2014

WEAK ISOMETRIES OF HAMMING SPACES

Ryan Walter Bruner
Michigan Technological University

WEAK ISOMETRIES OF HAMMING SPACES

By

Ryan Bruner

A THESIS

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

In Mathematical Sciences

MICHIGAN TECHNOLOGICAL UNIVERSITY

2014

This thesis has been approved in partial fulfillment of the requirements for the Degree of MASTER OF SCIENCE in Mathematical Sciences.

Department of Mathematical Sciences

Thesis Advisor: *Dr. Stefaan DeWinter*

Committee Member: *Dr. Timothy Havens*

Committee Member: *Dr. Donald Kreher*

Department Chair: *Dr. Mark Gockenbach*

Dedicated *to my mother, Linda M. Miller, my father, Mark A. Miller, and to the memory of my granmother Kathryn L. Bruner*

Contents

List of Tables

Acknowledgments

My deep appreciation and gratitude to Dr. Stefaan De Winter for his support, guidance, and patience while working on this thesis and finishing my courses. He was always willing to give me time when I needed help with research or needed to talk about my fears and worries. I am grateful for all of my professors who taught me so much about math and life along my journey here at MTU.

I would also like to thank my committee: Professors Stefaan De Winter, Donald Kreher, and Timothy Havens. Thank you for the time you spent reading my thesis and giving me helpful corrections as well as suggestions of what was lacking.

I would like to thank Melissa Keranen for being my mentor when I was about to start teaching, and Ann Humes who taught me how to teach and what it means to be a teacher.

I would like to thank all of my fellow graduate students. My time at MTU would not have been the same with out you and your friendship and support.

Finally I would like to thank my parents, my family, and the rest of my friends who were always so encouraging, and my grandmother who threatened to drag me by the ear if I didn't apply for college after my time in the military.

Abstract

In this thesis we study weak isometries of Hamming spaces. These are permutations of a Hamming space that preserve some but not necessarily all distances. We wish to find conditions under which a weak isometry is in fact an isometry. This type of problem was first posed by Beckman and Quarles for $\mathbb{R}^n$. In chapter 2 we give definitions pertinent to our research. The 3rd chapter focuses on some known results in this area with special emphasis on papers by V. Krasin as well as S. De Winter and M. Korb who solved this problem for the Boolean cube, that is, the binary Hamming space. We attempted to generalize some of their methods to the non-boolean case. The 4th chapter has our new results and is split into two major contributions. Our first contribution shows if $n = p$ or $p < \frac{n}{2}$, then every weak isometry of H_q^n that preserves distance p is an isometry. Our second contribution gives a possible method to check if a weak isometry is an isometry using linear algebra and graph theory.

Chapter 1

Introduction

An isometry of a metric space is a bijection of the metric space that preserves distances between elements. A weak isometry is not surprisingly a weaker version of an isometry: it is a permutation of a metric space that preserves certain prescribed distances (but not necessarily all distances). The study of weak isometries originates from the paper *On Isometries of Euclidean Spaces* by Beckman and Quarles [1]. There the authors show in the real Euclidean space $\mathbb{R}^n$, $n > 1$ and finite, preserving a single distance results in an isometry. Subsequently other Beckman-Quarles like problems have been studied in both infinite and finite metric spaces.

We wish to prove discrete Beckman-Quarles like theorems for non-boolean Hamming spaces. Our problem focuses on when does having a single preserved distance imply that all distances must be preserved.

We initially tried to use methods that originated from the papers of V. Krasin [6], [7] and

S. De Winter and M. Korb [5], but discovered that new methods were needed as the old methods did not easily translate to the non-boolean case.

We provide two approaches. The first approach is combinatorial. The main idea is to find substructures that have to be preserved by a weak isometry and then to combine these substructures to prove that a weak isometry in fact must preserve distance 1, from which it then follows that the weak isometry in fact is an isometry. In order to do this we used the theory of Bose-Mesner algebras related to Hamming spaces.

Our second approach uses linear algebra. The main idea here is to prove that the so-called adjacency matrix of our Hamming space commutes with the permutation matrix of our weak isometry. This then implies that the weak isometry must be an isometry.

Before turning to our new results we first provide necessary definitions in the next chapter, and give a short overview of some known results in Chapter 3.

Chapter 2

Definitions

We will now define key terms to be used throughout the paper.

Definition: A *metric* on a set S is a non-negative function $d : S \times S \rightarrow \mathbb{R}^{+}$ (describing the distance between points of the given set) satisfying the following:

- triangle inequality $d(x,y) + d(y,z) \geq d(x,z)$ for all $x,y,z \in S$;
- d is symmetric, that is $d(x,y) = d(y,x)$ for all $x,y \in S$;
- $d(x,y) = 0$ if an only if $x = y$.

Example: An example of a metric is the *Euclidean distance* on $\mathbb{R}^n$. The Euclidean distance between two points $p = (p_1, p_2, \ldots, p_n)$ and $q = (q_1, q_2, \ldots, q_n)$ is defined as $d(p,q) = d(q,p) = \sqrt{\sum_{i=1}^{n} (q_i - p_i)^2}$.

Definition: A *metric space* (S,d) is a set S along with a metric d on S.

In this paper will the metric space we will focus on is the Hamming space equipped with the Hamming distance. We provide the definitions below.

Definition: The q-ary *Hamming cube or Hamming space* denoted H_q^n is the set of words $\mathbb{Z}_q^n$ of length n from an alphabet of size q.

When q is 2, this space is also called the *Boolean cube*.

Addition and subtraction can be defined in a natural way on H_q^n, namely component wise and modulo q.

Definition: The set of indices of the non-zero positions of a word w in H_q^n is called the *support* of w.

Definition: The size of the support of a word in H_q^n is called the *Hamming weight* of the word.

Definition: The *Hamming distance* between two words x and y in H_q^n is the number of positions in which x and y differ.

Claim: The n-dimensional Hamming space H_q^n equipped with Hamming distance is a metric space.

We only need to show the triangle inequality holds as symmetry and zero distance comes directly from the definition of Hamming distance.

Let $x, y, z \in H_q^n$.

Triangle inequality: Show $d(x,y) + d(y,z) \geq d(x,z)$ for all $x, y, z \in H_q^n$.

Let $d(x,y) = a$, and $d(y,z) = b$. So x and y differ in a set P_1 of a positions. Also y and z differ in a set of P_2 of b positions. So

$$d(x,z) \leq |P_1 \cup P_2| = |P_1| + |P_2| - |P_1 \cap P_2| \leq a + b.$$

Definition: An *isometry* is a bijective map f between two metric spaces (S,d) and (S',d') that preserves distances. So $d(x,y) = d'(f(x), f(y))$ for all $x,y \in S$.

Definition: If $(S,d) = (S',d')$ then the isometry is called an isometry of (S,d).

Definition: Let (S,d) be a metric space. Let $D \subseteq \mathbb{R}^+$ be the image of d (all possible distances). A *weak-isometry* or *P-isometry* of (S,d) is a permutation f of S such that there is a $P \subseteq D$, $P \neq \emptyset$ with the property that $d(x,y) = d(f(x), f(y))$ if $d(x,y) \in P$. Note that if $P = D$, then this is exactly the definition of an isometry.

Definition: A *p-weak isometry* or simply a *p-isometry* is an weak isometry that only preserves distance p, where p is a single non-negative value.

We will now introduce some specific non-standard terminology that will turn out to be useful in our proofs in Chapter 4.

Definition: In H_q^n the *layer of weight k* denoted L_k is the subset of H_q^n of all words of weight k.

Definition: In H_q^n the *cloud of weights a through b* denoted $C(a,b)$ is the subset of H_q^n of all words whose weight is at least a and at most b. The *cloud of weight at least a* denoted $C(a)$ is the subset of H_q^n of all words whose weight is at least a.

For our linear algebraic approach we will need to provide a short discussion of the graphs and matrix algebras that are associated to each H_q^n. This is done below.

Definition: A (finite) *graph* $G = (V, E)$ is a finite set V the elements of which are called *vertices* together with a set E of unordered pairs of vertices $\{x, y\}$ called *edges* where $x \neq y \in V$. If $\{x, y\}$ is an edge we say that x and y are adjacent.

Definition: The *adjacency matrix* A of a graph G is the square matrix whose columns and rows are labeled by the vertices of G and is such that A_{ij} equals 1 if vertex i is adjacent to vertex j, and zero otherwise.

Definition: A *path* in a graph is a sequence of edges $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_k - 1, v_k\}$ adjoining a sequence of vertices $\{v_1, \ldots, v_k\}$. A path that starts at a vertex a and ends at a vertex b is called a *path between vertices a, b*.

Definition: The *length* of a path is the number of edges in the path.

Definition: The *distance* between two vertices is the length of the shortest path between them.

Definition: The *diameter* of a connected graph is the maximal distance between two vertices in the graph.

Definition: We say a graph is *connected* if there is a path between vertices $a, b \in V$ for all $a, b \in V$.

Definition: The *valency* of a vertex is the number of vertices adjacent to it.

Definition: A vertex is said to be a *neighbor* of another vertex if the vertices are adjacent.

Definition: A graph is called *regular* when every vertex of the graph has the same valency.

Given a Hamming space H_q^n a graph $\Gamma(H)$ can be constructed as follows: the vertices of $\Gamma(H)$ are the words of H_q^n, and two vertices are adjacent if the corresponding words are at distance 1. It turns out this graph has many nice properties.

Definition: A *distance regular graph of diameter* d is a regular graph of valency k and diameter d for which there exist integers b_i and c_i, $i = 0, 1, \dots, d$, such that for any two vertices v_1 and v_2 at distance i from each other there are exactly b_i neighbors of v_2 at distance $i+1$ from v_1, and there exactly c_i neighbors of v_2 at distance $i-1$ from v_1. The sequence

$$(b_0, b_1, \dots, b_{d-1}; c_1, c_2, \dots, c_d)$$

is called the *intersection array* of the graph. It is obvious that $b_0 = k$, $b_d = 0$, $c_0 = 0$ and $c_1 = 1$. Finally, one typically defines $a_i = k - b_i - c_i$. Hence, with the above notation a_i is the number of neighbors of v_2 at distance i from v_1.

Given a distance regular graph G with diameter d a square $(d+1) \times (d+1)$ tridiagonal matrix can be built

$$B := \begin{pmatrix} a_0 & b_0 & 0 & \dots & 0 & 0 \\ c_1 & a_1 & b_1 & \dots & 0 & 0 \\ 0 & c_2 & a_2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_{d-1} & b_{d-1} \\ 0 & 0 & 0 & \dots & c_d & a_d \end{pmatrix}$$

called the *intersection matrix*. It is easy to see that $a_0 = c_0 = b_d = 0$, and $a_i + b_i + c_i = k$ thus $b_0 = k$, where k is the valency of our distance regular graph. The intersection matrix is useful when dealing with distance regular graphs as the $d+1$ distinct eigenvalues of B are also eigenvalues of the adjacency matrix A of the graph G [4].

Example: The graph $\Gamma(H)$ is an example of a distance regular graph. It has intersection matrix

$$B = \begin{pmatrix} 0 & n(q\text{-}1) & 0 & \cdots & 0 & 0 \\ 1 & \ddots & \ddots & \ddots & & \vdots \\ 0 & \ddots & & (n\text{-}i)(q\text{-}1) & 0 & 0 \\ \vdots & \ddots & i & i(q\text{-}2) & \ddots & 0 \\ 0 & & 0 & \ddots & \ddots & (q\text{-}1) \\ 0 & \cdots & 0 & 0 & \text{n} & n(q\text{-}2) \end{pmatrix}.$$

Given a distance regular graph G of diameter d, $d-1$ related graphs $G_2, G_3, \ldots, G_d$ can be constructed as follows: the graph G_i has the same vertices as G, and two vertices are adjacent if and only if they are at distance i in G. Now let $A_0 = I$, let $A_1 = A$ be the adjacency matrix of G, and let A_i be the adjacency matrix of G_i, $i = 2, 3, \ldots, d$. These matrices satisfy the following properties [4]:

(i) $\sum_{i=0}^{d} A_i = J$;

(ii) $A_i = A_i^T$;

(iii) $A_i A_j = \sum_{k=0}^{d} p_{ij}^{k} A_k$;

for certain numbers p_{ij}^{k}.

It can be shown (see [4]) that these matrices generate a $(d+1)$-dimensional commutative algebra of symmetric matrices.

Definition: The $Bose-Mesner\ algebra\ \mathscr{A}$ of a distance regular graph is the matrix algebra $\mathscr{A}$ generated by the matrices $A_0, A_1, \ldots, A_d$. This algebra first appears in [3].

Chapter 3

Known Results

3.1 Beckman and Quarles' result

In this section we describe the result and proof technique from the original Beckman and Quarles paper *On Isometries of Euclidean Spaces* [1], as this provides the starting point for looking at weak isometries. The main result in their paper is that any transformation of Euclidean n-space $\mathbb{R}^n$, with $2 \leq n < \infty$, which preserves a single nonzero distance must be a Euclidean motion (isometry) of $\mathbb{R}^n$ onto $\mathbb{R}^n$. Hence, every p-isometry of $\mathbb{R}^n$ is an isometry. From our perspective the important thing to be taken away from their paper is the idea of looking for preserved substructures.

After normalization one can assume in $\mathbb{R}^n_q$ that a given p-isometry is in fact a 1-isometry. In [1] the authors start by showing that every 1-isometry of $\mathbb{R}^n_q$ must map equilateral triangles to equilateral triangles.

Next they show that a rhombus is preserved as a structure. Using the equilateral triangles to build a rhombus with distance $3^{1/2}$ between two opposite points, it follows that distance $3^{1/2}$ is preserved.

Gaining momentum the next structure in [1] that is considered is a regular hexagon with unit sides. This along with what we know about the rhombi and distance $3^{1/2}$ being preserved allows the preservation of distance 2 by constructing a hexagon with rhombi. Once distance two has been preserved it is possible to prove that all integral distances are preserved.

Moving to more complex structures the next thing Beckman and Quarles show is that a unit circle and its center will be transformed into a unit circle and its center. Using this result they then shown that a plane is transformed into a plane. This finally allows them to prove that all distances are preserved. We finish up our discussion of the Beckman and Quarles' paper with their main theorem which states:

Theorem 1 (Beckman And Quarles, [1]) *Let T be a transformation (possibly many-valued) of* $\mathbb{R}^n$ $(2 \leq n < \infty)$ *into itself. Let* $d(p,q)$ *be the distance between points* p *and* q *of* $\mathbb{R}^n$*, and let* Tp*,* Tq *be any images of* p *and* q*, respectively. If there is a length* $a > 0$ *such that* $d(Tp,Tq) = a$ *whenever* $d(p,q) = a$*, then* T *is a Euclidean transformation of* $\mathbb{R}^n$ *onto itself.*

3.2 The result of Krasin for the Boolean cube

It is now natural to try to generalize Theorem 1 to other metric spaces, and to provide explicit examples of weak isometries. However all of our attempts failed. We will focus on Hamming spaces equipped with the Hamming distance. This study was initiated by Krasin in [6, 7] in the case of the Boolean cube and completed (for the Boolean cube) by De Winter and Korb in [5]. Before turning our attention to the non-boolean case in the next chapter we will review the known results for the Boolean cube.

The key idea in [6, 7] is to study the words of weight p at distance p from a given word of weight $2k$. Now the number of words at distance p and of weight p from an arbitrary word v of weight $2k$ is denoted by A_{2k}^{p} (this is called the p-power of v and only depends on the weight of v). Once these p-powers have been computed Krasin proceeds to show via counting arguments which p-isometries are necessarily isometries. We describe his method in some more detail as we tried to generalize it for non-boolean Hamming spaces.

Krasin computes A_{2k}^{p} as $\binom{k}{2k}\binom{p-k}{n-2k}$ if $k \leq min\{p, n-p\}$, and zero otherwise. This is then used to show that when p is odd and $p \notin \{\frac{n-1}{2}, \frac{n+1}{2}, \frac{n}{2}, n\}$ we have $A_2^p = A_{2k}^p$ if and only if $k = 1$. This in turn implies that every p-isometry of H_2^n with p odd and $p \notin \{\frac{n-1}{2}, \frac{n+1}{2}, \frac{n}{2}, n\}$ preserves distance 2. Combining the fact that distance 2 is preserved with the fact that distance p which is odd is preserved we can conclude that every p-isometry with p odd and $p \notin \{\frac{n-1}{2}, \frac{n+1}{2}, \frac{n}{2}, n\}$ is also necessarily a 1-isometry and hence an isometry (see Lemma 2 below).

3.3 The weak-isometries of the Boolean cube

Krasin provided some examples of weak isometries that are not isometries for $p \in \{\frac{n-1}{2}, \frac{n+1}{2}, \frac{n}{2}, n\}$ or p even. In [5] De Winter and Korb provided a complete classification of all weak isometries of H_2^n. We will briefly describe their results below.

The first lemma in [5] shows that a 1-isometry of H_2^n is an isometry. We will now prove this is true for any q-nary Hamming space.

Lemma 2 *Let ϕ be a 1-isometry of a q-ary Hamming space, Then ϕ is an isometry.*

Proof. If ϕ is a 1-isometry, then ϕ is equivalent with a permutation of the vertices of the graph $\Gamma(H)$ which maps edges to edges, and hence preserves the distance between any two vertices. Consequently ϕ preserves all distances and hence is an isometry of H_q^n. ■

In the second lemma of [5] we see a proof showing for $n > 4$ every 2-isometry preserves all even distances. The proof is similar to that of Lemma 1 and relies on the fact that in the binary case the graph $\Gamma_2(H)$ is not connected.

The remainder of [5] focuses on classifying all remaining P-isometries where P is a subset of $\{\frac{n-1}{2}, \frac{n}{2}, \frac{n+1}{2}, n\} \bigcup \varepsilon$, where ε is the set of non-zero even integers smaller then n. The main result is that every P-isometry of H_2^n that is not an isometry is one of the following weak isometry types:

- n-isometries;

- even-isometries;
- $\{\frac{n}{2},n\}$-isometries;
- $\frac{n+1}{2}$-isometries;
- $\{\frac{n-1}{2},\frac{n+1}{2},n\}$-isometries.

For each of the cases a complete description of these P-isometries is obtained.

A somewhat remarkable consequence is that there are no $\frac{n-1}{2}$-isometries that are not a P-isometry where $\{\frac{n-1}{2}\} \subsetneq P$.

The class of n-isometries is an obvious result with ϕ being a permutation of the pairs $\{\overline{c},\overline{1}+\overline{c}\}$ This comes from there being only one word at distance n from a word $\overline{c}$, namely $\overline{1}+\overline{c}$.

The class of even isometries is covered by analyzing the action of a 2-isometry on the connected components of the graph $\Gamma_2(H)$. This is fairly easy and analogues to the classification of isometries of H_2^n.

From the third lemma in [5] which states every $\{p,n\}$-isometry is a $\{p,n-p,n\}$-isometry we know that every $\{\frac{n}{2}\}$-isometry is actually a $\{\frac{n}{2},n\}$-isometry. Thus we know from the class of n-isometries that ϕ permutes the pairs $\{\overline{c},\overline{1}+\overline{c}\}$. From this the authors show that ϕ induces a nice action on the words of weight less than $\frac{n}{2}$, and the words of weight $\frac{n}{2}$ with a zero in the first position. By studying this induced action De Winter and Krasin obtain a complete classification of $\{\frac{n}{2},n\}$-isometries. It turns out that the cases $n=4k+2$ and $n=4k$ are slightly different.

The class of $\frac{n+1}{2}$-isometries is handled by embedding H_q^n into H_{q+1}^n and then showing that every $\frac{n+1}{2}$-isometry of H_q^n induces a specific $\{\frac{n+1}{2}, n+1\}$-isometry of H_q^{n+1}. Using the classification of $\{\frac{n}{2}, n\}$-isometries then yields the classification of $\frac{n+1}{2}$-isometries.

The last class is of $\{\frac{n-1}{2}, \frac{n+1}{2}, n\}$-isometries and is classified by finding which of the $\frac{n+1}{2}$-isometries isometries are also n-isometries. Which then provides the complete classification of weak isometries of the Boolean cube. We do not mention here explicitly what all these mappings look like as some of these are rather long and complicated expressions (which we will not need in the rest of this paper).

The papers [6],[7], and [5] are not the only publications on discrete versions of the Beckman-Quarles theorem. Beckman-Quarles type theorems and finite subsets of $\mathbb{R}^2$ have been studied in [8], Beckman-Quarles type theorems for finite geometries have been the topic of [2],...

Chapter 4

New Results

4.1 Trying to generalize Krasin's method

In this chapter we discuss generalizations of the result of Krasin [6, 7] for Hamming spaces over larger alphabets. A first natural approach is to try a direct generalization of Krasin's methods. The idea behind this approach is to show that given a word of weight w, the number of words of weight p at distance p from this word is distinct for different values of w. This implies that every p-isometry that fixes the zero word must map words of weight 1 to words of weight 1. This can be used to prove that every p-isometry is in fact an isometry. We show in 3 the case $q = 3$ and $n < 2p$ why such an approach fails. Considering higher values of q and including the case $n \geq 2p$ only makes things worse.

Lemma 3 *Let H_q^n be the n-dimensional q-ary hamming space. When $n < 2p$ and $q = 3$, the number of words of weight p at distance p from a fixed word of weight x is*

$$\sum_{a_0=max\{0,x-p\}}^{min\{\lfloor \frac{x}{2} \rfloor,n-p\}} \binom{x-a_0}{a_0}\binom{x}{a_0}\binom{n-x}{p-x+a_o}2^{p-x+a_0}.$$

Proof. Let $\{0,1,2\}$ be the alphabet of $q = 3$ symbols. Consider an arbitrary fixed word w of weight x. Without loss of generality we can choose w to have a 1 in the first x positions and 0 in the remaining $n-x$ positions. Now let z be an arbitrary word of weight p and at distance p from w. Let a_0 be the number of zeros in z where w has a one in the same position, similarly let a_1 and a_2 be the number of ones or twos in z where w has a one in the same position. Lastly let a_* be the number of nonzero positions in z where w has a zero in the same position. Then our two words look as follows.

$$\begin{array}{lll} w: & \overbrace{1\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots 1}^{x} & 0\cdots\cdots\cdots\cdots\cdots 0 \\ z: & \underbrace{0\cdots\cdots 0}_{a_0}\ \underbrace{1\cdots\cdots 1}_{a_1}\ \underbrace{2\cdots\cdots 2}_{a_2} & \underbrace{*\cdots\cdots *}_{a_*}\ 0\cdots\cdots 0 \end{array}$$

From this we derive:

$$a_1 + a_2 + a_* = p \tag{4.1}$$

$$a_1 + a_2 + a_0 = x \tag{4.2}$$

$$a_2 + a_0 + a_* = p \tag{4.3}$$

From (4.1) and (4.2) we see that $a_o = a_1$. By replacing a_1 with a_0 equations (4.1) and (4.3) become equivalent. Also equation (4.2) becomes $2a_0 + a_2 = x$. If we subtract our new equation from equation (4.3) we see that $a_* - a_0 = p - x$. It follows that a_* is larger then a_0 if and only if the weight x of w is greater then p. When this happens $p - x + a_0 \geq 0$ or $a_0 \geq x - p$.

So for a fixed a_0 and x we have that a_1, a_2 and a_* are determined. Thus given x possible positions of z that contribute to a_0 we have $\binom{x}{a_0}$ choices. Then we have $\binom{x-a_0}{a_0}$ choices for possible positions contributing to a_1, because $a_1 = a_0$. Now we see that positions contributing to a_2 are given once we choose the a_0 and a_1 positions. Also we have $\binom{n-x}{a_*}2^{a_*}$ choices for positions and value of the nonzero position contributing to a_* (recall our alphabet has size 3). However we know that $a_* = p - x + a_0$ so by substitution this becomes $\binom{n-x}{p-x+a_0}2^{p-x+a_0}$. So for a fixed a_0 the number of words of weight p at distance p to our word w is $\binom{x-a_0}{a_0}\binom{x}{a_0}\binom{n-x}{p-x+a_o}2^{p-x+a_0}$. Now by summing over all possible a_0 we will get the total number of words of weight p at distance p from our word w. So then we just need to figure out what values our a_o can take and sum over them. We know $2a_0 \leq x$ from (2) above thus our a_0 can take integer values from 0 to $\lfloor \frac{x}{2} \rfloor$. However we have to be careful here, because we also know that $a_0 \leq n-p$ from the fact that $n-p$ is the number of all positions in our word z with the value 0. Also we know if $x > p$ then $a_0 = x - p + a_*$. This shows a_0 starts at $\max\{0, x-p\}$. So we get that $max\{0, x-p\} \leq a_0 \leq min\{\lfloor \frac{x}{2} \rfloor, n-p\}$. So we get as desired that the number of words of weight p at distance p from a fixed word of weight x is $\sum_{a_0=max\{0,x-p\}}^{min\{\lfloor \frac{x}{2} \rfloor, n-p\}} \binom{x-a_0}{a_0}\binom{x}{a_0}\binom{n-x}{p-x+a_o}2^{p-x+a_0}$. ■

Corollary 4 *When $n < 2p$ and $q = 3$ the number of words of weight p at distance p from a fixed word of weight one is $\binom{n-1}{p-1}2^{p-1}$.*

Proof. Using Lemma 3 we get that (using $x = 1$)

$$\sum_{a_0=0}^{min\{\lfloor \frac{x}{2} \rfloor, n-p\}} \binom{x-a_0}{a_0}\binom{x}{a_0}\binom{n-x}{p-x+a_o}2^{p-x+a_0}$$

$$= \binom{1}{0}\binom{1}{0}\binom{n-1}{p-1+0}2^{p-1+0} = \binom{n-1}{p-1}2^{p-1}. \blacksquare$$

As a next step one would want to show that $\sum_{a_0=max\{0,x-p\}}^{min\{\lfloor \frac{x}{2} \rfloor, n-p\}} \binom{x-a_0}{a_0}\binom{x}{a_0}\binom{n-x}{p-x+a_o}2^{p-x+a_0}$ can only equal $\binom{n-1}{p-1}2^{p-1}$ when $x = 1$ (as this would prove that a p-isometry has to map words of weight 1 to words of weight 1). However, analyzing this sum of products of binomials proved to be very difficult. Furthermore, even if one would succeed for this specific case, things would only get more complicated over larger alphabets. This is the reason why we looked for different approaches to our problem.

4.2 Combinatorial approach

We obtained a complete solution in the cases, $n > 2p$ and $n = p$. And we developed a method for studying the cases $n \leq 2p$. We start by discussing the cases $n > 2p$.

Lemma 5 *Let φ be a p-isometry of H_q^n fixing 0 and let $2p < n$. Then the layers of weight $kp \leq n$ are preserved as a set, and the clouds $C((k-1)p+1,\ kp-1)$, $kp \leq n$ are also preserved set-wise.*

Proof. We start by noticing only words of weight p have distance p from 0. Let w be in L_p. Then

$$p = d(\varphi(0), \varphi(w)) = d(0, \varphi(w)).$$

Thus $wt(\varphi(w)) = p$. This tells us then that $\varphi(w)$ is in L_p. So we can see that L_p is preserved as a set under φ. Then $C(1,\ p-1) \cup C(p+1,\ 2p-1) \cup L_{2p}$ are the only remaining words of our Hamming space that are at distance p from some word in L_p. So $C(1,\ p-1) \cup C(p+1,\ 2p-1) \cup L_{2p}$ is preserved as a set under φ. Let $C(2p+1,\ n)$ be all words of weight greater than $2p$. We know $C(2p+1,\ n)$ is not empty since $n > 2p$. We also know $C(2p+1,\ n)$ must be preserved as a set under φ as the complement of $C(2p+1,\ n)$ is preserved.

Because words in $C(p+1,\, 2p-1)$ and L_{2p} are at distance p from some words in $C(2p+1,$ $n)$ while words in $C(1,\, p-1)$ are not, we see that $C(1, p-1)$ is preserved set-wise as well as $C(p+1, 2p-1) \cup L_{2p}$. Next notice that words in L_{2p} can never be at distance p from words in $C(1,\ p-1)$ while every word in $C(p+1,\ 2p-1)$ is. Therefore both $C(p+1,$ $2p-1)$ and L_{2p} are preserved as sets.

Now we wish to show that L_{kp} and $C((k-1)p+1,\ kp-1)$ are preserved set-wise when $kp \leq n$. So let us assume that $kp \leq n$ and that $L_{(k-1)p}$ and $C((k-2)p+1,\ (k-1)p-1)$ are preserved set-wise. Then immediately we see words in $C((k-2)p+1,\ (k-1)p-1)$ are at distance p from words in in $C((k-1)p+1,\ kp-1)$ but not from words in L_{pk} or $C(kp+1, n)$, so $C((k-1)p+1, kp-1)$ is preserved set-wise by φ. Now words in $L_{(k-1)p}$ are at distance p from words in L_{pk} but not from words in $C(kp+1, n)$. Hence φ must map words from L_{kp} to words in L_{kp}. This tells us L_{kp} is preserved set-wise. So by induction we have shown that the layers of weight kp are preserved as a set, as well as the clouds $C((k-1)p+1, kp-1)$. ■

Lemma 6 *Let $2p < n$. Two words of weight p are disjoint if and only if there exists a unique word of weight $2p$ at distance p from both words.*

Proof. We start by showing the forward implication. Suppose α and β are disjoint words of weight p. Let $\gamma = \alpha + \beta$. Now, because α and β are disjoint we have that $wt(\gamma) = wt(\alpha) + wt(\beta) = 2p$. Also notice that $d(\gamma, \alpha) = d(\gamma, \beta) = p$. So γ is a word of weight $2p$ at distance p from α and β. Now let δ also be a word of weight $2p$ at distance p

from α and β. Then δ shares p common non-zero positions with α and similarly with β. However, both α and β only have p non-zero positions. Thus $\delta = \alpha + \beta = \gamma$. So γ is the unique word of weight $2p$ at distance p from both α and β.

Now we will show the second part of our bi-conditional statement. Suppose there exists a unique word γ of weight $2p$ at distance p from two given words α, β of weight p at distance p from γ. Then γ must share p non-zero positions with α. Now to maintain uniqueness the additional p non-zero positions from β must not share any positions with α's non-zero positions. Then we know from this that the intersection of the supports of α and β is the empty set. Thus α and β are disjoint. ■

Corollary 7 *Let φ be a p-isometry fixing 0 and let $2p < n$. Then φ maps disjoint words of weight p to disjoint words of weight p.*

Proof. Let α and β be the two disjoint words of weight p. Then by the previous lemma we know there exists a unique word γ of weight $2p$ that is at distance p from both α and β. By Lemma 5 φ maps α and β to words of weight p and γ to a word of weight $2p$. Furthermore, as φ is a p-isometry $\varphi(\alpha)$ and $\varphi(\beta)$ will be such that $\varphi(\gamma)$ is the unique word of weight $2p$ at distance p from both. Hence, again by the previous lemma, $\varphi(\alpha)$ and $\varphi(\beta)$ are disjoint.

■

Lemma 8 *Under the assumption $2p < n$, a word w in $C(1, p-1) \cup C(p+1, 2p-1)$ is even if and only if there are two words x_1 and x_2 such that $wt(x_1) = wt(x_2) = p, d(x_1, w) = d(x_2, w) = p$ and x_1 and x_2 are disjoint. Otherwise the word is odd.*

Proof. We start showing that for an even word w there are two words x_1 and x_2 such that $wt(x_1) = wt(x_2) = p, d(x_1,w) = d(x_2,w) = p$ and x_1 and x_2 are disjoint. Let w be a word of weight 2k in $C(1, p-1) \cup C(p+1, 2p-1)$. Then we can construct two words x_1 and x_2 using the simple construction shown below (note that $n \geq 2p$ is necessary here):

$$\begin{array}{lcccc}
 & \multicolumn{2}{c}{\overbrace{\qquad\qquad\qquad\qquad}^{2k}} & & \\
w: & *\cdots* & *\cdots* & 0\cdots\cdots0 & 0\cdots\cdots0 \\
x_1: & *\cdots* & 0\cdots0 & *\cdots\cdots* & 0\cdots\cdots0 \\
x_2: & \underbrace{0\cdots0}_{k} & \underbrace{*\cdots*}_{k} & \underbrace{0\cdots\cdots0}_{p-k} & \underbrace{*\cdots\cdots*}_{p-k}
\end{array}$$

Where * represent non-zero positions.

So all even words in $C(1, p-1) \cup C(p+1, 2p-1)$ have words x_1 and x_2 in L_p where $d(x_1,w) = d(x_2,w) = p$ and x_1 and x_2 are disjoint.

Next we show that an odd word w in $C(1, p-1) \cup C(p+1, 2p-1)$ will not allow for words x_1 and x_2 in L_p such that $d(x_1,w) = d(x_2,w) = p$ and x_1 and x_2 are disjoint. Assume for contradiction that for some word w of weight 2k+1 in $C(1, p-1) \cup C(p+1, 2p-1)$ there exists two disjoint words x_1 and x_2 in layer L_p such that $d(x_1,w) = d(x_2,w) = p$. Now by comparing these three words we can see a few key relations shown below.

$$\begin{array}{lll} w: & \overbrace{*\cdots\cdots\cdots\cdots\cdots*}^{2k} & 0\cdots\cdots\cdots0 \\ x_1: & \underbrace{0\cdots\cdots0}_{a}\ \ \underbrace{+\cdots+}_{b}\ \ \underbrace{*\cdots*}_{c} & \underbrace{*\cdots*}_{d}\ \ \underbrace{0\cdots0}_{e} \\ x_2: & \underbrace{+\cdots+}_{b'}\ \ \underbrace{*\cdots*}_{c'}\ \ \underbrace{0\cdots\cdots0}_{a'} & \underbrace{0\cdots0}_{e'}\ \ \underbrace{*\cdots*}_{d'} \end{array}$$

Where * represent non-zero positions and + is a non-zero, non-* position.

$$a+b+c=2k+1 \qquad a'+b'+c'=2k+1$$

$$b+c+d=p \qquad b'+c'+d'=p$$

$$a+b+d=p \qquad a'+b'+d'=p$$

$$b'+c'\leq a \qquad b+c\leq a'$$

So then

$$2k+1-(b'+c')=a' \text{ and } 2k+1-(b+c)=a.$$

Now by substitution we have

$$2k+1-a'\leq a \text{ and } 2k+1-a\leq a'$$

giving then that

$$2k+1 \leq a+a'.$$

Now with out loss of generality assume $a \geq a'$, then $k+1 \leq a$. This implies

$$k \geq b+c \text{ since } a+b+c = 2k+1.$$

Hence

$$d \geq p-k \text{ as } b+c+d = p \text{ or } d = p-(b+c).$$

Thus

$$a+b+d \geq k+1+p-k+b \geq p+1+b > p.$$

This contradicts that $a+b+d = p$, so for a word of odd weight w in $C(1, p-1) \cup C(p+1, 2p-1)$ there exists no two disjoint words x_1 and x_2 that are both at distance p from w and x_1. ■

Corollary 9 *Let φ be a p-isometry of H_q^n fixing 0 and let $2p < n$. Then even and odd words in $C(1, p-1)$ and $C(p+1, 2p-1)$ are mapped to even and odd words in $C(1, p-1)$ and $C(p+1, 2p-1)$ respectively.*

Proof. From Lemma 8 we know that even and odd words in $C(1, p-1) \cup C(p+1, 2p-1)$ satisfy specific properties that must be preserved by φ (because by Corollary 7 disjoint words of weight p are mapped to disjoint words of weight p) , thus even and odd words in $C(1, p-1) \cup C(p+1, 2p-1)$ are preserved set-wise. However, we also know from

Lemma 5 that words from $C(1,p-1)$ and $C(p+1,2p-1)$ are preserved set-wise. Thus even and odd words in $C(1,p-1)$ and $C(p+1,2p-1)$ are mapped to even and odd words in $C(1,p-1)$ and $C(p+1,2p-1)$ respectively. ■

Lemma 10 *Let φ be a p-isometry of H_q^n fixing 0 and let $2p<n$, then φ preserves words of weight 1.*

Proof. In the case where p is odd, let $p=2k+1$. Notice that the only words at distance p from a word of weight 1 in $C(p+1,2p-1)$ are words of weight $p+1=(2k+1)+1=2k+2$. So all words at distance p from a word of weight 1 in $C(p+1,2p-1)$ are even. Now let us look at words in $C(2,p-1)$. All these words are at distance p from both even and odd words in $C(p+1,2p-1)$. By Corollary 9 the parity of the words under consideration must be preserved by φ. It follows that words of weight 1 are mapped to words of weight 1.

In the same way, replacing even by odd and odd by even, we see that when p is even, words of weight 1 are mapped to words of weight 1. ■

Theorem 11 *Let φ be a p-isometry of H_q^n, and let $2p<n$. Then φ is an isometry.*

Proof. Let a and c be words such that $d(a,c)=1$. Let us assume by way of contradiction that $d(\varphi(a),\varphi(c))\neq 1$. Let $\varphi(a)=b$. Then we construct the p-isometry $\psi:=\tau_{-b}\circ\varphi\circ\tau_a$ where τ_{-b} and τ_a are translations defined by $\tau_a(w)=w+a$ and $\tau_{-b}(w)=w-b$ for all words w. Now we can see

$$\psi(0) = \tau_{-b} \circ \varphi \circ \tau_a(0) = \tau_{-b} \circ \varphi(a) = \tau_{-b}(b) = 0.$$

So ψ is a p-isometry that fixes 0. Then we see the following:

$$\begin{aligned} d(\tau_{-b} \circ \varphi(a), \tau_{-b} \circ \varphi(c)) &\neq 1 \\ d(\tau_{-b} \circ \varphi \circ \tau_a(0), \tau_{-b} \circ \varphi \circ \tau_a(c-a)) &\neq 1 \\ d(\psi(0), \psi(c-a)) &\neq 1 \\ d(0, \psi(c-a)) &\neq 1 \end{aligned}$$

However we also have that $d(c,a) = 1$ implies that $d(c-a,0) = d(0,c-a) = 1$. Now, since p-isometries that fix 0 preserve words of weight 1 by Lemma 10, we have $d(\psi(0), \psi(c-a)) = 1$. So then we also have $d(0, \psi(c-a)) = 1$. This is a contradiction. So we get that φ preserves distance 1 between words, thus, by Lemma 2, φ is an isometry. ■

Lemma 12 *Let φ be a p-isometry of H_q^n fixing 0 and let $p = n$. Then φ preserves words of weight 1.*

Proof. Let φ be an n-isometry that fixes 0 and let a be a word of weight x. Then if we count the number of words of weight n at distance n from a we get $(q-2)^x(q-1)^{n-x}$. So then the number of words of weight n at distance n from a word of weight 1 is $(q-2)^1(q-1)^{n-1}$.

Let us assume that for some word of weight y, we have

$$
\begin{aligned}
(q-2)^y(q-1)^{n-y} &= (q-2)^1(q-1)^{n-1} \\
(q-2)^{y-1} &= (q-1)^{y-1} \\
\left(\frac{q-1}{q-2}\right)^{y-1} &= 1
\end{aligned}
$$

Then clearly $y = 1$. Now we know that n-isometries that fix 0 preserve L_n. Hence if there are k words of weight n at distance n from a given word w, then there should also be k words of weight n at distance n from $\varphi(w)$. So φ preserves words of weight 1. ■

Theorem 13 *Let φ be a p-isometry of H_q^n. If $p = n$ then φ is an isometry.*

Proof. Let a and c be words such that $d(a,c) = 1$. Let us assume by way of contradiction that $d(\varphi(a), \varphi(c)) \neq 1$. Let $\varphi(a) = b$. Then we construct the p-isometry $\psi := \tau_{-b} \circ \varphi \circ \tau_a$ where τ_{-b} and τ_a are translations defined by $\tau_a(w) = w + a$ and $\tau_{-b}(w) = w - b$ for all words w. Now we can see

$$\psi(0) = \tau_{-b} \circ \varphi \circ \tau_a(0) = \tau_{-b} \circ \varphi(a) = \tau_{-b}(b) = 0.$$

So ψ is a p-isometry that fixes 0. Then we see the following:

$$d(\tau_{-b} \circ \varphi(a), \tau_{-b} \circ \varphi(c)) \neq 1$$

$$d(\tau_{-b} \circ \varphi \circ \tau_a(0), \tau_{-b} \circ \varphi \circ \tau_a(c-a)) \neq 1$$

$$d(\psi(0), \psi(c-a)) \neq 1$$

$$d(0, \psi(c-a)) \neq 1$$

However we also have that $d(c,a) = 1$ implies that $d(c-a,0) = d(0,c-a) = 1$. Now, since n-isometries that fix 0 preserve words of weight 1 by Lemma 12, we have $d(\psi(0), \psi(c-a)) = 1$. So then we also have $d(0, \psi(c-a)) = 1$. This is a contradiction. So we get that φ preserves distance 1 between words, thus, by Lemma 2, φ is an isometry. ■

4.3 Linear algebraic approach

As we did not succeed in generalizing the ideas from the previous results to also incorporate the cases $2p \geq n$ (with the exception of $p = n$) we tried to develop an alternative approach to the initial problem. This approach is based on an underlying algebraic structure: the Bose-Mesner algebra. It is possible to construct a distance regular graph $\Gamma(H)$ from H_q^n as follows. The vertex set V of $\Gamma(H)$ is the set of all words of the Hamming space, and two vertices are adjacent if and only if the corresponding words are at distance 1 in H_q^n. Then $\Gamma(H)$ is a distance regular graph with well known parameters, see e.g. [4]. As explained in the introduction every distance regular graph gives rise to a matrix algebra: the so called

Bose-Mesner algebra.

We will first provide a short discussion of certain elements in this algebra. This is based on [4].

Let $\Gamma_i(H)$ be the graph with vertices the words from H_q^n in which two vertices are adjacent if and only if the corresponding words are at distance i in H_q^n. Also let A_i be the adjacency matrix of $\Gamma_i(H)$. We have $\Gamma_1(H) = \Gamma(H)$ and we will write A for A_1. It is important to note that $\Gamma_i(H)$ is only guaranteed to be a distance regular graph when $i = 1$.

Now A generates a closed so-called Bose-Mesner algebra $\mathscr{A}$, where $\mathscr{A} = \{\alpha_0 I + \alpha_1 A + \ldots + \alpha_n A^n\}$. We want to explain $A_p = f_p(A)$ is a polynomial of degree p in A (belonging to $\mathscr{A}$). We will first show how each A_i is constructed recursively. The diameter of $\Gamma(H)$ is clearly n, and from [4] we know that the intersection array of a_i, b_i, and c_i is given by:

$$a_i = i(q-2)$$

$$b_i = (n-i)(q-1)$$

$$c_i = i$$

The following key formulas (also from [4]) provide the key to what we want to show.

$$A_0 = I, A_1 = A,$$

$$AA_i = c_{i+1}A_{i+1} + a_i A_i + b_{i-1}A_{i-1} \ (i = 0, \ldots, n)$$

$$A_0 + A_1 + \ldots + A_n = J,$$

where J is the all one matrix.

It is important to note that $A_{-1} = A_{n+1} = 0$ and that b_{-1} and c_{n+1} are unspecified. From the above it is obvious that A_p is a polynomial in our matrix A. We can rewrite the above key formula as follows

$$c_{i+1}A_{i+1} = (A - a_i I)A_i - b_{i-1}A_{i-1} \ (i = 0, \ldots, n).$$

So we can see inductively that A_k can be written as a polynomial of degree at most k in A. As for all $l < k$, A^l has a 0 in position ij if $d(i, j) = k$, and $(A_k)_{i,j}$ must have a 1 in position ij if $d(i, j) = k$, we see that A_k is a polynomial of degree exactly k in A. Hence A_p is a polynomial of degree p in A and obviously belongs to $\mathscr{A}$.

Given the above basic properties we can build up our approach to p-isometries of H_q^n. Let ρ be a p-isometry of H_q^n, and let P be the corresponding permutation matrix, that is, $(P)_{ij} = 1$ if vertex i is mapped to vertex j, and equals 0 otherwise. Then ρ induces an automorphism of $\Gamma_p(H)$. Hence $PA_pP^{-1} = A_p$. What we want to show then is that $PA_pP^{-1} = A_p$ implies $PAP^{-1} = A$ which would prove that ρ is an isometry of H_q^n. Now A_p defines in a natural way a subset of $\mathscr{A}$, namely $\mathscr{A}_p = \{a_0 I + a_1 A_p + \ldots + a_k A_p^k\}$, where $k + 1$ is the degree of the minimal polynomial of A_p. Let us for a moment assume that $n = k$, and for ease of notation let us consider A_p as a polynomial in A of degree n instead of p (that is, a polynomial of degree n with the highest $n - p$ coefficients equal to 0). If we let $A = x_1$,

$A^2 = x_2$, ..., $A^n = x_n$ be independent variables, we can form a series of linear equations with n unknowns using the A_p^i

$$A_p^1 = \alpha_{01} I + \alpha_{11} x_1 + \alpha_{21} x_2 + \ldots + \alpha_{n1} x_n$$

$$A_p^2 = \alpha_{02} I + \alpha_{12} A x_1 + \alpha_{22} x_2 + \ldots + \alpha_{n2} x_n$$

$$\vdots$$

$$A_p^n = \alpha_{0n} I + \alpha_{1n} x_1 + \alpha_{2n} x_2 + \ldots + \alpha_{nn} x_n$$

This gives us n linear equations and n unknowns. Now these equations must be linearly independent or our minimal polynomial for $\mathscr{A}_p$ would be of degree less than n which would be a contradiction as we are assuming $n = k$. Since our linear equations are linearly independent we can solve for $x_1 = A$. Thus we can express A as an expression of our $A_p^1, \ldots, A_p^n$. Therefore we get as a consequence that $\mathscr{A} = \mathscr{A}_p$. If $\mathscr{A}_p = \mathscr{A}$ then $A \in \mathscr{A}_p$ and since $PBP^{-1} = B$, $\forall B \in \mathscr{A}_p$ this implies $PAP^{-1} = A$. Hence our problem is reduced to showing that $n = k$.

Hence, if we can show that $n = k$ for a given p would prove that every p-isometry is an isometry. Below we describe a method to prove this, at least in certain cases.

From the above we do know that

$$A_i = f_i(A) \ (i = 0, \ldots, n+1)$$

where the f_i are polynomials of degree i defined recursively by

$$f_{-1}(x) = 0,\ f_0(x) = 1,\ f_1(x) = x,$$

$$c_{i+1} f_{i+1}(x) = (x - a_i) f_i(x) - b_{i-1} f_{i-1}(x)\ (i = 0, \ldots, n).$$

Now we really want to prove that $A_p, A_p^2, \ldots, A_p^n$ are linearly independent. A sufficient condition for this to be true is that A_p has $n+1$ distinct eigenvalues. However, as $A_p = f_p(A)$ the eigenvalues of A_p are the images under f_p of the eigenvalues of A. From [4] we know the $n+1$ eigenvalues of A are $(q-1)n - qi$ for $i = 0, \ldots, n$. Hence the eigenvalues of A_p are

$$\gamma_i = f_p(\lambda_i) \text{ for } i = 0, \ldots, n.$$

If all γ_i are distinct, then indeed by the above every p-isometry would be an isometry.

We first give two examples.

Example 1:

Let n=9, q=3, and p = 7, Then we wish to check if A_7 has 10 distinct eigenvalues.

We are given that $f_{-1}(x) = 0$, $f_0(x) = 1$, $f_1(x) = x$. Using these we will recursively build all $f_i(x)$ up to $f_7(x)$ in order to find A_7 as a polynomial in A. Recall

$$c_{i+1} f_{i+1}(x) = (x - a_i) f_i(x) - b_{i-1} f_{i-1}(x)\ (i = 0, \ldots, n).$$

So starting with $c_2 f_2(x)$ we have:

$$\begin{aligned} c_2 f_2(x) &= 2 f_2(x) \\ &= (x - a_1) f_1(x) - b_0 f_0 \\ &= (x-1)x - 18 * 1 \\ &= x^2 - x - 18 \end{aligned}$$

so if we now divide by $c_2 = 2$ we have

$$f_2(x) = \frac{1}{2}x^2 - \frac{1}{2}x - 9.$$

Continuing in the same way we obtain:

$$f_3(x) = \frac{x^3}{6} - \frac{x^2}{2} - 8x + 6$$

$$f_4(x) = \frac{x^4}{24} - \frac{x^3}{4} - \frac{27x^2}{8} + \frac{37x}{4} + 27$$

$$f_5(x) = \frac{x^5}{120} - \frac{x^4}{12} - \frac{7x^3}{8} + \frac{23x^2}{4} + \frac{86x}{5} - 36$$

$$f_6(x) = \frac{x^6}{720} - \frac{x^5}{48} - \frac{7x^4}{48} + \frac{101x^3}{48} + \frac{37x^2}{10} - \frac{143x}{4} - 15$$

$$f_7(x) = \frac{x^7}{5040} - \frac{x^6}{240} - \frac{x^5}{80} + \frac{25x^4}{48} + \frac{11x^3}{40} - \frac{297x^2}{20} + \frac{619x}{70} + 54$$

Now evaluating $f_7(x)$ at A we get

$$A_7 = \frac{A^7}{5040} - \frac{A^6}{240} - \frac{A^5}{80} + \frac{25A^4}{48} + \frac{11A^3}{40} - \frac{297A^2}{20} + \frac{619A}{70} + 54.$$

This matrix A_7 is our desired A_p so now all that is left is to find the eigenvalues γ_i of A_7 by evaluating f_7 at λ_i, the 10 eigenvalues of A. Now we know that $\lambda_i = (q-1)n - qi$ for $i = 0, \ldots, n$. So in our example the distinct eigenvalues of A are

$$\{18, 15, 12, 9, 6, 3, 0, -3, -6, -9\}.$$

Hence we find that the eigenvalues of A_7 are

$$\{4608, -768, -96, 144, -48, -24, 54, -57, 48, -36\}.$$

These eigenvalues are all distinct, and so we can conclude that every 7-isometry is indeed an isometry when $n = 9$ and $q = 3$.

Example 2:

Let n=10, q=3, and p = 7, Then we wish to check if A_7 has 11 distinct eigenvalues.

We are given that $f_{-1}(x) = 0$, $f_0(x) = 1$, $f_1(x) = x$. Using these we will recursively build all $f_i(x)$ up to $f_7(x)$ in order to find A_7 as a polynomial in A. Recall

$$c_{i+1} f_{i+1}(x) = (x - a_i) f_i(x) - b_{i-1} f_{i-1}(x) \ (i = 0, \ldots, n).$$

So starting with $c_2 f_2(x)$ we have:

$$
\begin{aligned}
c_2 f_2(x) &= 2 f_2(x) \\
&= (x - a_1) f_1(x) - b_0 f_0 \\
&= (x-1)x - 20 * 1 \\
&= x^2 - x - 20
\end{aligned}
$$

so if we now divide by $c_2 = 2$ we have

$$f_2(x) = \frac{1}{2}x^2 - \frac{1}{2}x - 10.$$

Continuing in the same way we obtain:

$$f_3(x) = \frac{x^3}{6} - \frac{x^2}{2} - 9x + \frac{20}{3}$$

$$f_4(x) = \frac{x^4}{24} - \frac{x^3}{4} - \frac{31x^2}{8} + \frac{125x}{12} + 35$$

$$f_5(x) = \frac{x^5}{120} - \frac{x^4}{12} - \frac{25x^3}{24} + \frac{79x^2}{12} + \frac{358x}{15} - \frac{140}{3}$$

$$f_6(x) = \frac{x^6}{720} - \frac{x^5}{48} - \frac{3x^4}{16} + \frac{355x^3}{144} + \frac{749x^2}{120} - \frac{97x}{2} - \frac{280}{9}$$

$$f_7(x) = \frac{x^7}{5040} - \frac{x^6}{240} - \frac{x^5}{48} + \frac{91x^4}{144} + \frac{4x^3}{15} - \frac{1301x^2}{60} + \frac{191x}{63} + \frac{280}{3}$$

Now evaluating $f_7(x)$ at A we get

$$A_7 = \frac{A^7}{5040} - \frac{A^6}{240} - \frac{A^5}{48} + \frac{91A^4}{144} + \frac{4A^3}{15} - \frac{1301A^2}{60} + \frac{191A}{63} + \frac{280}{3}.$$

This matrix A_7 is our desired A_p so now all that is left is to find the eigenvalues γ_i of A_7 by evaluating f_7 at λ_i, the 11 eigenvalues of A. Now we know that $\lambda_i = (q-1)n - qi$ for $i = 0, \ldots, n$. So in our example the distinct eigenvalues of A are

$$\{20, 17, 14, 11, 8, 5, 2, -1, -4, -7, -10\}.$$

Hence we find that the eigenvalues of A_7 are

$$\{15360, -768, -768, 240, 96, -120, 24, 69, -120, 132, -120\}.$$

Unfortunately these eigenvalues are not all distinct, and we cannot conclude that every 7-isometry is indeed an isometry when $n = 10$ and $q = 3$.

By writing a mathematica program to compute when the eigenvalues of A_p are distinct and then running over multiple values of n, p, and q we get the following tables. Note here if there is a value of true in a cell then this represents that the eigenvalues of A^p are distinct. This then shows for that n, p, and q the p-isometry is also an isometry. However if the value is false in the cell then we know that the eigenvalues are not distinct. This does not mean that for this given n, p, and q our p-isometry can not be an isometry. It merely means that this method came up inconclusive.

We start by looking at the distinctness for $n = \{3, \ldots, 12\}$. This is since $n = 1$ and $n = 2$ are uninteresting cases and are covered by lemmas already and known to result in isometries. Our p values go from 2 to 11 since $p = 1$ and $p = n$ are known to result in isometries. Now in this first group of tables we check when $q = \{3, \ldots, 7\}$ this is our first five q values.

Table 4.1
$q = 3$

q=3	$p=2$	3	4	5	6	7	8	9	10	11
$n=3$	True									
4	False	False								
5	True	False	True							
6	True	True	True	True						
7	False	False	True	False	False					
8	True	True	True	True	True	True				
9	True	True	True	True	True	True	True			
10	False	False	False	False	False	False	False	False		
11	True	False	True	True	False	True	False	False	True	
12	True	True	True	True	True	True	True	True	True	True

Table 4.2
$q = 4$

q=4	$p=2$	3	4	5	6	7	8	9	10	11
$n=3$	False									
4	True	True								
5	False	False	False							
6	True	True	True	True						
7	False	True	False	True	False					
8	True	True	True	True	True	True				
9	False	False	True	False	True	False	False			
10	True	True	True	True	True	True	True	True		
11	False	True	False	True	False	True	False	True	False	
12	True	True	True	True	True	True	True	True	True	True

Table 4.3

$q = 5$

q=5	$p = 2$	3	4	5	6	7	8	9	10	11
$n = 3$	True									
4	True	True								
5	True	True	True							
6	False	False	True	False						
7	True	True	True	True	True					
8	True	True	True	True	True	True				
9	True	True	True	True	True	True	True			
10	True	True	True	True	True	True	True	True		
11	False	False	True	False	True	True	True	False	False	
12	True	True	True	True	True	True	True	True	True	True

Table 4.4

$q = 6$

q=6	$p = 2$	3	4	5	6	7	8	9	10	11
$n = 3$	True									
4	False	True								
5	True	False	True							
6	True	True	True	True						
7	False	False	True	True	False					
8	True	True	True	True	True	True				
9	True	True	True	True	True	True	True			
10	False	False	False	False	True	False	False	True		
11	True	False	False	True	False	True	True	True	True	
12	True	True	True	True	True	True	True	True	True	True

Table 4.5

$q = 7$

q=7	$p = 2$	3	4	5	6	7	8	9	10	11
$n = 3$	True									
4	True	True								
5	True	True	True							
6	True	True	True	True						
7	True	True	True	True	True					
8	False	False	False	True	True	False				
9	True	True	True	True	True	True	True			
10	True	True	True	True	True	True	True	True		
11	True	True	True	True	True	True	True	True	True	
12	True	True	True	True	True	True	True	True	True	True

Notice that as q gets larger we see that slowly our values for our given n and p are true more often then false. The first case where we have all true for a given n, p, and q is when $q = 13$. However this is not to say that for all values this will hold as we could raise our n and p respectively to show that eventually false values will come back. This can be seen in our next two tables where $q = 13$.

Table 4.6

$q = 13$

q=13	$p=2$	3	4	5	6	7	8	9	10	11
$n=3$	True									
4	True	True								
5	True	True	True							
6	True	True	True	True						
7	True	True	True	True	True					
8	True	True	True	True	True	True				
9	True	True	True	True	True	True	True			
10	True	True	True	True	True	True	True	True		
11	True	True	True	True	True	True	True	True	True	
12	True	True	True	True	True	True	True	True	True	True

Table 4.7

$q = 13$

q=13	$p=2$	3	4	5	6	7	8	9	10	11
$n=3$	True									
4	True	True								
5	True	True	True							
6	True	True	True	True						
7	True	True	True	True	True					
8	True	True	True	True	True	True				
9	True	True	True	True	True	True	True			
10	True	True	True	True	True	True	True	True		
11	True	True	True	True	True	True	True	True	True	
12	True	True	True	True	True	True	True	True	True	True
13	True	True	True	True	True	True	True	True	True	True
14	False	False	True	True	True	True	True	True	True	True

Lastly we look to larger values of q to see if this behavior continues and it does. Notice that we have distinct eigenvalues for our values of n and p where q is between 100 and 105.

Table 4.8
$q = 100$

q=100	$p = 2$	3	4	5	6	7	8	9	10	11
$n = 3$	True									
4	True	True								
5	True	True	True							
6	True	True	True	True						
7	True	True	True	True	True					
8	True	True	True	True	True	True				
9	True	True	True	True	True	True	True			
10	True	True	True	True	True	True	True	True		
11	True	True	True	True	True	True	True	True	True	
12	True	True	True	True	True	True	True	True	True	True

Table 4.9
$q = 101$

q=101	$p = 2$	3	4	5	6	7	8	9	10	11
$n = 3$	True									
4	True	True								
5	True	True	True							
6	True	True	True	True						
7	True	True	True	True	True					
8	True	True	True	True	True	True				
9	True	True	True	True	True	True	True			
10	True	True	True	True	True	True	True	True		
11	True	True	True	True	True	True	True	True	True	
12	True	True	True	True	True	True	True	True	True	True

Table 4.10
$q = 102$

q=102	$p = 2$	3	4	5	6	7	8	9	10	11
$n = 3$	True									
4	True	True								
5	True	True	True							
6	True	True	True	True						
7	True	True	True	True	True					
8	True	True	True	True	True	True				
9	True	True	True	True	True	True	True			
10	True	True	True	True	True	True	True	True		
11	True	True	True	True	True	True	True	True	True	
12	True	True	True	True	True	True	True	True	True	True

Table 4.11
$q = 103$

q=103	$p = 2$	3	4	5	6	7	8	9	10	11
$n = 3$	True									
4	True	True								
5	True	True	True							
6	True	True	True	True						
7	True	True	True	True	True					
8	True	True	True	True	True	True				
9	True	True	True	True	True	True	True			
10	True	True	True	True	True	True	True	True		
11	True	True	True	True	True	True	True	True	True	
12	True	True	True	True	True	True	True	True	True	True

Table 4.12
$q = 104$

q=104	$p = 2$	3	4	5	6	7	8	9	10	11
$n = 3$	True									
4	True	True								
5	True	True	True							
6	True	True	True	True						
7	True	True	True	True	True					
8	True	True	True	True	True	True				
9	True	True	True	True	True	True	True			
10	True	True	True	True	True	True	True	True		
11	True	True	True	True	True	True	True	True	True	
12	True	True	True	True	True	True	True	True	True	True

Table 4.13
$q = 105$

q=105	$p = 2$	3	4	5	6	7	8	9	10	11
$n = 3$	True									
4	True	True								
5	True	True	True							
6	True	True	True	True						
7	True	True	True	True	True					
8	True	True	True	True	True	True				
9	True	True	True	True	True	True	True			
10	True	True	True	True	True	True	True	True		
11	True	True	True	True	True	True	True	True	True	
12	True	True	True	True	True	True	True	True	True	True

Chapter 5

Summary and future work

The major results of this thesis can be stated as follows:

- In chapter 4 section 2 we used combinatorics to show that when $n = p$ or $n \geq 2p$ a p-isometry of Hamming space H_q^n, $q > 2$, is in fact an isometry

  Theorem 11 Let φ be a p-isometry of H_q^n, $q > 2$, and let $2p < n$. Then φ is an isometry.

  Theorem 13 Let φ be a p-isometry of H_q^n, $q > 2$. If $p = n$ then φ is an isometry.

- In chapter 4 section 3 we developed a process to determine, for given values of n, p, and q, whether the adjacency matrix A_p of the distance-p-graph of the distance regular graph $\Gamma(H)$ associated to H_q^n has $n+1$ distinct eigenvalues. Whenever A_p has $n+1$ distinct eigenvalues, we know that a p-isometry of H_q^n must be an isometry. If we do not obtain $n+1$ distinct eigenvalues no new information pertaining to the

p-isometries of H_q^n is obtained.

In the future we would like to continue to look at the following question: "*When does the matrix A_p have $n+1$ distinct eigenvalues?*". We would be interested in using Algebra to possibly find conditions on p, n, and q that would guarantee this to be true. As a special case of this we would like to prove that when $q \geq n$, A_p has $n+1$ distinct eigenvalues.

References

[1] Beckman, F. S., and Quarles, D. A., Jr. On isometries of Euclidean spaces. *Proceedings of the American Mathematical Society* **4**, 810-815, 1953.

[2] Benz, W., A Beckman-Quarles type theorem for finite Desarguesian planes, *J*ournal of Geometry **19**, 89-93, 1982.

[3] Bose, R. C., and Mesner, Dale M, On linear associative algebras corresponding to association schemes of partially balanced designs. *The Annals of Mathematical Statistics* **30**, 21-38, 1959.

[4] Brouwer, Andries E., Cohen, A.M. and Neumaier, A., *Distance-Regular Graphs*. Springer-Verlag, 1989.

[5] De Winter, S., and Korb, M., Weak isometries of the Boolean cube, *s*ubmitted to Discrete Mathematics.

[6] Krasin, V. Yu, On the weak isometries of the Boolean cube. *Diskretnyi Analiz i Issledovanie Operatsii* **13**, 26-32, 2006 *In Russian*.

[7] Krasin, V.Yu. On the weak isometries of the Boolean cube. *Journal of Applied and Industrial Mathematics* **1**, 463-467, 2007.

[8] Tyszka, A. A Discrete Form of the Beckman-Quarles Theorem. *Mathematical Association of America* **104** (1997), 757-761.

[9] http://www.win.tue.nl/ aeb/graphs/Hamming.html