$. Then the covering radius $\rho(\mathcal{C}) = max\{d(u,\mathcal{C}) : u \in \mathbb{F}^n\}$.

Definition 3.1.3. *The word $u \in \mathbb{F}_q^n$ is called a deep hole of $\mathcal{C}$ if and only if $d(u,\mathcal{C}) = \rho(\mathcal{C})$ where $\rho(\mathcal{C})$ is a covering radius of $\mathcal{C}$.*

Proposition 3.1.1. *[3]*

$$\rho(\mathcal{C}) = min\{j : Any\ y \in \mathbb{F}_q^{n-k} is\ a\ linear\ combination\ of\ some\ j\ columns\ of\ H\}$$

Proof. Let $v = syn(u)$. Suppose we can write v as a linear combination of some j columns of H, which implies there is a word $w \in \mathbb{F}_q^n$ such that $w = u - c$ for some $c \in \mathcal{C}$ and $wt(w) = j$

and vice versa. From this we can rewrite $d(u, \mathcal{C})$ as below,

$$d(u, \mathcal{C}) = min\{j : syn(u) \text{ is a linear combination of some } j \text{ columns of } H\}$$

Let $S = \{Hu : u \in \mathbb{F}_q^n\}$ be the set of all the syndromes of $u \in \mathbb{F}_q^n$. Since H has full rank, we get that $S = \mathbb{F}_q^{n-k}$. So we can rewrite $\rho(\mathcal{C})$ as below,

$$\rho(\mathcal{C}) = min\{j : Any\ y \in \mathbb{F}_q^{n-k} \text{ is a linear combination of some } j \text{ columns of } H\}$$

□

Let $\mathcal{C}$ be an $[n, k]_q$ MDS code.

Proposition 3.1.2. *$\rho(\mathcal{C}) \leq n - k$.*

Proof. Matrix H has rank $n - k$. So we can always write $y \in \mathbb{F}_q^{n-k}$ as a linear combination of some $n - k$ columns of H. Hence using proposition 3.1.1, we get $\rho(\mathcal{C}) \leq n - k$. □

Proposition 3.1.3. *[3] Suppose $\rho(\mathcal{C}) = n - k$. Word u is a deep hole of an $[n, k]_q$ MDS code $\mathcal{C}$ if and only if we can extend $\mathcal{C}^{\perp}$ with one unit without losing an MDS property, i.e. $[H|Hu]$ is an $[n + 1, n - k, k + 2]_q$ MDS code.*

Proof. Let u be a deep hole of an $[n, k, d]_q$ MDS code. Then Hu can not be written in a linear combination of less or equal to $n - k - 1$ columns of H(proposition 3.1.1). So, any $(n - k) \times (n - k)$ minors of the matrix $[H|Hu]$ are non-zero, i.e. it's an MDS matrix.

Suppose $[H|v]$ is an $[n + 1, n - k, k + 2]_q$ MDS matrix. We can always find $u \in \mathbb{F}_q^n$ such that $Hu = v$ (if not clear, check proposition 3.1.1). Since $[H|v]$ is an MDS matrix, v can not be written as a linear combination of $n - k - 1$ or less columns of H, i.e. $d(u, \mathcal{C}) \geq n - k$. Proposition 3.1.2 implies $d(u, \mathcal{C}) = n - k$ and $\rho(\mathcal{C}) = n - k$. So u is a deep hole of $\mathcal{C}$. □

3.2 Projective Reed-Solomon codes

Definition 3.2.1. *The $[q + 1, k]_q$ RS code generated by the matrix $G_k = [G_k(\mathbb{F}_q)|c_k(\infty)]$ is called projective Reed-Solomon code of dimension k and it is denoted by $PRS(q, k)$.*

Let $\mathcal{C}$ be a $PRS(q,k)$. The matrix $G_k = [G_k(\mathbb{F}_q)|c_k(\infty)]$ is a generator matrix of $\mathcal{C}$. The columns of G_k represent all the points on RNC of $\mathbb{P}^{k-1}(\mathbb{F}_q)$. It is easy to check that matrix $G_{q+1-k} = [G_{q+1-k}(\mathbb{F}_q)|c_{q+1-k}]$ is a parity check matrix of $\mathcal{C}$. The $PRS(q, q+1-k)$ is the dual code of $\mathcal{C}$. We have

$$G_k = [c_k(x_1)| \cdots |c_k(x_q)|c_k(\infty)] \text{ and}$$

$$G_{q+1-k} = [c_{q+1-k}(x_1)| \cdots |c_{q+1-k}(x_q)|c_{q+1-k}(\infty)].$$

Definition 3.2.2. *Word u_1 and u_2 are called coset equivalent if $u_1 - u_2 \in \mathcal{C}$ and equivalent if $u_1 - au_2 \in \mathcal{C}$ for some $a \in \mathbb{F}_q^\times$.*

Definition 3.2.3. *Let $\mathcal{C}$ be a $G_k(\mathcal{D})$ RS code. The generating polynomial of a received word $u \in \mathbb{F}_q^n$ of $\mathcal{C}$ is a Lagrange interpolation polynomial $u(X)$ of the data points $\{(x_1, u_1), \cdots, (x_n, u_n)\}$. It has degree at most $n-1$.*

Let projective syndrome be a image of syndrome in projective space. Coset equivalence classes of deep holes are in one to one correspondence with the set of syndromes of deep holes because deep holes are coset equivalent if and if they have same syndrome. Similarly equivalence classes of deep holes are in one to one correspondence with projective syndromes of deep holes. For PRS codes if $v = (v_1, \cdots, v_{q+1-k})$ is a syndrome of a deep hole u then the generating polynomial of the deep hole u is $u(X) = (-1)(X^{q-1}v_1 + X^{q-2}v_2 + \cdots + X^{k-1}v_{q+1-k})$(We can check that $Hu^T = v^T$) and coset equivalence class of u is $(u(x_1), u(x_2), \cdots, u(x_q), 0) + \mathcal{C}$. So, determining equivalence classes of deep holes of the PRS codes is equivalent to determing projective syndromes of deep holes.

3.3 PRS codes and the covering radius conjecture

MDS conjecture implies there is no MDS code of length $q+2$ except when q is even and $k = 3$ or $q-1$. From this we get the following proposition. Let $\mathcal{C}$ be a $PRS(q,k)$ code.

Proposition 3.3.1. *Suppose the MDS-conjecture is true. Then $\rho(\mathcal{C}) = q-k$ except when q is even and $k = q-2$ or 2 then $\rho(\mathcal{C}) = q-k+1$.*

Proof. MDS conjecture implies there is no MDS extension of a $PRS(q, q+1-k)$ code except when q is even and $k = q-2$ or 2. So from proposition 3.1.3, $\rho(\mathcal{C}) \neq q+1-k$

except when q is even and $k = q-2$ or 2. So, $\rho(\mathcal{C}) < q+1-k$ except exceptions. If we find $u \in \mathbb{F}_q^n$ such that $d(u, \mathcal{C}) = q-k$ then we are done. Let word u with generating polynomial $u(X) = X(X-x_1)\cdots(X-x_{k-1})$ where $x_i \in \mathbb{F}_q$ for $i \in \{1, \cdots, k-1\}$. Then

$$d(u, \mathcal{C}) = q + 1 - max\{(u-c)_0 : c \in \mathcal{C}\},$$

where $(u-c)_0$ is the number of zeros of $u-c$. In terms of polynomials, c is represented by a polynomial (X) of degree at most $k-1$. So, maximum zeros of $u(X) - c(X)$ is k and $(u-c)_0 = k+1$ when $c(X) = 0$(because $u(\infty) = c(\infty) = 0$). Hence in this case $max\{(u-c)_0 : c \in \mathcal{C}\} = k+1$ implies $d(u, \mathcal{C}) = q-k$. That proves $\rho(\mathcal{C}) = q-k$.
In the case when q is even and $k = q-2$ or 2, we know there is an MDS extension by one unit. So from proposition 3.1.2 and 3.1.3 we get $\rho(\mathcal{C}) = q-k+1$. □

Above proposition can be written as following conjecture which is known as covering radius conjecture.

Conjecture 3.3.2. *For $2 \leq k \leq q-2$, the covering radius of a $PRS(q,k)$ code is $q-k$ except when q is even and $k = q-2$ or 2 in which case covering radius is $q-k+1$.*

Roth and Seroussi's result proves the conjecture 3.3.2 in cases given in next theorem.

Theorem 3.3.3. *(R. Roth and G. Seroussi)[5]: Suppose $n - m \geq (q-1)/2$. The matrix*

$$[c_m(x_1)| \cdots |c_m(x_n)|v]$$

generates a $[n+1, m]_q$ MDS code if and only if $v = c_m(y), y \in \{\mathbb{F}_q \cup \infty\} \setminus \{x_1, \cdots, x_n\}$, except when q is even and $m = 3$ then $v = [0\ 1\ 0]$ is also possible.

Roth and Seroussi's result implies for $m \leq q/2 + 1$, there is no MDS extension of a $PRS(q,m)$ except when q is even and $m = 3$. So from proposition 3.3.1 for $k \geq q/2$ covering radius of $PRS(q,k)$ code is $q-k$ except when q even and $k = q-2$ then $\rho(\mathcal{C}) = q+1-k$. So, for $q > 5$ Roth and Seroussi's result implies $\rho(\mathcal{C}) = q-k$ for $PRS(q, q-2)$ when q odd and $PRS(q, q-3)$. Our next aim is to find all the deep holes in these cases.

3.4 Deep holes of $PRS(q, q-2)$ when q odd

Following proposition is used to find deep hole syndromes of $PRS(q, q-2)$ if q odd.

Proposition 3.4.1. *[3] Let $2 \leq k \leq q-2$ and if q even then $k \notin \{q-2, 2\}$. If u is a deep hole of $PRS(q, k)$ then it's syndrome Hu can not be written as a linear combination of any $q-k-1$ columns of H.*

Proof. From the proof of proposition 3.1.1, we get

$$d(u, \mathcal{C}) = min\{j : Hu \text{ is a linear combination of some } j \text{ columns of } H.\}$$

Next, $d(u, \mathcal{C}) = \rho(\mathcal{C})$ if and only if Hu is not in a linear combination of $\rho(\mathcal{C}) - 1$ or less columns of H. In our case $\rho(\mathcal{C}) = q - k$. So, all the vectors of $\mathbb{F}_q^{q+1-k}$ which are not in a linear span of any $q-k-1$ columns of H are syndromes of deep holes of $PRS(q, q-2)$ when q is odd. □

For $PRS(q, q-2)$, the value of $q-k-1 = 1$. Hence the vectors of $\mathbb{F}_q^3$ which are are not in the span of any column of G_3 are syndromes of deep holes of $\mathcal{C}$. There are $(q+1)(q-1)+1$ vectors in $\mathbb{F}_q^3$ which are in linear span of 1 columns of $PRS(q, q-2)$. So, number of syndromes of deep holes of $\mathcal{C}$ is $q^3 - ((q+1)(q-1)+1) = q^2(q-1)$. So, number of projective syndromes is q^2. So, there are q^2 equivalence classes of deep holes of $\mathcal{C}$ [3].

3.5 Deep holes of $PRS(q, q-3)$

Matrix G_{q-3} is a generator matrix and G_4 is a parity check matrix of $PRS(q, q-3)$.

Proposition 3.5.1. *[9] Number of deep holes of $PRS(q, q-3)$ is $(q-1)(q^3/2 + q^2 + q/2)$.*

Proof. Proposition 3.4.1 implies all the vectors of $\mathbb{F}_q^4$ which are not in a linear span of any $q-k-1 = 2$ columns of G_4 are syndromes of deep holes of $PRS(q, q-3)$. There are $(\binom{q+1}{2}(q-1)^2 + (q+1)(q-1) + 1)$ number of vectors which are in linear span of at max 2 columns of G_4. So, number of syndromes of deep holes of $PRS(q, q-3)$ is

$$\begin{aligned} & q^4 - \left(\binom{q+1}{2}(q-1)^2 + (q+1)(q-1) + 1\right) \\ = \quad & (q-1)(q^3/2 + q^2 + q/2) \end{aligned}$$

and $(q^3/2 + q^2 + q/2)$ equivalence classes of deep holes of $\mathcal{C}$. □

Let $\mathcal{N}_k = (0, \cdots, 1, 0)$, only $k-1$th coordinate of is 1, all other coordinates are zero.

Theorem 3.5.2. *[9] Let $2 \leq k \leq q-2$ and if q even then $k \notin \{q-2, 2\}$. There are $q(q+1)$ equivalence classes of deep holes of $PRS(q, k)$, represented by the polynomial $u(X) = X^k$.*

Proof. The word $u = (u_1, u_2, \cdots, u_q, 0)$, where $u_i = u(x_i)$, has syndrome $\mathcal{N}_{q+1-k}$. We need to show that $\mathcal{N}_{q+1-k}$ is a syndrome of a deep hole. For that we need to show that $d(u, \mathcal{C}) = q-k$. For that we need to show that $\mathcal{N}_{q+1-k}$ is not a linear combination of any $q-k-1$ columns of H. Then the matrix $K = [c_{q+1-k}(y_1)| \cdots |c_{q+1-k}(y_{q-k-1})|\mathcal{N}_{q+1-k}]$, where $\{y_1, \cdots, y_{q-k-1}\} \subset \mathbb{F}_q \cup \{\infty\}$, has rank $q-k$. So, it is enough to show that at least one $q-k \times q-k$ minor of K is non-zero.

- If one of the columns of K is $c_{q+1-k}(\infty)$ then wlog suppose $y_{q-k-1} = \infty$. By removing third last column we get $q-k \times q-k$ submatrix of K whose determinant is non-zero.
- In this case there is no $c_{q+1-k}(\infty)$ column in K. Then removing last column of K we get $q-k \times q-k$ submatrix whose determinant is non-zero.

That completes the proof that the word u is a deep hole of $\mathcal{C}$. □

Definition 3.5.1. *Projective linear group $PGL_k(\mathbb{F}_q)$ is a quotient of the group $GL_k(\mathbb{F}_q)$ with center $\mathbb{F}_q^\times$. So, $PGL_k(\mathbb{F}_q) = \frac{GL_k(\mathbb{F}_q)}{\mathbb{F}_q^\times}$. It can be viewed as the set of equivalence classes of GL_k with the equivalence relation - $G \sim \lambda G$ for $G \in GL_k(\mathbb{F}_q)$ and $\lambda \in \mathbb{F}_q^\times$ - two matrices are equivalent if and only if one is scalar multiple of other.*

Define $\mathbb{S}_{q+1-k} = \{$set of all the projective syndromes of deep holes of $PRS(q, k)\}$. Next, we consider action of the group $PGL_2(\mathbb{F}_q)$ on $\mathbb{S}_{q+1-k}$. Then we find size of the orbit of the deep hole syndrome $\mathcal{N}_{q+1-k}$.

From an action of $GL_2(\mathbb{F}_q)$ on $\mathbb{F}_q^2$, we get action of $PGL_2(\mathbb{F}_q)$ on $\mathbb{P}^1(\mathbb{F}_q)$. Next, we identify $\mathbb{F}_q \cup \{\infty\}$ with $\mathbb{P}^1(\mathbb{F}_q)$ by the map $x \mapsto [c_2(x)]$. Hence we get action of $PGL_2(\mathbb{F}_q)$ on $\mathbb{F}_q \cup \{\infty\}$. So for $[g] = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \in PGL_2(\mathbb{F}_q)$, we have $[g]x = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \begin{pmatrix} 1 \\ x \end{pmatrix}$. So, for each $x \in \mathbb{F}_q$ we take $[g]x$ as $g(x) = \frac{c+dx}{a+bx}$, where $ad - bc \neq 0$.

Action of $PGL_2(\mathbb{F}_q)$ on $\mathbb{P}^{m-1}(\mathbb{F}_q)$: There is an injective group homomorphism $\phi : PGL_2(\mathbb{F}_q) \to PGL_m(\mathbb{F}_q)[2]$, which we denote $[g_2] \mapsto [g_m]$, with the property that for each $[g_2]$ we get $[g_m] \cdot [c_m(x)] = [c_m(g_2(x))]$. If $g_2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then we get g_m such that its ijth entry is the coefficient of X^{j-1} of the polynomial $(a+bX)^{m-i}(c+dX)^{i-1}$. Then action of g_2 on $[v] \in \mathbb{P}^{m-1}(\mathbb{F}_q)$ is $[g_m v]$.

Lemma 3.5.3. *[9] Let $\phi([g_2]) = [g_m]$. There exit a monomial matrix $M \in aut(\mathcal{C})$ such that $g_m G_m = G_m M$.*

Proof. Let P be a permutation matrix such that

$$g_2[x_1, \cdots, x_{q+1}] = [g_2(x_1), \cdots, g_2(x_{q+1})] = [x_1, \cdots, x_{q+1}]P.$$

Then,

$$\begin{aligned} g_m G_m = g_m[c_m(x_1), \cdots, c_m(x_{q+1})] &= [g_m c_m(x_1), \cdots, g_m c_m(x_{q+1})] \\ &= [c_m(x_1), \cdots, c_m(x_{q+1})]PD = G_m PD, \end{aligned}$$

where D is a diagonal matrix. Let $D = diag(d_1, \cdots, d_{q+1})$.
If $b_i \neq 0$ then

$$d_i = \begin{cases} (a+bx_i)^{m-1} & x_i \neq -a/b, \infty \\ (c-ad/b)^{m-1} & x_i = -a/b \\ b^{m-1} & x_i = \infty \end{cases}.$$

If $b_i = 0$ then

$$d_i = \begin{cases} a^{m-1} & x_i \neq \infty \\ d^{m-1} & x_i = \infty \end{cases}.$$

So, we have monomial matrix $M = PD$ such that $g_m G_m = G_m M$.

□

Proposition 3.5.4. *[9] u is a deep hole of $PRS(q,k)$ if and only if Mu is also a deep hole of $PRS(q,k)$, where $M \in Aut(\mathcal{C})$(M is a monomial matrix).*

Proof. Let $m = q+1-k$. u is a deep hole of $PRS(q,k)$ if and only if $syn(u)$ is not a linear combination of any $q-k-1$ columns of G_m. Given this we need to show that $syn(Mu) = g_m syn(u)$(since $g_m syn(u) = g_m G_m u = G_m M u = syn(Mu)$) is not a linear combination of any $q-k-1$ columns of G_m. Suppose it is a linear combination of some $q-k-1$ columns of G_m. We get a matrix $P = [c_m(y_1)|\cdots|c_m(y_{q-k-1})|g_m syn(u)]$, where $\{y_1, \cdots, y_{q-k-1}\} \subset \mathbb{F}_q \cup \{\infty\}$, having rank $q-k-1$. We multiply P with g_m^{-1} and get that $syn(u)$ is a linear combination of some $q-k-1$ columns of G_m which implies u is not a deep hole of $PRS(q,k)$. Similarly we can prove inverse. □

Lemma 3.5.5. *Let $p = char(\mathbb{F}_q)$. For $k > 3$ stabilizer of $\mathcal{N}_k$ under the action of $PGL_2(\mathbb{F}_q)$ on $\mathbb{P}^{k-1}(\mathbb{F}_q)$ is:*

$$\begin{cases} \{\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} : d \in \mathbb{F}_q^{\times}\} & k \not\equiv 1 \ mod \ p \\ \{\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} : c \in \mathbb{F}_q, d \in \mathbb{F}_q^{\times}\} & k \equiv 1 \ mod \ p \end{cases}$$

Proof. Applying g_k on $\mathcal{N}_k$ we get $g_k\mathcal{N}_k = \begin{pmatrix} (k-1)ab^{k-2} \\ cb^{k-2} + (k-2)dab^{k-3} \\ \vdots \\ (k-2)d^{k-3}cb + ad^{k-2} \\ (k-1)cd^{k-2} \end{pmatrix}$.

If $k \not\equiv 1 \ mod \ p$ then $g_k\mathcal{N}_k$ is projectively equivalent to $\mathcal{N}_k$ if and only if $b = c = 0$.
If $k \equiv 1 \ mod \ p$ then $g_k\mathcal{N}_k$ is projectively equivalent to $\mathcal{N}_k$ if and only if $b = 0$.

□

Let group G acts on set S. For $s \in S$, $|\mathcal{O}(s)| = |G|/|stab(s)|$. We use this formula to find the size of orbit of N_4.

First we show that $\mathcal{N}_4 + c_4(\infty)$ is a deep hole syndrome of $PRS(q, q-3)$. Suppose it is not a deep hole syndrome then it is in a linear combination of some 2 columns of G_4. So,

$\mathcal{N}_4 + c_4(\infty) = \alpha c_4(x) + \beta c_4(y)$. Consider first 3 coordinates of $\mathcal{N}_4 + c_4(\infty)$, we get that $c_3(\infty) = \alpha c_3(x) + \beta c_3(y)$ where $\alpha, \beta \in \mathbb{F}_q$. Hence 3 columns of G_3 are linearly dependent which is not possible. Therefore $\mathcal{N}_4 + c_4(\infty)$ is a deep hole syndrome of $PRS(q-3)$.

Theorem 3.5.6. *There are $q(q+1)$ elements of $\mathbb{S}_4$ which form orbit of $\mathcal{N}_4 = (0,0,1,0)$ when $char(\mathbb{F}_q) \neq 3$ and union of the orbits of $\mathcal{N}_4$ and $\mathcal{N}_4 + c_4(\infty)$ when $char(\mathbb{F}_q) = 3$ under the action of $PGL_2(\mathbb{F}_q)$ on $\mathbb{P}^3(\mathbb{F}_q)$.*

Proof. If $char(\mathbb{F}_q) \neq 3$ then from lemma 3.5.5, $|stab(\mathcal{N}_4)| = q-1$ implies $|\mathcal{O}(\mathcal{N}_4)| = q(q+1)$. If $char(\mathbb{F}_q) = 3$ then from lemma 3.5.5 $|stab(\mathcal{N}_4)| = (q-1)q$ implies $|\mathcal{O}(\mathcal{N}_4)| = (q+1)$. In this case $\mathcal{O}(\mathcal{N}_4 + c_4(\infty))$ is different from the $\mathcal{O}(\mathcal{N}_4)$. Applying g_k on $\mathcal{N}_4 + c_4(\infty)$ we get

$$g_k(\mathcal{N}_4 + c_4(\infty)) = \begin{pmatrix} 3ab^2 + b^3 \\ cb^2 + 2dab + db^2 \\ 2dcb + ad^2 + d^2b \\ 3cd^2 + d^3 \end{pmatrix}.$$

Matrix g_k stabilizes $\mathcal{N}_4 + c_4(\infty)$ if and only if $b = 0$ and $a = d$. So,

$$stab(\mathcal{N}_4 + c_4(\infty)) = \{\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} : c \in \mathbb{F}_q\}.$$

Hence $|stab(\mathcal{N}_4 + c_4(\infty))| = q$ implies $|\mathcal{O}(\mathcal{N}_4 + c_4(\infty))| = (q-1)(q+1)$. □

Theorem 3.5.7. *Let $\mathbb{F}_{q^2}$ be a 2 degree extension of $\mathbb{F}_q$ and σ be a non-trivial element of $Gal(\mathbb{F}_{q^2}/\mathbb{F}_q)$. The vectors*

$$v(\lambda, x) = \lambda c_{q+1-k}(x) + \sigma(\lambda) c_{q+1-k}(\sigma(x)), \text{ where } x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \text{ and } \lambda \in \mathbb{F}_{q^2}^{\times}$$

in $\mathbb{F}_q^{q+1-k}$ are syndromes of deep holes of $PRS(q,k)$. For $k \leq q-3$, this gives $(q-1)q(q^2-1)/2$ coset equivalence classes of deep holes([9],Theorem 3.6).

Proof. Let $m = q+1-k$. Vector in $\mathbb{F}_q^m$ of the form,

$$v(\lambda, x) = \lambda c_m(x) + \sigma(\lambda) c_m(\sigma(x)), \text{ where } x \in \mathbb{F}_{q^2}/\mathbb{F}_q \text{ and } \lambda \in \mathbb{F}_{q^2}^{\times}$$

is a syndrome of deep hole of $\mathcal{C}$ because otherwise we can write $v(\lambda, x)$ as a linear combination of some m columns of $G_m(\mathbb{F}_{q^2})$(generator matrix of $PRS(q^2, m)$), which implies some m

columns of $G_m(\mathbb{F}_{q^2})$ are linearly dependent.

Two such deep holes corresponding to (λ, x) and (λ', x') are coset equivalent if and only if syndromes $v(\lambda, x) = v(\lambda', x')$. Let $\lambda_2 \neq \lambda_1$ and $x_2 \neq x_1$ then for $m \geq 4$, i.e. $k \leq q-3$, vector $v(\lambda_1, x_1) = v(\lambda_2, x_2)$(4 columns of $G_m(\mathbb{F}_{q^2})$ are linearly dependent) is not possible except when $(\lambda_2, x_2) = (\sigma(\lambda_1), \sigma(x_1))$. So for $k \leq q-3$, total number of such syndromes is $(q^2-1)(q^2-q)/2$.

Syndromes found in above theorem are different from $\mathcal{N}_m$ because otherwise $\mathcal{N}_m$ would be a linear combination of 2 columns of $G_m(\mathbb{F}_{q^2})$, contradicting the fact that $\mathcal{N}_m$ is a syndrome of deep hole of $PRS(q^2, k)$. □

Chapter 4

Deep holes of $PRS(q, q-4)$

Let $\mathbb{S}_5$ denote the set of projective deep hole syndromes of $PRS(q, q-4)$. Group $PGL_2(\mathbb{F}_q)$ acts on $\mathbb{S}_5$. We decompose $\mathbb{P}^4(\mathbb{F}_q)$ into the orbits under the subgroup $H = \{t \to d(t+c) : d \in \mathbb{F}_q^\times, c \in \mathbb{F}_q\}$ of $PGL_2(\mathbb{F}_q)$. Then we check which of these orbits are in $\mathbb{S}_5$. Let $\mu([v])$ denote the position of the first non-zero entry of $[v] \in \mathbb{P}^4(\mathbb{F}_q)$. Under the action of H on $[v] \in \mathbb{P}^4(\mathbb{F}_q)$, the value of μ is invariant because the image of $h_2 \in H$ in $PGL_5(\mathbb{F}_q)$, h_5, is an lower triangular matrix. Hence μ is constant on each H-orbit of $\mathbb{P}^4(\mathbb{F}_q)$.

Let $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^l$ denote a set of representatives for the equivalence classes of $\mathbb{F}_q^\times$ under the equivalence relation $x \sim y$ if $x/y = t^l$ for some $t \in \mathbb{F}_q$. For q even, let $\mathbb{F}_q/\mathbb{F}_q''$ denote a set of representatives for the equivalence classes of $\mathbb{F}_q$ under $x \sim y$ if $y = x + c + c^2$ for some $c \in \mathbb{F}_q$. We take $h' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in PGL_2(\mathbb{F}_q)$.

Lemma 4.0.1. *[4] Representatives of distinct H-orbits of $\mathbb{P}^4(\mathbb{F}_q)$ are,*
(1) $\mu = 5 : c_5(\infty)$
(2) $\mu = 4 : \mathcal{N}_5 = (0,0,0,1,0)$ *if q odd and* $\mathcal{N}_5, \mathcal{N}_5 + c_5(\infty)$ *if q even.*
(3) $\mu = 3 :$
(a) $(0,0,1,0,0)$
(b) $\{(0,0,1,0,\epsilon) : \epsilon \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2\}$
(c) $(0,0,1,1,0)$ *only if $char(\mathbb{F}_q) = 3$*
(4) $\mu = 2 :$
(a) $(0,1,0,0,0)$

(b) $\{(0,1,0,0,\alpha) : \alpha \in \mathbb{F}_q^{\times}/(\mathbb{F}_q^{\times})^3\}$

(c) $\{(0,1,1,\beta,\alpha) : \alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q/\mathbb{F}_q^{''}\}$ *only if* $char(\mathbb{F}_q) = 2$

(d) $\{(0,1,0,\epsilon,0) : \epsilon \in \mathbb{F}_q^{\times}/(\mathbb{F}_q^{\times})^2\}$ *if* q *odd*

(e) $\{(0,1,0,\alpha,\alpha) : \alpha \in \mathbb{F}_q^{\times}\}$ *if* q *odd*

(5) $\mu = 1$:

(a) $c_5(0)$

(b) $\{c_5(0) + \lambda c_5(\infty) : \lambda \in \mathbb{F}_q^{\times}/(\mathbb{F}_q^{\times})^4\}$

(c) $\{c_5(0) + \lambda \mathcal{N}_5 : \lambda \in \mathbb{F}_q^{\times}/(\mathbb{F}_q^{\times})^3\}$

(d) $\{(1,0,0,\lambda,\lambda) : \lambda \in \mathbb{F}_q^{\times}\}$

(e) $\{(\epsilon^{-1},0,1,\alpha,\beta) : \alpha,\beta \in \mathbb{F}_q, \epsilon \in \mathbb{F}_q^{\times}/(\mathbb{F}_q^{\times})^2\}$

Proof. Let $v = (v_0, v_1, v_2, v_3, v_4) \in \mathbb{S}_5$.
Let $h(t \to d(t+c)) \in H$. Then

$$\begin{aligned} h_5 v = (v_0, d(v_1 + cv_0), d^2(v_2 + 2cv_1 + c^2 v_0), d^3(v_3 + 3cv_2 + 3c^2 v_1 + c^3 v_0),\\ d^4(v_4 + 4cv_3 + 6c^2 v_2 + 4c^3 v_1 + c^4 v_0)). \end{aligned} \tag{4.1}$$

(1) $\mu = 5$, then only $v_4 \neq 0$. So $v = \lambda c_5(\infty)$, where $\lambda \in \mathbb{F}_q^{\times}$ implies $[v] = c_5(\infty)$.

(2) $\mu = 4$. In this case $v_0 = v_1 = v_2 = 0, v_3 = 1$ and $v_4 \in \{0, v_4 \neq 0\}$.

Let $v = (0,0,0,1,v_4)$, then from equation 4.1,

$$[h_5 v] = (0,0,0,1,d(v_4 + 4c))$$

(i) $v_4 = 0$. In this case $[h_5 v] = (0,0,0,1,4dc)$. We take h_2 such that $c = 0$. So, this case is $[h_5 v] = \mathcal{N}_5$.

(ii) $v_4 \neq 0$. In this case $[h_5 v] = (0,0,0,1,d(v_4 + 4c))$.

If $char(\mathbb{F}_q) \neq 2$, we take h_2 with $c = -v_4/4$, then this case is $[h_5 v] = \mathcal{N}_5$.

If $char(\mathbb{F}_q) = 2$ then $[h_5 v] = (0,0,0,1,dv_4)$.

So, take h_2 with $d = v_4^{-1}$ then $[h_5 v] = \mathcal{N}_5 + c_5(\infty)$.

(3) $\mu = 3$. In this case $v_0 = v_1 = 0, v_2 = 1$ and
$(v_3, v_4) \in \{(0,0), (0, v_4 \neq 0), (v_3 \neq 0, 0), (v_3 \neq 0, v_4 \neq 0)\}$.

Let $v = (0,0,1,v_3,v_4)$ then

$$[h_5 v] = (0,0,1,d(v_3 + 3c), d^2(v_4 + 4cv_3 + 6c^2)).$$

If $char(\mathbb{F}_q) \neq 3$ then by taking h_2 with $c = -v_3/3$, we get $[h_5v] = (0,0,1,0,v'_4)$.

Now again applying $h'_2 \in H$ on $[h_5v]$, we get

$$[h'_5(h_5v)] = (0,0,1,3d'c', d'^2(v'_4 + 6c'^2)).$$

We take h' with $c' = 0$, then we get $[h'_5(h_5v)] = (0,0,1,0,d'^2v'_4)$. So we get two cases:

(i)$v'_4 = 0$ implies $[h'_5(h_5v)] = (0,0,1,0,0)$ and

(ii)$v'_4 \neq 0$ implies $[h'_5(h_5v)] = (0,0,1,0,\epsilon)$ where $\epsilon \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$.

If $char(\mathbb{F}_q) = 3$ then

$$[h_5v] = (0,0,1,dv_3,d^2(v_4 + cv_3)).$$

(a) If $v_3 \neq 0$ then we take h_2 with $c = -v_4/v_3$ and $d = v_3^{-1}$, we get $[h_5v] = (0,0,1,1,0)$.

(b) If $v_3 = 0$ then $[h_5v] = (0,0,1,0,d^2v_4)$. So we get two cases:

(i)$v_4 = 0$ then $[h_5v] = (0,0,1,0,0)$ and

(ii)$v_4 \neq 0$ then $[h_5v] = (0,0,1,0,\epsilon)$ where $\epsilon \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$.

(4) $\mu = 2$. In this case $v_0 = 0$ and $v_1 = 1$.

Let $v = (0,1,v_2,v_3,v_4)$ then

$$[h_5v] = (0,1,d(v_2+2c),d^2(v_3+3cv_2+3c^2),d^3(v_4+4cv_3+6c^2v_2+4c^3)).$$

If $char(\mathbb{F}_q) \neq 2$ then by taking $h \in H$ with $c = -v_2/2$, we get $[h_5v] = (0,1,0,v'_3,v'_4)$.

Then again applying h'_2 on $[h_5v]$, we get

$$[h'_5(h_5v)] = (0,1,2d'c',d'^2(v'_3+3c'^2),d'^3(v'_4+4c'v'_3+4c'^3)).$$

We take $h'_2 \in H$ with $c' = 0$ then $[h'_5(h_5v)] = (0,1,0,d'^2v'_3,d'^3v'_4)$. So, we have 4 subcases.

(i) $(v'_3,v'_4) = (0,0)$. In this case $[h'_5(h_5v)] = (0,1,0,0,0)$.

(ii) $(v'_3,v'_4) = (0,v'_4 \neq 0)$. In this case $[h'_5(h_5v)] = (0,1,0,0,d^3v'_4)$. So $[v]$ is in the orbit of $(0,1,0,0,\alpha)$ for some $\alpha \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^3$.

(iii) $(v'_3,v'_4) = (v'_3 \neq 0,0)$. In this case $[h'_5(h_5v)] = (0,1,0,d^2v'_3,0)$. So $[v]$ is in the orbit of $(0,1,0,\alpha,0)$ for some $\alpha \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$.

(iv) $(v'_3,v'_4) = (v'_3 \neq 0, v'_4 \neq 0)$. In this case $[h'_5(h_5v)] = (0,1,0,d^2v'_3,d^3v'_4)$. So we take $d' = v'_3/v'_4$ in h_2 then $[h'_5(h_5v)] = (0,1,0,\alpha,\alpha)$ where $\alpha \in \mathbb{F}_q^\times$.

If $char(\mathbb{F}_q) = 2$ then

$$[h_5v] = (0,1,dv_2,d^2(v_3+cv_2+c^2),d^3v_4).$$

(i) If $v_2 \neq 0$ then taking $d = v_2^{-1}$ we get $[h_5v] = (0,1,1,(\frac{v_3}{v_2^2}+\frac{c}{v_2}+(\frac{c}{v_2})^2),\frac{v_4}{v_2^3})$. So v is in the orbit of $(0,1,1,\beta,\alpha)$ where $\beta \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)''$ and $\alpha \in \mathbb{F}_q$.

(ii) If $v_2 = 0$ then $[h_5 v] = (0,1,0,d^2(v_3+c^2), d^3 v_4)$. From the Frobenious automorphism of $\mathbb{F}_q$, $x \mapsto x^p$ where $p = char(\mathbb{F}_q)$, we can say that square root of all elements of $\mathbb{F}_q$ exist in $\mathbb{F}_q$ if q is even. So, let $h_2 \in H$ with $c = \sqrt{v_3}$ then $[h_5 v] = (0,1,0,0,d^3 v_4)$. So $[h_5 v] \in \{(0,1,0,0,\alpha) : \alpha \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^3\}$.

(5) $\mu = 1$. In this case $v_0 = 1$.

Let $v = (1, v_1, v_2, v_3, v_4)$ then

$$[h_5 v] = (1, d(v_1+c), d^2(v_2+2cv_1+c^2), d^3(v_3+3cv_2+3c^2v_1+c^3),$$
$$d^4(v_4+4cv_3+6c^2v_2+4c^3v_1+c^4)).$$

Let $h \in H$ with $c = -v_1$, then $[h_5 v] = (1,0,v_2',v_3',v_4')$.

Then again applying h_2' on $h_5 v$, we get

$$[h_5'(h_5 v)] = (1, d'c', d'^2(v_2'+c'^2), d'^3(v_3'+3c'v_2'+c'^3), d'^4(v_4'+4c'v_3'+6c'^2v_2'+c'^4)).$$

We take $h' \in H$ with $c' = 0$ then $[h_5'(h_5 v)] = (1,0,d'^2 v_2', d'^3 v_3', d'^4 v_4')$.

(a) If $v_2' \neq 0$ we get v in the orbit of $(1,0,\epsilon,\epsilon d\frac{v_3'}{v_2'},\epsilon d^2\frac{v_4'}{v_2'})$ which is equivalent to $(\epsilon^{-1},0,1,\alpha,\beta)$ where $\alpha,\beta \in \mathbb{F}_q$.

(b) Next $v_2' = 0$ implies

$$[h_5'(h_5 v)] = (1,0,0,d^3 v_3', d^4 v_4').$$

So we get 4 subcases.

(i) $(v_3',v_4') = (0,0)$. In this case $[h_5'(h_5 v)] = (1,0,0,0,0)$. So $[v]$ is in the orbit of $c_5(0)$.

(ii) $(v_3',v_4') = (0, v_4' \neq 0)$. In this case $[h_5'(h_5 v)] = (1,0,0,0,d^4 v_4')$. So $[v]$ is in the orbit of $c_5(0) + \lambda c_5(\infty)$ for some $\lambda \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^4$.

(iii) $(v_3',v_4') = (v_3' \neq 0, 0)$. In this case $[h_5'(h_5 v)] = (0,1,0,d^3 v_3', 0)$. So $[v]$ is in the orbit of $c_5(0) + \lambda \mathcal{N}_5$ for some $\lambda \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^3$.

(iv) $(v_3',v_4') = (v_3' \neq 0, v_4' \neq 0)$. In this case $[h_5'(h_5 v)] = (0,1,0,d^3 v_3', d^4 v_4')$. So $[v]$ is in the orbit of $(1,0,0,\alpha,\alpha)$ for some $\alpha \in \mathbb{F}_q$.

□

Lemma 4.0.2. *[4] Let $v = (v_0,v_1,v_2,v_3,v_4) \in \mathbb{F}_q^5$. Let $v' = (v_0,\cdots,v_3)$ and $v'' = (v_1,\cdots,v_4)$. Then, $[v] \in \mathbb{S}_5$ if and only if following 3 conditions holds,*

(1) Either A) $v' \in \mathbb{S}_4$, or B) $v' = \lambda c_4(x) + c_4(\infty)$, where $\lambda, x \in \mathbb{F}_q$.

(2) Either A) $v'' \in \mathbb{S}_4$*, or B)* $v'' = \lambda c_4(x) + c_4(0)$*, where* $\lambda \in \mathbb{F}_q$*,* $x \in \{\mathbb{F}_q^\times \cup \infty\}$

(3) $v = ac_5(x) + bc_5(y) + cc_5(z)$ *has no solution for* $a, b, c \in \mathbb{F}_q$ *and distinct* $x, y, z \in \mathbb{F}_q^\times$*. If* v' *or* v'' *are in* $\mathbb{S}_4$ *then it is in one of the following forms,*

(A1) $(3b^2a, b^2c + 2abd, d^2a + 2bcd, 3d^2c)$ *and when* $char(\mathbb{F}_q) = 3$ *also* $(b^3, b^2d + b^2c + 2abd, bd^2 + d^2a + 2bcd, d^3)$*, for some* $h(t) = (c + dt)/(a + bx)$ *in* $PGL_2(\mathbb{F}_q)$*.*

(A2) $(a + a^q, ax + a^qx^q, ax^2 + a^qx^{2q}, ax^3 + a^qx^{3q})$ *for* $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *and* $a \in \mathbb{F}_{q^2}^\times$*.*

Proof. $[v] \in \mathbb{S}_5$ if and only if

$$v = ac_5(x) + bc_5(y) + cc_5(z) \text{ for } a, b, c \in \mathbb{F}_q \text{ and distinct } x, y, z \in \{\mathbb{F}_q \cup \infty\} \qquad (4.2)$$

has no solution.

Suppose equation 4.2 has a solution with x, y or $z = \infty$, wlog let $z = \infty$, then $v = ac_5(x) + bc_5(y) + cc_5(\infty)$ which implies $v' = ac_4(x) + bc_4(y)$ for distinct $x, y \in \mathbb{F}_q$. Hence in this case if $v' = \lambda c_4(x) + c_4(\infty)$ for $\lambda, x \in \mathbb{F}_q$ or $v' \in \mathbb{S}_4$ then equation 4.2 does not has solution.

Similarly if equation 4.2 has a solution with x, y or $z = 0$, wlog let $z = 0$, then $v = ac_5(x) + bc_5(y) + cc_5(0)$ which implies $v' = ac_4(x) + bc_4(y)$ for distinct $x, y \in \{\mathbb{F}_q^\times \cup \infty\}$. Hence in this case if $v'' = \lambda c_4(x) + c_4(0)$ for $\lambda \in \mathbb{F}_q,\ x \in \{\mathbb{F}_q \cup \infty\}$ or $v'' \in \mathbb{S}_4$ then equation 4.2 does not has solution.

We left with the case when for distinct $x, y, z \in \mathbb{F}_q^\times$, the equation 4.2 has a solution. Hence $[v] \in \mathbb{S}_4$ if and only if conditions $(1), (2)$ and (3) of the lemma holds. As we have seen in chapter 4 if $[v] \in \mathbb{S}_4$ then $[v]$ is either in the orbit of $\mathcal{N}_4$ and also $\mathcal{N}_4 + c_4(\infty)$ when $char(\mathbb{F}_q) = 3$ or $v = ac_4(x) + a^qc_4(x^q)$ for $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $a \in \mathbb{F}_{q^2}^\times$. That proves the second assertion of lemma.

□

Further analysis require the solution of the following two problems.

$$\text{1)Problem } P_{\alpha,\lambda} : x + y + z = -\alpha, xyz = \lambda;\ x, y, z \in \mathbb{F}_q^\times \text{ are distinct.} \qquad (4.3)$$

$$\text{2)Problem } Q_{\alpha,\beta} : x + y + z + xyz/\epsilon = \alpha, \epsilon(1 + xy/\epsilon)(1 + yz/\epsilon)(1 + zx/\epsilon) = \epsilon + \alpha^2 - \beta;$$
$$\text{for distinct } x, y, z \in \mathbb{F}_q^\times. \qquad (4.4)$$

Solution to these problems are given in [4].

Now we determine which of these $H - orbits$ are in $\mathbb{S}_5$.

Theorem 4.0.3. *[4] Representatives of distinct $PGL_2(\mathbb{F}_q)$-orbits of $\mathbb{S}_5$.*
For sufficiently large q,

(1) $\mathcal{N}_5$ if q odd and $\{\mathcal{N}_5,\ \mathcal{N}_5 + c_5(\infty)\}$ if q even.

(2) $\{v_i : 0 \leq i \leq q\}$, where $v_i = \theta^i c_5(\theta) + \theta^{iq} c_5(\theta^q)$ and θ is a generator of the multiplicative group $\mathbb{F}_{q^2}^\times$.

(3) $(0,0,1,0,0)$ if $q \not\equiv 1$ mod 3.

(4) $(0,0,1,0,\epsilon^{-1})$, $q \equiv 0$ mod 3, where ϵ is a quadratic non-residue.

(5) $(0,1,1,\alpha,0)$ if q is even and $q \equiv 1$ mod 3, where α is a fixed element of $\mathbb{F}_q \setminus \mathbb{F}''$.

Proof. If one of the conditions in Lemma 4.0.2 does not hold for v then $[v] \notin \mathbb{S}_5$.
(1) $\mu = 5$, then $v = c_5(\infty)$.
(2) $\mu = 4$. In this case $\mathcal{N}_5$ if q odd and $\{\mathcal{N}_5, \mathcal{N}_5 + c_5(\infty)\}$ if q even are in $\mathbb{S}_5$.
(3) $\mu = 3$.

(a) $v = (0,0,1,0,0)$.

Here v' and v'' are in case $A1)$ of Lemma 4.0.2 because $v' = (0,0,1,0) = \mathcal{N}_4$ and $v'' = (0,1,0,0) = h_4\mathcal{N}_4$ for $h \in PGL_2(\mathbb{F}_q)$ such that $h_2(t) = 1/t$.
The equation $v = ac_5(x) + bc_5(y) + cc_5(z)$ for x, y, z distinct in $\mathbb{F}_q^\times$ and $a, b, c \in \mathbb{F}_q$, is equivalent to the equations

$$x + y + z = 0 \ (1) \text{ and } xy + yz + xz = 0 \ (2) \text{ for distinct } x, y, z \in \mathbb{F}_q^\times$$

have a solution(See Appendix A).
We put value of z from equation (1) into equation (2) and get

$$x^2 + y^2 + xy = 0 \text{ has a solution for distinct } x, y \in \mathbb{F}_q^\times.$$

If $char(\mathbb{F}_q) \equiv 0$ mod 3 then,

$$x^2 + y^2 + xy = 0 \Leftrightarrow x^2 + y^2 - 2xy = 0 \Leftrightarrow (x-y)^2 = 0 \Leftrightarrow x = y \ (3)$$

From equation (1) and (3), we get $x = y = z$. So, $v \in \mathbb{S}_5$ when $char(\mathbb{F}_q) \equiv 0$ mod 3.

If $char(\mathbb{F}_q) \neq 3$ then,

$$\left(\frac{y}{x}\right)^2 + \frac{y}{x} + 1 = 0 \Leftrightarrow \left(\frac{y}{x} - 1\right)\left(\left(\frac{y}{x}\right)^2 + \frac{y}{x} + 1\right) = 0 \Leftrightarrow \left(\frac{y}{x}\right)^3 - 1 = 0.$$

It has a solution when cube root of 1 exist in $\mathbb{F}_q$, that is when $char(\mathbb{F}_q) \equiv 1 \bmod 3$. In this case $(x, y, z) = (a, a\omega, a\omega^2)$ where $a \in \mathbb{F}_q^\times$ and ω is a cube root of unity. So, $v \notin \mathbb{S}_5$ when $char(\mathbb{F}_q) \equiv 1 \bmod 3$ and when $char(\mathbb{F}_q) \equiv 2 \bmod 3$ then $v \in \mathbb{S}_5$.

(b) $v = (0, 0, 1, 0, \epsilon)$ where $\epsilon \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$.

Consider $h \in PGL_2(\mathbb{F}_q)$ such that $h(t) = 1/t$. Then $\mu(h_5 v) = 1$ which we deal later in case $\mu(v) = 2$.

(c) $v = (0, 0, 1, 1, 0)$ when $char(\mathbb{F}_q) = 3$.

Take $h \in PGL_2(\mathbb{F}_q)$ such that $h(t) = 1 + 1/t$. Then $h_5 v = (0, 1, 0, 0, 1)$ which we deal later in case $\mu(v) = 2$.

(4) $\mu = 2$.

(a) $v = (0, 1, 0, 0, 0)$.

Then v is in the orbit of $\mathcal{N}_5$. So, $v \in \mathbb{S}_5$.

(b) $v = (0, 1, 0, 0, \alpha)$.

Then take $h \in PGL_2(\mathbb{F}_q)$ such that $h(t) = 1/t$, then $\mu(h_5 v) = 1$ which we deal in the case $\mu(v) = 1$.

(c) $v = (0, 1, 1, \beta, \alpha)$ when $char(\mathbb{F}_q) = 2$.

If $\alpha \neq 0$ then we take $h \in PGL_2(\mathbb{F}_q)$ such that $h(t) = 1/t$, then $\mu(h_5 v) = 1$ which we deal in the case $\mu = 1$. So, we can assume $\alpha = 0$.

$v = (0, 1, 1, \beta, 0)$ with $char(\mathbb{F}_q) = 2$.

Here the case B of Lemma 4.0.2 does not hold for v' because $(0, 1, 1) \neq c_3(x)$ for any $x \in \mathbb{F}_q$. Also the case $A1$ not hold for v' because $(0, 1, 1, \beta) = (b^2 a, b^2 c, d^2 a, d^2 c)$ implies $ab = 0$ but $bc \neq 0$ and $ad \neq 0$ which is not possible. Only remaining case $A2$ holds for v' if and only if $X^2 + X + \beta + 1$ is irreducible over $\mathbb{F}_q$ (see Appendix), that is when $1 + \beta \notin \mathbb{F}''$.

If $q \equiv 1 \bmod 3$ then $1 \in \mathbb{F}_q''$, so we take $\beta \notin \mathbb{F}''$.

If $q \equiv 2 \bmod 3$ then $1 \notin \mathbb{F}''$, so we take $\beta = 0 \in \mathbb{F}''$.

Let $q \equiv 2 \bmod 3$. Then $\beta = 0$ and hence $[v] = (0, 1, 1, 0, 0)$.

We apply g_2 with $g(t) = 1 + 1/t$ on v, then $[g_5 v] = (0, 0, 1, 0, 0)$. That we have studied in case $\mu = 3$.

Let $q \equiv 1 \bmod 3$ then we take $\beta \notin \mathbb{F}''$.

The only possible case of Lemma 4.0.2 which holds for v'' is $A2$, when polynomial

$x^2 + x + \beta = 0 \in \mathbb{F}_q[X]$ is irreducible. Since $\beta \notin \mathbb{F}''$, case $A2$ holds for v''. Next, we check if condition (3) of Lemma 4.0.2 holds for v.

The equation $v = ac_5(x) + bc_5(y) + cc_5(z)$ for x, y, z distinct in $\mathbb{F}_q^\times$ and $a, b, c \in \mathbb{F}_q$, is equivalent to the equations

$$\begin{aligned} x + y + z + xy + yz + zx = \alpha \text{ and} \\ x^2 + y^2 + z^2 + xy + yz + xz + (x + y)(y + z)(x + z) = 0; \\ \text{for distinct } x, y, z \in \mathbb{F}_q^\times \end{aligned}$$

have a solution(See Appendix A). It has solution only when $\alpha = 1$. Since $1 \in \mathbb{F}''$ and $\alpha \notin \mathbb{F}''$, these equation does not have a solution. Hence $[v] \in \mathbb{S}_5$. We show that elements in $PGL_2(\mathbb{F}_q)$ has zero on first and last coordinate and other coordinates are non-zero. For $g \in PGL_2(\mathbb{F}_q)$ with $g(t) = \frac{c+dt}{a+bt}$,

$$[g_5 v] = (0, a^2 + ab + b^2\alpha, ad - bc, c^2 + cd + d^2\alpha, 0).$$

Since $\alpha \notin \mathbb{F}''$ and $ad - bc \neq 0$, we get $a^2 + ab + b^2\alpha, ad - bc$ and $c^2 + cd + d^2\alpha$ are non-zero. Since this is not true for the orbits (1) and (2) of Theorem 4.0.3, we get that orbit of $[v]$ is different from orbits (1),(2) of Theorem 4.0.3.

(d) $v = (0, 1, 0, \epsilon, 0)$ where $\epsilon \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$, when q odd.

Here only case $A2$ of Lemma 4.0.2 holds for both v' and v'' if and only if ϵ is an quadratic non-residue.

So, $v = ac_5(x) + a^q c_5(x^q)$ for some $a \in \mathbb{F}_{q^2}^\times$ with $a^q = -a$ and $x = \sqrt{\epsilon}$.

(e) $v = (0, 1, 0, \alpha, \alpha)$ where $\alpha \in \mathbb{F}_q^\times$, when q odd.

Then take $h \in PGL_2(\mathbb{F}_q)$ such that $h(t) = 1/t$ then $\mu(h_5 v) = 1$ which we deal in the case $\mu = 1$.

(5) $\mu = 1$.

Case (a) and (b) are clearly not in $\mathbb{S}_5$.

(c) : $v = c_5(0) + \lambda\mathcal{N}_5$ where $\lambda \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^3$.

We check when condition (3) holds for v. If $v = ac_5(x) + bc_5(y) + cc_5(z)$, where $x, y, z \in \mathbb{F}_q^\times$ are distinct, has solution then we get following equations

$$x + y + z = 0 \text{ and } xyz = \lambda, \text{ for distinct } x, y, z \in \mathbb{F}_q^\times$$

have a solution(See Appendix A). That is if problem $P_{\alpha,\lambda}$ has a solution for $\alpha = 0$

and $\lambda \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^3$. Theorem 4.0.4 implies $v \notin \mathbb{S}_5$ if any of the following holds.

$$\begin{aligned} (i) &\quad q \geq 8 \text{ when } char(\mathbb{F}_q) \in \{2,3\} \\ (ii) &\quad q \geq 23 \text{ when } char(\mathbb{F}_q) \notin \{2,3\}. \end{aligned}$$

(d) : $v = (1, 0, 0, \lambda, \lambda)$ where $\lambda \in \mathbb{F}_q^\times$.

If $v = ac_5(x) + bc_5(y) + cc_5(z)$, where $x, y, z \in \mathbb{F}_q^\times$ are distinct, has solution then we get following equations

$$x + y + z = 1 \text{ and } xyz = \lambda, \text{ for distinct } x, y, z \in \mathbb{F}_q^\times$$

have a solution(Appendix A). That is if problem $P_{\alpha,\lambda}$ has solution for $\alpha = -1$ and $\lambda \in \mathbb{F}_q^\times$. Theorem 4.0.4 implies $v \notin \mathbb{S}_5$ if any of the following holds.

$$\begin{aligned} (i) &\quad q \geq 16 \text{ when } char(\mathbb{F}_q) \in \{2,3\} \\ (ii) &\quad q \geq 23 \text{ when } char(\mathbb{F}_q) \notin \{2,3\}. \end{aligned}$$

(e) : $v = (\epsilon^{-1}, 0, 1, \alpha, \beta)$ where $\alpha, \beta \in \mathbb{F}_q$ and $\epsilon \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$.

We use Lemma 4.0.2 to determine when $v \in \mathbb{S}_5$. First we find cases when v' and v'' satisfy sequentially conditions (1) and (2) of Lemma 4.0.2, then we check if v satisfy condition (3) of Lemma 4.0.2 in this cases.

(i) The case $A1$ of Lemma 4.0.2 holds for v' if and only if $\alpha = 2\sqrt{-\epsilon}$.

(ii) The case $A2$ holds for v' if and only if the polynomial $X^2 - \alpha X - \epsilon \in$ is irreducible over $\mathbb{F}_q$.

(iii) The case B does not hold for v' for any $\lambda, x \in \mathbb{F}_q$.

Similarly we check for v''.

(iv) The case $A1$ holds for v'' if and only if $4\beta = 3\alpha^2$.

(v) The case $A2$ holds for v'' if and only if polynomial $X^2 - \alpha X + \beta - \alpha^2$ is irreducible over $\mathbb{F}_q$.

(vi) The case B holds for v'' if and only if $\beta = \alpha^2 \neq 0$.

Here $v = ac_5(x) + bc_5(y) + cc_5(z)$ for distinct $x, y, z \in \mathbb{F}_q^\times$ is equivalent to the following equations have a solution

$$x+y+z+xyz/\epsilon=\alpha \text{ and } \epsilon(1+xy/\epsilon)(1+yz/\epsilon)(1+zx/\epsilon)=\epsilon+\alpha^2-\beta; \quad \text{for distinct } x,y,z\in\mathbb{F}_q^{\times} \tag{4.5}$$

i.e. Solution to the problem $Q_{\alpha,\beta}$.
We say α to be Type-I if $\alpha=2\sqrt{-\epsilon}$ and Type-II if $X^2-\alpha X-\epsilon\in\mathbb{F}_q[X]$ is irreducible.
If $\beta=\epsilon+\alpha^2$ then $v\in\mathbb{S}_5$ when α is of Type-I or Type-II.
If α is of Type-I and if q odd then

$$v=g_5(\mathcal{N}_5) \text{ for } g(t)=\frac{\sqrt{-\epsilon}(-3a+bt)}{a+bt}$$

and if q even then

$$v=g_5(\mathcal{N}_5+c_5(\infty)) \text{ for } g(t)=\frac{\sqrt{-\epsilon}(a+b+bt)}{a+bt}.$$

If α is of Type-II then

$$v=ac_5(x)+a^qc_5(x^q), \text{ where } a=\frac{\alpha^2+2\epsilon-\alpha x}{\epsilon(\alpha^2+4\epsilon)} \text{ and } x \text{ is a root of the polynomial } X^2-\alpha X-\epsilon \text{ over } \mathbb{F}_{q^2}.$$

Combining details of v' and v'', we get the following cases for (α,β):
Let q be odd, if α be of Type-I,

(i) We say (α,β) to be Type-Ia if $X^2-\alpha X+\alpha^2-\beta$ is reducible over $\mathbb{F}_q$ and $\beta\neq\alpha^2$.

(ii) We say (α,β) to be Type-Ib if either $X^2-\alpha X+\alpha^2-\beta$ is irreducible over $\mathbb{F}_q$ or $\beta=\alpha^2$.

If α be of Type-II,

(iii) We say (α,β) to be Type-IIa if $X^2-\alpha X+\alpha^2-\beta$ is reducible over $\mathbb{F}_q$ and $\beta\notin\{\alpha^2,3\alpha^2/4\}$.

(iv) We say (α,β) to be Type-IIb if either $X^2-\alpha X+\alpha^2-\beta$ is irreducible over $\mathbb{F}_q$ or $\beta\in\{\alpha^2,3\alpha^2/4\}$ but $\alpha\neq 0$.

We say (α,β) to be Type-IIc if $\alpha=\beta=0$.

Now We consider q even. If α to be Type-I($\alpha=0$),

(i) We say (α,β) to be Type-Ia if $\beta\neq 0$.

(ii) We say (α, β) to be Type-Ib if $\beta = 0$.

If α be of Type-II,

(iii) We say (α, β) to be Type-IIa if $X^2 - \alpha X + \alpha^2 - \beta \in \mathbb{F}_q[X]$ is reducubile and $\beta \neq \alpha^2$.

(iv) We say (α, β) to be Type-IIb if either $X^2 - \alpha X + \alpha^2 - \beta \in \mathbb{F}_q[X]$ is irreducible or if $\beta = \alpha^2$.

(Here one thing to note is that from Frobenious automorphism, $x \mapsto x^2$, of $\mathbb{F}_q$ there exist square root of every element of $\mathbb{F}_q$ inside $\mathbb{F}_q$ when $char(\mathbb{F}_q) = 2$.)

If $q \geq 32$ then, from Theorem 4.0.5, $[v] \notin \mathbb{S}_5$ except when $char(\mathbb{F}_q) \neq 3$ and $Q_{\alpha,\beta}$ is of Type-IIc.. □

Solution of the problems $P_{\alpha,\lambda}$ and $Q_{\alpha,\beta}$ is given below [4].

Theorem 4.0.4. *[4] The problem $P_{\alpha,\lambda}$, equation 4.3, has a solution for all $\alpha \in \mathbb{F}_q$ and $\lambda \in \mathbb{F}_q^{\times}$ when*

1. $q \geq 9$ if $char(\mathbb{F}_q) = 3$ and $\alpha = 0$.

2. $q \geq 27$ if $char(\mathbb{F}_q) = 3$ and $\alpha \neq 0$.

3. $q \geq 8$ if $char(\mathbb{F}_q) = 2$, and either $\alpha = 0$ or $\alpha \neq 0, \lambda = -(\alpha/3)^3$.

4. $q \geq 16$ if $char(\mathbb{F}_q) = 2$, and either $\alpha \neq 0$ and $\lambda \neq -(\alpha/3)^3$.

5. $q \geq 7$ if $char(\mathbb{F}_q) \neq 2, 3$, $\alpha \neq 0$ $\lambda = -(\alpha/3)^3$.

6. $q \geq 23$ if $char(\mathbb{F}_q) \neq 2, 3$, and either $\alpha = 0$ or $\alpha \neq 0, \lambda \neq -(\alpha/3)^3$.

Theorem 4.0.5. *[4] Suppose $q > 5$. The problem $Q_{\alpha,\beta}$, equation 4.4, has a solution when*

1. $q \geq 8$ if $char(\mathbb{F}_q) = 2$ and (α, β) of Type-Tb.

2. $q \geq 7$ if q odd, $char(\mathbb{F}_q) \neq 3$ and (α, β) is of Type-IIc

3. $Q_{\alpha,\beta}$ has no solution if $char(\mathbb{F}_q) = 3$ and (α, β) is of Type-IIc

4. $q \geq 16$ if $char(\mathbb{F}_q) = 2$, (α, β) of Type-Ia and Type-IIb

5. $q \geq 32$ if $char(\mathbb{F}_q) \neq 2$, (α, β) of Type-IIa

6. $q \geq 29$ if q is odd and (α, β) of Type-Ia and Type-IIa

7. $q \geq 23$ if q is odd and (α, β) of Type-Ib and Type-IIb

Bibliography

[1] Noga Alon. Combinatorial nullstellensatz. *Comb. Probab. Comput.*, 8(1-2):7–29, January 1999.

[2] Peter Beelen, David G. Glynn, Tom Høholdt, and Krishna V. Kaipa. Counting generalized reed-solomon codes. *Adv. in Math. of Comm.*, 11(4):777–790, 2017.

[3] Krishna Kaipa. Deep holes and MDS extensions of reed-solomon codes. *IEEE Trans. Information Theory*, 63(8):4940–4948, 2017.

[4] Krishna Kaipa, Jun Zhang, and Daqing Wan. (preprint) Deep holes of projective Reed-Solomon codes of dimension $q-4$. 2019.

[5] Krishna V. Kaipa. (preprint) The MDS conjecture, completeness of rational normal curves and the polynomial method. 2018.

[6] Beniamino Segre. Ovals in a finite projective plane. *Canad. J. Math.*, 7:414–416, 1955.

[7] Gadiel Seroussi and Ron M. Roth. On MDS extensions of generalized Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 32(3):349–354, 1986.

[8] Joseph A. Thas. M.D.S. codes and arcs in projective spaces: a survey. *Matematiche (Catania)*, 47(2):315–328 (1993), 1992. Combinatorics 92 (Catania, 1992).

[9] Jun Zhang, Daqing Wan, and Krishna Kaipa. Deep holes of projective reed-solomon codes. *CoRR*, abs/1901.05445, 2019.

Appendix A

: Use of Lemma 4.0.2

Statement of the Lemma 4.0.2 is given below. Here we will see how this lemma is used to determine which of H-orbits of Lemma 4.0.1 are in $\mathbb{S}_5$.

Lemma A.0.1. *Let $v = (v_0, v_1, v_2, v_3, v_4) \in \mathbb{F}_q^5$. Let $v' = (v_0, \cdots, v_3)$ and $v'' = (v_1, \cdots, v_4)$. Then, $[v] \in \mathbb{S}_5$ if and only if following 3 conditions holds,*

(1) Either A) $v' \in \mathbb{S}_4$, or B) $v' = \lambda c_4(x) + c_4(\infty)$, where $\lambda, x \in \mathbb{F}_q$.

(2) Either A) $v'' \in \mathbb{S}_4$, or B) $v'' = \lambda c_4(x) + c_4(0)$, where $\lambda \in \mathbb{F}_q$, $x \in \{\mathbb{F}_q^\times \cup \infty\}$

(3) $v = ac_5(x) + bc_5(y) + cc_5(z)$ has no solution for $a, b, c \in \mathbb{F}_q$ and distinct $x, y, z \in \mathbb{F}_q^\times$.

If v' or v'' are in $\mathbb{S}_4$ then it is in one of the following forms,

(A1) $(3b^2a, b^2c + 2abd, d^2a + 2bcd, 3d^2c)$ and when $char(\mathbb{F}_q) = 3$ also $(b^3, b^2d + b^2c + 2abd, bd^2 + d^2a + 2bcd, d^3)$, for some $h(t) = (c + dt)/(a + bx)$ in $PGL_2(\mathbb{F}_q)$.

(A2) $(a + a^q, ax + a^q x^q, ax^2 + a^q x^{2q}, ax^3 + a^q x^{3q})$ for $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $a \in \mathbb{F}_{q^2}^\times$.

A.1 Case $A1$

Consider $v = (\epsilon^{-1}, 0, 1, \alpha, \beta)$.
Let's see when codition (1) holds for $v' = (\epsilon^{-1}, 0, 1, \alpha)$.
The **case A1)** holds for v', when v' is of the form $(3b^2a, b^2c + 2abd, d^2a + 2bcd, 3d^2c)$ with $ad - bc \neq 0$. So,

$$(\epsilon^{-1}, 0, 1, \alpha) = \lambda(3b^2a, b^2c + 2abd, d^2a + 2bcd, 3d^2c), \text{ for some } \lambda \in \mathbb{F}_q^\times. \tag{A.1}$$

From the first and Second coordinate of v' in equation A.1, we get

$$\epsilon \neq 0 \text{ implies } b \neq 0 \text{ and } \; b(bc + 2ad) = 0 \text{ then } bc = -2ad. \qquad (1)$$

From the first and third coordinate of v' in equation A.1, we get

$$\begin{aligned} & \frac{3b^2a}{d^2a + 2bcd} = \epsilon^{-1} \\ \Leftrightarrow \quad & \frac{3b^2a}{-3ad^2} = \epsilon^{-1} \quad \text{(from (1))} \\ \Leftrightarrow \quad & \frac{b^2}{d^2} = -\epsilon^{-1}. \qquad (2) \end{aligned}$$

From the first and fourth coordinate of v' in equation A.1, we get

$$\begin{aligned} & \frac{b^2a}{d^2c} = \frac{\epsilon^{-1}}{\alpha} \\ \Leftrightarrow \quad & \frac{b^2}{d^2} \times \frac{-b}{2d} = \frac{\epsilon^{-1}}{\alpha} \quad \text{(from (1))} \\ \Leftrightarrow \quad & \frac{b^6}{d^6} = \frac{4\epsilon^{-2}}{\alpha^2}. \qquad (3) \end{aligned}$$

From (2) and (3),

$$\begin{aligned} & -\epsilon^{-3} = \frac{4\epsilon^{-2}}{\alpha^2} \\ \Leftrightarrow \quad & \alpha^2 = -4\epsilon \\ \Leftrightarrow \quad & \alpha = 2\sqrt{-\epsilon}. \end{aligned}$$

A.2 Case $A2$

Consider $v = (\epsilon^{-1}, 0, 1, \alpha, \beta)$.
Let's see when codition (1) holds for $v' = (\epsilon^{-1}, 0, 1, \alpha)$.
The **case A2)** holds for v', when v' is of the form $(a+a^q, ax+a^qx^q, ax^2+a^qx^{2q}, ax^3+a^qx^{3q})$ for $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $a \in \mathbb{F}_{q^2}^{\times}$. So,

$$(\epsilon^{-1}, 0, 1, \alpha) = \lambda(a+a^q, ax+a^qx^q, ax^2+a^qx^{2q}, ax^3+a^qx^{3q}), \text{ for some } \lambda \in \mathbb{F}_q^{\times}. \qquad \text{(A.2)}$$

First coordinate of v' in equation A.2, we get

$$a^q = (\epsilon\lambda)^{-1} - a. \qquad (1)$$

Second coordinate of v' implies,

$$\begin{aligned} & ax + a^qx^q = 0 \\ \Leftrightarrow\ & ax + ((\epsilon\lambda)^{-1} - a)x^q = 0 \text{ (from (1))} \\ \Leftrightarrow\ & a = \frac{-(\epsilon\lambda)^{-1}x^q}{x - x^q}. \qquad (2) \end{aligned}$$

Third coordinate of v' implies,

$$\begin{aligned} & ax^2 + a^qx^{2q} = \lambda^{-1} \\ \Leftrightarrow\ & ax^2 + ((\epsilon\lambda)^{-1} - a)x^{2q} = \lambda^{-1} \qquad \text{(from (1))} \\ \Leftrightarrow\ & \frac{-(\epsilon\lambda)^{-1}x^q}{x - x^q} \times (x^2 - x^{2q}) = \lambda^{-1} - (\epsilon\lambda)^{-1}x^{2q} \qquad \text{(from (2))} \\ \Leftrightarrow\ & (\epsilon\lambda)^{-1}x^q(x + x^q) = -\lambda^{-1} + (\epsilon\lambda)^{-1}x^{2q} \\ \Leftrightarrow\ & (\epsilon\lambda)^{-1}x^{q+1} = -\lambda^{-1} \\ \Leftrightarrow\ & x^q = \frac{-\epsilon}{x}. \qquad (3) \end{aligned}$$

Fourth coordinate of v' implies,

$$\begin{aligned}
& ax^3 + a^q x^{3q} = \lambda^{-1}\alpha \\
\Leftrightarrow\quad & ax^3 + ((\epsilon\lambda)^{-1} - a)x^{3q} = \lambda^{-1}\alpha (\text{from (1)}) \\
\Leftrightarrow\quad & a(x^3 - x^{3q}) = \lambda^{-1}\alpha - (\epsilon\lambda)^{-1}x^{3q} \\
\Leftrightarrow\quad & \frac{-(\epsilon\lambda)^{-1}x^q}{x - x^q}(x^3 - x^{3q}) = \lambda^{-1}\alpha - (\epsilon\lambda)^{-1}x^{3q} (\text{from(2)}) \\
\Leftrightarrow\quad & -(\epsilon\lambda)^{-1}x^q(x^2 + x^{2q} + x^{q+1}) = \lambda^{-1}\alpha - (\epsilon\lambda)^{-1}x^{3q} \\
\Leftrightarrow\quad & -\epsilon^{-1}x^{q+2} - \epsilon^{-1}x^{2q+1} = \alpha \\
\Leftrightarrow\quad & x^2(\frac{-\epsilon}{x}) + x(\frac{-\epsilon}{x})^2 = -\epsilon\alpha \text{ (from (3))} \\
\Leftrightarrow\quad & -\epsilon x^2 + \epsilon^2 = -\epsilon\alpha x \\
\Leftrightarrow\quad & x^2 - \alpha x - \epsilon = 0.
\end{aligned}$$

Since $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, polynomial $x^2 - \alpha x - \epsilon = 0$ is irreducible over $\mathbb{F}_q$.
Similarly we check, when condition (2) of Lemma 4.0.2 holds for v''.

A.3 Condition (3)

To check when **condition (3)** of Lemma 4.0.2 hold for v, we do the following:
let $v = ac_5(x) + bc_5(y) + cc_5(z)$ has a solution for $a, b, c \in \mathbb{F}_q$ and distinct $x, y, z \in \mathbb{F}_q^{\times}$. Let's take $v = (v_0, v_1, v_2, v_3, v_4)$. We consider first 3 coordinates of v to get values of a, b and c. Let $V(x, y, z) = (z - y)(z - x)(y - x)$. Then $(v_0, v_1, v_2) = ac_3(x) + bc_3(y) + cc_3(z)$ implies

$$a = \frac{det\begin{pmatrix} v_0 & 1 & 1 \\ v_1 & y & z \\ v_2 & y^2 & z^2 \end{pmatrix}}{V(x,y,z)},\ b = \frac{det\begin{pmatrix} 1 & v_0 & 1 \\ x & v_1 & z \\ x^2 & v_2 & z^2 \end{pmatrix}}{V(x,y,z)} \text{ and } c = \frac{det\begin{pmatrix} 1 & 1 & v_0 \\ x & y & v_1 \\ x^2 & y^2 & v_2 \end{pmatrix}}{V(x,y,z)}. \qquad (*)$$

We use this value of a, b and c in the equation which we get from third and fourth coordinate of v.

$$\begin{pmatrix} v_3 \\ v_4 \end{pmatrix} = \begin{pmatrix} x^3 & y^3 & z^3 \\ x^4 & y^4 & z^4 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

.

Example 1. *Consider $v = (\epsilon^{-1}, 0, 1, \alpha, \beta)$.*

Suppose

$$v = (\epsilon^{-1}, 0, 1, \alpha, \beta) = ac_5(x) + bc_5(y) + cc_5(z) \text{ for } a, b, c \in \mathbb{F}_q^{\times}$$
$$\text{and distinct } x, y, z \in \mathbb{F}_q.$$

We take first 3 coordinates to find the value of a, b and c,

$$(\epsilon^{-1}, 0, 1) = ac_3(x) + bc_3(y) + cc_3(z).$$

Using (*), we get that

$$a = \frac{(\epsilon^{-1}yz + 1)(z - y)}{V(x, y, z)}, \; b = \frac{-(\epsilon^{-1}xz + 1)(z - x)}{V(x, y, z)} \text{ and } c = \frac{(\epsilon^{-1}xy + 1)(y - x)}{V(x, y, z)}. \qquad (1)$$

The third and fourth coordinates of v gives following two equations,

$$ax^3 + by^3 + cz^3 = \alpha \qquad (2)$$
$$ax^4 + by^4 + cz^4 = \beta. \qquad (3)$$

Multiplying equation (2) with x, we get,

$$\begin{aligned}
& ax^4 + bxy^3 + cxz^3 = \alpha x \\
\Leftrightarrow \quad & \beta - by^4 - cz^4 + bxy^3 + cxz^3 = \alpha x \qquad (from(3)) \\
\Leftrightarrow \quad & by^3(x - y) + cz^3(x - z) = \alpha x - \beta \\
\Leftrightarrow \quad & \frac{-(\epsilon^{-1}xz + 1)(z - x)(x - y)y^3}{V(x, y, z)} + \frac{(\epsilon^{-1}xy + 1)(y - x)(x - z)z^3}{V(x, y, z)} = \alpha x - \beta \; (from(1)) \\
\Leftrightarrow \quad & \frac{(\epsilon^{-1}xz + 1)y^3}{z - y} + \frac{-(\epsilon^{-1}xy + 1)z^3}{z - y} = \alpha x - \beta \\
\Leftrightarrow \quad & \epsilon^{-1}xyz(y^2 - z^2) + (y^3 - z^3) = (\alpha x - \beta)(z - y) \\
\Leftrightarrow \quad & \epsilon^{-1}xyz(y + z) + y^2 + z^2 + yz = -\alpha x + \beta. \qquad (4)
\end{aligned}$$

By similar process, multiplying equation (2) with y and z, we get following equations

$$\epsilon^{-1}xyz(x+z)+x^2+z^2+xz=-\alpha y+\beta \qquad (5)$$
$$\epsilon^{-1}xyz(x+y)+x^2+y^2+xy=-\alpha z+\beta. \qquad (6)$$

Subtract equation (4) from (5), we get,

$$\begin{aligned} & \epsilon^{-1}xyz(x-y)+(x^2-y^2)+z(x-y)=\alpha(x-y) \\ \Leftrightarrow \quad & \frac{xyz}{\epsilon}+x+y+z=\alpha. \qquad (7) \end{aligned}$$

Multiply (4) with y and (5) with x, then subtracting later from former equation, we get,

$$\begin{aligned} & \epsilon^{-1}xyz(y^2+yz-x^2-xz)+(y^3-x^3)+z^2(y-x)+z(y^2-x^2)=\beta(y-x) \\ \Leftrightarrow \quad & \epsilon^{-1}xyz(y+x+z)+y^2+x^2+xy+z^2+yz+xz=\beta \\ \Leftrightarrow \quad & \epsilon^{-1}xyz(y+x+z)+(x+y+z)^2-(xy+yz+xz)=\beta. \qquad (8) \end{aligned}$$

From (7) and (8),

$$\begin{aligned} & (\epsilon^{-1}xyz)^2+2\epsilon^{-1}xyz(x+y+z)-\epsilon^{-1}xyz(y+x+z)+(xy+yz+xz)=\alpha^2-\beta \\ \Leftrightarrow \quad & (\epsilon^{-1}xyz)^2+\epsilon^{-1}xyz(x+y+z)+(xy+yz+xz)=\alpha^2-\beta \\ \Leftrightarrow \quad & \epsilon+xy+yz+\epsilon^{-1}xy^2z+zx+\epsilon^{-1}x^2yz+\epsilon^{-1}xyz^2+(\epsilon^{-1}xyz)^2=\epsilon+\alpha^2-\beta \\ \Leftrightarrow \quad & (1+xy\epsilon^{-1})(\epsilon+yz+zx+\epsilon^{-1}xyz^2)=\epsilon+\alpha^2-\beta \\ \Leftrightarrow \quad & (1+xy\epsilon^{-1})(1+yz\epsilon^{-1})(\epsilon+zx)=\epsilon+\alpha^2-\beta \\ \Leftrightarrow \quad & \epsilon\left(1+\frac{xy}{\epsilon}\right)\left(1+\frac{yz}{\epsilon}\right)\left(1+\frac{zx}{\epsilon}\right)=\epsilon+\alpha^2-\beta. \qquad (9) \end{aligned}$$

So, we need to check that if following equations

$$x+y+z+xyz/\epsilon=\alpha,\ \ \epsilon(1+xy/\epsilon)(1+yz/\epsilon)(1+zx/\epsilon)=\epsilon+\alpha^2-\beta;$$
$$\textit{for distinct } x,y,z\in\mathbb{F}_q^\times$$

have a solution.