The MacWilliams Identity for Krawtchouk Association Schemes

FRIEDLANDER, ISOBEL,SOPHIE,AIMEE

The MacWilliams Identity for Krawtchouk Association Schemes

Isobel Sophie Aimee Friedlander

Student ID: 000848327

A Thesis presented for the degree of

Doctor of Philosophy

Department of Computer Science
Durham University
United Kingdom
1st February 2024

Abstract

The weight distribution of an error correcting code is a crucial statistic in determining its performance. One key tool for relating the weight of a code to that of its dual is the MacWilliams Identity, first developed for the Hamming association scheme. This identity has two forms: one is a functional transformation of the weight enumerators, while the other is a direct relation of the weight distributions via eigenvalues of the association scheme. The functional transformation form can, in particular, be used to derive important moment identities for the weight distribution of codes. In this thesis, we focus initially on extending the functional transformation to codes based on skew-symmetric and Hermitian matrices. A generalised b-algebra and new fundamental homogeneous polynomials are then identified and proven to generate the eigenvalues of a specific subclass of association schemes, Krawtchouk association schemes. Based on the new set of MacWilliams Identities as a functional transform, we derive several moments of the weight distribution for all of these codes.

Declaration

The work in this thesis is based on research carried out at the Department of Computer Science, Durham University, United Kingdom. No part of this thesis has been submitted elsewhere for any other degree or qualification and it is all my own work unless referenced to the contrary in the text.

Acknowledgements

I am profoundly grateful to my supervisors, Dr. Maximilien Gadouleau and Prof. Thanasis Bouganis, for their guidance, invaluable insights, and continuous support throughout the journey of this research. Their expertise, patience, and encouragement have been instrumental in shaping the direction of my work and fostering an environment where intellectual growth could flourish.

I extend my heartfelt appreciation to my parents, Jill and Colin, for their boundless love, encouragement, and unwavering belief in my aspirations. Their sacrifices, constant motivation, and enduring support have been the foundation upon which I built this academic pursuit. Your faith in me has been my driving force.

To my dearest partner, David, your steadfast belief in me and your understanding during the long hours of research and writing have been my refuge. Your encouragement, patience, and continual presence, even through the darkest hours we've ever faced, have provided the emotional support necessary to weather the challenges of our journey.

I am also deeply grateful to my brother, Nic, who provided extensive technical support with LaTeX over the course of the four years. His expertise, troubleshooting skills, and willingness to assist have been crucial in overcoming formatting challenges and ensuring the polished presentation of this work.

In conclusion, this thesis stands as a testament to the collective efforts of many individuals, and I am deeply thankful to each and every one of them for being a part of this extremely challenging journey in work and in life.

With profound gratitude,

Izzy Friedlander

January 2024

Contents

List of Figures

List of Tables

Chapter 1

Introduction

“Codes are a puzzle. A game, just like any other game.” - Alan Turing.

This piece of the puzzle is a small part of a very big picture. We begin with a step back in time to Ancient Egypt.

1.1 A brief history

Back around 1900 BC, the tomb of Khnumhotep II [34, Chapter 3] is carved out of stone in the necropolis and adorned with decorations and inscriptions about his life. A few of them contain abnormal hieroglyphs that some believe were a deliberate attempt to hide details of sacred rituals, a very early example of cryptography [59]. Taking a huge leap forward in time by 1300 years we arrive in Ancient Sparta. The Spartans wrote on a strip of parchment paper wrapped around a cylinder [63], which could only be deciphered by a reader if they had an identical cylinder. This could be the first example of a shared key used to encrypt and decrypt messages.

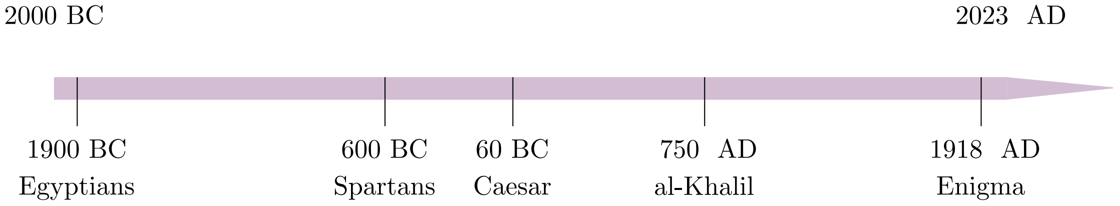

Figure 1.1.1: Some selected known developments of cryptography

Jumping to the time of Julius Caesar [46] where a more sophisticated concealment was deployed, again for military purposes. He was known to use a substitution cipher [24] to hide messages, a key part of his strategic success. Walking through the modern calendar we stumble across the man who wrote the first dictionary of the Arabic language and the “Book of Cryptographic Messages”, al-Khalil, [31] in southern Arabia. Being an independent thinker he pioneered the use of mathematics to analyse all permutations and combinations of Arabic letters, which in turn influenced decryption using frequencies. This led to an extended period of Arab focus on cryptanalysis, the use of mathematics to break codes systematically.

Running through the Middle Ages, cryptography is used more widely across the globe. One of the more famous examples in England involved Mary Queen of Scots who was implicated in the Babington Plot [7], designed to assassinate Queen Elizabeth I, when her encrypted messages were intercepted and deciphered. We land in Germany at the end WWI. The famous Engima machine is invented by Arthur Scherbius [49], a German engineer. Most notably it was used intensively by the German military in WWII. The advantage of Enigma was not just the complexity of the coding, but also the ability to change the configuration of the key, which the Germans did on a daily basis.

1.2 The Digital Age

The use of cryptography rapidly picks up the pace into the Digital Age. Long distance communications became the norm in every day life. For the average person the need for efficient transmission and storage of data became essential. Early systems such as semaphore and Morse code rapidly evolved into advanced digital encoding systems such as those used in space communications. The challenge for those applications was to overcome the frequency of errors induced by noisy interference or faulty storage of data. Codes that could detect and correct errors efficiently became imperative.

The internet is born. With it came the need for secure communication between people who aren't able to share a secret key beforehand. The Diffie-Hellman key exchange [14] was invented to conceal a message using mathematics that is very difficult to reverse. This is at the heart of the public key systems still in use today such as RSA [52] and ECC [35]. Fast forward to the late 20th century, the first scheme to use randomisation in its encryption system is introduced, the McEliece cryptosystem.

1.3 Into the Quantum Era

We drop over the precipice and free fall into the Quantum Era. As the quantum computer arrives, the length of time required to break conventional algorithms will plummet. It has already been shown that Shor's algorithm [56] can be used by quantum computers to break existing codes in a reasonable time. There is a constant tension between those who are devising new ways of keeping a message secret and those who are just as determined to intercept and decipher it. That is why there is a continuous need for ongoing research into ever more sophisticated techniques to thwart the ever more ingenious and powerful attackers.

1.4 This piece of the puzzle

With the general big picture painted, we can now turn to the piece of the puzzle that this thesis contributes. Error-correcting codes could themselves be a standalone motivation for this research. For instance, rank metric codes have been shown to be optimal when correcting criss-cross errors used in digital communications [19]. They are powerful in their own right, but are also a strong contender for advanced cryptosystems.

One of those contenders that is believed to be secure against Shor's algorithm is the classical McEliece cryptosystem. A weakness of this scheme is the very large public key used to scramble the message. To combat this, Delsarte first spots the potential of the rank metric in the use of error correcting codes. Rank metric codes are known to be more efficient in some circumstances [36]. Gabidulin also notes this and, after identifying other potential metrics, focuses on the rank metric and produces encoding and decoding algorithms for maximal codes in this new setting [21]. Their lateral thinking opens the door to the possibilities of using other metrics with other association schemes.

One way to improve on the existing codes in the rank metric is to seek better underlying structures that retain the level of security but improve efficiency. The natural progression from the standard rank metric is to explore other rank-based metrics, such as the skew rank that we first investigate here. The well known MacWilliams Identity is a tool that has long been used to find and evaluate new codes and their potential. In particular we offer a unified functional transform that covers the Hamming, rank, skew rank and Hermitian association schemes, inspired by MacWilliams' original identity for the Hamming association scheme [41] and the use of a q-algebra by Gadouleau and Yan [22]. Moreover we establish new generalised identities for the moments of the weight distribution of these schemes.

The structure of this thesis is as follows. Chapter 2 introduces cryptosystems based on error correcting codes before presenting an overview of association schemes, the different scenarios we are exploring. We then outline different association schemes and the existing theory in each instance, including the familiar Hamming case. Chapter 3 is the first association scheme investigated in detail. A new q-algebra for skew-symmetric matrices is developed, and homogeneous polynomials are identified which are used to prove the new MacWilliams Identity as a functional transform specifically for skew-symmetric matrices. Chapter 4 confirms the idea that we can find a new form of the MacWilliams Identity as a functional transform for Hermitian matrices using the same methods as for skew-symmetric matrices. In Chapter 5 the previous chapters are analysed and used to prove a new generalised form of the identity and a generator for the eigenvalues of Krawtchouk association schemes. The resulting moments of their weight distributions are then developed. Finally Chapter 6 offers conclusions and some suggestions for future work. My work in this thesis has been extracted into a published paper with some guidance from both of my supervisors.

Chapter 2

Background

In this thesis we are particularly interested in error-correcting codes, frequently used in public key cryptosystems, which involve both a public key and a private key. The public key is openly available and used to encrypt a message and the private key is used to decrypt it and is only known by those who are authorised [60]. This eliminates the need for any two parties to “meet” beforehand to agree a secret key before sending a secure message between themselves. The public key is like an open padlock which is given out freely to lock any message (encrypt) but only those who possess the private key to open it once it has been locked (decrypt).

Two of the most commonly used public key cryptosystems today are RSA [52] (named after its inventors Rivest, Shamir, and Adlemen in 1977) and Elliptic Curve Cryptography [35] (ECC). RSA depends on the hardness of factorising a product of large primes whereas ECC depends on the difficulty of solving the discrete logarithm problem [44] [35]. As the speed and efficiency of computers and algorithms for breaking these codes has increased, so have the parameters of these (and other) systems to keep them secure. The National Institute of Standards and Technology (NIST) at the US Department of Commerce provides recommendations on the size of RSA and ECC keys which have increased over time. For example, they have risen from 1024 bits [47] in around 2002 to 2048 bits for RSA and from P-256 to P-384 for ECC [16].

The goal is to find crypto-systems which have an easy to use (not too large) public key, high difficulty of decoding without the private key, and sufficiently efficient decoding with the private key.

2.1 Error-Correcting Codes

The first effective error-correcting code was invented by Richard Hamming in 1950 [30] and is still used in some computer storage applications today. Other early examples include the

Hadamard code that was used in NASA's Mariner 9 Probe to send images of Mars back to Earth. The Golay code [26] and Reed Solomon codes [41, Chapter 9] were used in the later Voyager 1 and 2 missions to Jupiter and beyond. More recently, Reed-Solomon codes are extensively used in commercial products today such as CD and DVD storage and are still extensively used in 2-dimensional bar codes such as QR codes to minimise reading errors in damaged images [65]. These examples and many other types of error-correcting codes are described in [41].

In general, error-correcting codes work by taking an encoding of a message using a finite alphabet (e.g. binary) and adding some additional information which increases the message length in such a way that errors can be detected and corrected [41, Chapter 1]. The aim is to transmit (or store) information as efficiently as possible while correcting as many errors as possible. These two goals are conflicting: the more redundant information is added the less efficient the code, but the more errors can be detected and corrected.

Many, but not all, codes have a fixed block length, n, and are linear subspaces of an n-dimensional vector space over a finite field. Linear algebra and algebraic geometry have been used extensively [41], [32], [39] to look for optimal (or "extremal") codes. This is using the block length, the dimension of the code as a subspace, a distance metric on the vector space (such as the Hamming, Euclidean or rank metrics), and a bilinear form (such as the Euclidean or Hermitian inner products) on the space to define duality (orthogonality). Most notably Hamming weight enumerators (and more recently those of other association schemes) have been analysed to classify the structure of "good" codes. A well known tool is the MacWilliams Identity relating the weight enumerator of a code to that of its dual [39], together with Andrew Gleason's follow on theorems about the properties of self dual codes [25].

Again many, but not all, codes can be generated by evaluating a function at a set of points which are rational over the underlying finite field. This can be generalised by defining curves over the field with a number of rational points. In the case of Reed-Solomon codes, for example, the points lie on a projective straight line [32].

It is the variations of these alphabets, parameters, metrics and bilinear forms that offer many opportunities to explore further optimisation of code performance.

2.2 Cryptosystems based on Error Correcting Codes

In 1978 Robert McEliece published a proposal to link these two areas by using an error-correcting code to create a public key cryptosystem. The "difficult" problem for any interceptor to solve would depend on the difficulty of recovering the original unencrypted message, rather than on the difficulty of factorising integers or solving a discrete logarithm. McEliece's idea was to use a binary Goppa code [4], a scrambled form of its generator matrix and a random additional error vector to the resulting message word [43].

The current public key cryptosystems, such as 2048-bit RSA, are considered secure against attacks using current computer technology [16] but in 1994 Peter Shor [57] devised an algorithm which would allow a quantum computer, whenever one is built, to break them in polynomial time. In other words, they will be broken.

As a result, cryptographers are racing to develop alternative cryptosystems that might not be so vulnerable to quantum algorithms. NIST launched a competition to find a future standard for post-quantum cryptography at the end of 2016 [47]. In January 2019, the seventeen candidates remaining in the 'semi-finals' were: seven based on error-correcting codes, one on isogenies of supersingular elliptic curves and nine based on lattices [45]. The code based candidates used a mixture of Hamming metric and rank metric based codes and included McEliece type cryptosystems. In 2022 NIST announced four candidates as finalists, one of which is the Classic McEliece, and a further one to standardise and implement (Crystals-Kyber based on lattices, not error correcting codes).

2.3 Association Schemes and Distance Regular Graphs

Association schemes give a particular structure to a set and that structure has been found to be useful when investigating properties of linear codes. Here we introduce the basic properties of an association scheme, focusing in particular on metric association schemes. We also identify their relationship with distance regular graphs which offers further understanding of these abstract concepts by visualisation.

2.3.1 Preliminaries

Definition 2.3.1. A ***symmetric association scheme with n classes***, $(\mathscr{X}, R)$, is defined as a finite set $\mathscr{X}$ of v points and $n+1$ relations $R = \{R_0, \dots, R_n\}$, which satisfy the following conditions:

$$R_0 = \{(x,x) \mid x \in \mathscr{X}\} \tag{2.3.1}$$

$$(x,y) \in R_i \implies (y,x) \in R_i \tag{2.3.2}$$

$$\{R_0, R_1, \dots, R_n\} \text{ is a partition of } \mathscr{X} \times \mathscr{X} \tag{2.3.3}$$

$$(x,y) \in R_k \implies |\{z \in \mathscr{X} \mid (x,z) \in R_i, (z,y) \in R_j\}| = c_{ijk} \tag{2.3.4}$$

where c_{ijk} is a constant and is called the ***intersection number***. That is, if $x, y \in R_k$, the number of $z \in \mathscr{X}$ that are i away from x and j away from y is a constant, c_{ijk}, independent of the choice of x and y. In other words, the relations satisfy having an identity, are symmetric, form a partition and have intersection numbers.

We note that many different texts use the notation $p_{i,j}^{(k)}$ instead of c_{ijk}, as in [8, (2.1)].

Definition 2.3.2. If $(x,y) \in R_i$ we call x and y ***i^{th} associates***.

The ***valency*** [3, p43] of each relation is defined as $v_i = c_{ii0}$ which, for any $x \in \mathscr{X}$ is the number of $z \in \mathscr{X}$ such that $(x, z) \in R_i$. It is immediately obvious that $\sum_i c_{ii0} = v$.

We note that there are non-symmetric association schemes but we are only focusing on those which are "symmetric" in this thesis.

There are some well known identities for the valencies and the intersection numbers that can be useful when using the theory of association schemes [3, Lemma 2.1.1]. The most interesting identity to note is that

$$\sum_{j=0}^{n} c_{ijk} = v_i.$$

This identity can be explained in a bit more detail. Using Figure 2.3.1, let $x, y \in \mathscr{X}$, $(x, y) \in R_k$. Then we see that

$$\begin{aligned} v_i &= |\{z : (x, z) \in R_i\}| \\ &= \sum_j |\{z : (x, z) \in R_i, (z, y) \in R_j\}| \\ &= \sum_j c_{ijk}. \end{aligned}$$

We go on to define the set of adjacency matrices that can be used to record and analyse the properties of the association scheme.

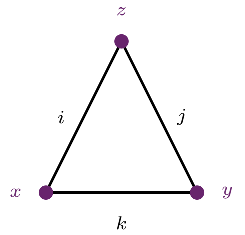

Figure 2.3.1: Visualisation of points and relations in an association scheme.

Definition 2.3.3 ([41, p613])**.** The ***adjacency matrix***, D_i, of R_i is defined to be a $v \times v$ matrix where each row and each column represents a point in $\mathscr{X}$ and where

$$(D_i)_{x,y} = \begin{cases} 1 & \text{if } (x, y) \in R_i, \\ 0 & \text{otherwise.} \end{cases} \tag{2.3.5}$$

Lemma 2.3.4. *Using the properties of an $(\mathscr{X}, R)$ symmetric association scheme [3, Lemma 2.1.1] we have that,*

1.
$$D_0 = I \tag{2.3.6}$$

2.
$$D_i^T = D_i \tag{2.3.7}$$

3.

$$\sum_{i=0}^{n} D_i = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix} = J \tag{2.3.8}$$

4.

$$D_i D_j = \sum_{k=0}^{n} c_{ijk} D_k = D_j D_i, \ \textit{for } i, j = 0, \dots, n. \tag{2.3.9}$$

5.

$$D_i J = J D_i = v_i J \tag{2.3.10}$$

Conversely, any set of $\{0,1\}$ *matrices,* $D_0, \dots, D_n$*, that satisfies* (2.3.6) - (2.3.10) *with* $c_{ijk}, v_i \in \mathbb{Z}^+$ *is the collection of adjacency matrices of an association scheme.*

Proof. (1) $D_0 = I$ holds immediately from (2.3.1).

(2) $D_i^T = D_i$ holds immediately from (2.3.2).

(3) $\sum_{i=0}^{n} D_i = J$ holds immediately from (2.3.3).

(4) Proving Equation (2.3.9), if $(x, y) \in R_k$, then the matrix $(D_i D_j)_{x,y} = c_{ijk}$ by (2.3.4), and by (2.3.5), $(D_k)_{x,y} = 1$. So we have

$$(D_i D_j)_{x,y} = c_{ijk}(D_k)_{x,y}.$$

Now since $(D_i D_j)_{x,y}$ takes the intersection number of $(x, y) \in R_k$, we need to include all values of k, therefore

$$D_i D_j = \sum_{k=0}^{n} c_{ijk} D_k = D_j D_i$$

as required.

(5) Now we prove Equation (2.3.10). By definition of D_i, every row and column contains v_i 1's. Therefore when we multiply by J, we sum these 1's, which is v_i in every case by (2.3.4).

□

2.3.2 The Bose-Mesner Algebra

The eigenvalues of these adjacency matrices play an important part in looking for optimal codes. That is, those with maximal distance for a given size. The algebra of these matrices was first explored by Bose and Nair [2] in 1939 and later developed by Bose and Mesner [1] after whom it was named. The important results are outlined here.

To work with these adjacency matrices we define a set which consists of all complex linear combinations of the adjacency matrices. That is,

$$\mathscr{B} = \left\{ B = \sum_{i=0}^{n} b_i D_i \mid b_i \in \mathbb{C} \right\}.$$

This set then forms a ring with the operations of matrix addition and matrix multiplication with the added property of the multiplication being commutative by (2.3.9). As this set is a ring and also a vector space, it forms an algebra and is called the ***Bose-Mesner Algebra*** of the association scheme.

Since $\mathscr{B}$ is commutative the members of $\mathscr{B}$ can be simultaneously diagonalised [23], i.e. there exists a single invertible matrix $P \in \mathscr{B}$, such that $P^{-1}BP$ is a diagonal matrix for each $B \in \mathscr{B}$. As a consequence there exists a unique alternative basis consisting of primitive idempodent matrices $E_0, \ldots, E_n$, of size $v \times v$. A primitive idempotent, E_i, is an idempotent such that it cannot be written as a direct sum of two other non-zero idempotents. So these idempotent matrices in the alternative basis satisfy the following equations,

$$E_i^2 = E_i \ \forall \ i \tag{2.3.11}$$

$$E_i E_j = 0 \text{ if } i \neq j \tag{2.3.12}$$

$$\sum_{i=0}^{n} E_i = I.$$

It is conventional to choose $E_0 = \frac{1}{v} J$.

Since $\{E_0, \ldots, E_n\}$ is a basis for $\mathscr{B}$ there exist uniquely defined complex numbers $p_k(i)$ such that

$$D_k = \sum_{i=0}^{n} p_k(i) E_i, \quad k = 0, \ldots, n. \tag{2.3.13}$$

We also have,

$$\begin{aligned} D_k E_i &= \sum_{j=0}^{n} p_k(j) E_j E_i \\ &\overset{(2.3.12)}{=} p_k(i) E_i E_i \\ &\overset{(2.3.11)}{=} p_k(i) E_i. \end{aligned} \tag{2.3.14}$$

Thus the $p_k(i)$'s are the ***eigenvalues*** of D_k by definition. The rank of each matrix E_i, denoted ψ_i, is the multiplicity of each eigenvalue $p_k(i)$ [3, p45].

Since the D_i's also form a basis of $\mathscr{B}$ we can also express each E_k as a linear combination of the D_i. We then define

$$E_k = \frac{1}{v} \sum_{i=0}^{n} q_k(i) D_i, \quad k = 0, \ldots n \tag{2.3.15}$$

such that $q_k(i)$ represent the coefficients of the change of basis matrix from D_i's to the E_i's. We then call the $q_k(i)$'s the ***dual eigenvalues*** [42] of the association scheme. We also define the ***eigenmatrices*** of the association scheme, $P = (p_{ik})$ and $Q = (q_{ik})$, to be the $(n+1) \times (n+1)$ matrices consisting of the eigenvalues $p_k(i)$ and $q_k(i)$ respectively. The eigenmatrices P and Q have the following properties.

Theorem 2.3.5. *For P and Q eigenmatrices of a symmetric association scheme, we have,*

1.

$$p_0(i) = q_0(i) = 1 \tag{2.3.16}$$

2.

$$p_k(0) = v_k, \quad q_k(0) = \psi_k \tag{2.3.17}$$

3.

$$\sum_{i=0}^{n} \psi_k p_k(i) p_\ell(i) = v v_k \delta_{k\ell} \tag{2.3.18}$$

4.

$$\sum_{i=0}^{n} v_i q_k(i) q_\ell(i) = v \psi_k \delta_{k\ell} \tag{2.3.19}$$

5.

$$\psi_j p_i(j) = v_i q_j(i), \quad i, j = 0, \ldots, n \tag{2.3.20}$$

6.

$$|p_k(i)| \leq v_k, \quad |q_k(i)| \leq \psi_k \tag{2.3.21}$$

7.

$$\sum_{j=0}^{n} p_k(i) = \sum_{i=0}^{n} c_{iki} \tag{2.3.22}$$

The proofs for these properties are well known and can be found at [3, Lemma 2.2.1]. The equations (2.3.18) and (2.3.19) are called the ***orthogonality relations*** [41, Theorem 3]. For emphasis, $p_0(i) = 1$ since by Equation (2.3.14) and we have $D_0 = I$, immediately, $p_0(i) = 1$.

We briefly introduce the idea of a ***formal dual association scheme***. Delsarte [13, Section II C] proves that under some assumptions (explained below) on an $(\mathscr{X}, R)$ n-class association scheme, you can find the dual association scheme which is an $(\mathscr{X}', R')$ n-class association scheme derived from the valencies, v_i, multiplicities, ψ_i and eigenmatrices, P and Q of the original scheme by

$$v_i' = \psi_i \quad \psi_i' = v_i \quad P' = Q \quad Q' = P.$$

The ability to find a dual is, however, dependent on the scheme being "regular" as defined in [8, Section 2.6.1]. We do not discuss regularity in more detail here as it is beyond the scope of this thesis. In this thesis Delsarte's condition of regularity is met and in fact, since $\mathscr{X}$ is always a vector space, the association schemes we consider here are all translation schemes. That is, if for all $z \in \mathscr{X}$, $i = 0, \dots, n$ we have $(x, y) \in R_i \implies (x + z, y + z) \in R_i$, then it is regular and we can find the scheme's dual. Futhermore we only consider association schemes which are ***formally self dual***, i.e. when $P = Q$. In fact, the association schemes studied in this paper are all metric translation schemes. So when we discuss a code, $\mathscr{C}$ and its dual, $\mathscr{C}^\perp$ in an $(\mathscr{X}, R)$ n-class association scheme, we have $\mathscr{C}, \mathscr{C}^\perp \in \mathscr{X}$.

2.3.3 Metric Association Schemes and Distance Regular Graphs

In this thesis we only consider association schemes that have a distance metric, which confers on the scheme an ordering of the relations.

Definition 2.3.6. For a $(\mathscr{X}, R)$ symmetric n-class association scheme, we define a function $d : \mathscr{X} \times \mathscr{X} \to \mathbb{R}$ with $d(x, y) = i$ whenever $(x, y) \in R_i$ and the function satisfies the following conditions,

$$\begin{aligned} &d(x, y) \geq 0 \\ &d(x, y) = 0 \iff x = y \\ &d(x, y) = d(y, x). \end{aligned}$$

We say the association scheme is ***metric*** if d is a metric on $\mathscr{X}$, i.e. for all $x, y, z \in \mathscr{X}$ we have

$$d(x, y) + d(y, z) \geq d(x, z). \tag{2.3.23}$$

This is equivalent to for $(x, y) \in R_i$, $(y, z) \in R_j$, $(x, z) \in R_k$ we have that for $c_{ijk} \neq 0$, then $k \leq i + j$.

If an association scheme is metric, then we can relate a graph G with it by setting the edges to be $E = \{(x, y) \in R_1\}$ [3, Chapter 1]. A simple example is shown in Figure 2.4.3 in Section 2.4.2 which has 8 codewords over $\mathbb{F}_2^3$.

This graph is known as a distance regular graph and is defined below. For any n-class metric association scheme there is an associated distance regular graph, and vice versa, for every distance regular graph there is an associated n-class metric association scheme.

Definition 2.3.7 ([3, Chapter 1])**.** A ***distance regular graph*** is a graph $G = (V, E)$ in which for any two vertices $x, y \in V$, the number of vertices at distance i from x and j from y depend only on i and j, and the distance between x and y.

Briefly, if we have a distance regular graph, then we define the points of the association scheme to be the vertices and $(x, y) \in R_1$ if there is an edge between x and y. From that, we can say that $(x, z) \in R_i$ if the shortest path between x and z is length i.

So then, the natural question to ask is, can we take any finite set together with a metric and always find a distance regular graph/metric association scheme? Unfortunately this isn't the case, as proven by [55, Theorem 8].

We now define a P-polynomial scheme and conclude that a metric association scheme is a P-polynomial scheme.

Definition 2.3.8 ([41, p660])**.** An association scheme is called a ***P-polynomial*** scheme if there exists non-negative real numbers $z_0, \ldots, z_n$, with $z_0 = 0$ and real polynomials $\Phi_0(z), \ldots, \Phi_k(z)$, where the degree of $\Phi_k(z)$, is k such that

$$p_k(i) = \Phi_k(z_i), \quad i, k = 0, \ldots, n.$$

Theorem 2.3.9 ([8, Theorem 5.6, Theorem 5.16])**.** *An association scheme is metric if and only if it is a P-polynomial scheme, so the eigenvalues of the association scheme, $p_k(i)$, are indeed polynomials.*

Although not proven here, there are multiple ways of proving this statement. One is from MacWilliams and Sloane [41, Theorem 6, Chapter 21], another is from Brouwer [3, Proposition 2.7.1] and originally proved by Delsarte [8, Theorem 5.6, Theorem 5.16].

Considering metric association schemes where $\mathscr{X}$ is a finite dimensional vector space over a finite field and therefore a finite abelian group, we can introduce the concept of an ***inner product***, $\langle\ ,\ \rangle$. More details on how the inner product arises in this situation can be found in [3, p72].

In this situation, given an inner product, and since we have a finite vector space, we can identify a ***dual vector subspace***, $\mathscr{C}^\perp$, for any subspace $\mathscr{C} \subseteq \mathscr{X}$, such that

$$\mathscr{C}^\perp = \Big\{x \in \mathscr{X} \mid \langle x, y\rangle = 0 \ \forall\ y \in \mathscr{C}\Big\}.$$

In this thesis we only consider finite dimensional vector spaces over a finite field, $\mathscr{X}$, so to find the orthogonal points we only need to consider when the inner product is 0 and not involve character theory. We can note that as in Delsarte [9, Section 3] this would be equivalent to the character of the inner product being 1 if the two points are orthogonal.

2.3.4 Generalised Krawtchouk Polynomials

From the orthogonality relations (2.3.18), (2.3.19) we can see the polynomials, $p_k(i)$, form a set of polynomials which take the same form but with a range of parameters which we call a family. For the association schemes studied in this thesis, this family has been shown to be the generalised Krawtchouk Polynomials introduced by Delsarte [11][61].

First we present a notation used by Delsarte [12, p21] called the b-nary Gaussian coefficients. Also note, for ease, we define $\sigma_i = \frac{i(i-1)}{2}$ for $i \geq 0$.

Definition 2.3.10. For $x, k \in \mathbb{Z}^+$, $b \in \mathbb{R}$, $b \neq 1$ the ***b-nary Gaussian coefficients*** are defined as

$$ {}_b\begin{bmatrix} x \\ k \end{bmatrix} = \prod_{i=0}^{k-1} \frac{b^x - b^i}{b^k - b^i} $$

with

$$ {}_b\begin{bmatrix} x \\ 0 \end{bmatrix} = 1. $$

It is useful to note that if we take the limit as b tends to 1, we in fact obtain the usual binomial coefficients,

$$ \begin{aligned} \lim_{b \to 1} \prod_{i=0}^{k-1} {}_b\frac{b^x - b^i}{b^k - b^i} &= \lim_{b \to 1} \prod_{i=0}^{k-1} \frac{(b-1)}{(b-1)} \frac{\left(b^{x-i-1} + b^{x-i-2} + \ldots + 1\right)}{(b^{k-i-1} + \ldots + 1)} \\ &= \prod_{i=0}^{k-1} \frac{x-i}{k-i} \\ &= \binom{x}{k}. \end{aligned} $$

This relationship helps when comparing the similarities between the analysis for the Hamming, the rank, the skew rank and the Hermitian association schemes.

Below are some identities relating to the b-nary Gaussian coefficients which are useful in simplifying notation, and can be used for different values of b from [12]. For $b \in \mathbb{R}/\{1\}$, $x, i, j, k \in \mathbb{Z}^+$, $y \in \mathbb{R}$ we have

$$ {}_b\begin{bmatrix} x \\ k \end{bmatrix} = {}_b\begin{bmatrix} x \\ x-k \end{bmatrix} \tag{2.3.24} $$

$$ {}_b\begin{bmatrix} x \\ i \end{bmatrix} {}_b\begin{bmatrix} x-i \\ k \end{bmatrix} = {}_b\begin{bmatrix} x \\ k \end{bmatrix} {}_b\begin{bmatrix} x-k \\ i \end{bmatrix} \tag{2.3.25} $$

$$ \prod_{i=0}^{x-1} \left(y - b^i\right) = \sum_{k=0}^{x} (-1)^{x-k} b^{\sigma_{x-k}} {}_b\begin{bmatrix} x \\ k \end{bmatrix} y^k \tag{2.3.26} $$

$$ \sum_{k=0}^{x} {}_b\begin{bmatrix} x \\ k \end{bmatrix} \prod_{i=0}^{k-1} \left(y - b^i\right) = y^x \tag{2.3.27} $$

$$ \sum_{k=i}^{j} (-1)^{k-i} b^{\sigma_{k-i}} {}_b\begin{bmatrix} k \\ i \end{bmatrix} {}_b\begin{bmatrix} j \\ k \end{bmatrix} = \delta_{ij} \tag{2.3.28} $$

where δ_{ij} is the Kronecker delta function. The following identities are each used in the rest of this thesis but can be shown trivially to be equal.

$$\begin{aligned}
{}_b\begin{bmatrix}x\\k\end{bmatrix} &= {}_b\begin{bmatrix}x-1\\k\end{bmatrix} + b^{x-k}\,{}_b\begin{bmatrix}x-1\\k-1\end{bmatrix} && (2.3.29)\\
&= {}_b\begin{bmatrix}x-1\\k-1\end{bmatrix} + b^{k}\,{}_b\begin{bmatrix}x-1\\k\end{bmatrix} && (2.3.30)\\
&= \frac{b^{x-k+1}-1}{b^k-1}\,{}_b\begin{bmatrix}x\\k-1\end{bmatrix} && (2.3.31)\\
&= \frac{b^{x}-1}{b^{x-k}-1}\,{}_b\begin{bmatrix}x-1\\k\end{bmatrix} && (2.3.32)\\
&= \frac{b^{x}-1}{b^{k}-1}\,{}_b\begin{bmatrix}x-1\\k-1\end{bmatrix}. && (2.3.33)
\end{aligned}$$

We also define a b-nary beta function which is closely related to the b-nary Gaussian coefficients, and aid us in notation throughout this thesis.

Definition 2.3.11. We define a ***b-nary beta function*** for $x \in \mathbb{R}$, $k \in \mathbb{Z}^+$ as

$$\beta_b(x,k) = \prod_{i=0}^{k-1} {}_b\begin{bmatrix}x-i\\1\end{bmatrix}. \tag{2.3.34}$$

Lemma 2.3.12. *We have for all $x \in \mathbb{R}$, $k \in \mathbb{Z}^+$,*

1.
$$\beta_b(x,k) = {}_b\begin{bmatrix}x\\k\end{bmatrix}\beta_b(k,k) \tag{2.3.35}$$

2.
$$\beta_b(x,x) = {}_b\begin{bmatrix}x\\k\end{bmatrix}\beta_b(k,k)\beta_b(x-k,x-k) \tag{2.3.36}$$

3.
$$\beta_b(x,k)\beta_b(x-k,1) = \beta_b(x,k+1). \tag{2.3.37}$$

Proof. (1) We have

$$\begin{aligned}
\beta_b(x,k) = \prod_{i=0}^{k-1} {}_b\begin{bmatrix}x-i\\1\end{bmatrix} &= \prod_{i=0}^{k-1} \frac{b^{x-i}-1}{b-1}\\
&= \prod_{i=0}^{k-1} \frac{\left(b^{x-i}-1\right)\left(b^{k-i}-1\right)}{\left(b^{k-i}-1\right)(b-1)}\\
&= \prod_{i=0}^{k-1} \frac{b^x-b^i}{b^k-b^i} \prod_{i=0}^{k-1} \frac{b^{k-i}-1}{b-1}\\
&= {}_b\begin{bmatrix}x\\k\end{bmatrix}\beta_b(k,k)
\end{aligned}$$

as required.

(2) Now we have

$$\begin{aligned}
{}_b\begin{bmatrix} x \\ k \end{bmatrix} \beta_b(k,k)\beta_b(x-k,x-k) &= \prod_{i=0}^{k-1} \frac{b^x - b^i}{b^k - b^i} \prod_{r=0}^{k-1} \frac{b^{k-r}-1}{b-1} \prod_{s=0}^{x-k-1} \frac{b^{x-k-s}-1}{b-1} \\
&= \prod_{i=0}^{x-1} \frac{b^{x-i}-1}{b-1} \\
&= \beta_b(x,x)
\end{aligned}$$

as required.

(3) And finally we have,

$$\begin{aligned}
\beta_b(x,k)\beta_b(x-k,1) &= {}_b\begin{bmatrix} x-k \\ 1 \end{bmatrix} \prod_{i=0}^{k-1} {}_b\begin{bmatrix} x-i \\ 1 \end{bmatrix} \\
&= \beta_b(x,k+1).
\end{aligned}$$

□

Now that we have some additional notation, we can write Delsarte's [11, (15)] generalised Krawtchouk polynomials neatly.

Definition 2.3.13. For $b, c \in \mathbb{R}$, $b \geq 1$, $c > \frac{1}{b}$, $n \in \mathbb{Z}^+$ $x, k \in \{0, \ldots, n\}$, then Delsarte's [11] ***generalised Krawtchouk polynomials*** are defined as

$$P_k(x,n) = \sum_{j=0}^{k} (-1)^{k-j} \left(cb^n\right)^j b^{\binom{k-j}{2}} {}_b\begin{bmatrix} n-j \\ n-k \end{bmatrix} {}_b\begin{bmatrix} n-x \\ j \end{bmatrix}. \tag{2.3.38}$$

Again, if we take $b \to 1$, then the generalised Krawtchouk polynomials become the Krawtchouk polynomials in the usual sense. That is, the Hamming Krawtchouk polynomials for $q \geq 2$ are,

$$P_k(x,n) = \sum_{j=0}^{k} (-1)^{k-j} q^j \binom{n-j}{n-k} \binom{n-x}{j}. \tag{2.3.39}$$

We note that equation (2.3.39) is equal to [41, (53), (55), (56)], specifically for obtaining [41, (56)] we use the substitution $j =$ "$k - j$" and rearrange the sum.

Delsarte proved that the eigenvalues of an association scheme satisfy a recurrence relation with specific initial values, namely for $b \in \mathbb{R}^+$, $y \in \mathbb{Z}^+$ and $x, k \in \{0, 1, \ldots, y\}$ the recurrence relation is

$$P_{k+1}(x+1, y+1) = b^{k+1} P_{k+1}(x,y) - b^k P_k(x,y) \tag{2.3.40}$$

with initial values,

$$P_k(0,y) = {}_b\begin{bmatrix} y \\ k \end{bmatrix} \prod_{i=0}^{k-1} \left(cb^y - b^i\right)$$
$$P_0(x,y) = 1,$$

with $c \in \mathbb{R}$, $c > \frac{1}{b}$. He then concluded that the only solution to this recurrence relation with these specific initial values are the generalised Krawtchouk polynomials as defined in Equation (2.3.38).

Delsarte also considers any association scheme to find a relationship between the inner distribution of an association scheme and its dual [8, (6.9)]. Before we do this, we need to introduce some notation.

Definition 2.3.14. Let $(\mathscr{X}, R)$ be an n-class association scheme. The ***inner distribution*** of a subgroup $X \subseteq \mathscr{X}$, is the $(n+1)$-tuple, $\boldsymbol{c} = (c_0, \dots, c_n)$, where c_i is the average number of points of X being i^{th} associates of a fixed point of X.

We note that in this thesis we only consider association schemes where the inner distribution becomes a weight distribution with an associated metric.

Theorem 2.3.15 (The MacWilliams Identity for Association Schemes)**.** *Let $(\mathscr{X}, R)$ be an n-class association scheme with dual n-class association scheme $(\mathscr{X}, R')$. For a pair of dual subgroups $X, X' \subseteq \mathscr{X}$, let $\mathbf{c} = (c_0, \dots, c_n)$ be the inner distribution of X and $\mathbf{c'} = (c'_0, \dots c'_n)$ be the inner distribution of X'. If P and Q are the eigenmatrices of $(\mathscr{X}, R)$ then*

$$|X|\boldsymbol{c'} = \boldsymbol{c}Q$$
$$|X'|\boldsymbol{c} = \boldsymbol{c'}P.$$

2.4 The Hamming Association Scheme

2.4.1 Introduction, Background and Jessie MacWilliams

Richard Hamming invented the first error-correcting code, where the distance between two codewords is the number of places where they differ. This distance metric is now known as the Hamming metric. The Hamming metric has been extensively used since its conception in 1950, initially alongside a binary code where each word has a fixed length and each position is 0 or 1. One example of a code that was implemented successfully using the Hamming metric was the Golay Code [26], a $[24, 12, 8]$-code, which transmitted one of the first few "mosaics" of the planet Jupiter, pictured in Figure 2.4.1, from the Voyager 1 spacecraft. It is comprised of nine separate photographs taken from around 4.7 million miles away from Jupiter itself.

Jessie MacWilliams contributed much into the study of coding theory and most importantly, alongside Neil Sloane, identified the well known MacWilliams Identity that relates the weight enumerator of a code to that of its dual using a functional transformation.

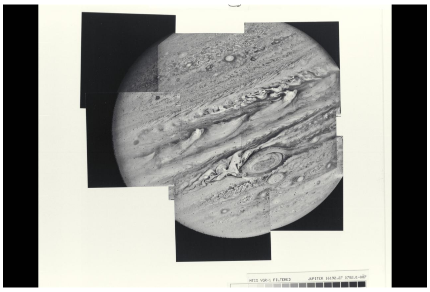

Figure 2.4.1: Mosaic of Jupiter as seen by Voyager 1 [33]

2.4.2 Preliminaries

To introduce the well known Hamming scheme we first must summarise some definitions and properties.

Definition 2.4.1. For all $\boldsymbol{a} = (a_1, \ldots, a_n), \boldsymbol{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$, we define the ***Hamming distance*** between $\boldsymbol{a}$ and $\boldsymbol{b}$ to be

$$d_H(\boldsymbol{a}, \boldsymbol{b}) = |\{i \mid a_i \neq b_i\}|.$$

In other words, the number of entries in the vectors which differ.

Any subspace of $\mathbb{F}_q^n$ can be considered as an $\mathbb{F}_q$-linear code, $\mathscr{C}$.

The ***minimum Hamming distance*** of such a code $\mathscr{C}$, denoted as $d_H(\mathscr{C})$, is simply the minimum Hamming distance over all possible pairs of distinct codewords in $\mathscr{C}$. When there is no ambiguity about $\mathscr{C}$, we denote the minimum Hamming distance as d_H. It is common in the literature for the Hamming metric to denote the minimum distance as d when there is no ambiguity on the distance metric. If the dimension of the subspace (code) is k, then the code is referred to as a $[n, k, d_H]$-code.

To illustrate the idea of error correction more clearly in the Hamming scheme, we introduce the concept of spheres around each codeword.

Definition 2.4.2. A ***ball***, of radius $r \in \mathbb{Z}$, $r \leq n$, about a point $a \in \mathbb{F}_q^n$, is

$$B_r(a) = \{b \in \mathbb{F}_q^n \mid d(a, b) \leq r\}.$$

So the ball about a contains all the possible words that differ from a by up to r places.

If the number of errors is less than half of the minimum distance then it is guaranteed that, in theory at least, the original intended codeword can be identified and corrected. The two different situations when d_H is odd and when d_H is even are illustrated in Figure 2.4.2. If $d_H = 2m$ then $d_H - 1$ errors can be detected but only $m - 1$ errors can be corrected; if $d_H = 2m + 1$ then $2m$ errors can be detected and m errors corrected.

More formally,

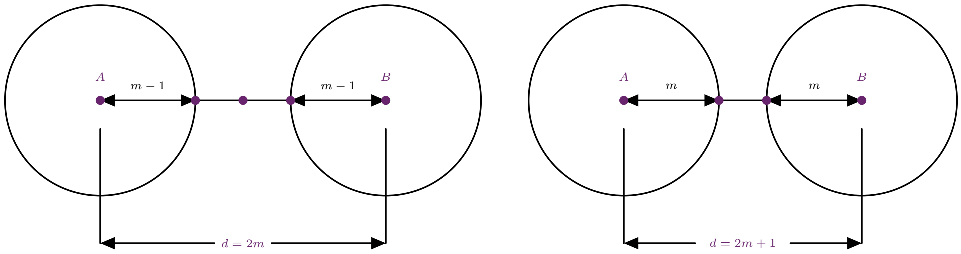

Figure 2.4.2: Balls of radius $\lfloor \frac{d_H-1}{2} \rfloor$.

Theorem 2.4.3 ([50, Theorem 2, Chapter 1])**.** *A code C with minimum distance d_H can detect up to $d_H - 1$ errors and correct up to $r = \lfloor \frac{d_H-1}{2} \rfloor$ errors.*

Proof. Suppose that is not the case, so there exists two codewords $a, b \in \mathbb{F}_q^n$ such that $B_r(a) \cap B_r(b) \neq \emptyset$. Then there exists $c \in B_r(a) \cap B_r(b)$ such that $d_H(a, c) \leq r$ and $d(b, c) \leq r$. So

$$d_H(a, b) \leq d_H(a, c) + d_H(c, b) \leq 2r \leq d_H - 1$$

which is a contradiction of minimum distance. □

Now a weight enumerator for the Hamming metric is introduced which records the number of codewords of each weight in a code.

Definition 2.4.4. For all $\boldsymbol{a} \in \mathbb{F}_q^n$ the ***Hamming weight***, w is the number of non-zero entries in $\boldsymbol{a}$. It is clear that if $\mathscr{C} \subseteq \mathbb{F}_q^n$ is a linear code then the ***minimum Hamming weight*** of $\mathscr{C}$ is d_H. Then ***Hamming weight function*** of $\boldsymbol{a}$ is defined as the homogeneous polynomial

$$f_H(\boldsymbol{a}) = Y^w X^{n-w}.$$

Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a code. Suppose there are c_i codewords in $\mathscr{C}$ with Hamming weight i for $0 \leq i \leq n$. Then the ***Hamming weight enumerator*** of $\mathscr{C}$, denoted as $W_{\mathscr{C}}^H(X, Y)$, is defined to be

$$W_{\mathscr{C}}^H(X, Y) = \sum_{\boldsymbol{a} \in \mathscr{C}} f_H(\boldsymbol{a}) = \sum_{i=0}^{n} c_i Y^i X^{n-i}. \tag{2.4.1}$$

We call the $(n+1)$-tuple, $\boldsymbol{c} = (c_0, \ldots, c_n)$ of coefficients of the Hamming weight enumerator, the ***Hamming weight distribution*** of the code $\mathscr{C}$.

Example 2.4.5. A simple example to look at is the well known Hamming code of length

7, explicitly written out below.

$$\left\{\begin{array}{l}(0,0,0,0,0,0,0),(0,0,0,1,1,0,1),(0,0,1,0,1,1,1),(0,0,1,1,0,1,0)\\(0,1,0,0,0,1,1),(0,1,0,1,1,1,0),(0,1,1,0,1,0,0),(0,1,1,1,0,0,1)\\(1,0,0,0,1,1,0),(1,0,0,1,0,1,1),(1,0,1,0,0,0,1),(1,0,1,1,1,0,0)\\(1,1,0,0,1,0,1),(1,1,0,1,0,0,0),(1,1,1,0,0,1,0),(1,1,1,1,1,1,1)\end{array}\right\}$$

There are 16 codewords in total and it forms a 4-dimensional subspace of $\mathbb{F}_2^7$. There is 1 codeword of weight 0, 7 of weight 3, 7 of weight 4 and 1 of weight 7. Thus the weight enumerator is $X^7 + 7Y^3X^4 + 7Y^4X^3 + Y^7$. This example is shown with other details in Appendix A.1.

The number of vectors in $\mathbb{F}_q^n$ of Hamming weight w is $(q-1)^w\binom{n}{w}$. The total number of vectors in $\mathbb{F}_q^n$ is q^n. So the ***Hamming weight enumerator*** of $\mathbb{F}_q^n$ is

$$\Omega_n = \sum_{i=0}^{n}(q-1)^i\binom{n}{i}Y^iX^{n-i}. \tag{2.4.2}$$

Some more examples can be found in Appendix A.1 which give a general idea of a code and its properties.

To be able to define a dual code in this association scheme, we first need an inner product. For the Hamming association scheme we take the usual scalar product.

Definition 2.4.6. The ***dual code***, $\mathscr{C}^\perp \subseteq \mathbb{F}_q^n$, of a code, $\mathscr{C} \subseteq \mathbb{F}_q^n$, is defined as

$$\mathscr{C}^\perp = \Big\{\boldsymbol{a} \in \mathbb{F}_q^n \mid \boldsymbol{a}\cdot\boldsymbol{b} = 0 \;\forall\; \boldsymbol{b} \in \mathscr{C}\Big\}.$$

2.4.3 Eigenvalues of the Hamming Association Scheme

MacWilliams and Sloane claim that the most important example for coding theory is the Hamming or "hypercubic" association scheme [41, Chapter 1, Section 3]. A frequently used clear example of the association scheme with $n = 3$ and $q = 2$ can be seen in Figure 2.4.3.

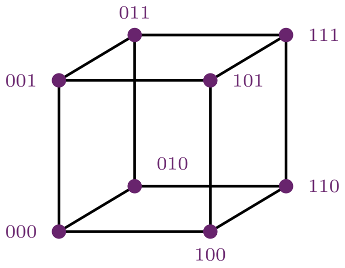

Figure 2.4.3: Distance regular graph of a Hamming Scheme with $q = 2$ and $n = 3$.

Explicitly, we have the $(\mathscr{X}, R)$ n-class Hamming association scheme where $\mathscr{X} = \mathbb{F}_q^n$ and $R_i = \{(x,y) \mid d_H(x,y) = i\}$, and is a metric association scheme as the triangle inequality holds for the Hamming distance. In this scheme, the eigenvalues are defined as

$$p_k(i) = P_k(i,n)$$

where $P_k(i,n)$ are the Hamming Krawtchouk polynomials (2.3.39).

2.4.4 MacWilliams Identity as a Functional Transform

Here we introduce the seminal result for relating the weight enumerator of a code with the weight enumerator of the code's dual for the Hamming association scheme, developed by Jessie MacWilliams.

Theorem 2.4.7 (The MacWilliams Identity for the Hamming Scheme)**.** *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be an $[n,k,d_H]$-linear code, with Hamming weight distribution $\mathbf{c} = (c_0,\ldots,c_n)$ and $\mathscr{C}^\perp \subseteq \mathbb{F}_q^n$ its dual code, with Hamming weight distribution $\mathbf{c'} = (c'_0,\ldots,c'_n)$. Then*

$$W^H_{\mathscr{C}^\perp}(X,Y) = \frac{1}{|\mathscr{C}|} W^H_{\mathscr{C}}\left(X+(q-1)Y, X-Y\right). \tag{2.4.3}$$

The proof of the MacWilliams Identity for the Hamming association scheme uses character theory and the Hadamard transform, and can be found at [41, Theorem 13, p146]. The theorem above can also equivalently be written as

$$\sum_{i=0}^{n} c'_i Y^i X^{n-i} = \frac{1}{|\mathscr{C}|} \sum_{i=0}^{n} c_i (X-Y)^i (X+(q-1)Y)^{n-i}. \tag{2.4.4}$$

2.4.5 Moments of the Hamming Weight Distribution

MacWilliams and Sloane then investigate the weights of a code further by looking at their binomial moments. We follow their analysis in the general case here and show the example for the binary case at the end. These moments are calculated so that statistical data about the weights within a code can be used to give insight into details of the code such as the spread, centering and skewness.

Theorem 2.4.8. *For an $[n,k,d_H]-$linear code, $\mathscr{C} \in \mathbb{F}_q^n$, with weight distribution $\mathbf{c} = (c_0,\ldots,c_n)$, and dual code $\mathscr{C}^\perp$ with weight distribution $\mathbf{c'} = (c'_0 \ldots, c'_n)$, the binomial moments of the Hamming weight distribution are, for all $\varphi \in \{0,\ldots,n\}$,*

$$\sum_{i=0}^{n-\varphi} \binom{n-i}{\varphi} c_i = q^{k-\varphi} \sum_{i=0}^{n} \binom{n-i}{n-\varphi} c'_i \tag{2.4.5}$$

and

$$\sum_{i=\varphi}^{n} \binom{i}{\varphi} c_i = q^{k-\varphi} \sum_{i=0}^{\varphi} (-1)^i (q-1)^{\varphi-i} \binom{n-i}{n-\varphi} c'_i. \tag{2.4.6}$$

Proof. MacWilliams herself used two different methods to derive these moments. The first used set theory and combinatorics and the other used character theory [38].

First we prove (2.4.5). We extend the idea of the proof in [41, p131] in the case where $q = 2$, for general prime powers, q, using differentiation and the Leibniz Rule, to illustrate that the later proofs presented in this thesis can also be applied here. We have directly from (2.4.4), applied to the dual code,

$$\sum_{i=0}^{n} c_i Y^i X^{n-i} = \frac{1}{q^{n-k}} \sum_{i=0}^{n} c_i'(X-Y)^i \left(X+(q-1)Y\right)^{n-i}.$$

To anticipate the proofs in Chapters 3 and 4 we use the notation (φ) for differentiation with respect to X and $\{\varphi\}$ for differentiation with respect to Y. So on the LHS we take the φ^{th} derivative with respect to X.

$$\left(\sum_{i=0}^{n} c_i Y^i X^{n-i}\right)^{(\varphi)} = \varphi! \sum_{i=0}^{n-\varphi} \binom{n-i}{\varphi} c_i Y^i X^{n-i-\varphi}.$$

The RHS is slightly more complicated. Again we take the derivative but we need to use the Leibniz Rule in order to do so.

$$\begin{aligned}
&\left(\frac{1}{q^{n-k}} \sum_{i=0}^{n} c_i' \; (X-Y)^i \left(X+(q-1)Y\right)^{n-i}\right)^{(\varphi)} \\
&\qquad = \frac{1}{q^{n-k}} \sum_{i=0}^{n} \sum_{k=0}^{\varphi} c_i' \binom{\varphi}{k} \left((X-Y)^i\right)^{(\varphi-k)} \left((X+(q-1)Y)^{n-i}\right)^{(k)} \\
&\qquad = \frac{1}{q^{n-k}} \sum_{i=0}^{n} \sum_{k=0}^{\varphi} c_i' \binom{\varphi}{k} \frac{(n-i)!}{(n-i-k)!} \frac{i!}{(i-\varphi+k)!} \\
&\qquad\qquad \times (X-Y)^{i-\varphi+k}(X+(q-1)Y)^{n-i-k}.
\end{aligned}$$

Now evaluate at $X = Y = 1$, which means that all terms are 0 except when, $i - \varphi + k = 0$ so,

$$\begin{aligned}
\left(\frac{1}{q^{n-k}} \sum_{i=0}^{n} c_i'(X-Y)^i \left(X+(q-1)Y\right)^{n-i}\right)^{(\varphi)} &= \frac{1}{q^{n-k}} \sum_{i=0}^{n} c_i' \binom{\varphi}{\varphi-i} \frac{(n-i)!}{(n-\varphi)!} \frac{i!}{(0)!} q^{n-\varphi} \\
&= \frac{1}{q^{n-k}} \sum_{i=0}^{n} c_i' \varphi! \binom{n-i}{n-\varphi} q^{n-\varphi}.
\end{aligned}$$

Now equating the LHS and RHS we obtain,

$$\varphi! \sum_{i=0}^{n-\varphi} \binom{n-i}{\varphi} c_i = \frac{1}{q^k} \sum_{i=0}^{n} c_i' \varphi! \binom{n-i}{n-\varphi} q^{n-\varphi}.$$

Therefore,

$$\sum_{i=0}^{n-\varphi} \binom{n-i}{\varphi} c_i = q^{k-\varphi} \sum_{i=0}^{n} \binom{n-i}{n-\varphi} c_i'.$$

Now we prove (2.4.6). Differentiating with respect to Y we have,

$$\left(\sum_{i=0}^{n} c_i Y^i X^{n-i}\right)^{\{\varphi\}} = \varphi! \sum_{i=\varphi}^{n} \binom{i}{\varphi} c_i Y^{i-\varphi} X^{n-i}.$$

Again the RHS is more complicated. We take a similar approach and use the Leibniz Rule, again with respect to Y.

$$\begin{aligned}
&\left(\frac{1}{q^{n-k}} \sum_{i=0}^{n} c_i' \ (X-Y)^i \, (X+(q-1)Y)^{n-i}\right)^{\{\varphi\}} \\
&\qquad = \frac{1}{q^{n-k}} \sum_{i=0}^{n} \sum_{k=0}^{\varphi} c_i' \binom{\varphi}{k} \left((X-Y)^i\right)^{\{\varphi-k\}} \left((X+(q-1)Y)^{n-i}\right)^{\{k\}} \\
&\qquad = \frac{1}{q^{n-k}} \sum_{i=0}^{n} \sum_{k=0}^{\varphi} c_i' (-1)^{\varphi-k} (q-1)^k \binom{\varphi}{k} \frac{(n-i)!}{(n-i-k)!} \frac{i!}{(i-\varphi+k)!} \\
&\qquad\qquad \times (X-Y)^{i-\varphi+k} (X+(q-1)Y)^{n-i-k}.
\end{aligned}$$

Now evaluate at $X = Y = 1$, which means that all terms are 0 except when, $i - \varphi + k = 0$ so,

$$\begin{aligned}
\left(\frac{1}{q^{n-k}} \sum_{i=0}^{n} c_i' (X-Y)^i \, (X+(q-1)Y)^{n-i}\right)^{\{\varphi\}} &= \frac{1}{q^{n-k}} \sum_{i=0}^{\varphi} c_i' (-1)^i (q-1)^{\varphi-i} \binom{\varphi}{\varphi-i} \\
&\qquad \times \frac{(n-i)!}{(n-\varphi)!} \frac{i!}{(0)!} q^{n-\varphi} \\
&= \frac{1}{q^{n-k}} \sum_{i=0}^{\varphi} c_i' (-1)^i (q-1)^{\varphi-i} \varphi! \binom{n-i}{n-\varphi} q^{n-\varphi}.
\end{aligned}$$

Now equating the LHS and RHS we obtain,

$$\varphi! \sum_{i=\varphi}^{n} \binom{i}{\varphi} c_i = \frac{1}{q^{n-k}} \sum_{i=0}^{\varphi} c_i' (-1)^i (q-1)^{\varphi-i} \varphi! \binom{n-i}{n-\varphi} q^{n-\varphi}.$$

Therefore,

$$\sum_{i=\varphi}^{n} \binom{i}{\varphi} c_i = q^{k-\varphi} \sum_{i=0}^{\varphi} (-1)^i (q-1)^{\varphi-i} \binom{n-i}{n-\varphi} c_i'.$$

□

We can in fact simplify Theorem 2.4.8 if φ is less than the minimum distance of the dual code.

Corollary 2.4.9. *Let d_H' be the minimum Hamming distance of $\mathscr{C}^\perp$. If $0 \le \varphi < d_H'$ then*

$$\sum_{i=0}^{n-\varphi} \binom{n-i}{\varphi} c_i = q^{k-\varphi} \binom{n}{\varphi} \tag{2.4.7}$$

and

$$\sum_{i=\varphi}^{n} \binom{i}{\varphi} c_i = q^{k-\varphi}(q-1)^{\varphi}\binom{n}{\varphi}. \tag{2.4.8}$$

Proof. Since $0 \leq \varphi < d'_H$ then $c'_0 = 1$ and $c'_1 = c'_2 = \ldots = c'_\varphi = 0$ and the corollary follows. □

Example 2.4.10. Consider the case where $q = 2$. When $\varphi = 0$, then using (2.4.6)

$$\sum_{i=0}^{n} c_i = 2^k c'_0 = 2^k$$

as expected. Setting $\varphi = 1$, we have

$$\begin{aligned}\sum_{i=1}^{n} i c_i &= 2^{k-1}\sum_{i=0}^{1}(-1)^i\binom{n-i}{n-1}c'_i \\ &= \frac{2^k}{2}\left(n - c'_1\right)\end{aligned}$$

So if $c'_1 = 0$ i.e. the minimum distance of the dual is greater than 1 then,

$$\sum_{i=1}^{n} \frac{i c_i}{2^k} = \frac{n}{2}$$

the average, as expected. Now if we consider $\varphi = 2$ we have,

$$\begin{aligned}\sum_{i=2}^{n}\binom{i}{2}c_i &= 2^{k-2}\sum_{i=0}^{2}(-1)^i(2-1)^{2-i}\binom{n-i}{n-2}c'_i \\ &= 2^{k-2}\left(\frac{n(n-1)}{2}c'_0 - (n-1)c'_1 + c_2\right).\end{aligned}$$

So if $c'_1 = c'_2 = 0$ i.e. the minimum distance of the dual is greater than 2 then,

$$\sum_{i=0}^{n}\frac{i(i-1)}{2}c_i = 2^{k-2}\frac{n(n-1)}{2}.$$

Thus from the average above we have,

$$\sum_{i=0}^{n}\frac{i^2 c_i}{2^k} - \sum_{i=0}^{n}\frac{i c_i}{2^k} = \sum_{i=0}^{n}\frac{i^2 c_i}{2^k} - \frac{n}{2} = \frac{1}{4}n(n-1),$$

Simplifying gives

$$\sum_{i=0}^{n}\frac{i^2 c_i}{2^k} = \frac{1}{4}n(n+1),$$

the second moment of the code.

2.4.6 Maximum Distance Separable Codes

Codes that attain the Singleton Bound (2.4.9) are called Maximum Distance Separable (MDS) codes, which for an $[n, k, d_H]$-code means that $d_H = n - k + 1$. MDS codes have been studied extensively since they offer the maximum potential efficiency for a given rate of error correction. Surprisingly the Hamming weight distribution is completely determined by its parameters, which is also presented in, for example, [41, Theorem 6, Chapter 11]. In this section we derive those parameters using the MacWilliams Identity and moments of the Hamming association scheme in a manner that we then extend to the skew rank association scheme (Section 3.5) and the Hermitian rank association scheme (Section 4.5). First we shall state and prove the Singleton bound and we also need a little lemma.

Theorem 2.4.11 (The Singleton Bound for the Hamming Metric)**.** *If $\mathscr{C} \subseteq \mathbb{F}_q^n$ is a linear $[n, k, d_H]$-code then,*

$$|\mathscr{C}| \leq q^{n-d_H+1}. \tag{2.4.9}$$

Codes that attain the Singleton bound are referred to as maximal codes or Maximum Distance Separable (MDS) codes.

Proof. First we note that the number of codewords in $\mathbb{F}_q^n$ is q^n. Now since every codeword in $\mathscr{C}$ is distinct, and deleting each $d_H - 1$ first letters of each codeword, then all pairs of resulting codewords must be distinct as the minimum distance between the original codewords is d_H. Since the length of each word is $n - d_H + 1$ then there are at most q^{n-d_H+1} words. Therefore $|\mathscr{C}| \leq q^{n-d_H+1}$. Furthermore, since $\mathscr{C}$ is a linear $[n, k, d_H]$-code, then $q^k \leq q^{n-d_H+1}$ we also have $n - k \geq d_H - 1$. □

We follow on with a useful lemma. Equivalent theorems are stated and proved in Sections 3.5.3 and 4.5.3.

Lemma 2.4.12. *If $a_0, a_1, \ldots, a_\ell$ and $b_0, b_1, \ldots, b_\ell$ are two sequences of real numbers and if*

$$a_j = \sum_{i=0}^{j} \binom{\ell - i}{\ell - j} b_i$$

for $0 \leq j \leq \ell$, then

$$b_i = \sum_{j=0}^{i} (-1)^{i-j} \binom{\ell - j}{\ell - i} a_j \tag{2.4.10}$$

for $0 \leq i \leq \ell$.

Proof. This result uses the property of binomial coefficients (2.3.28), that

$$\sum_{k=i}^{j} (-1)^{k-i} \binom{k}{i} \binom{j}{k} = \delta_{ij}.$$

Then for $0 \leq i \leq \ell$,

$$\begin{aligned}
\sum_{j=0}^{i}(-1)^{i-j}\binom{\ell-j}{\ell-i}a_j &= \sum_{j=0}^{i}(-1)^{i-j}\binom{\ell-j}{\ell-i}\left(\sum_{k=0}^{j}\binom{\ell-k}{\ell-j}b_k\right) \\
&= \sum_{k=0}^{i}\sum_{j=k}^{i}(-1)^{i-j}\binom{\ell-j}{\ell-i}\binom{\ell-k}{\ell-j}b_k \\
&= \sum_{k=0}^{i}b_k\left(\sum_{s=\ell-i}^{\ell-k}(-1)^{i-\ell+s}\binom{s}{\ell-i}\binom{\ell-k}{s}\right) \\
&\overset{(2.3.28)}{=} \sum_{k=0}^{i}b_k\delta_{(\ell-i)(\ell-k)} = \sum_{k=0}^{i}b_k\delta_{ik} \\
&= b_i
\end{aligned}$$

as required. □

We also have the following theorem which is used in the proof of 2.4.14.

Theorem 2.4.13 ([41, Theorem 2, p318])**.** *If a linear $[n,k,d_H]$-code $\mathscr{C} \subseteq \mathbb{F}_q^n$ is MDS, then its dual $\mathscr{C}^\perp \subseteq \mathbb{F}_q^n$ is also MDS and is a linear $[n, n-k, k+1]$-code.*

It is interesting to note that the weight distribution of an MDS code is only dependent on the parameters n, k, d_H and not on the particular choice of the code.

Proposition 2.4.14 ([41, Theorem 6, Chapter 11])**.** *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear MDS code with weight distribution $\boldsymbol{c}$, and minimum distance d_H. Then we have $c_0 = 1$ and for $0 \leq r \leq n - d_H$,*

$$c_{d_H+r} = \sum_{i=0}^{r}(-1)^{r-i}\binom{d_H+r}{d_H+i}\binom{n}{d_H+r}\left(q^{i+1}-1\right).$$

Proof. The proof of this statement is left as an exercise for the reader in [41], so we have the proof here instead. We have from Corollary 2.4.9, for $0 \leq \varphi < d'_H$,

$$\sum_{i=0}^{n-\varphi}\binom{n-i}{\varphi}c_i = q^{k-\varphi}\binom{n}{\varphi}.$$

Now if a linear code $\mathscr{C}$ is MDS, with minimum distance d_H then $\mathscr{C}^\perp$ is also MDS with minimum distance $d'_H = n - d_H + 2$ [41, Theorem 2, Chapter 11]. So (2.4.7) holds for $0 \leq \varphi \leq n - d_H = d'_H - 2$. We note that the proposition so far holds for $\varphi \leq d'_H - 1$ but $d'_H - 2$ is sufficient here. We therefore have $c_0 = 1$ and $c_1 = c_2 = \ldots = c_{d_H-1} = 0$ and setting $\varphi = n - d_H - j$ for $0 \leq j \leq n - d_H$ we obtain

$$\binom{n}{n-d_H-j} + \sum_{i=d_H}^{d_h+j} \binom{n-i}{n-d_H-j} c_i = q^{k-n+d_H+j} \binom{n}{n-d_H-j}$$

$$\sum_{r=0}^{j} \binom{n-d_H-r}{n-d_H-j} c_{r+d_H} = \binom{n}{n-d_H-j} \left(q^{k-n+d_H+j} - 1\right).$$

Applying Lemma 2.4.12, setting $\ell = n - d_H$ and $b_r = c_{r+d_H}$ then letting

$$a_j = \binom{n}{n-d_H-j} \left(q^{k-n+d_H+j} - 1\right)$$

gives

$$\sum_{r=0}^{j} \binom{n-d_H-r}{n-d_H-j} b_r = a_j$$

and so

$$\begin{aligned} b_r = c_{r+d_H} &\overset{(2.4.10)}{=} \sum_{i=0}^{r} (-1)^{r-i} \binom{n-d_H-i}{n-d_H-r} a_i \\ &= \sum_{i=0}^{r} (-1)^{r-i} \binom{n-d_H-i}{n-d_H-r} \binom{n}{n-d_H-i} \left(q^{k-n+d_H+i} - 1\right). \end{aligned}$$

But we have

$$\begin{aligned} \binom{n-d_H-i}{n-d_H-r} \binom{n}{n-d_H-i} &\overset{(2.3.24)}{=} \binom{n-(d_H+i)}{n-(d_H+r)} \binom{n}{d_H+i} \\ &\overset{(2.3.25)}{=} \binom{d_H+r}{d_H+i} \binom{n}{n-(d_H+r)} \\ &\overset{(2.3.24)}{=} \binom{d_H+r}{d_H+i} \binom{n}{d_H+r}. \end{aligned}$$

Therefore

$$c_{r+d_H} = \sum_{i=0}^{r} (-1)^{r-i} \binom{d_H+r}{d_H+i} \binom{n}{d_H+r} \left(q^{i+1} - 1\right)$$

since $d_H = n - k + 1$ as $\mathscr{C}$ is MDS, as required. □

2.5 The Rank Association Scheme

2.5.1 Introduction and Background

In the search for an improved error-correcting code to use as the base for a new cryptosystem, changing the alphabet is just one choice that can be made. Another choice is the metric used to measure the distance between any two words in the code. Traditionally that has been the Hamming metric as mentioned.

Gabidulin [18] prepared a whole list of different metrics. One was the rank metric which was first proposed for use in error-correcting codes by Delsarte in 1975 [9] and further developed by Gabidulin himself in 1985 [21]. The approaches of Gabidulin and Delsarte are described and compared in Section 2.5.2 below.

McEliece type cryptosystems have been proposed based on rank metric codes [20],[48] and in particular on Maximum Rank Distance (MRD) linear codes because they have efficient decoding algorithms and much smaller public keys than comparable Hamming metric systems [22]. Unfortunately, some MRD codes have significant invariant subspaces which make them vulnerable to attack [37] and they have been broken in original and modified forms. The challenge is still there, though, to find secure cryptosystems based on rank metric codes because of their smaller public keys and, for example, Loidreau [37] has proposed more recently yet another variation which is claimed to be secure, by scrambling the Gabidulin structures sufficiently.

Less research has been applied to the corresponding identities for rank metric codes. Delsarte [9] did find relations between the rank weights of a code and its dual using association schemes but it was Gadouleau and Yan [22] who found the rank weight enumerator of a linear code [21] as a functional transformation of the rank weight enumerator of its dual. Ravagnani [51] generalised the proof to all Delsarte rank metric codes and established that all linear codes can be regarded as a "Delsarte rank metric code". Gadouleau and Yan [22] used a method of proof similar to MacWilliams and Sloane [41] whereas Ravagnani [51] focused on the linear algebra and combinatoric approach.

Consequently, it seems that there is value in exploring further codes based on the rank metric. To explore this further it is first necessary to understand in detail the theories used in Delsarte [9] and Gadouleau and Yan [22]. These theories are outlined in this section, 2.5.

2.5.2 Delsarte, Gabidulin, Gadouleau and Yan

Delsarte and Gabidulin developed two distinct definitions of the codes with the rank metric. Delsarte [9] worked with $m \times n$ arrays or matrices over $\mathbb{F}_q$ whereas Gabidulin [21] used vector subspaces of $\mathbb{F}_{q^m}^n$.

Gabidulin [20] gives a useful summary and comparison of the two representations and shows that all linear vector representation codes can be mapped onto a linear matrix representation code. (Note that a linear matrix code mapped in the other direction to a vector code is not necessarily linear [20, Section 2]). In [21] he specifies a norm on the space of matrices, which defines the rank metric, and goes on to develop theories for codes (subspaces) based on the rank distance. He also investigates the characteristics of maximal codes and their constructions. Ravagnani [51] further proved that the mapping from vector to matrix preserves cardinality and rank distribution and that therefore matrix rank metric codes can be considered as a generalisation of vector rank metric codes.

Delsarte [9] introduces codes based on a rank metric by considering matrices of a certain size over a finite field. Identifying a bijection between matrices and bilinear forms, Delsarte applies his theory of association schemes to rebuild the MacWilliams Identity for codes with the rank metric.

Gadouleau and Yan [22] extended the known theories of rank metric codes by developing the MacWilliams Identity as a functional transform in the same way as MacWilliams did originally for the Hamming metric. Having a version of this theorem in this form allows weight enumerators of potentially unknown dual codes to be found from the weight enumerators of known codes. They subsequently used the functional transform to develop previously undiscovered identities between the moments of the rank weight distribution of codes and their duals. Their method was based on character theory and q-algebra rather than association schemes or combinatorics as used by Delsarte [9] and Grant and Varanasi [29] [28]. Finally from these new identities, called "moments of the rank distribution", the rank weight distribution of maximal codes in this setting is derived as an alternative to Delsarte's [9] and Gabidulin's [21] derivation.

Below are the key definitions and results for the two representations of rank metric codes. Notation in the different sources varies so the notation of Gadouleau and Yan [22] has been adopted here where possible for consistency with their later proofs, but material from Gabidulin [20], [21] and Ravagnani [51] has been used.

2.5.3 Preliminaries

The definitions below are equivalent to the theory in Gadouleau and Yan [22], but have been adapted to match this interpretation of the underlying space.

Definition 2.5.1. Let $\boldsymbol{A} = (a_{ij})$ be a matrix of size $m \times n$ with entries in a finite field $\mathbb{F}_q$ where q is a prime power. This could be represented as an n-dimensional vector,

$$\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$$

where for $i = 1, \ldots, n$, $x_i = \displaystyle\sum_{j=1}^{m} a_{ij}\alpha_j$ with $\{\alpha_1, \ldots, \alpha_m\}$ being a basis of $\mathbb{F}_{q^m}$

Each matrix, $\boldsymbol{A}$, can be associated with a corresponding bilinear form, which is a map

$$\boldsymbol{A}:\ V \times W \to \mathbb{F}_q$$

where V is an m-dimensional vector space over $\mathbb{F}_q$ with fixed basis $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_m\}$, W is an n-dimensional vector space over $\mathbb{F}_q$ with fixed basis $\{\boldsymbol{e}'_1, \boldsymbol{e}'_2, \ldots, \boldsymbol{e}'_n\}$ where

$$\boldsymbol{A}\left(\boldsymbol{e}_i, \boldsymbol{e}'_j\right) = a_{ij}.$$

Definition 2.5.2. For all $\boldsymbol{A} \in \mathbb{F}_q^{m\times n}$ we define the ***rank weight*** of $\boldsymbol{A}$, $R(\boldsymbol{A}) = r$, to be the usual column rank of the matrix over $\mathbb{F}_q$. For all $\boldsymbol{A}, \boldsymbol{B} \in \mathbb{F}_q^{m\times n}$, we define the ***rank***

distance between $\boldsymbol{A}$ and $\boldsymbol{B}$ to be

$$d_R(\boldsymbol{A}, \boldsymbol{B}) = R(\boldsymbol{A} - \boldsymbol{B}).$$

Any subspace of $\mathbb{F}_q^{m\times n}$ can be considered as an $\mathbb{F}_q$-linear code, $\mathscr{C}$, with each matrix of rank r in $\mathscr{C}$ representing a codeword of weight r and with the distance metric being the rank metric. That is, for $\boldsymbol{A}, \boldsymbol{B} \in \mathbb{F}_q^{m\times n}$ and $a, b \in \mathbb{F}_q$, $a\boldsymbol{A}+b\boldsymbol{B} \in \mathscr{C}$. For clarity, the rank distance must always be less than the minimum of $\{m, n\}$ as the column rank must be less than or equal to n, the row rank must be less than or equal to m and the column rank and row rank must be the same, a common result of linear algebra.

The ***minimum rank distance*** of such a code $\mathscr{C}$, denoted as $d_R(\mathscr{C})$, is simply the minimum rank distance over all possible pairs of distinct codewords in $\mathscr{C}$. When there is no ambiguity about $\mathscr{C}$, we denote the minimum rank distance as d_R.

As with the Hamming metric, bounds can be established [22, (1)] on the maximum size of a code $\mathscr{C}$ over $\mathbb{F}_q^{m\times n}$ with minimum rank distance d_R given by

$$|\mathscr{C}| \leq \min\left\{q^{m(n-d_R+1)}, q^{n(m-d_R+1)}\right\}. \tag{2.5.1}$$

We call the bound (2.5.1) the Singleton bound for codes with the rank metric. Codes that attain the Singleton bound are referred to as maximal codes or Maximum Rank Distance (MRD) codes.

Again, similar to the Hamming metric, we introduce a weight enumerator for the rank metric to count the number of codewords of each weight.

Definition 2.5.3. For all $\boldsymbol{A} \in \mathbb{F}_q^{m\times n}$ with rank weight r, the ***rank weight function*** of $\boldsymbol{A}$ is defined as the homogeneous polynomial

$$f_R(\boldsymbol{A}) = Y^r X^{n-r}.$$

Let $\mathscr{C} \subseteq \mathbb{F}_q^{m\times n}$ be a code. Suppose there are c_i codewords in $\mathscr{C}$ with rank weight i for $0 \leq i \leq n$. Then the ***rank weight enumerator*** of $\mathscr{C}$, denoted as $W_{\mathscr{C}}^R(X, Y)$, is defined to be

$$W_{\mathscr{C}}^R(X, Y) = \sum_{\boldsymbol{A}\in\mathscr{C}} f_R(\boldsymbol{A}) = \sum_{i=0}^{n} c_i Y^i X^{n-i}. \tag{2.5.2}$$

We call the $(n+1)$-tuple, $\boldsymbol{c} = (c_0, \ldots, c_n)$ of coefficients of the weight enumerator the ***rank weight distribution*** of the code $\mathscr{C}$.

Example 2.5.4. An example of such a code with $q = 2$ and $n = m = 3$ is where $\mathscr{C}$ is the subspace generated by the following matrices;

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

There are 16 matrices (codewords) in this code. The only codeword of rank 0 is the all-zero matrix and there are none of rank 1. There are exactly 9 codewords of rank 2, and exactly 6 codewords of rank 3 and the rank weight enumerator of the code is $X^3 + 9Y^2X + 6Y^3$.

It is readily checked that the set of $n \times m$ matrices over $\mathbb{F}_q$ together with the rank distance defined above, forms a metric association scheme by satisfying the axioms in Definitions 2.3.1, 2.3.6 and Equation (2.3.23).

Before going any further, we take the general b-nary Gaussian coefficients and b-nary beta function as defined in Section 2.3.1 with the parameter b set to q, $q > 1$, for the rank metric,

$$\begin{aligned} {}_q\begin{bmatrix} x \\ k \end{bmatrix} &= \prod_{i=0}^{k-1} \frac{q^x - q^i}{q^k - q^i}, \\ \beta_q(x,k) &= \prod_{i=0}^{k-1} {}_q\begin{bmatrix} x-i \\ 1 \end{bmatrix}. \end{aligned}$$

We also have the alpha function as defined in [22, Section 2.3] for $x, k \in \mathbb{Z}^+$,

$$\alpha(x,k) = \prod_{i=0}^{k-1} \left(q^x - q^i\right). \tag{2.5.3}$$

Here we have a useful theorem proven by Laksov which counts the number of matrices of a given rank in $\mathbb{F}_q^{n\times m}$ [64, Proposition 3.1].

Theorem 2.5.5. *The number of matrices in* $\mathbb{F}_q^{m\times n}$ *of rank* r *is*

$$\xi_{m,n,r} = \prod_{i=0}^{r-1} \frac{\left(q^m - q^i\right)\left(q^n - q^i\right)}{\left(q^r - q^i\right)} \tag{2.5.4}$$

which can also be written as

$$\xi_{m,n,r} = {}_q\begin{bmatrix} n \\ r \end{bmatrix} \alpha(m,r). \tag{2.5.5}$$

We also note the rank weight enumerator of the whole space, $\mathbb{F}_q^{m\times n}$ is

$$\Omega_{m,n} = \sum_{i=0}^{n} \xi_{m,n,i} Y^i X^{n-i}.$$

Using Theorem 2.5.5 it is useful to see some coefficients of the rank weight enumerator for some small size matrices over $\mathbb{F}_q$. We note that the rank weight for a $m \times n$ matrix, is equal to that of its transpose. A good example of this is shown in Table 2.5.1.

$m \times n$	Total	Rank Weight			Enumerator
		$\xi_{m,n,0}$	$\xi_{m,n,1}$	$\xi_{m,n,2}$	$\Omega_{m,n}$
1×1	q	1	$q-1$	-	$X + (q-1)Y$
1×2	q^2	1	q^2-1	0	$X + (q^2-1)Y$
2×1	q^2	1	q^2-1	0	$X + (q^2-1)Y$
2×2	q^4	1	$\left(q^2-1\right)(q+1)$	$q\left(q^2-1\right)(q-1)$	$X^2 + \left(q^2-1\right)(q+1)XY + q\left(q^2-1\right)(q-1)Y^2$

Table 2.5.1: Coefficients of the rank weight enumerator for small matrices over $\mathbb{F}_q$.

In this setting we define an inner product as follows

$$\langle \boldsymbol{A}, \boldsymbol{B} \rangle = Tr\left(\boldsymbol{A}\boldsymbol{B}^T\right)$$

where $Tr(\boldsymbol{A})$ means the trace of $\boldsymbol{A}$. We note that also $Tr\left(\boldsymbol{A}\boldsymbol{B}^T\right) = Tr\left(\boldsymbol{B}\boldsymbol{A}^T\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}b_{ij}$ where $\boldsymbol{A} = (a_{ij})$ and $\boldsymbol{B} = (b_{ij})$, so satisfies the symmetric condition for an inner product.

Now we define the dual of a code.

Definition 2.5.6. The ***dual code***, $\mathscr{C}^\perp \subseteq \mathbb{F}_q^{m\times n}$, of a code, $\mathscr{C} \subseteq \mathbb{F}_q^{m\times n}$, is defined as

$$\mathscr{C}^\perp = \left\{\boldsymbol{A} \in \mathbb{F}_q^{m\times n} \mid \langle \boldsymbol{A}, \boldsymbol{B} \rangle = 0 \ \forall \ \boldsymbol{B} \in \mathscr{C}\right\}.$$

The following theorem by Gabidulin relates the minimum distance of a maximal rank code to the minimum distance of its dual which is also proven to be maximal.

Theorem 2.5.7 ([21, Theorem 3])**.** *Without loss of generality, assume $n \leq m$. A code $\mathscr{C} \subseteq \mathbb{F}_q^{m\times n}$ with minimum rank distance d_R is MRD if and only if its dual $\mathscr{C}^\perp \subseteq \mathbb{F}_q^{m\times n}$ is also MRD with minimum rank distance $d'_R = n - d_R + 2$.*

q-Product, q-Power and q-Transform

The weight enumerator of a linear code $\mathscr{C} \subseteq \mathbb{F}_q^{m\times n}$ is a homogeneous polynomial. Gadouleau and Yan introduce an operation, the q-product [22, Definiton 3], on homogeneous polynomials that help to express the relation between the weight enumerator of a code and that of its dual.

Definition 2.5.8. Let

$$a(X, Y; \lambda) = \sum_{i=0}^{r} a_i(\lambda) Y^i X^{r-i},$$
$$b(X, Y; \lambda) = \sum_{i=0}^{s} b_i(\lambda) Y^i X^{s-i},$$

be two homogeneous polynomials in X and Y, of degrees r and s respectively, and coefficients $a_i(\lambda)$ and $b_i(\lambda)$ respectively, which are real functions of λ and are 0 unless otherwise specified. For example $b_i(\lambda) = 0$ if $i \notin \{0, 1, \ldots, s\}$.

The ***q*-product**, $*$, of $a(X, Y; \lambda)$ and $b(X, Y; \lambda)$ is defined as

$$\begin{aligned} c(X, Y; \lambda) &= a(X, Y; \lambda) * b(X, Y; \lambda) \\ &= \sum_{u=0}^{r+s} c_u(\lambda) Y^u X^{r+s-u} \end{aligned} \tag{2.5.6}$$

with

$$c_u(\lambda) = \sum_{i=0}^{u} q^{is} a_i(\lambda) b_{u-i}(\lambda - i).$$

Definition 2.5.9 ([22, Defintion 4])**.** The ***q*-power** of $a(X, Y; \lambda)$ is defined by

$$\begin{cases} a^{[0]}(X, Y; \lambda) = 1, \\ a^{[1]}(X, Y; \lambda) = a(X, Y; \lambda), \\ a^{[k]}(X, Y; \lambda) = a(X, Y; \lambda) * a^{[k-1]}(X, Y; \lambda) \quad \text{for } k \geq 2. \end{cases}$$

Definition 2.5.10 ([22, Definition 5])**.** Let $a(X, Y; \lambda) = \sum_{i=0}^{r} a_i(\lambda) Y^i X^{r-i}$. The ***q*-transform** of $a(X, Y; \lambda)$ is defined to be the homogeneous polynomial

$$\overline{a}(X, Y; \lambda) = \sum_{i=0}^{r} a_i(\lambda) Y^{[i]} * X^{[r-i]}$$

where $Y^{[i]}$ is the i^{th} q-power of the homogeneous polynomial Y and $X^{[r-i]}$ is the $(r-i)^{th}$ q-power of the homogeneous polynomial X.

In the theory that follows, relating the weight enumerator of a code to its dual, we consider the following two polynomials which turn out to be critical to formulate and prove the MacWilliams Identity as a functional transform.

First let

$$\mu(X, Y; \lambda) = X + \left(q^{\lambda} - 1\right) Y. \tag{2.5.7}$$

The q-powers of $\mu(X, Y; m)$ provide an explicit form for the weight enumerator of $\mathbb{F}_q^{m \times n}$, the set of matrices of order $m \times n$. Theorem 2.5.11 and Theorem 2.5.12, seen below, are noted in [22, Lemma 2].

Theorem 2.5.11. *If $\mu(X, Y; \lambda)$ is as defined above, then for all $k \geq 1$*

$$\mu^{[k]}(X, Y; \lambda) = \sum_{u=0}^{k} \mu_u(\lambda, k) Y^u X^{k-u}$$

where

$$\mu_u(\lambda, k) = {}_q\begin{bmatrix}k\\u\end{bmatrix}\alpha(\lambda, u).$$

Specifically, the weight enumerators for $\mathbb{F}_q^{m\times n}$*, the set of matrices of size* $m \times n$ *over* $\mathbb{F}_q$*, denoted by* $\Omega_{m,n}$*, is given by,*

$$\Omega_{m,n} = \mu^{[n]}(X, Y; m).$$

Second, consider the polynomial

$$\nu(X, Y; \lambda) = X - Y. \tag{2.5.8}$$

Theorem 2.5.12. *If* $\nu(X, Y; \lambda)$ *is as defined above, then for all* $k \geq 1$*,*

$$\nu^{[k]}(X, Y; \lambda) = \sum_{u=0}^{k}(-1)^u q^{\sigma_u}\, {}_q\begin{bmatrix}k\\u\end{bmatrix} Y^u X^{k-u}. \tag{2.5.9}$$

2.5.4 Eigenvalues of the Association Scheme of Matrices over a Finite Field

The following theory uses the results from Gadouleau and Yan [22]. Here we take the polynomials which are proven to be generalised Krawtchouk polynomials which in turn are the eigenvalues of this association scheme.

We begin by considering the set of matrices over a finite field with the rank metric. The relations are defined by $\boldsymbol{A}, \boldsymbol{B} \in \mathbb{F}_q^{m\times n}$ being i^{th} associates if they have rank distance i apart, i.e. $d_R(\boldsymbol{A}, \boldsymbol{B}) = i$. Then, again similar to the Hamming association scheme, it can be readily shown that [9, p229] it is a metric association scheme and we will call it the rank association scheme. In this scheme, the eigenvalues are defined as [9, (A10)]

$$p_k(i) = P_k(i, n)$$

where $P_k(i, n)$ are the generalised Krawtchouk polynomials (2.3.38) with $b = q$ and $c = 1$. So specifically the rank Krawtchouk polynomials for $q \geq 2$ are [11, (15)],

$$P_k(x, n) = \sum_{j=0}^{k}(-1)^{k-j} q^{jm} q^{\sigma_{k-j}}\, {}_q\begin{bmatrix}n-j\\n-k\end{bmatrix} {}_q\begin{bmatrix}n-x\\j\end{bmatrix} \tag{2.5.10}$$

with,

$$P_k(0, n) = {}_q\begin{bmatrix}n\\k\end{bmatrix}\alpha(m, k).$$

The initial values follow from the theory of association schemes and represent the valencies of each relation.

2.5.5 MacWilliams Identity as a Functional Transform

Again similar to the Hamming metric, here we have an identity that relates the rank weight enumerator of a code to the rank weight enumerator of its dual code, taken from [22, Theorem 1].

Theorem 2.5.13 (The MacWilliams Identity for the Rank Association Scheme)**.** *Let $\mathscr{C} \subseteq \mathbb{F}_q^{m\times n}$ be an $[n,k,d_R]$ linear code, with rank weight distribution $\boldsymbol{c} = (c_0,\dots,c_n)$ and $\mathscr{C}^\perp \subseteq \mathbb{F}_q^{m\times n}$ its dual code, with rank weight distribution $\boldsymbol{c'} = (c'_0,\dots,c'_n)$. Then*

$$W^R_{\mathscr{C}^\perp}(X,Y) = \frac{1}{|\mathscr{C}|}\overline{W}^R_{\mathscr{C}}(X+(q^m-1)Y, X-Y) \tag{2.5.11}$$

$$= \frac{1}{|\mathscr{C}|}\sum_{i=0}^{n} c_i(X-Y)^{[i]} * (X+(q^m-1)\,Y)^{[n-i]}\,. \tag{2.5.12}$$

The proof of this theorem uses the q-algebra on homogeneous polynomials as in Equation (2.5.7) and Equation (2.5.8) in order to present the MacWilliams Identity in the desired polynomial form. It then identifies subspaces of the code that are generated by a single element and are shown to be themselves MRD. Since they are MRD, the rank weight enumerators of their duals can be found and are only dependent on the rank of the selected codeword [22, Proposition 1]. The formula is proved directly by induction by considering how many extensions of a codeword will be linearly dependent on the original. They conclude by finding the rank weight enumerator of each of these subcodes as a q-product of q-powers of $\mu(X,Y,;\lambda)$ and $\nu(X,Y;\lambda)$. This allows the MacWilliams Identity for the rank metric to be expressed in a form analogous to the original MacWilliams Identity for the Hamming metric, Theorem 2.4.7.

The proof is only shown in outline here because it could not be mimicked for the skew rank association scheme due to its lack of maximal properties in the subspaces. That is, the proof relies on subspaces of the code that are generated by a single element and are maximal. For the skew rank association scheme no such relevant subspaces could be found that were maximal. As a result an alternative approach had to be devised.

2.5.6 Delsarte's MacWilliams Identity

Delsarte explicitly studies the association scheme of matrices over a finite field with the rank metric in his paper [9]. Here he writes his MacWilliams Identity [9, Theorem 3.3], in terms of matrices built from generalised Krawtchouk polynomials.

Theorem 2.5.14 (The MacWilliams Identity for the Rank Metric)**.** *Let $\mathscr{C} \subseteq \mathbb{F}_q^{m\times n}$ be a code with weight distribution $\boldsymbol{c} = (c_0,c_1,\dots,c_n)$ and $\mathscr{C}^\perp \subseteq \mathbb{F}_q^{m\times n}$ be its dual code with weight distribution $\boldsymbol{c}' = (c'_0,c'_1,\dots,c'_n)$. Then,*

$$\boldsymbol{c}' = \frac{1}{|\mathscr{C}|}\boldsymbol{cP} \tag{2.5.13}$$

where $\boldsymbol{P} = (p_{xk})$ *is defined as the* $(n+1)\times(n+1)$ *matrix with* $p_{xk} = P_k(x,n)$*, and* $P_k(x,n)$ *are the rank Krawtchouk polynomials as defined in equation* (2.5.10)*.*

Delsarte gives an elegant proof based on ring theory.

2.5.7 Moments of the Rank Weight Distribution

Since we are working in a new q-algebra, we state here the q-derivatives that are defined [22, Definition 5 & Definition 6] and some properties that are proven [22, Lemma 3-6], before going on to investigate the moments of the rank weight distribution of linear codes.

Definition 2.5.15. For $q \geq 2$, the ***q*-derivative** at $X \neq 0$ of a real-valued function $f(X)$ is defined as

$$f^{(1)}(X) = \frac{f(qX) - f(X)}{(q-1)X}$$

and the q^{-1}***-derivative*** at $Y \neq 0$ of a real-valued function $g(Y)$ is defined as

$$g^{\{1\}}(Y) = \frac{g(q^{-1}Y) - g(Y)}{(q^{-1}-1)\,Y}.$$

Here we list the important results of the derivatives. The proofs and theory that generated these results can be seen in [22, Lemma 3, Lemma 5].

Lemma 2.5.16. *1. The* φ^{th} *q-derivative of* $f(X,Y;\lambda) = \sum_{i=0}^{r} f_i(\lambda) Y^i X^{r-i}$ *is given by*

$$f^{(\varphi)}\left(X,Y;\lambda\right) = \sum_{i=0}^{r-\varphi} f_i(\lambda) q^{\varphi(1-i)+\sigma_\varphi} \beta_q(i,\varphi) Y^i X^{r-i-\varphi}. \qquad (2.5.14)$$

2. The φ^{th} q^{-1}*-derivative of* $g(X,Y;\lambda) = \sum_{i=0}^{s} g_i(\lambda) Y^i X^{s-i}$ *is given by*

$$g^{\{\varphi\}}\left(X,Y;\lambda\right) = \sum_{i=\varphi}^{s} g_i(\lambda) q^{\varphi(1-i)+\sigma_\varphi} \beta_q(i,\varphi) Y^{i-\varphi} X^{s-i}. \qquad (2.5.15)$$

Theorem 2.5.17 is an amalgamation of [22, Proposition 4, Proposition 5]. These equations are known as the q-moments of the weight distribution for codes using the rank metric.

Theorem 2.5.17. *For an* $[n,k,d_R]-$*linear code,* $\mathscr{C} \subseteq \mathbb{F}_q^{m\times n}$*, with weight distribution* $\boldsymbol{c} = (c_0,\ldots,c_n)$*, and dual code* $\mathscr{C}^\perp \subseteq \mathbb{F}_q^{m\times n}$ *with rank weight distribution* $\boldsymbol{c'} = (c'_0\ldots,c'_n)$*, we have*

$$\sum_{i=0}^{n-\varphi} \begin{bmatrix} n-i \\ \varphi \end{bmatrix}_q c_i = q^{m(k-\varphi)} \sum_{i=0}^{n} \begin{bmatrix} n-i \\ n-\varphi \end{bmatrix}_q c'_i \qquad (2.5.16)$$

and

$$\sum_{i=\varphi}^{n} q^{\varphi(n-i)} \begin{bmatrix} i \\ \varphi \end{bmatrix}_q c_i = q^{m(k-\varphi)} \sum_{i=0}^{\varphi} (-1)^i q^{\sigma_i} q^{i(\varphi-i)} \begin{bmatrix} n-i \\ n-\varphi \end{bmatrix}_q \alpha(m-i,\varphi-i) c'_i. \qquad (2.5.17)$$

Note. The proof of this theorem follows the same method as that outlined in Theorem 2.4.8 for the Hamming metric.

Corollary 2.5.18. *Let d'_R be the minimum rank distance of $\mathscr{C}^\perp$. If $0 \leq \varphi < d'_R$ then*

$$\sum_{i=0}^{n-\varphi} \begin{bmatrix} n-i \\ \varphi \end{bmatrix}_q c_i = q^{m(k-\varphi)} \begin{bmatrix} n \\ \varphi \end{bmatrix}_q$$

and

$$\sum_{i=\varphi}^{n} q^{\varphi(n-i)} \begin{bmatrix} i \\ \varphi \end{bmatrix}_q c_i = q^{m(k-\varphi)} \begin{bmatrix} n \\ \varphi \end{bmatrix}_q \alpha(m,\varphi).$$

Proof. For $0 \leq \varphi < d'_R$, then $c'_0 = 1$, $c'_1 = \ldots = c'_\varphi = 0$. □

2.5.8 Maximum Rank Distance Codes

In the special case when $\mathscr{C}$ is an MRD code (i.e. when it attains the Singleton bound (2.5.1) for codes with the rank metric), Gadouleau and Yan [22] provide a method for finding the rank weight distribution of MRD codes with minimum distance d_R. Similar to the case in the Hamming metric, the rank weight distribution for MRD codes depends only on the parameters of the code and not the code itself. The following theorem is first developed by Delsarte and Gabidulin [9, Theorem 5.6], [21, Theorem 5] and was re-proven by Gadouleau and Yan [22, Proposition 9] using Theorem 2.5.17 and Corollary 2.5.18.

Proposition 2.5.19. *Let $\mathscr{C} \subseteq \mathbb{F}_q^{m\times n}$ be a linear MRD code with weight distribution $\mathbf{c}$, and minimum distance d_R. Then we have $c_0 = 1$ and for $0 \leq r \leq n - d_R$*

$$c_{d_R+r} = \sum_{i=0}^{r} (-1)^{r-i} q^{\sigma_{r-i}} \begin{bmatrix} d_R+r \\ d_R+i \end{bmatrix}_q \begin{bmatrix} n \\ d_R+r \end{bmatrix} \left(q^{m(i+1)} - 1\right).$$

2.6 The Skew Rank Association Scheme

2.6.1 Introduction and Background

Inspired by the work of Gadouleau and Yan, it was natural to ask the question of what other metrics could we build a "q-algebra" for and for what association schemes could we identify a version of the MacWilliams Identity as a functional transform. The obvious first choice to explore after the rank metric, is the skew rank metric applied to the association scheme of skew-symmetric matrices. We shall call this the skew rank association scheme.

2.6.2 Delsarte

Delsarte was particularly motivated by association schemes [8] and that seems to be what drove him to study different metrics and consequently to investigate different codes based on these metrics. One of the cases he considered was alternating bilinear forms over a finite field, which we can directly relate to the association scheme of skew-symmetric matrices with the skew rank metric [12]. Many of Delsarte's results in this paper and his earlier work have formed the basis of the further developments presented in this thesis.

2.6.3 Preliminaries

We first introduce key definitions and background theory required for formation of the MacWilliams Identity as a functional transform for the skew rank association scheme.

Definition 2.6.1. Let $\boldsymbol{A}$ be a matrix of size $t \times t$ with entries in a finite field $\mathbb{F}_q$, where q is a prime power. Then $\boldsymbol{A} = (a_{ij})$ is called a ***skew-symmetric*** matrix, if $\boldsymbol{A}^T = -\boldsymbol{A}$.

The set of these skew-symmetric matrices is denoted $\mathscr{A}_{q,t}$ and the order of the matrix is t.

Although the following aspect of the theory is not used in this thesis, it is interesting to note that each skew-symmetric matrix, $\boldsymbol{A}$, can be associated with a corresponding alternating bilinear form and more information on alternating bilinear forms can be found in [12, Section 2.1].

Theorem 2.6.2. *$\mathscr{A}_{q,t}$ is a $\binom{t}{2}$-dimensional vector space over $\mathbb{F}_q$.*

The proof of this theorem is trivial and hence omitted. For $\mathscr{A}_{q,t}$ we define the parameters

$$n = \left\lfloor \frac{t}{2} \right\rfloor, \ m = \frac{t(t-1)}{2n}.$$

We also follow the convention that the empty product is taken to be 1 and the empty sum is taken to be 0.

Again similar to the rank metric, we take the general b-nary Gaussian coefficients and b-nary beta function as defined in Section 2.3.1 with the parameter b set to q^2, $q > 1$. We have,

$${}_{q^2}\begin{bmatrix} x \\ k \end{bmatrix} = \prod_{i=0}^{k-1} \frac{q^{2x} - q^{2i}}{q^{2k} - q^{2i}},$$
$$\beta_{q^2}(x,k) = \prod_{i=0}^{k-1} {}_{q^2}\begin{bmatrix} x-i \\ 1 \end{bmatrix}.$$

We use a significant number of definitions for the skew rank metric taken from Delsarte [12]. We note that the column rank of a skew-symmetric matrix is always even, so we can write the rank as $2s$ for some $s \in \mathbb{Z}^+$.

Definition 2.6.3. For all $\boldsymbol{A} \in \mathscr{A}_{q,t}$ with column rank $2s$ we define the ***skew rank weight*** of $\boldsymbol{A}$, $SR(\boldsymbol{A})$, to be s.

For all $\boldsymbol{A}, \boldsymbol{B} \in \mathscr{A}_{q,t}$, we define the ***skew rank distance*** between $\boldsymbol{A}$ and $\boldsymbol{B}$ to be

$$d_{SR}(\boldsymbol{A}, \boldsymbol{B}) = SR(\boldsymbol{A} - \boldsymbol{B}).$$

It is easily verified that $d_{SR}(\boldsymbol{A}, \boldsymbol{B})$ is a metric over $\mathscr{A}_{q,t}$ since $SR(\boldsymbol{A} - \boldsymbol{B})$ is the rank metric [21] [22] divided by 2 and we will call it the ***skew rank metric***.

Any subspace of $\mathscr{A}_{q,t}$ can be considered as an $\mathbb{F}_q$-linear code, $\mathscr{C}$, with each matrix of skew rank s in $\mathscr{C}$ representing a codeword of weight s and with the distance metric being the skew rank metric.

The ***minimum skew rank distance*** of such a code $\mathscr{C}$, denoted as $d_{SR}(\mathscr{C})$, is simply the minimum skew rank distance over all possible pairs of distinct codewords in $\mathscr{C}$. When there is no ambiguity about $\mathscr{C}$, we denote the minimum skew rank distance as d_{SR}.

It can be shown that [12, p.33] the cardinality, $|\mathscr{C}|$, of a code, $\mathscr{C}$, over $\mathbb{F}_q$ based on $t \times t$ skew-symmetric matrices and minimum skew rank distance d_{SR} satisfies

$$|\mathscr{C}| \leq q^{m(n-d_{SR}+1)}. \tag{2.6.1}$$

In this thesis, we call the bound in (2.6.1) the Singleton bound for codes with the skew rank metric. Codes that attain the Singleton bound are referred to as maximal codes or Maximum Skew Rank Distance (MSRD) codes.

Once again, an equivalent skew rank weight enumerator is introduced.

Definition 2.6.4. For all $\boldsymbol{A} \in \mathscr{A}_{q,t}$ with skew rank weight s, the ***skew rank weight function*** of $\boldsymbol{A}$ is defined as the homogeneous polynomial

$$f_{SR}(\boldsymbol{A}) = Y^s X^{n-s}.$$

Let $\mathscr{C} \subseteq \mathscr{A}_{q,t}$ be a code. Suppose there are c_i codewords in $\mathscr{C}$ with skew rank weight i for $0 \leq i \leq n$. Then the ***skew rank weight enumerator*** of $\mathscr{C}$, denoted as $W_{\mathscr{C}}^{SR}(X, Y)$, is defined to be

$$W_{\mathscr{C}}^{SR}(X, Y) = \sum_{\boldsymbol{A} \in \mathscr{C}} f_{SR}(\boldsymbol{A}) = \sum_{i=0}^{n} c_i Y^i X^{n-i}. \tag{2.6.2}$$

The $(n+1)$-tuple, $\boldsymbol{c} = (c_0, \ldots, c_n)$ of coefficients of the weight enumerator, is called the ***skew rank weight distribution*** of the code $\mathscr{C}$.

Example 2.6.5. An example of such a code with $q = 3$ and $t = 4$ is where $\mathscr{C}$ is the set of skew-symmetric matrices, $\boldsymbol{A} = (a_{ij})$ with $1 \leq i, j \leq 4$, such that;

$$\begin{cases} a_{1j} \in \mathbb{F}_q, \ j > 1 \\ a_{23} = a_{24} = 0 \\ a_{34} \in \mathbb{F}_q. \end{cases} \quad \rightarrow \quad \begin{pmatrix} 0 & a_{12} & a_{13} & a_{14} \\ -a_{12} & 0 & 0 & 0 \\ -a_{13} & 0 & 0 & a_{34} \\ -a_{14} & 0 & -a_{34} & 0 \end{pmatrix}$$

There are 81 matrices (codewords) in this code. It is easily seen that a codeword has skew rank 2 if and only if a_{12} and a_{34} are both nonzero. Therefore, there is 1 codeword of skew rank 0, 44 codewords of skew rank 1 and 36 codewords of skew rank 2. Thus, the skew rank weight enumerator of the code is $X^2 + 44XY + 36Y^2$.

Many ways of describing the number of skew-symmetric matrices have been developed by various authors such as [62, Proposition 2.1, p627], [40, Theorem 3, p155] and [41, Theorem 2, p437]. The following is (for the purpose of this thesis) in the best format.

Theorem 2.6.6 ([5, Theorem 3, p24]). *The number of skew symmetric matrices of order t and skew rank s, for $0 \leq s \leq n$ is*

$$\xi_{t,s} = q^{2\sigma_s} \frac{\prod\limits_{i=0}^{2s-1} \left(q^{t-i} - 1\right)}{\prod\limits_{i=1}^{s} \left(q^{2i} - 1\right)}. \tag{2.6.3}$$

We also then note the skew rank weight enumerator of $\mathscr{A}_{q,t}$ is

$$\Omega_t = \sum_{i=0}^{n} \xi_{t,i} Y^i X^{n-i}. \tag{2.6.4}$$

It is useful to see the resulting skew rank weight enumerators for some small size matrices. From the results of the counts of matrices of skew rank s,($s = 0, \ldots, n$), and size t we list the coefficients of the skew rank weight enumerator in Table 2.6.7 for matrices of size $1 \times 1, 2 \times 2, 3 \times 3$ and 4×4 over $\mathbb{F}_q$.

$t \times t$	Total	Skew Rank Weight			Enumerator
		$\xi_{t,0}$	$\xi_{t,1}$	$\xi_{t,2}$	Ω_t
1×1	1	1	-	-	1
2×2	q	1	$q-1$	-	$X + (q-1)Y$
3×3	q^3	1	q^3-1	-	$X + (q^3-1)Y$
4×4	q^6	1	$\left(q^2+1\right)\left(q^3-1\right)$	$q^2\left(q^3-1\right)(q-1)$	$X^2 + \left(q^2+1\right)\left(q^3-1\right)XY + q^2\left(q^3-1\right)(q-1)Y^2$

Table 2.6.7: Coefficients of the skew rank weight enumerator for small matrices in $\mathscr{A}_{q,t}$.

Example 2.6.1. For $t = 4$ and $q = 3$ the skew rank weight enumerator of $\mathscr{A}_{3,4}$ is

$$X^2 + \left(3^2+1\right)\left(3^3-1\right)XY + 3^2\left(3^3-1\right)(3-1)Y^2 = X^2 + 260XY + 468Y^2.$$

The coefficients for 6×6 skew-symmetric matrices have been listed in Appendix A.2. We now define an **inner product** on $\mathscr{A}_{q,t}$ by

$$(\boldsymbol{A}, \boldsymbol{B}) \mapsto \langle \boldsymbol{A}, \boldsymbol{B} \rangle = Tr\left(\boldsymbol{A}^T \boldsymbol{B}\right)$$

where $Tr(\boldsymbol{A})$ means the trace of $\boldsymbol{A}$.

Definition 2.6.2. The ***dual code***, $\mathscr{C}^{\perp} \subseteq \mathscr{A}_{q,t}$, of a code, $\mathscr{C} \subseteq \mathscr{A}_{q,t}$, is defined as

$$\mathscr{C}^{\perp} = \Big\{ \boldsymbol{A} \in \mathscr{A}_{q,t} \mid \langle \boldsymbol{A}, \boldsymbol{B} \rangle = 0 \ \forall \ \boldsymbol{B} \in \mathscr{C} \Big\}.$$

The following theorem by Delsarte relates the minimum distance of a maximal skew rank code to the minimum distance of its dual which is also proven to be maximal.

Theorem 2.6.3 ([12, Theorem 5])**.** *A code $\mathscr{C} \subseteq \mathscr{A}_{q,t}$ with minimum skew rank distance d_{SR} is MSRD if and only if its dual $\mathscr{C}^{\perp}$ is also MSRD with minimum skew rank distance $d'_{SR} = n - d_{SR} + 2$.*

2.6.4 Eigenvalues of the Association Scheme of Skew-Symmetric Matrices

We consider the set of skew-symmetric matrices over a finite field with the skew rank metric. We then have an n-class $(\mathscr{A}_{q,t}, R)$ metric association scheme with $R_i = \{(\boldsymbol{A}, \boldsymbol{B}) \mid d_{SR}(\boldsymbol{A}, \boldsymbol{B}) = i\}$ which we will call the skew rank association scheme. In this scheme, the eigenvalues are defined as [9, (A10)]

$$p_k(i) = P_k(i, n)$$

where $P_k(i, n)$ are the generalised Krawtchouk polynomials (2.3.38) with $b = q^2$, and $n = \left\lfloor \frac{t}{2} \right\rfloor$, $m = \frac{t(t-1)}{2n}$. So the skew rank Krawtchouk polynomials for $q \geq 2$ are [12, p31]

$$P_k(x, n) = \sum_{j=0}^{k} (-1)^{k-j} q^{mj} q^{2\sigma_{k-j}} \begin{bmatrix} n-j \\ n-k \end{bmatrix}_{q^2} \begin{bmatrix} n-x \\ j \end{bmatrix}_{q^2}. \tag{2.6.5}$$

2.6.5 Maximum Skew Rank Distance Codes

In the special case when $\mathscr{C}$ is an MSRD code (i.e. when it attains the Singleton bound (2.6.1) for codes with the skew rank metric), Delsarte provides a method for finding the skew rank weight distribution of MSRD codes with minimum distance d_{SR}. Again similar to the cases in the Hamming and rank metric, the skew rank weight distribution for MSRD codes depends only on the parameters of the code and not the code itself.

Proposition 2.6.4 ([12, (31)])**.** *Let $\mathscr{C} \subseteq \mathscr{A}_{q,t}$ be a linear MSRD code with weight distribution $\boldsymbol{c}$, and minimum distance d_{SR}. Then we have $c_0 = 1$ and for $0 \leq i \leq n - d_{SR}$,*

$$c_{n-i} = \sum_{j=i}^{n-d_{SR}} (-1)^{j-i} q^{2\sigma_{j-i}} \begin{bmatrix} j \\ i \end{bmatrix}_{q^2} \begin{bmatrix} n \\ j \end{bmatrix}_{q^2} \left(q^{m(n-d_{SR}+1-j)} - 1 \right).$$

Delsarte uses a proof involving the $\boldsymbol{P}$-transform on the properties of the $P_k(i)$'s, [12, (29)].

2.7 The Hermitian Association Scheme

2.7.1 Introduction and Background

After Hermitian matrices came on the mathematics scene in 1855, named after Charles Hermite, they were first used to investigate new ideas in number theory since they have the property, shared with real symmetric matrices, that their eigenvalues are always real. This definition of a matrix that is equal to the conjugate transpose of itself was then extended not just to complex matrices but to matrices over a finite field. In 1954 Carlitz and Hodges [6] focused on counting the numbers of Hermitian matrices with particular properties and in 1981 Stanton [61] investigated the association scheme of Hermitian matrices with the related Krawtchouk polynomials. Stanton also studied different schemes such as the rank association scheme, but used hypergeometric series to formulate his results. Certain rank properties of Hermitian matrices were investigated in the 2010's by Sheekey, Gow et al. [15][27] but the matrices that are relevant to the rank weight enumerator of subspaces of Hermitian matrices were developed by Schmidt [53], published in 2017.

2.7.2 Schmidt

Schmidt investigates sets of $n \times n$ Hermitian matrices over $\mathbb{F}_{q^2}$ with distance function defined by the rank metric. He studies codes in this association scheme, which we call the Hermitian association scheme, that arise from these parameters and in particular those with a given minimum distance. Importantly he develops bounds on the size of these codes and identifies the conditions for the weight distribution of such codes to be determined entirely by their parameters. Unlike the rank association scheme with general $m \times n$ matrices, Schmidt shows that weight distributions of maximal additive codes are not uniquely determined and proves this using counterexamples. It is also interesting to note that within the theory building to his results, he generates a form of the eigenvalues of these association schemes which is integral to his development of the bounds.

2.7.3 Preliminaries

We begin with some assumptions and definitions relating to Hermitian matrices over a finite field, $\mathbb{F}_{q^2}$, where q is a prime power. Once again we follow the convention that the empty product is taken to be 1 and the empty sum is taken to be 0. We also use $\sigma_i = \frac{i(i-1)}{2}$ for $i \geq 0$.

We write the conjugate of $x \in \mathbb{F}_{q^2}$ as $\overline{x} = x^q$. Then for a $t \times t$ matrix over $\mathbb{F}_{q^2}$, we write $\boldsymbol{H}^\dagger$ for the conjugate transpose matrix of $\boldsymbol{H}$.

Definition 2.7.1. Let $\boldsymbol{H}$ be a $t \times t$ matrix over $\mathbb{F}_{q^2}$. Then $\boldsymbol{H} = (h_{ij})$ is called a ***Hermitian*** matrix if $\boldsymbol{H} = \boldsymbol{H}^\dagger$. The set of these Hermitian matrices is denoted $\mathscr{H}_{q,t}$.

Theorem 2.7.2. *$\mathscr{H}_{q,t}$ is a t^2-dimensional vector space over $\mathbb{F}_q$.*

The proof of Theorem 2.7.2 is trivial and hence omitted.

Since we will need a Gaussian coefficient, we take the definition used by Schmidt [53, p3]. It turns out that if we set $b = -q$ we can then use our general b-nary Gaussian coefficients and the b-nary beta function as defined in Section 2.3.1 as these two definitions of the Gaussian coefficients are equivalent. So we have,

$$\begin{aligned} {}_{-q}\begin{bmatrix} x \\ k \end{bmatrix} &= \prod_{i=0}^{k-1} \frac{(-q)^x - (-q)^i}{(-q)^k - (-q)^i}, \\ \beta_{-q}(x,k) &= \prod_{i=0}^{k-1} {}_{-q}\begin{bmatrix} x-i \\ 1 \end{bmatrix}. \end{aligned}$$

Definition 2.7.3. For all $\boldsymbol{H} \in \mathscr{H}_{q,t}$ we define the ***Hermitian rank weight*** of $\boldsymbol{H}$, $HR(\boldsymbol{A}) = h$, to be the usual column rank of the matrix over $\mathbb{F}_q$. For all $\boldsymbol{H}, \boldsymbol{J} \in \mathscr{H}_{q,t}$, we define the ***Hermitian rank distance*** between $\boldsymbol{H}$ and $\boldsymbol{J}$ to be

$$d_{HR}(\boldsymbol{H}, \boldsymbol{J}) = HR(\boldsymbol{H} - \boldsymbol{J}).$$

It is easily verified that $d_{HR}(\boldsymbol{H}, \boldsymbol{J})$ is a metric over $\mathscr{H}_{q,t}$.

Note. This definition is identical to Definition 2.5.2 for the rank metric, but we call it the Hermitian rank distance to distinguish between cases.

Again similar to the other metrics, any subspace of $\mathscr{H}_{q,t}$ can be considered as an $\mathbb{F}_q$-linear code, $\mathscr{C}$, with each matrix of rank h in $\mathscr{C}$ representing a codeword of weight h, defined below, and with the distance metric being the rank metric defined in Definition 2.7.3.

The ***minimum Hermitian rank distance*** of such a code $\mathscr{C}$, denoted as $d_{HR}(\mathscr{C})$, is simply the minimum Hermitian rank distance over all possible pairs of distinct codewords in $\mathscr{C}$. When there is no ambiguity about $\mathscr{C}$, we denote the minimum Hermitian rank distance as d_{HR}.

The following bound is proven explicitly in [53, Theorem 1] using the relationship between the inner distributions and the eigenvalues of the association scheme which happens to also obtain one of the sets of moments of the association scheme. It then uses the subgroup properties of the code to show that the bound holds. So we have that the cardinality $|\mathscr{C}|$ of a code $\mathscr{C}$ over $\mathbb{F}_{q^2}$ based on $t \times t$ Hermitian matrices and minimum Hermitian rank distance d_{HR} satisfies

$$|\mathscr{C}| \leq q^{t(t-d_{HR}+1)}. \tag{2.7.1}$$

In this thesis, we call the bound (2.7.1) the Singleton bound for codes with the Hermitian rank distance. Codes that attain the Singleton bound are referred to as maximal codes or Maximum Hermitian Rank Distance (MHRD) codes. Yet again, we introduce a Hermitian rank weight function for codes using the Hermitian rank distance.

Definition 2.7.4. For all $\boldsymbol{H} \in \mathscr{H}_{q,t}$ with Hermitian rank weight h, the ***Hermitian rank weight function*** of $\boldsymbol{H}$ is defined as the homogeneous polynomial

$$f_{HR}(\boldsymbol{H}) = Y^h X^{t-h}.$$

Let $\mathscr{C} \subseteq \mathscr{H}_{q,t}$ be a code. Suppose there are c_i codewords in $\mathscr{C}$ with Hermitian rank weight i for $0 \leq i \leq t$. Then the ***Hermitian rank weight enumerator*** of $\mathscr{C}$, denoted as $W_{\mathscr{C}}^{HR}(X,Y)$ is defined to be

$$W_{\mathscr{C}}^{HR}(X,Y) = \sum_{\boldsymbol{H}\in\mathscr{C}} f_{HR}(\boldsymbol{H}) = \sum_{i=0}^{t} c_i Y^i X^{t-i}. \tag{2.7.2}$$

The $(t+1)$-tuple, $\boldsymbol{c} = (c_0, \ldots, c_t)$ of coefficients of the Hermitian rank weight enumerator, is called the ***Hermitian rank weight distribution*** of the code $\mathscr{C}$.

Example 2.7.5. An example of such a code with $q = 2$ and $t = 3$ is where $\mathscr{C}$ is the set of Hermitian matrices, $\boldsymbol{H}$ over $\mathbb{F}_4$ such that;

$$\mathscr{C} = \left\{ \begin{array}{c} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \alpha & 0 \\ 1+\alpha & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \alpha \\ 0 & 1 & 0 \\ 1+\alpha & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1+\alpha \\ 0 & \alpha & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & \alpha & \alpha \\ 1+\alpha & 1 & 0 \\ 1+\alpha & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \alpha & 0 \\ 1+\alpha & 0 & 1+\alpha \\ 0 & \alpha & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \alpha \\ 0 & 1 & 1+\alpha \\ 1+\alpha & \alpha & 1 \end{pmatrix}, \begin{pmatrix} 1 & \alpha & \alpha \\ 1+\alpha & 1 & 1+\alpha \\ 1+\alpha & \alpha & 1 \end{pmatrix} \end{array} \right\}$$

with multiplication table below.

	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Thus there are 8 matrices (codewords) in this code, 1 of Hermitian rank 0, 3 of Hermitian rank 2 and 4 of Hermitian rank 3. Thus its Hermitian rank weight enumerator is $X^3 + 3Y^2X + 4Y^3$.

Here we have a way of describing the number of Hermitian matrices adapted from [6, Theorem 3, p398].

Theorem 2.7.6. *The number of Hermitian matrices of order t and Hermitian rank weight* *h is given by*

$$\xi_{t,h} = q^{\sigma_h} \times \frac{\prod_{i=0}^{h-1} q^{2t-2i} - 1}{\prod_{i=1}^{h} q^i - (-1)^i} = (-1)^h(-q)^{\sigma_h} \times \frac{\prod_{i=0}^{h-1} (-q)^{2t-2i} - 1}{\prod_{i=1}^{h} (-q)^i - 1}.$$

We also then note the Hermitian rank weight enumerator of $\mathscr{H}_{q,t}$ is

$$\Omega_t = \sum_{i=0}^{t} \xi_{t,i} Y^i X^{t-i}.$$

Using Theorem 2.7.6 it is useful to see some coefficients of the Hermitian rank weight enumerator for some small size matrices over $\mathbb{F}_q$ in Table 2.7.7 below.

$t \times t$	Total	Hermitian Rank Weight				Enumerator
		$\xi_{t,0}$	$\xi_{t,1}$	$\xi_{t,2}$	$\xi_{t,3}$	Ω_t
1×1	q	1	$q-1$	-	-	$X + (q-1)Y$
2×2	q^4	1	$(q^2+1)(q-1)$	$q(q^2+1)(q-1)$	-	$X^2 + (q^2+1)(q-1)YX + q(q^2+1)(q-1)Y^2$
3×3	q^9	1	$(q-1)(1+q^2+q^4)$	$q(q^2+1)(q-1)(1+q^2+q^4)$	$q^3(q^3-1)(q^2+1)(q-1)$	$X^3 + (q-1)(1+q^2+q^4)YX^2 + q(q^2+1)(q-1)(1+q^2+q^4)Y^2X + q^3(q^3-1)(q^2+1)(q-1)Y^3$

Table 2.7.7: Coefficients of the Hermitian rank weight enumerator for small matrices in $\mathscr{H}_{q,t}$.

Example 2.7.1. For $t = 3$ and $q = 2$ the Hermitian rank weight enumerator of $\mathscr{H}_{2,3}$ is

$$X^3 + 21YX^2 + 210Y^2X + 280Y^3.$$

We define an **inner product** on $\mathscr{H}_{q,t}$ by

$$(\boldsymbol{H}, \boldsymbol{J}) \mapsto \langle \boldsymbol{H}, \boldsymbol{J} \rangle = Tr\left(\boldsymbol{H}^\dagger \boldsymbol{J}\right)$$

where $Tr(\boldsymbol{H})$ means the trace of $\boldsymbol{H}$.

Definition 2.7.2. The ***dual code***, $\mathscr{C}^\perp \subseteq \mathscr{H}_{q,t}$, of a code, $\mathscr{C} \subseteq \mathscr{H}_{q,t}$, is defined as

$$\mathscr{C}^\perp = \left\{ \boldsymbol{H} \in \mathscr{H}_{q,t} \mid \langle \boldsymbol{H}, \boldsymbol{J} \rangle = 0 \ \forall \ \boldsymbol{J} \in \mathscr{C} \right\}.$$

2.7.4 Eigenvalues of the Association Scheme of Hermitian Matrices

We consider the set of Hermitian matrices over a finite field with the Hermitian rank metric. We have an n-class $(\mathscr{H}_{q,t}, R)$ metric association scheme with $R_i = \{(\boldsymbol{H}, \boldsymbol{J}) \mid d_{HR}(\boldsymbol{H}, \boldsymbol{J}) = i\}$. Then, again similar to the Hamming, rank and skew rank association schemes, it can be readily shown that [3, Section 9.5 C] it is an association scheme, and we call it the Hermitian association scheme. In this scheme, the eigenvalues are defined as [53, (4)]

$$p_k(i) = P_k(i,t)$$

where $P_k(i,t)$ are the eigenvalues, which we call the Hermitian rank Krawtchouk polynomials, as defined in Schmidt [53, (4)] as

$$P_k(x,t) = (-1)^k \sum_{j=0}^{k} (-q)^{\sigma_{k-j}+tj} {}_{-q}\begin{bmatrix} t-j \\ t-k \end{bmatrix}_{-q} \begin{bmatrix} t-x \\ j \end{bmatrix}. \tag{2.7.3}$$

We note that the eigenvalues, $P_k(i,t)$, are the only solution to the following recurrence relation with specific initial values, seemingly different to the recurrence relation by Delsarte [11, (1)]. So for $q \in \mathbb{R}$, $x, y \in \mathbb{Z}^+$ and $x, k \in \{0, 1, \ldots, y\}$ the recurrence relation as defined in [53, Lemma 7] is

$$P_{k+1}(x+1, t+1) = P_{k+1}(x, t+1) + (-q)^{2t+1-x} P_k(x,t) \tag{2.7.4}$$

with initial values

$$P_k(0,t) = \xi_{t,k} \tag{2.7.5}$$

$$P_0(x,t) = 1. \tag{2.7.6}$$

Schmidt proves that these Hermitian rank Krawtchouk polynomials satisfy this recurrence relation (2.7.4) and the initial values, and are therefore the eigenvalues of the Hermitian association scheme.

2.7.5 Moments of the Hermitian Rank Weight Distribution

The following proposition is obtained in the proof of [53, Theorem 1] by Schmidt, by combining the eigenvalues of the association scheme [53, (5)] with the entries of the dual inner distribution [53, (7)]. The following are not stated directly as a proposition or corollary, but we write them here in the notation used in this thesis so we can draw parallels with the comparable results from other association schemes.

Proposition 2.7.3. *For $0 \leq \varphi \leq n$, $q \geq 2$ a prime power, and a linear code $\mathscr{C} \subseteq \mathscr{H}_{q,t}$ and its dual $\mathscr{C}^\perp \subseteq \mathscr{H}_{q,t}$ with weight distributions $\boldsymbol{c} = (c_0, \ldots, c_t)$ and $\boldsymbol{c'} = (c'_0, \ldots, c'_t)$, respectively we have*

$$\sum_{i=0}^{t-\varphi} {}_{-q}\begin{bmatrix} t-i \\ \varphi \end{bmatrix} c_i = \frac{1}{|\mathscr{C}^\perp|} \left(-(-q)^t\right)^{t-\varphi} \sum_{i=0}^{\varphi} {}_{-q}\begin{bmatrix} t-i \\ t-\varphi \end{bmatrix} c'_i.$$

We can simplify Proposition 2.7.3 if φ is less than the minimum distance of the dual code.

Corollary 2.7.4. *Let d'_R be the minimum rank distance of $\mathscr{C}^\perp$. If $0 \leq \varphi < d'_{HR}$ then*

$$\sum_{i=0}^{t-\varphi} {\begin{bmatrix} t-i \\ \varphi \end{bmatrix}}_{-q} c_i = \frac{1}{|\mathscr{C}^\perp|} \left(-(-q)^t\right)^{t-\varphi} {\begin{bmatrix} t \\ \varphi \end{bmatrix}}_{-q}.$$

Proof. We have $c'_0 = 1$ and $c'_1 = \ldots = c'_\varphi = 0$. □

2.7.6 Maximum Hermitian Rank Distance Codes

Unlike the skew rank, rank and Hamming association schemes, there isn't an equation that shows that the Hermitian rank weight distribution of all MHRD codes are uniquely determined by their parameters. It can be shown that for d_{HR} odd, the dual of an MHRD code, $\mathscr{C}^\perp$ is also MHRD. In that case, the weight distribution can be uniquely determined by [53, Theorem 3]. That is

$$c_{n-i} = \sum_{j=i}^{n-d_{HR}} (-1)^{j-i}(-q)^{\sigma_{j-i}} {\begin{bmatrix} j \\ i \end{bmatrix}}_{-q} {\begin{bmatrix} n \\ j \end{bmatrix}}_{-q} \left(\frac{|\mathscr{C}|}{q^{nj}}(-1)^{(n+1)j} - 1 \right).$$

If, on the other hand, the minimum distance of an MHRD code is even, then it has been shown that codes which are maximal with given parameters can have multiple different weight distributions. However, their dual weight distributions are not always maximal. Schmidt gives examples where the minimum distance is 2 [53, Section 3] to show this explicitly. So if a MHRD code has minimum distance even, then the weight distribution is not necessarily uniquely determined by its parameters.

Chapter 3

The Skew Rank Association Scheme

Now considering the association scheme of skew-symmetric matrices with the skew rank metric, the aim is to find the MacWilliams Identity as a functional transform using an appropriate type of "q-algebra". Firstly we shall present an overview of what we already know from Section 2.6, before going on to some more specific preliminaries in Section 3.1. In Section 3.2 we introduce an adapted version of the q-algebra used in [22, Section 3.1] and we identify two homogeneous polynomials which are integral to the development of the transform of the MacWilliams Identity. In fact, the powers of one of these polynomials turn out to be the weight enumerator of the space of skew-symmetric matrices of a given size t. Armed with these polynomials, we can derive a new explicit form of the Krawtchouk polynomials. It is proven that these new forms are indeed the generalised Krawtchouk polynomials and therefore are the eigenvalues of the association scheme using a recurrence relation heavily studied by Delsarte [11]. Finally, we can then state the MacWilliams Identity for the skew rank association scheme as a functional transform.

After we have established the MacWilliams Identity, it is useful to think about the moments of the skew rank weight distribution. Firstly we shall introduce two derivatives on this space, analogous to the q-derivative and the q^{-1} derivative developed by Gadouleau and Yan [22, Definiton 5, 6]. Once these have been defined and some properties developed, they are used to generate moments of the skew rank weight distribution which can be utilised to explore characteristics of the codes. In the special case of MSRD codes, i.e. when the code attains the Singleton bound (2.6.1), it shown that the weight distribution of the code is uniquely determined by its parameters and is not dependent on the code itself.

3.1 Preliminaries

3.1.1 Parameters

As a reminder, as we are considering the skew rank association scheme, $(\mathscr{A}_{q,t}, R)$, we have $b = q^2$ and we set $n = \left\lfloor \frac{t}{2} \right\rfloor$ and $m = \frac{t(t-1)}{2n}$.

For the skew rank association scheme we have the general b-nary Gaussian coefficients and b-nary beta function as defined in Section 2.3.1. Namely,

$$\begin{aligned} {}_{q^2}\begin{bmatrix} x \\ k \end{bmatrix} &= \prod_{i=0}^{k-1} \frac{q^{2x} - q^{2i}}{q^{2k} - q^{2i}}, \\ \beta_{q^2}(x,k) &= \prod_{i=0}^{k-1} {}_{q^2}\begin{bmatrix} x-i \\ 1 \end{bmatrix}. \end{aligned}$$

To make notation simpler and while there is no ambiguity, in this section we shall write ${}_{q^2}\begin{bmatrix} x \\ k \end{bmatrix} = \begin{bmatrix} x \\ k \end{bmatrix}$ and $\beta_{q^2}(x,k) = \beta(x,k)$. We also have that $\sigma_i = \frac{i(i-1)}{2}$ as usual.

As a reminder we can also now re-state the generalised Krawtchouk (2.6.5) polynomials for the skew rank association scheme as defined by Delsarte [12, (15)],

$$P_k(x,n) = \sum_{j=0}^{k} (-1)^{k-j} q^{mj} q^{2\sigma_{k-j}} \begin{bmatrix} n-j \\ n-k \end{bmatrix} \begin{bmatrix} n-x \\ j \end{bmatrix}.$$

We also take Delsarte's MacWilliams Identity for general association schemes and write it here explicitly for the skew rank association scheme, as we will use it later in the proof of the MacWilliams Identity as a functional transform in Section 3.3.2.

Theorem 3.1.1. *Let $\mathscr{C} \subseteq \mathscr{A}_{q,t}$ be a code with skew rank weight distribution $\boldsymbol{c} = (c_0, \ldots, c_n)$ and $\mathscr{C}^\perp$ be its dual code with skew rank weight distribution $\boldsymbol{c'} = (c'_0, \ldots, c'_n)$ and the $(n+1) \times (n+1)$ eigenmatrix of the skew rank association scheme $\boldsymbol{P} = (p_{xk})$, consisting of the eigenvalues $P_k(x,n) = p_{xk}$, then we have*

$$\boldsymbol{c'} = \frac{1}{|\mathscr{C}|} \boldsymbol{cP}. \tag{3.1.1}$$

3.1.2 The Gamma Function

To aid us in notation, we define a new function, that we call the gamma function, for this setting. This is analogous to the alpha function introduced by Gadouleau and Yan [22, Section 2.3].

Definition 3.1.2. The ***skew-q-ary gamma function*** for $x \in \mathbb{R}$, $k \in \mathbb{Z}$ is defined to be

$$\gamma(x,k) = \prod_{i=0}^{k-1} \left(q^x - q^{2i} \right).$$

The statement of the count of matrices of size $t \times t$, Theorem 2.6.6, can then be rewritten as

$$\xi_{t,k} = \begin{bmatrix} n \\ k \end{bmatrix} \gamma(m,k). \tag{3.1.2}$$

Proof. We have,

$$\begin{aligned}
\begin{bmatrix} n \\ k \end{bmatrix} \gamma(m,k) &= \prod_{i=0}^{k-1} \frac{q^{2n} - q^{2i}}{q^{2k} - q^{2i}} \prod_{i=0}^{k-1} \left(q^m - q^{2i}\right) \\
&= \frac{\prod\limits_{i=0}^{k-1} q^{2i} \left(q^{2n-2i} - 1\right) \prod\limits_{i=0}^{k-1} q^{2i} \left(q^{m-2i} - 1\right)}{\prod\limits_{i=0}^{k-1} q^{2i} \left(q^{2k-2i} - 1\right)} \\
&= \begin{cases} q^{2\sigma_k} \dfrac{\prod\limits_{i=0}^{2k-1} \left(q^{2n-i} - 1\right)}{\prod\limits_{i=1}^{k} \left(q^{2i} - 1\right)} & \text{if } t = 2n, \\ q^{2\sigma_k} \dfrac{\prod\limits_{i=0}^{2k-1} \left(q^{2n+1-i} - 1\right)}{\prod\limits_{i=1}^{k} \left(q^{2i} - 1\right)} & \text{if } t = 2n+1. \end{cases} \\
&= q^{2\sigma_k} \frac{\prod\limits_{i=0}^{2k-1} \left(q^{t-i} - 1\right)}{\prod\limits_{i=1}^{k} \left(q^{2i} - 1\right)}
\end{aligned}$$

as required. □

Lemma 3.1.3. *We have the following identities for the skew-q-ary gamma function:*

1. $$\gamma(x,k) = q^{k(k-1)} \prod_{i=0}^{k-1} \left(q^{x-2i} - 1\right),$$

2. $$\frac{\gamma(2x,k)}{\gamma(2k,k)} = \begin{bmatrix} x \\ k \end{bmatrix} = \frac{\prod_{i=0}^{k-1} \left(q^{2x-2i} - 1\right)}{\prod_{i=1}^{k} \left(q^{2i} - 1\right)},$$

3. $$\gamma(x+2,k+1) = \left(q^{x+2} - 1\right) q^{2k} \gamma(x,k), \tag{3.1.3}$$

4. $$\gamma(x,k+1) = \left(q^x - q^{2k}\right) \gamma(x,k). \tag{3.1.4}$$

Proof.

(1)

$$\begin{aligned}\gamma(x,k) &= \prod_{i=0}^{k-1}\left(q^x - q^{2i}\right)\\ &= \prod_{i=0}^{k-1} q^{2i} \prod_{i=0}^{k-1}\left(q^{x-2i} - 1\right)\\ &= q^{k(k-1)} \prod_{i=0}^{k-1}\left(q^{x-2i} - 1\right).\end{aligned}$$

(2)

$$\begin{bmatrix} x\\ k\end{bmatrix} = \frac{\prod_{i=0}^{k-1}\left(q^{2x} - q^{2i}\right)}{\prod_{i=0}^{k-1}\left(q^{2k} - q^{2i}\right)} = \frac{\gamma(2x,k)}{\gamma(2k,k)} = \frac{\prod_{i=0}^{k-1}\left(q^{2x-2i} - 1\right)}{\prod_{i=1}^{k}\left(q^{2i} - 1\right)}.$$

(3)

$$\begin{aligned}\gamma(x+2,k+1) &= \prod_{i=0}^{k}\left(q^{x+2} - q^{2i}\right)\\ &= \left(q^{x+2} - 1\right)\prod_{i=1}^{k}\left(q^{x+2} - q^{2i}\right)\\ &= \left(q^{x+2} - 1\right) q^{2k} \prod_{i=0}^{k-1}\left(q^{x} - q^{2i}\right)\\ &= \left(q^{x+2} - 1\right) q^{2k}\gamma(x,k).\end{aligned}$$

(4)

$$\begin{aligned}\gamma(x,k+1) &= \prod_{i=0}^{k}\left(q^x - q^{2i}\right)\\ &= \left(q^x - q^{2k}\right)\prod_{i=0}^{k-1}\left(q^x - q^{2i}\right)\\ &= \left(q^x - q^{2k}\right)\gamma(x,k).\end{aligned}$$

□

3.2 The Skew-q-Algebra

The skew rank weight enumerators of any linear code $\mathscr{C} \subseteq \mathscr{A}_{q,t}$ are homogeneous polynomials. Taking inspiration from [22, Definition 3] we introduce operations, the skew-q-product, the skew-q-power and the skew-q-transform, on homogeneous polynomials that will help to express the relation between the weight enumerator of a code and that of its dual.

3.2.1 The Skew-q-Product, Skew-q-Power and the Skew-q-Transform

Definition 3.2.1. Let

$$a(X,Y;\lambda) = \sum_{i=0}^{r} a_i(\lambda) Y^i X^{r-i}$$
$$b(X,Y;\lambda) = \sum_{i=0}^{s} b_i(\lambda) Y^i X^{s-i}$$

be two homogeneous polynomials in X and Y with coefficients $a_i(\lambda)$ and $b_i(\lambda)$ respectively, which are real functions of λ that are 0 unless otherwise specified. For example $b_i(\lambda) = 0$ if $i \notin \{0, 1, \ldots, s\}$. The ***skew-$q$-product***, $*$, of $a(X,Y;\lambda)$, of degree r, and $b(X,Y;\lambda)$ of degree s, is defined as

$$\begin{aligned} c(X,Y;\lambda) &= a(X,Y;\lambda) * b(X,Y;\lambda) \\ &= \sum_{u=0}^{r+s} c_u(\lambda) Y^u X^{r+s-u} \end{aligned} \tag{3.2.1}$$

with

$$c_u(\lambda) = \sum_{i=0}^{u} q^{2is} a_i(\lambda) b_{u-i}(\lambda - 2i). \tag{3.2.2}$$

We note that as with the q-product in [22, Lemma 1], the skew-q-product is not commutative or distributive in general. However, if $a(X,Y;\lambda) = a$ is a constant independent of λ, the following property holds:

$$a * b(X,Y;\lambda) = b(X,Y;\lambda) * a = ab(X,Y;\lambda).$$

Another property is that if the degree of $a(X,Y;\lambda)$ and $c(X,Y;\lambda)$ are the same then,

$$\{a(X,Y;\lambda) + c(X,Y;\lambda)\} * b(X,Y;\lambda) = a(X,Y;\lambda) * b(X,Y;\lambda) + c(X,Y;\lambda) * b(X,Y;\lambda)$$

and

$$a(X,Y;\lambda) * \{b(X,Y;\lambda) + c(X,Y;\lambda)\} = a(X,Y;\lambda) * b(X,Y;\lambda) + a(X,Y;\lambda) * c(X,Y;\lambda).$$

Definition 3.2.2. The ***skew-q-power*** is defined by

$$\begin{cases} a^{[0]}(X,Y;\lambda) = 1, \\ a^{[1]}(X,Y;\lambda) = a(X,Y;\lambda), \\ a^{[k]}(X,Y;\lambda) = a(X,Y;\lambda) * a^{[k-1]}(X,Y;\lambda) \quad \text{for } k \geq 2. \end{cases}$$

Definition 3.2.3 ([22, Definition 4])**.** Let $a(X,Y;\lambda) = \sum_{i=0}^{r} a_i(\lambda) Y^i X^{r-i}$. We define the

skew-q-transform to be the homogeneous polynomial

$$\overline{a}(X,Y;\lambda)=\sum_{i=0}^{r} a_i(\lambda)Y^{[i]} * X^{[r-i]}$$

where $Y^{[i]}$ is the i^{th} skew-q-power of the homogeneous polynomial Y and $X^{[r-i]}$ is the $(r-i)^{th}$ skew-q-power of the homogeneous polynomial X.

3.2.2 Using the Skew-q-Product in the Skew Rank Association Scheme

In the theory that follows we consider the following special polynomials which fulfil a similar role in each chapter. First, let

$$\mu(X,Y;\lambda)=X+\left(q^{\lambda}-1\right)Y. \tag{3.2.3}$$

The skew-q-powers of $\mu(X,Y;m)$ provide an explicit form for the weight enumerator of $\mathscr{A}_{q,t}$, the set of skew-symmetric matrices of order t.

Theorem 3.2.4. *If $\mu(X,Y;\lambda)$ is as defined above, then*

$$\mu^{[k]}(X,Y;\lambda)=\sum_{u=0}^{k}\mu_u(\lambda,k)Y^uX^{k-u} \qquad \textit{for } k\geq 1, \tag{3.2.4}$$

where

$$\mu_u(\lambda,k)=\begin{bmatrix}k\\u\end{bmatrix}\gamma(\lambda,u).$$

Specifically, the weight enumerators for $\mathscr{A}_{q,t}$, the set of skew-symmetric matrices of size $t\geq 1$, denoted by Ω_t, is given by,

$$\Omega_t=\mu^{[n]}(X,Y;m)$$

where $n=\left\lfloor \frac{t}{2}\right\rfloor$ and $m=\frac{t(t-1)}{2n}$.

Proof. The proof follows the method of induction. Consider $k=1$, so

$$\mu^{[1]}(X,Y;\lambda)=\mu(X,Y;\lambda)=X+\left(q^{\lambda}-1\right)Y.$$

Then

$$\mu_0(\lambda,1)=1=\begin{bmatrix}1\\0\end{bmatrix}\gamma(\lambda,0)$$
$$\mu_1(\lambda,1)=\left(q^{\lambda}-1\right)=\begin{bmatrix}1\\1\end{bmatrix}\gamma(\lambda,1).$$

So

$$\mu_u(\lambda,1)=\begin{bmatrix}1\\u\end{bmatrix}\gamma(\lambda,u) \tag{3.2.5}$$

as required for $k = 1$. Now assume the theorem is true for $k \geq 1$. Then

$$\begin{aligned}\mu^{[k+1]}(X,Y;\lambda) &= \mu(X,Y;\lambda) * \mu^{[k]}(X,Y;\lambda)\\ &= \left(X + \left(q^{\lambda}-1\right)Y\right) * \left(\sum_{u=0}^{k} \begin{bmatrix} k\\ u\end{bmatrix} \gamma(\lambda,u) Y^{u} X^{k-u}\right)\\ &= \sum_{i=0}^{k+1} f_i(\lambda) Y^i X^{k+1-i}\end{aligned}$$

where,

$$\begin{aligned}f_i(\lambda) = &\sum_{j=0}^{i} q^{2jk} \mu_j(\lambda,1)\mu_{i-j}(\lambda-2j,k)\\ =&\mu_0(\lambda,1)\mu_i(\lambda,k) + q^{2k}\mu_1(\lambda,1)\mu_{i-1}(\lambda-2,k)\\ \overset{(3.2.5)}{=}& \begin{bmatrix} k\\ i\end{bmatrix}\gamma(\lambda,i) + q^{2k}\left(q^{\lambda}-1\right)\begin{bmatrix} k\\ i-1\end{bmatrix}\gamma(\lambda-2,i-1)\\ \overset{(3.1.3)(2.3.32)}{=}& \frac{q^{2(k-i+1)}-1}{q^{2(k+1)}-1}\begin{bmatrix} k+1\\ i\end{bmatrix}\gamma(\lambda,i) + q^{2k}\frac{q^{2i}-1}{q^{2(k+1)}-1}q^{2(1-i)}\begin{bmatrix} k+1\\ i\end{bmatrix}\gamma(\lambda,i)\\ =& \gamma(\lambda,i)\begin{bmatrix} k+1\\ i\end{bmatrix}\left(\frac{q^{2(k-i+1)}-1+q^{2(k-i+1)}\left(q^{2i}-1\right)}{q^{2(k+1)}-1}\right)\\ =& \gamma(\lambda,i)\begin{bmatrix} k+1\\ i\end{bmatrix}\end{aligned}$$

since for $i \geq 1$ we only need to consider the first two coefficients as when $j \geq 2$ then $\mu_j(\lambda,1) = \left[\begin{smallmatrix}1\\ j\end{smallmatrix}\right]\gamma(\lambda,j) = 0$ since $\left[\begin{smallmatrix}1\\ j\end{smallmatrix}\right] = 0$ when $j \geq 2$. So it is true for $k+1$. Therefore by induction the first part of the theorem is true. Now consider $\mu^{[n]}(X,Y;m)$, then clearly

$$\begin{aligned}\mu^{[n]}(X,Y;m) &= \sum_{u=0}^{n}\begin{bmatrix} n\\ u\end{bmatrix}\gamma(m,u)Y^u X^{n-u}\\ &\overset{(3.1.2)}{=} \sum_{u=0}^{n} \xi_{t,u} Y^u X^{n-u} \overset{(2.6.4)}{=} \Omega_t\end{aligned}$$

as required. □

Second, consider the polynomial

$$\nu(X,Y;\lambda) = X - Y.$$

Theorem 3.2.5. *If $\nu(X,Y;\lambda)$ is as defined above, then for all $k \geq 1$,*

$$\nu^{[k]}(X,Y;\lambda) = \sum_{u=0}^{k}\nu_u(\lambda,k)Y^u X^{k-u} = \sum_{u=0}^{k}(-1)^u q^{u(u-1)}\begin{bmatrix} k\\ u\end{bmatrix}Y^u X^{k-u}. \qquad (3.2.6)$$

Proof. We perform induction on k. It is easily checked that the theorem holds for $k = 1$.

Now assume the theorem holds for $k \geq 1$. For clarity, $\nu_0(\lambda, 1) = 1$ and $\nu_1(\lambda, 1) = -1$. Then,

$$\begin{aligned}
\nu^{[k+1]}(X, Y; \lambda) &= \nu(X, Y; \lambda) * \nu^{[k]}(X, Y; \lambda) \\
&= (X - Y) * \left(\sum_{u=0}^{k} (-1)^u q^{u(u-1)} \begin{bmatrix} k \\ u \end{bmatrix} Y^u X^{k-u} \right) \\
&= \sum_{i=0}^{k+1} g_i(\lambda) Y^i X^{k+1-i}
\end{aligned}$$

where

$$\begin{aligned}
g_i(\lambda) &= \sum_{j=0}^{i} q^{2jk} \nu_j(\lambda, k) \nu_{i-j}(\lambda - j, k) \\
&\overset{(3.2.6)}{=} (-1)^i q^0 q^{i(i-1)} \begin{bmatrix} k \\ i \end{bmatrix} + (-1)(-1)^{i-1} q^{2k} q^{(i-1)(i-2)} \begin{bmatrix} k \\ i-1 \end{bmatrix} \\
&\overset{(2.3.32)(2.3.33)}{=} (-1)^i q^{i(i-1)} \frac{q^{2(k-i+1)} - 1}{q^{2(k+1)} - 1} \begin{bmatrix} k+1 \\ i \end{bmatrix} \\
&\qquad + (-1)^i q^{2k} q^{i(i-1)} q^{-2(i-1)} \frac{q^{2i} - 1}{q^{2(k+1)} - 1} \begin{bmatrix} k+1 \\ i \end{bmatrix} \\
&= \frac{(-1)^i q^{i(i-1)}}{q^{2(k+1)} - 1} \begin{bmatrix} k+1 \\ i \end{bmatrix} \left\{ q^{2(k-i+1)} - 1 + q^{2k-2i+2+2i} - q^{2k-2i+2} \right\} \\
&= (-1)^i q^{i(i-1)} \begin{bmatrix} k+1 \\ i \end{bmatrix}
\end{aligned}$$

since if $i \geq 1$ we only consider the first two terms of the sum as when $j \geq 2$ then $\nu_j(\lambda, 1) = 0$ as required.

□

3.3 The MacWilliams Identity for the Skew Rank Association Scheme

In this section we introduce the skew-q-Krawtchouk polynomials which we prove are equal to the generalised Krawtchouk polynomials that are identified in [11, (15)] and [9, (A10)] for the skew rank association scheme. In this way a new q-analog of the MacWilliams Identity for dual subgroups (or codes) of skew-symmetric matrices over $\mathbb{F}_q$ is presented and proven. The proof is by comparison with a traditional form of the identity as given in [12, Theorem 3] and proved in [9, (3.14)]. We note that this method for proving the MacWilliams Identity as a functional transform is different to the one presented in Gadouleau and Yan [22, Theorem 1]. They use character theory, the Hadamard transform and a decomposition of the subspace into component MRD subspaces. We are unable to mimic that proof in this case, due to the lack of relevant maximal subspaces that are generated by a single element in the skew rank association scheme. In exploring the possibility of using subspaces in this new way we found the skew rank weight enumerator for the dual of a specific skew-symmetric matrix, an example of which has been included in Appendix A.3.

3.3.1 The Skew-q-Krawtchouk Polynomials

We now consider the following set of polynomials which arise in finding the skew-q-transform of $\mu(X,Y;m)$ and $\nu(X,Y;m)$ as defined in Section 3.2.2.

Definition 3.3.1. For $t \in \mathbb{Z}^+$, $x,k \in \{0,1,\ldots,n\}$ where $n = \lfloor \frac{t}{2} \rfloor$, and $m = \frac{t(t-1)}{2n}$ we define the ***the skew-q-Krawtchouk Polynomial*** as

$$C_k(x,n) = \sum_{j=0}^{k} (-1)^j q^{2j(n-x)} q^{j(j-1)} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k-j \end{bmatrix} \gamma(m-2j, k-j).$$

The value of the skew-q-Krawtchouk polynomial, $C_k(x,n)$, depends on m, which in turn depends on the parity of t. However, it behaves in the same way regardless of the parity of t, and so we shall use our shorthand notation and only make the dependence on n explicit.

We first prove that the $C_k(x,n)$ satisfy the recurrence relation (2.3.40) and the specific initial values and are therefore the generalised Krawtchouk polynomials. That is, for the skew rank association scheme with $q \in \mathbb{R}^+$, $n \in \mathbb{Z}^+$ and $x,k \in \{0,1,\ldots,n\}$ the recurrence relation is

$$P_{k+1}(x+1, n+1) = q^{2(k+1)} P_{k+1}(x,n) - q^{2k} P_k(x,n)$$

and the specific initial values the $C_k(x,n)$ need to meet are the initial values for the generalised Krawtchouk polyonimals, $P_k(x,n)$, namely

$$P_k(0,n) = \begin{bmatrix} n \\ k \end{bmatrix} \gamma(m,k) \tag{3.3.1}$$

$$P_0(x,k) = 1. \tag{3.3.2}$$

Proposition 3.3.2. *For all $x,k \in \{0,\ldots,n\}$ we have*

$$C_{k+1}(x+1, n+1) = q^{2(k+1)} C_{k+1}(x,n) - q^{2k} C_k(x,n). \tag{3.3.3}$$

Proof. We consider all three terms sequentially. First note that $\begin{bmatrix} x \\ j-1 \end{bmatrix} = 0$ when $j = 0$.

Then

$$
\begin{aligned}
&C_{k+1}(x+1,n+1)\\
&\quad=\sum_{j=0}^{k+1}(-1)^j q^{2j(n-x)}q^{j(j-1)}\begin{bmatrix}x+1\\ j\end{bmatrix}\begin{bmatrix}n-x\\ k+1-j\end{bmatrix}\gamma\left(m+2-2j,k+1-j\right)\\
&\quad= C_{k+1}(x+1,n+1)|_{j=k+1}\\
&\qquad\overset{(2.3.30)}{+}\sum_{j=0}^{k}(-1)^j q^{2j(n-x)+j(j-1)}\left\{\begin{bmatrix}x\\ j-1\end{bmatrix}+q^{2j}\begin{bmatrix}x\\ j\end{bmatrix}\right\}\\
&\qquad\times\begin{bmatrix}n-x\\ k+1-j\end{bmatrix}\gamma\left(m+2-2j,k+1-j\right)\\
&\quad= C_{k+1}(x+1,n+1)|_{j=k+1}\\
&\qquad+\sum_{j=1}^{k}(-1)^j q^{2j(n-x)+j(j-1)}\begin{bmatrix}x\\ j-1\end{bmatrix}\begin{bmatrix}n-x\\ k+1-j\end{bmatrix}\gamma(m+2-2j,k+1-j) \qquad (3.3.4)\\
&\qquad\overset{(3.1.3)}{+}\sum_{j=0}^{k}(-1)^j q^{2j(n-x)+j(j-1)+m+2+2(k-j)}\begin{bmatrix}x\\ j\end{bmatrix}\begin{bmatrix}n-x\\ k+1-j\end{bmatrix}\gamma\left(m-2j,k-j\right)\\
&\qquad\qquad (3.3.5)\\
&\qquad-\sum_{j=0}^{k}(-1)^j q^{2j(n-x)+j(j-1)+2k}\begin{bmatrix}x\\ j\end{bmatrix}\begin{bmatrix}n-x\\ k+1-j\end{bmatrix}\gamma(m-2j,k-j) \qquad (3.3.6)\\
&\quad= C_{k+1}(x+1,n+1)|_{j=k+1}+\alpha_1+\alpha_2+\alpha_3
\end{aligned}
$$

where α_1, α_2, α_3 represent summands (3.3.4), (3.3.5), (3.3.6) respectively and for notation, $|_{j=k+1}$ means “the term when $j=k+1$”.

Second,

$$
\begin{aligned}
&q^{2(k+1)}C_{k+1}(x,n)\\
&\quad=\sum_{j=0}^{k+1}(-1)^j q^{2(k+1)}q^{2j(n-x)}q^{j(j-1)}\begin{bmatrix}x\\ j\end{bmatrix}\begin{bmatrix}n-x\\ k+1-j\end{bmatrix}\gamma(m-2j,k+1-j)\\
&\quad=q^{2(k+1)}\ C_{k+1}(x,n)|_{j=k+1}\\
&\qquad\overset{(3.1.4)}{+}\sum_{j=0}^{k}(-1)^j q^{2j(n-x)+j(j-1)+m+2+2(k-j)}\begin{bmatrix}x\\ j\end{bmatrix}\begin{bmatrix}n-x\\ k+1-j\end{bmatrix}\gamma(m-2j,k-j)\\
&\qquad\qquad (3.3.7)\\
&\qquad-\sum_{j=0}^{k}(-1)^j q^{2j(n-x)+j(j-1)+2k+2(k-j+1)}\begin{bmatrix}x\\ j\end{bmatrix}\begin{bmatrix}n-x\\ k+1-j\end{bmatrix}\gamma(m-2j,k-j)\\
&\qquad\qquad (3.3.8)\\
&\quad=q^{2(k+1)}\ C_{k+1}(x,n)|_{j=k+1}+\alpha_2+\beta_1
\end{aligned}
$$

where β_1 represents the summand (3.3.8). Third,

$$\begin{aligned} q^{2k}C_k(x,n) &= \sum_{j=0}^{k}(-1)^j q^{2j(n-x)+j(j-1)+2k} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k-j \end{bmatrix} \gamma(m-2j,k-j), \\ &= \rho, \text{ say.} \end{aligned}$$

So let $C = C_{k+1}(x+1,n+1) - q^{2(k+1)}C_{k+1}(x,n) + q^{2k}C_k(x,n)$. Then,

$$C = \alpha_1 + \alpha_3 - \beta_1 + \rho + C_{k+1}(x+1,n+1)\big|_{j=k+1} - q^{2(k+1)}\; C_{k+1}\big|_{j=k+1}.$$

Consider $\alpha_3 - \beta_1 + \rho$. Then we have

$$\begin{aligned} \alpha_3 - \beta_1 &= \sum_{j=0}^{k}(-1)^{j+1} q^{2j(n-x)+j(j-1)+2k} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k+1-j \end{bmatrix} \gamma(m-2j,k-j) \left(1-q^{2(k-j+1)}\right) \\ &\overset{(2.3.31)}{=} \sum_{j=0}^{k}(-1)^{j+1} q^{2j(n-x)+j(j-1)+2k} \left(1-q^{2(k-j+1)}\right) \begin{bmatrix} x \\ j \end{bmatrix} \\ &\qquad \times \frac{q^{2((n-x)-(k-j))}-1}{q^{2(k+1-j)}-1} \begin{bmatrix} n-x \\ k-j \end{bmatrix} \gamma(m-2j,k-j) \\ &= \sum_{j=0}^{k}(-1)^j q^{2(j+1)(n-x)+j(j+1)} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k-j \end{bmatrix} \gamma(m-2j,k-j) \qquad (3.3.9) \\ &\qquad - \sum_{j=0}^{k}(-1)^j q^{2j(n-x)+j(j-1)+2k} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k-j \end{bmatrix} \gamma(m-2j,k-j) \\ &= \tau - \rho \end{aligned}$$

where τ represents the summand in (3.3.9). Thus,

$$C = \alpha_1 + \tau + C_{k+1}(x+1,n+1)\big|_{j=k+1} - q^{2(k+1)}\; C_{k+1}(x,n)\big|_{j=k+1}.$$

Now,

$$\begin{aligned} &C_{k+1}\;(x+1,n+1)\big|_{j=k+1} - q^{2(k+1)}\; C_{k+1}(x,n)\big|_{j=k+1} \\ &\qquad = (-1)^{k+1} q^{2(k+1)(n-x)} q^{(k+1)k} \left\{ \begin{bmatrix} x+1 \\ k+1 \end{bmatrix} - q^{2(k+1)} \begin{bmatrix} x \\ k+1 \end{bmatrix} \right\} \\ &\qquad \overset{(2.3.30)}{=} (-1)^{k+1} q^{2(k+1)(n-x)} q^{(k+1)k} \begin{bmatrix} x \\ k \end{bmatrix} \\ &\qquad = -\tau\big|_{j=k}. \end{aligned}$$

Now consider α_1.

$$\begin{aligned}
\alpha_1 &= \sum_{j=1}^{k} (-1)^j q^{2j(n-x)+j(j-1)} \begin{bmatrix} x \\ j-1 \end{bmatrix} \begin{bmatrix} n-x \\ k+1-j \end{bmatrix} \gamma(m+2-2j, k+1-j) \\
&= \sum_{j=0}^{k-1} (-1)^{j+1} q^{2(j+1)(n-x)+j(j+1)} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k-j \end{bmatrix} \gamma(m-2j, k-j) \\
&= -\tau + \tau|_{j=k}.
\end{aligned}$$

Thus $C = 0$ and so the $C_k(x,n)$ satisfy the recurrence relation (3.3.3). □

Lemma 3.3.3. *The $C_k(x,n)$ are the generalised Krawtchouk polynomials. In other words,*

$$C_k(x,n) = P_k(x,n). \tag{3.3.10}$$

Proof. The $C_k(x,n)$ satisfy the recurrence relation (3.3.3) and the initial values of the $C_k(x,n)$ are

$$\begin{aligned}
C_k(0,n) &= \sum_{j=0}^{k} (-1)^j q^{2jn} q^{j(j-1)} \begin{bmatrix} 0 \\ j \end{bmatrix} \begin{bmatrix} n \\ k-j \end{bmatrix} \gamma(m-2j, k-j) \\
&= \begin{bmatrix} n \\ k \end{bmatrix} \gamma(m,k)
\end{aligned}$$

since $\begin{bmatrix} 0 \\ j \end{bmatrix} = 0$ for $j > 0$, and

$$\begin{aligned}
C_0(x,n) &= (-1)^0 q^{0(n-x)} q^0 \begin{bmatrix} x \\ 0 \end{bmatrix} \begin{bmatrix} n-x \\ 0 \end{bmatrix} \gamma(m,0) \\
&= 1
\end{aligned}$$

as required. □

We note that this explicit form for the generalised Krawtchouk polynomials is distinct from the three forms presented in [11, (15)] as shown in Example 5.2.10.

3.3.2 The MacWilliams Identity for the Skew Rank Association Scheme

We now use the skew-q-Krawtchouk polynomials to prove the q-analog form of the MacWilliams Identity for the skew rank association scheme. We note that this form is similar to the q-analog of the MacWilliams Identity developed in [22, Theorem 1] for linear rank metric codes over $\mathbb{F}_{q^m}$ but differs in the parameters of the q-algebra and the meaning of the variable m.

Let the skew rank weight enumerator of $\mathscr{C} \subseteq \mathscr{A}_{q,t}$ be

$$W_{\mathscr{C}}^{SR}(X,Y) = \sum_{i=0}^{n} c_i Y^i X^{n-i}$$

and of its dual, $\mathscr{C}^\perp \subseteq \mathscr{A}_{q,t}$ be

$$W_{\mathscr{C}^\perp}^{SR}(X,Y) = \sum_{i=0}^{n} c_i' Y^i X^{n-i}.$$

Theorem 3.3.4 (The MacWilliams Identity for the Skew Rank Association Scheme)**.** *Let $\mathscr{C} \subseteq \mathscr{A}_{q,t}$ be a linear code with weight distribution $\boldsymbol{c} = (c_0, \ldots, c_n)$ with $n = \left\lfloor \frac{t}{2} \right\rfloor$ and $m = \frac{t(t-1)}{2n}$, and $\mathscr{C}^\perp \subseteq \mathscr{A}_{q,t}$ its dual code with weight distribution $\boldsymbol{c'} = (c_0', \ldots, c_n')$. Then*

$$W_{\mathscr{C}^\perp}^{SR}(X,Y) = \frac{1}{|\mathscr{C}|} \overline{W}_{\mathscr{C}}^{SR} \left(X + (q^m-1)Y, X - Y\right).$$

Proof. For $0 \le i \le n$ we have

$$\begin{aligned}
&(X-Y)^{[i]} * (X + (q^m-1)\,Y)^{[n-i]} \\
&\quad = \left(\nu^{[i]}(X,Y;n)\right) * \left(\mu^{[n-i]}(X,Y;m)\right) \\
&\quad \overset{(3.2.4)(3.2.6)}{=} \left(\sum_{u=0}^{i} (-1)^u q^{u(u-1)} \begin{bmatrix} i \\ u \end{bmatrix} Y^u X^{i-u}\right) * \left(\sum_{j=0}^{n-i} \begin{bmatrix} n-i \\ j \end{bmatrix} \gamma(m,j) Y^j X^{n-i-j}\right) \\
&\quad \overset{(3.2.1)}{=} \sum_{k=0}^{n} \left(\sum_{\ell=0}^{k} q^{2\ell(n-i)} (-1)^\ell q^{\ell(\ell-1)} \begin{bmatrix} i \\ \ell \end{bmatrix} \begin{bmatrix} n-i \\ k-\ell \end{bmatrix} \gamma(m-2\ell, k-\ell)\right) Y^k X^{n-k} \\
&\quad = \sum_{k=0}^{n} C_k(i,n) Y^k X^{n-k} \\
&\quad \overset{(3.3.10)}{=} \sum_{k=0}^{n} P_k(i,n) Y^k X^{n-k}.
\end{aligned}$$

So then we have

$$\begin{aligned}
\frac{1}{|\mathscr{C}|} \overline{W}_{\mathscr{C}}^{SR} \left(X + (q^m-1)\,Y, X - Y\right) &= \frac{1}{|\mathscr{C}|} \sum_{i=0}^{n} c_i \sum_{k=0}^{n} P_k(i,n) Y^k X^{n-k} \\
&= \sum_{k=0}^{n} \left(\frac{1}{|\mathscr{C}|} \sum_{i=0}^{n} c_i P_k(i,n)\right) Y^k X^{n-k} \\
&\overset{(3.1.1)}{=} \sum_{k=0}^{n} c_k' Y^k X^{n-k} \\
&= W_{\mathscr{C}^\perp}^{SR}(X,Y).
\end{aligned}$$

□

In this way we have shown that the MacWilliams Identity for a code and its dual based on skew-symmetric matrices over $\mathbb{F}_q$ can be expressed as a q-transform of homogeneous polynomials in a form analogous to the original MacWilliams Identity for the Hamming association scheme and the q-analog developed by Gadouleau and Yan [22] for the rank association scheme.

3.4 The Skew-q-Derivatives

To complete our skew-q-algebra, in this section we develop a new skew-q-derivative and skew-q^{-1}-derivative to help analyse the coefficients of skew rank weight enumerators. This is analogous to the q-derivatives applied to the rank association scheme [22, Definition 5, 6] with the parameter q replaced by q^2.

3.4.1 The Skew-q-Derivative

Definition 3.4.1. For $q \geq 2$, the ***skew-q-derivative*** at $X \neq 0$ for a real-valued function $f(X)$ is defined as

$$f^{(1)}(X) = \frac{f\left(q^2 X\right) - f(X)}{(q^2-1)X}.$$

For $\varphi \geq 0$ we denote the φ^{th} skew-q-derivative (with respect to X) of $f(X,Y;\lambda)$ as $f^{(\varphi)}(X,Y;\lambda)$. The 0^{th} skew-q-derivative of $f(X,Y;\lambda)$ is $f(X,Y;\lambda)$. For any $a \in \mathbb{R}$, $X \neq 0$, and real-valued function $g(X)$, we have

$$[f(X) + ag(X)]^{(1)} = f^{(1)}(X) + ag^{(1)}(X).$$

Lemma 3.4.2.

1. *For $0 \leq \varphi \leq \ell$, $\varphi \in \mathbb{Z}^+$ and $\ell \geq 0$,*

$$\left(X^{\ell}\right)^{(\varphi)} = \beta(\ell,\varphi)X^{\ell-\varphi}.$$

2. *The φ^{th} skew-q-derivative of $f(X,Y;\lambda) = \sum_{i=0}^{r} f_i(\lambda)Y^i X^{r-i}$ is given by*

$$f^{(\varphi)}(X,Y;\lambda) = \sum_{i=0}^{r-\varphi} f_i(\lambda)\beta(r-i,\varphi)Y^i X^{r-i-\varphi}. \tag{3.4.1}$$

3. *Also,*

$$\mu^{[k](\varphi)}(X,Y;\lambda) = \beta(k,\varphi)\mu^{[k-\varphi]}(X,Y;\lambda) \tag{3.4.2}$$

$$\nu^{[k](\varphi)}(X,Y;\lambda) = \beta(k,\varphi)\nu^{[k-\varphi]}(X,Y;\lambda). \tag{3.4.3}$$

Proof.

(1) For $\varphi = 1$ we have

$$\left(X^\ell\right)^{(1)} = \frac{\left(q^2X\right)^\ell - X^\ell}{(q^2-1)X} = \frac{q^{2\ell}-1}{q^2-1}X^{\ell-1} = \begin{bmatrix}\ell\\1\end{bmatrix} = \beta(\ell,\varphi)X^{\ell-1}.$$

The rest of the proof follows by induction on φ and is omitted.

(2) Now consider $f(X,Y;\lambda) = \sum_{i=0}^{r} f_i(\lambda)Y^iX^{r-i}$. We have,

$$\begin{aligned}
f^{(1)}(X,Y;\lambda) &= \left(\sum_{i=0}^{r} f_i(\lambda)Y^iX^{r-i}\right)^{(1)}\\
&= \sum_{i=0}^{r} f_i(\lambda)Y^i\left(X^{r-i}\right)^{(1)}\\
&= \sum_{i=0}^{r-1} f_i(\lambda)\beta(r-i,\varphi)Y^iX^{r-i-1}.
\end{aligned}$$

Then the case of $\varphi = 1$ holds. The rest of the proof follows by induction on φ and is omitted.

(3) Now consider $\mu^{[k]} = \sum_{u=0}^{k} \mu_u(\lambda,k)Y^uX^{k-u}$ where $\mu_u(\lambda,k) = \begin{bmatrix}k\\u\end{bmatrix}\gamma(\lambda,u)$ as in Equation (3.2.4). Then we have

$$\begin{aligned}
\mu^{[k](1)}(X,Y;\lambda) &= \left(\sum_{u=0}^{k} \mu_u(\lambda,k)Y^uX^{k-u}\right)^{(1)}\\
&= \sum_{u=0}^{k} \mu_u(\lambda,k)Y^u\left(\frac{\left(q^2X\right)^{k-u} - X^{k-u}}{(q^2-1)X}\right)\\
&= \sum_{u=0}^{k-1} \frac{q^{2(k-u)}-1}{q^2-1}\begin{bmatrix}k\\u\end{bmatrix}\gamma(\lambda,u)Y^uX^{k-u-1}\\
&\overset{(2.3.32)}{=} \sum_{u=0}^{k-1} \frac{\left(q^{2k}-1\right)\left(q^{2(k-u)}-1\right)}{(q^{2(k-u)}-1)(q^2-1)}\begin{bmatrix}k-1\\u\end{bmatrix}\gamma(\lambda,u)Y^uX^{k-u-1}\\
&= \left(\frac{q^{2k}-1}{q^2-1}\right)\mu^{[k-1]}(X,Y;\lambda)\\
&\overset{(2.3.34)}{=} \beta(k,1)\mu^{[k-1]}(X,Y;\lambda).
\end{aligned}$$

Then the case of $\varphi = 1$ holds. The statement of the theorem, $\mu^{[k](\varphi)}(X,Y;\lambda) = \beta(k,\varphi)\mu^{[k-\varphi]}(X,Y;\lambda)$, then follows by induction on φ and is omitted.

Now consider $\nu^{[k]}(X,Y;\lambda) = \sum_{u=0}^{k}(-1)^uq^{u(u-1)}\begin{bmatrix}k\\u\end{bmatrix}Y^uX^{k-u}$ as in Equation (3.2.6).

Then we have

$$\begin{aligned}
\nu^{[k](1)}(X,Y;\lambda) &= \sum_{u=0}^{k}(-1)^u q^{u(u-1)}\frac{q^{2(k-u)}-1}{q^2-1}\begin{bmatrix}k\\u\end{bmatrix}Y^uX^{k-u-1}\\
&\overset{(2.3.32)}{=} \sum_{u=0}^{k-1}(-1)^u q^{u(u-1)}\frac{\left(q^{2k}-1\right)\left(q^{2(k-u)}-1\right)}{\left(q^{2(k-u)}-1\right)\left(q^2-1\right)}\begin{bmatrix}k-1\\u\end{bmatrix}Y^uX^{k-1-u}\\
&= \left(\frac{q^{2k}-1}{q^2-1}\right)\nu^{[k-1]}(X,Y;\lambda)\\
&\overset{(2.3.34)}{=} \beta(k,1)\nu^{[k-1]}(X,Y;\lambda).
\end{aligned}$$

So $\nu^{[k](\varphi)}(X,Y;\lambda)=\beta(k,\varphi)\nu^{[k-\varphi]}(X,Y;\lambda)$ follows by induction also and is omitted.

□

We now need a few smaller lemmas in order to prove the Leibniz rule for the skew-q-derivative.

Lemma 3.4.3. *Let*

$$\begin{aligned}
u\left(X,Y;\lambda\right) &= \sum_{i=0}^{r}u_i(\lambda)Y^iX^{r-i}\\
v\left(X,Y;\lambda\right) &= \sum_{i=0}^{s}v_i(\lambda)Y^iX^{s-i}.
\end{aligned}$$

1. *If $u_r(\lambda)=0$ then*

$$\frac{1}{X}\left[u\left(X,Y;\lambda\right)*v\left(X,Y;\lambda\right)\right]=\frac{u\left(X,Y;\lambda\right)}{X}*v\left(X,Y;\lambda\right). \tag{3.4.4}$$

2. *If $v_s(\lambda)=0$ then*

$$\frac{1}{X}\left[u\left(X,Y;\lambda\right)*v\left(X,Y;\lambda\right)\right]=u\left(X,q^2Y;\lambda\right)*\frac{v\left(X,Y;\lambda\right)}{X}. \tag{3.4.5}$$

Proof.

(1) If $u_r(\lambda)=0$,

$$\frac{u\left(X,Y;\lambda\right)}{X}=\sum_{i=0}^{r-1}u_i(\lambda)Y^iX^{r-i-1}.$$

Hence

$$\begin{aligned}
\frac{u\left(X,Y;\lambda\right)}{X} * v\left(X,Y;\lambda\right) &\overset{(3.2.2)}{=} \sum_{k=0}^{r+s-1}\left(\sum_{\ell=0}^{k} q^{2\ell s}u_\ell(\lambda)v_{k-\ell}(\lambda-2\ell)\right)Y^kX^{r+s-1-k}\\
&= \frac{1}{X}\sum_{k=0}^{r+s-1}\left(\sum_{\ell=0}^{k} q^{2\ell s}u_\ell(\lambda)v_{k-\ell}(\lambda-2\ell)\right)Y^kX^{r+s-k}\\
&\qquad + \frac{1}{X}\sum_{\ell=0}^{r+s} q^{2\ell s}u_\ell(\lambda)v_{r+s-\ell}(\lambda-2\ell)Y^{r+s}X^0\\
&= \frac{1}{X}\sum_{k=0}^{r+s}\left(\sum_{\ell=0}^{k} q^{2\ell s}u_\ell(\lambda)v_{k-\ell}(\lambda-2\ell)\right)Y^kX^{r+s-k}\\
&= \frac{1}{X}\left(u\left(X,Y;\lambda\right) * v\left(X,Y;\lambda\right)\right)
\end{aligned}$$

since $v_{r+s-\ell}(\lambda-2\ell)=0$ for $0\le\ell\le r-1$ and $u_\ell(\lambda)=0$ for $r\le\ell\le r+s$. So

$$\frac{1}{X}\sum_{\ell=0}^{r+s} q^{2\ell s}u_\ell(\lambda)v_{r+s-\ell}(\lambda-2\ell)Y^{r+s}X^0=0.$$

(2) Now if $v_s(\lambda)=0$,

$$\frac{v\left(X,Y;\lambda\right)}{X}=\sum_{i=0}^{s-1} v_i(\lambda)Y^iX^{s-1-i}.$$

Then similarly,

$$\begin{aligned}
u\left(X,q^2Y;\lambda\right) * \frac{v\left(X,Y;\lambda\right)}{X} &\overset{(3.2.2)}{=} \sum_{k=0}^{r+s-1}\left(\sum_{\ell=0}^{k} q^{2\ell(s-1)}q^{2\ell}u_\ell(\lambda)v_{k-\ell}(\lambda-2\ell)\right)Y^kX^{r+s-1-k}\\
&= \frac{1}{X}\sum_{k=0}^{r+s-1}\left(\sum_{\ell=0}^{k} q^{2\ell(s-1)}q^{2\ell}u_\ell(\lambda)v_{k-\ell}(\lambda-2\ell)\right)Y^kX^{r+s-k}\\
&\qquad + \frac{1}{X}\sum_{\ell=0}^{r+s} q^{2\ell s}u_\ell(\lambda)v_{r+s-\ell}(\lambda-2\ell)Y^{r+s}X^0\\
&= \frac{1}{X}\sum_{k=0}^{r+s}\left(\sum_{\ell=0}^{k} q^{2\ell(s-1)}q^{2\ell}u_\ell(\lambda)v_{k-\ell}(\lambda-2\ell)\right)Y^kX^{r+s-k}\\
&= \frac{1}{X}\left[u(X,Y;\lambda) * v(X,Y;\lambda)\right]
\end{aligned}$$

since $v_{r+s-\ell}(\lambda-2\ell)=0$ for $0\le\ell\le r$ and $u_\ell(\lambda)=0$ for $r+1\le\ell\le r+s$. So

$$\frac{1}{X}\sum_{\ell=0}^{r+s} q^{2\ell s}u_\ell(\lambda)v_{r+s-\ell}(\lambda-2\ell)Y^{r+s}X^0=0$$

as required. □

Theorem 3.4.4 (Leibniz rule for the skew-q-derivative)**.** *For two homogeneous polynomials in X and Y, $f(X,Y;\lambda)$ and $g(X,Y;\lambda)$ with degrees r and s respectively, and for $\varphi\ge 0$, the φ^{th} skew-q-derivative of their skew-q-product is given by*

$$[f(X,Y;\lambda) * g(X,Y;\lambda)]^{(\varphi)} = \sum_{\ell=0}^{\varphi} \begin{bmatrix}\varphi\\ \ell\end{bmatrix} q^{2(\varphi-\ell)(r-\ell)} f^{(\ell)}(X,Y;\lambda) * g^{(\varphi-\ell)}(X,Y;\lambda). \quad (3.4.6)$$

Proof. For simplification, we shall write $f(X,Y;\lambda)$ as $f(X,Y)$ and similarly $g(X,Y;\lambda)$ as $g(X,Y)$. Now by differentiation we have

$$\begin{aligned}
[f(X,Y) * g(X,Y)]^{(1)} &= \frac{f\left(q^2X,Y\right) * g\left(q^2X,Y\right) - f(X,Y) * g(X,Y)}{(q^2-1)X} \\
&= \frac{1}{(q^2-1)X}\Big\{ f\left(q^2X,Y\right) * g\left(q^2X,Y\right) - f\left(q^2X,Y\right) * g(X,Y) \\
&\qquad + f\left(q^2X,Y\right) * g(X,Y) - f(X,Y) * g(X,Y) \Big\} \\
&= \frac{1}{(q^2-1)X}\left\{ f\left(q^2X,Y\right) * \left(g\left(q^2X,Y\right) - g(X,Y)\right)\right\} \\
&\qquad + \frac{1}{(q^2-1)X}\Big\{ \left(f\left(q^2X,Y\right) - f(X,Y)\right) * g(X,Y) \Big\} \\
&\overset{(3.4.5)}{=} f\left(q^2X,q^2Y\right) * \left\{\frac{g\left(q^2X,Y\right) - g(X,Y)}{(q^2-1)X}\right\} \\
&\qquad \overset{(3.4.4)}{+} \left\{\frac{f\left(q^2X,Y\right) - f(X,Y)}{(q^2-1)X}\right\} * g(X,Y) \\
&= q^{2r} f(X,Y) * g^{(1)}(X,Y) + f^{(1)}(X,Y) * g(X,Y) \qquad (3.4.7)
\end{aligned}$$

since $g_s(\lambda)Y^s\left(q^2X\right)^0 = g_s(\lambda)Y^sX^0$, so we can use (3.4.5). Similarly, $f_r(\lambda)Y^r\left(q^2X\right)^0 = f_r(\lambda)Y^rX^0$, so we can use (3.4.4) So the initial case holds. Assume the statement holds true for $\varphi = \overline{\varphi}$, i.e.

$$[f(X,Y) * g(X,Y)]^{(\overline{\varphi})} = \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} q^{2(\overline{\varphi}-\ell)(r-\ell)} f^{(\ell)}(X,Y) * g^{(\overline{\varphi}-\ell)}(X,Y).$$

Now considering $\overline{\varphi}+1$ and for simplicity writing $f(X,Y;\lambda)$, $g(X,Y;\lambda)$ as f, g we have

$$\begin{aligned}
[f * g]^{(\overline{\varphi}+1)} &= \left[\sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} q^{2(\overline{\varphi}-\ell)(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}-\ell)}\right]^{(1)} \\
&= \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} q^{2(\overline{\varphi}-\ell)(r-\ell)} \left[f^{(\ell)} * g^{(\overline{\varphi}-\ell)}\right]^{(1)} \\
&\overset{(3.4.7)}{=} \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} q^{2(\overline{\varphi}-\ell)(r-\ell)} \left(q^{2(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}-\ell+1)} + f^{(\ell+1)} * g^{(\overline{\varphi}-\ell)}\right) \\
&= \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} q^{2(\overline{\varphi}-\ell+1)(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}-\ell+1)} \\
&\qquad + \sum_{\ell=1}^{\overline{\varphi}+1} \begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix} q^{2(\overline{\varphi}-\ell+1)(r-\ell+1)} f^{(\ell)} * g^{(\overline{\varphi}-\ell+1)} \\
&= \begin{bmatrix}\overline{\varphi}\\ 0\end{bmatrix} q^{2(\overline{\varphi}+1)r} f * g^{(\overline{\varphi}+1)} + \sum_{\ell=1}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} q^{2(\overline{\varphi}+1-\ell)(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}-\ell+1)} \\
&\qquad + \begin{bmatrix}\overline{\varphi}\\ \overline{\varphi}\end{bmatrix} q^{2(\overline{\varphi}+1-\overline{\varphi}-1)(r-\overline{\varphi}-1+1)} f^{(\overline{\varphi}+1)} * g \\
&\qquad + \sum_{\ell=1}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix} q^{2(\overline{\varphi}+1-\ell)(r-\ell+1)} f^{(\ell)} * g^{(\overline{\varphi}-\ell+1)} \\
&= q^{2(\overline{\varphi}+1)r} f * g^{(\overline{\varphi}+1)} + f^{(\overline{\varphi}+1)} * g \\
&\qquad + \sum_{\ell=1}^{\overline{\varphi}} \left(\begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} + q^{2(\overline{\varphi}-\ell+1)} \begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix}\right) q^{2(\overline{\varphi}-\ell+1)(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}-\ell+1)} \\
&\overset{(2.3.29)}{=} \sum_{\ell=1}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}+1\\ \ell\end{bmatrix} q^{2(\overline{\varphi}+1-\ell)(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}+1-\ell)} + \begin{bmatrix}\overline{\varphi}+1\\ 0\end{bmatrix} q^{2(\overline{\varphi}+1)r} f * g^{(\overline{\varphi}+1)} \\
&\qquad + \begin{bmatrix}\overline{\varphi}+1\\ \overline{\varphi}+1\end{bmatrix} q^{2(\overline{\varphi}+1-\overline{\varphi}-1)} f^{(\overline{\varphi}+1)} * g \\
&= \sum_{\ell=0}^{\overline{\varphi}+1} \begin{bmatrix}\overline{\varphi}+1\\ \ell\end{bmatrix} q^{2(\overline{\varphi}+1-\ell)(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}+1-\ell)}
\end{aligned}$$

as required. □

3.4.2 The Skew-q^{-1}-Derivative

Definition 3.4.5. For $q \geq 2$, the ***skew-q^{-1}-derivative*** at $Y \neq 0$ for a real-valued function $g(Y)$ is defined as

$$g^{\{1\}}(Y) = \frac{g\left(q^{-2}Y\right) - g\left(Y\right)}{(q^{-2}-1)Y}.$$

For $\varphi \geq 0$ we denote the φ^{th} skew-q^{-1}-derivative (with respect to Y) of $g(X, Y; \lambda)$ as $g^{\{\varphi\}}(X, Y; \lambda)$. The 0^{th} skew-q^{-1}-derivative of $g(X, Y; \lambda)$ is $g(X, Y; \lambda)$. For any $a \in \mathbb{R}$, $Y \neq 0$ and real-valued function $f(Y)$,

$$[f(Y) + ag(Y)]^{\{1\}} = f^{\{1\}}(Y) + ag^{\{1\}}(Y).$$

Lemma 3.4.6.

1. *For* $0 \leq \varphi \leq \ell$, $\varphi \in \mathbb{Z}^+$ *and* $\ell \geq 0$,

$$\left(Y^\ell\right)^{\{\varphi\}} = q^{2(\varphi(1-\ell)+\sigma_\varphi)}\beta(\ell,\varphi)Y^{\ell-\varphi}.$$

2. *The* φ^{th} *skew-*q^{-1}*-derivative of* $g(X,Y;\lambda) = \sum_{i=0}^{s} g_i(\lambda)Y^iX^{s-i}$ *is given by*

$$g^{\{\varphi\}}(X,Y;\lambda) = \sum_{i=\varphi}^{s} g_i(\lambda)q^{2(\varphi(1-i)+\sigma_\varphi)}\beta(i,\varphi)Y^{i-\varphi}X^{s-i}. \tag{3.4.8}$$

3. *Also,*

$$\mu^{[k]\{\varphi\}}(X,Y;\lambda) = q^{-2\sigma_\varphi}\beta(k,\varphi)\gamma(\lambda,\varphi)\mu^{[k-\varphi]}(X,Y;\lambda-2\varphi) \tag{3.4.9}$$

$$\nu^{[k]\{\varphi\}}(X,Y;\lambda) = (-1)^\varphi\beta(k,\varphi)\nu^{[k-\varphi]}(X,Y;\lambda). \tag{3.4.10}$$

Proof.

(1) For $\varphi = 1$ we have

$$\begin{aligned}\left(Y^\ell\right)^{\{1\}} = \frac{\left(q^{-2}Y\right)^\ell - Y^\ell}{(q^{-2}-1)Y} &= \left(\frac{q^{-2\ell}-1}{q^{-2}-1}\right)Y^{\ell-1}\\ &= q^{-2\ell+2}\beta(\ell,1)Y^{\ell-1}.\end{aligned}$$

So the initial case holds. Assume the case for $\varphi = \overline{\varphi}$ holds. Then we have

$$\begin{aligned}\left(Y^\ell\right)^{\{\overline{\varphi}+1\}} &= \left(q^{2(\overline{\varphi}(1-\ell)+\sigma_{\overline{\varphi}})}\beta(\ell,\overline{\varphi})Y^{\ell-\overline{\varphi}}\right)^{\{1\}}\\ &= q^{2(\overline{\varphi}(1-\ell)+\sigma_{\overline{\varphi}})}\beta(\ell,\overline{\varphi})\frac{q^{-2(\ell-\overline{\varphi})}Y^{\ell-\overline{\varphi}} - Y^{\ell-\overline{\varphi}}}{\left(q^{-2}-1\right)Y}\\ &= q^{2(\overline{\varphi}(1-\ell)+\sigma_{\overline{\varphi}})}\left(\frac{q^{-2(\ell-\overline{\varphi})}-1}{q^{-2}-1}\right)\beta(\ell,\overline{\varphi})Y^{\ell-\overline{\varphi}-1}\\ &\overset{(2.3.34)}{=} q^{2\overline{\varphi}(1-\ell)}q^{\overline{\varphi}(\overline{\varphi}-1)}q^{-2(\ell-\overline{\varphi})}q^2\frac{q^{2(\ell-\overline{\varphi})}-1}{q^2-1}\prod_{i=0}^{\overline{\varphi}-1}\begin{bmatrix}\ell-i\\1\end{bmatrix}Y^{\ell-\overline{\varphi}-1}\\ &= q^{2((\overline{\varphi}+1)(1-\ell)+\sigma_{\overline{\varphi}+1})}\beta(\ell,\overline{\varphi}+1)Y^{\ell-\overline{\varphi}+1}.\end{aligned}$$

Thus the statement holds by induction.

(2) Now consider $g(X,Y;\lambda) = \sum_{i=0}^{s} g_i(\lambda)Y^iX^{s-i}$. For $\varphi = 1$ we have

$$g^{\{1\}}(X,Y;\lambda) = \left(\sum_{i=0}^{s} g_i(\lambda)Y^iX^{s-i}\right)^{\{1\}} = \sum_{i=0}^{s} g_i(\lambda)q^{2(-i+1)}\beta(i,1)Y^{i-1}X^{s-i}.$$

As $\beta(i,1)=0$ when $i=0$ we have

$$g^{\{1\}}(X,Y;\lambda)=\sum_{i=1}^{s} g_i(\lambda)q^{2((1-i)+\sigma_1)}\beta(i,1)Y^{i-1}X^{s-i}.$$

So the initial case holds. Now assume the case holds for $\varphi=\overline{\varphi}$ i.e. $g^{\{\overline{\varphi}\}}(X,Y;\lambda)=\sum_{i=\overline{\varphi}}^{s} g_i(\lambda)q^{2\overline{\varphi}(1-i)+2\sigma_{\overline{\varphi}}}\beta(i,\overline{\varphi})Y^{(i-\overline{\varphi})}X^{s-i}$. Then we have

$$\begin{aligned}
g^{\{\overline{\varphi}+1\}}(X,Y;\lambda) &= \left(\sum_{i=\overline{\varphi}}^{s} g_i(\lambda)q^{2(\overline{\varphi}(1-i)+\sigma_{\overline{\varphi}})}\beta(i,\overline{\varphi})Y^{i-\overline{\varphi}}X^{s-i}\right)^{\{1\}}\\
&= \sum_{i=\overline{\varphi}}^{s} g_i(\lambda)q^{2(\overline{\varphi}(1-i)+\sigma_{\overline{\varphi}})}\beta(i,\overline{\varphi})q^{-2(i-\overline{\varphi}-1)}\beta(i-\overline{\varphi},1)Y^{i-\overline{\varphi}-1}X^{s-i}\\
&\overset{(2.3.34)}{=} \sum_{i=\overline{\varphi}}^{s} g_i(\lambda)q^{2(\overline{\varphi}+1)(1-i)+2\sigma_{\overline{\varphi}}}\left(\prod_{j=0}^{\overline{\varphi}-1}\frac{q^{2(i-j)}-1}{q^2-1}\right)\\
&\qquad\times\frac{\left(q^{2(i-\overline{\varphi})}-1\right)}{q^2-1}Y^{i-\overline{\varphi}-1}X^{s-i}\\
&= \sum_{i=\overline{\varphi}}^{s} g_i(\lambda)q^{2(\overline{\varphi}+1)(1-i)+2\sigma_{\overline{\varphi}}}\beta(i,\overline{\varphi}+1)Y^{i-\overline{\varphi}-1}X^{s-i}\\
&= \sum_{i=\overline{\varphi}+1}^{s} g_i(\lambda)q^{2(\overline{\varphi}+1)(1-i)+2\sigma_{\overline{\varphi}}}\beta(i,\overline{\varphi}+1)Y^{i-\overline{\varphi}-1}X^{s-i}
\end{aligned}$$

since when $i=\overline{\varphi}$, $\beta(\overline{\varphi},\overline{\varphi}+1)=0$. So by induction Equation (3.4.8) holds.

(3) Now consider $\mu^{[k]}(X,Y;\lambda)=\sum_{u=0}^{k}\mu_u(\lambda,k)Y^uX^{k-u}$ where $\mu_u(\lambda,k)=\begin{bmatrix}k\\u\end{bmatrix}\gamma(\lambda,u)$ as in Equation (3.2.6). Then we have

$$\begin{aligned}
\mu^{[k]\{1\}}(X,Y;\lambda) &= \left(\sum_{u=0}^{k}\mu_u(\lambda,k)Y^uX^{k-u}\right)^{\{1\}}\\
&= \sum_{u=1}^{k}\mu_u(\lambda,k)q^{2(1-u)}\beta(u,1)Y^{u-1}X^{k-u}\\
&= \sum_{r=0}^{k-1}\mu_{r+1}(\lambda,k)q^{2(1-(r+1))}\beta(r+1,1)Y^{r+1-1}X^{k-r-1}\\
&= \sum_{r=0}^{k-1}\begin{bmatrix}k\\r+1\end{bmatrix}\gamma(\lambda,r+1)q^{-2r}\beta(r+1,1)Y^rX^{k-1-r}\\
&\overset{(2.3.33)(3.1.3)}{=} \sum_{r=0}^{k-1}\begin{bmatrix}k-1\\r\end{bmatrix}\frac{q^{2k}-1}{q^{2(r+1)}-1}\left(q^{\lambda}-1\right)q^{2r}q^{-2r}\gamma(\lambda-2,r)\\
&\qquad\times\beta(r+1,1)Y^rX^{k-1-r}\\
&\overset{(2.3.37)}{=} \sum_{r=0}^{k-1}\begin{bmatrix}k-1\\r\end{bmatrix}\frac{q^{2k}-1}{q^2-1}\left(q^{\lambda}-1\right)q^{2r}q^{-2r}\gamma(\lambda-2,r)Y^rX^{k-1-r}\\
&= q^{-2\sigma_1}\beta(k,1)\gamma(\lambda,1)\mu^{[k-1]}(X,Y;\lambda-2).
\end{aligned}$$

Now assume that the statement holds for $\varphi = \overline{\varphi}$. Then we have

$$\begin{aligned}
\mu^{[k]\{\overline{\varphi}+1\}}(X,Y;\lambda) &= \left[q^{-2\sigma_{\overline{\varphi}}}\beta(k,\overline{\varphi})\gamma(\lambda,\overline{\varphi})\mu^{[k-\overline{\varphi}]}(X,Y;\lambda-2\overline{\varphi})\right]^{\{1\}} \\
&\overset{(3.2.4)}{=} q^{-2\sigma_{\overline{\varphi}}}\beta(k,\overline{\varphi})\gamma(\lambda,\overline{\varphi})\left(\sum_{r=0}^{k-\overline{\varphi}}\begin{bmatrix}k-\overline{\varphi}\\ r\end{bmatrix}\gamma(\lambda-2\overline{\varphi},r)Y^rX^{k-\overline{\varphi}-r}\right)^{\{1\}} \\
&= q^{-2\sigma_{\overline{\varphi}}}\beta(k,\overline{\varphi})\gamma(\lambda,\overline{\varphi})\sum_{r=1}^{k-\overline{\varphi}}\begin{bmatrix}k-\overline{\varphi}\\ r\end{bmatrix}\gamma(\lambda-2\overline{\varphi},r)\left(Y^r\right)^{\{1\}}X^{k-\overline{\varphi}-r} \\
&= q^{-2\sigma_{\overline{\varphi}}}\beta(k,\overline{\varphi})\gamma(\lambda,\overline{\varphi})\sum_{u=0}^{k-\overline{\varphi}-1}\begin{bmatrix}k-\overline{\varphi}\\ u+1\end{bmatrix}\gamma(\lambda-2\overline{\varphi},u+1) \\
&\qquad\times\left(Y^{u+1}\right)^{\{1\}}X^{k-\overline{\varphi}-u-1} \\
&= q^{-2\sigma_{\overline{\varphi}}}\beta(k,\overline{\varphi})\gamma(\lambda,\overline{\varphi})\sum_{u=0}^{k-\overline{\varphi}-1}\begin{bmatrix}k-\overline{\varphi}\\ u+1\end{bmatrix}\gamma(\lambda-2\overline{\varphi},u+1) \\
&\qquad\times q^{2(1-(u+1))}\beta(u+1,1)Y^{u+1-1}X^{k-\overline{\varphi}-u-1} \\
&\overset{(2.3.33)(3.1.3)}{=} q^{-2\sigma_{\overline{\varphi}}}\beta(k,\overline{\varphi})\gamma(\lambda,\overline{\varphi})\sum_{u=0}^{k-(\overline{\varphi}+1)}\begin{bmatrix}k-\overline{\varphi}-1\\ u\end{bmatrix} \\
&\qquad\times\frac{\left(q^{2(k-\overline{\varphi})}-1\right)\left(q^{2(u+1)}-1\right)}{\left(q^{2(u+1)}-1\right)\left(q^2-1\right)}q^{2u}q^{-2u}\left(q^{\lambda-2\overline{\varphi}}-1\right) \\
&\qquad\times\gamma(\lambda-2(\overline{\varphi}+1),u)Y^uX^{k-(\overline{\varphi}+1)-u} \\
&= q^{-2\sigma_{\overline{\varphi}}}q^{-2\overline{\varphi}}\gamma(\lambda,\overline{\varphi}+1)\beta(k,\overline{\varphi}+1)\mu^{[k-(\overline{\varphi}+1)]}(X,Y;\lambda-2(\overline{\varphi}+1)) \\
&= q^{-2\sigma_{\overline{\varphi}+1}}\gamma(\lambda,\overline{\varphi}+1)\beta(k,\overline{\varphi}+1)\mu^{[k-(\overline{\varphi}+1)]}(X,Y;\lambda-2(\overline{\varphi}+1))
\end{aligned}$$

as required. Now consider $\nu^{[k]} = \sum_{u=0}^{k}(-1)^uq^{u(u-1)}\begin{bmatrix}k\\ u\end{bmatrix}Y^uX^{k-u}$ as defined in Theorem 3.2.5. Then we have

$$\begin{aligned}
\nu^{[k]\{1\}}(X,Y;\lambda) &= \left(\sum_{u=0}^{k}(-1)^uq^{u(u-1)}\begin{bmatrix}k\\ u\end{bmatrix}Y^uX^{k-u}\right)^{\{1\}} \\
&= \sum_{u=1}^{k}(-1)^uq^{u(u-1)}\begin{bmatrix}k\\ u\end{bmatrix}\left(Y^u\right)^{\{1\}}X^{k-u} \\
&= \sum_{r=0}^{k-1}(-1)^{(r+1)}q^{r(r+1)}q^{2(1-(r+1))}\begin{bmatrix}k\\ r+1\end{bmatrix}\beta(r+1,1)Y^{r+1-1}X^{k-r-1} \\
&\overset{(2.3.33)}{=} -\sum_{r=0}^{k-1}(-1)^rq^{r(r-1)}q^{2r}q^{-2r}\begin{bmatrix}k-1\\ r\end{bmatrix}\frac{\left(q^{2k}-1\right)\left(q^{2(r+1)}-1\right)}{\left(q^{2(r+1)}-1\right)\left(q^2-1\right)}Y^rX^{k-r-1} \\
&= (-1)^1\beta(k,1)\nu^{[k-1]}(X,Y;\lambda).
\end{aligned}$$

So the case for $\varphi = 1$ holds Now assume that the statement holds for $\varphi = \overline{\varphi}$. Then we have

$$\begin{aligned}
\nu^{[k]}(X,Y;\lambda)^{\{\overline{\varphi}+1\}} &= \left[(-1)^{\overline{\varphi}}\beta(k,\overline{\varphi})\nu^{[k-\overline{\varphi}]}(X,Y;\lambda)\right]^{\{1\}} \\
&= (-1)^{\overline{\varphi}}\beta(k,\overline{\varphi})\sum_{u=1}^{k-\overline{\varphi}}(-1)^u q^{u(u-1)}\begin{bmatrix}k-\overline{\varphi}\\ u\end{bmatrix}\left(Y^u\right)^{\{1\}}X^{k-\overline{\varphi}-u} \\
&= (-1)^{\overline{\varphi}}\beta(k,\overline{\varphi})\sum_{r=0}^{k-\overline{\varphi}-1}(-1)^{r+1}q^{r(r+1)}q^{-2(r+1)+2}\begin{bmatrix}k-\overline{\varphi}\\ r+1\end{bmatrix} \\
&\qquad\times\beta(r+1,1)Y^{r+1-1}X^{k-\overline{\varphi}-r-1} \\
&\overset{(2.3.33)}{=} (-1)^{\overline{\varphi}+1}\beta(k,\overline{\varphi})\sum_{r=0}^{k-\overline{\varphi}-1}(-1)^r q^{r(r-1)}\begin{bmatrix}k-(\overline{\varphi}+1)\\ r\end{bmatrix} \\
&\qquad\times\frac{\left(q^{2(k-\overline{\varphi})}-1\right)\left(q^{2(r+1)}-1\right)}{\left(q^{2(r+1)}-1\right)\left(q^2-1\right)}Y^rX^{k-\overline{\varphi}-1-r} \\
&= (-1)^{\overline{\varphi}+1}\beta(k,\overline{\varphi}+1)\nu^{[k-(\overline{\varphi}+1)]}(X,Y;\lambda)
\end{aligned}$$

as required. □

Now we need a few smaller lemmas in order to prove the Leibniz rule for the skew-q^{-1}-derivative.

Lemma 3.4.7. *Let*

$$\begin{aligned}
u\left(X,Y;\lambda\right) &= \sum_{i=0}^{r}u_i(\lambda)Y^iX^{r-i} \\
v\left(X,Y;\lambda\right) &= \sum_{i=0}^{s}v_i(\lambda)Y^iX^{s-i}.
\end{aligned}$$

1. *If $u_0(\lambda)=0$ then*

$$\frac{1}{Y}\left[u\left(X,Y;\lambda\right)*v\left(X,Y;\lambda\right)\right] = q^{2s}\frac{u\left(X,Y;\lambda\right)}{Y}*v\left(X,Y;\lambda-2\right). \tag{3.4.11}$$

2. *If $v_0(\lambda)=0$ then*

$$\frac{1}{Y}\left[u\left(X,Y;\lambda\right)*v\left(X,Y;\lambda\right)\right] = u\left(X,q^2Y;\lambda\right)*\frac{v\left(X,Y;\lambda\right)}{Y}. \tag{3.4.12}$$

Proof.

(1) Suppose $u_0(\lambda)=0$. Then

$$\frac{u\left(X,Y;\lambda\right)}{Y} = \sum_{i=1}^{r}u_i(\lambda)Y^{i-1}X^{r-i} = \sum_{i=0}^{r-1}u_{i+1}(\lambda)Y^iX^{r-i-1}.$$

Hence

$$\begin{aligned}
&q^{2s}\frac{u\left(X,Y;\lambda\right)}{Y}*v\left(X,Y;\lambda-2\right)\\
&\qquad=q^{2s}\sum_{u=0}^{r+s-1}\left(\sum_{\ell=0}^{u}q^{2\ell s}u_{\ell+1}(\lambda)v_{u-\ell}(\lambda-2\ell-2)\right)Y^{u}X^{r+s-1-u}\\
&\qquad=q^{2s}\sum_{u=0}^{r+s-1}\left(\sum_{i=1}^{u+1}q^{2(i-1)s}u_{i}(\lambda)v_{u-i+1}(\lambda-2i)\right)Y^{u}X^{r+s-1-u}\\
&\qquad=q^{2s}\sum_{j=1}^{r+s}\left(\sum_{i=1}^{j}q^{2(i-1)s}u_{i}(\lambda)v_{j-i}(\lambda-2j)\right)Y^{j-1}X^{r+s-j}\\
&\qquad=\frac{1}{Y}\sum_{j=0}^{r+s}\left(\sum_{i=0}^{j}q^{2is}u_{i}(\lambda)v_{j-i}(\lambda-2i)\right)Y^{j}X^{r+s-j}\\
&\qquad=\frac{1}{Y}\left(u\left(X,Y;\lambda\right)*v\left(X,Y;\lambda\right)\right)
\end{aligned}$$

since when $j=0$, $\sum_{i=0}^{j}q^{2is}u_i(\lambda)v_{j-i}(\lambda-2i)=0$ as $u_0(\lambda)=0$.

(2) Now if $v_0(\lambda)=0$, then

$$\begin{aligned}
\frac{v\left(X,Y;\lambda\right)}{Y}&=\sum_{j=1}^{s}v_j(\lambda)Y^{j-1}X^{s-j}\\
&=\sum_{i=0}^{s-1}v_{i+1}(\lambda)Y^{i}X^{s-i-1}.
\end{aligned}$$

So,

$$\begin{aligned}
&u\left(X,q^2Y;\lambda\right)*\frac{v\left(X,Y;\lambda\right)}{Y}\\
&\qquad=\sum_{u=0}^{r+s-1}\left(\sum_{j=0}^{u}q^{2j(s-1)}q^{2j}u_j(\lambda)v_{u-j+1}(\lambda-2j)\right)Y^{u}X^{r+s-1-u}\\
&\qquad=\sum_{\ell=1}^{r+s}\left(\sum_{j=0}^{\ell-1}q^{2js}u_j(\lambda)v_{\ell-j}(\lambda-2j)\right)Y^{\ell-1}X^{r+s-\ell}\\
&\qquad=\frac{1}{Y}\sum_{\ell=1}^{r+s}\left(\sum_{j=0}^{\ell}q^{2js}u_j(\lambda)v_{\ell-j}(\lambda-2j)\right)Y^{\ell}X^{r+s-\ell}\\
&\qquad=\frac{1}{Y}\sum_{\ell=0}^{r+s}\left(\sum_{j=0}^{\ell}q^{2js}u_j(\lambda)v_{\ell-j}(\lambda-2j)\right)Y^{\ell}X^{r+s-\ell}\\
&\qquad=\frac{1}{Y}\left(u\left(X,Y;\lambda\right)*v\left(X,Y;\lambda\right)\right)
\end{aligned}$$

since when $j=\ell$, $\sum_{j=0}^{\ell}q^{2js}u_j(\lambda)v_{\ell-j}(\lambda-2j)=0$ as $v_0(\lambda)=0$. □

Theorem 3.4.8 (Leibniz rule for the skew-q^{-1}-derivative)**.** *For two homogeneous polynomials in Y, $f(X,Y;\lambda)$ and $g(X,Y;\lambda)$ with degrees r and s respectively and for $\varphi\geq 0$, the*

φ^{th} *skew-q^{-1}-derivative of their skew-q-product is given by*

$$[f(X,Y;\lambda)*g(X,Y;\lambda)]^{\{\varphi\}} = \sum_{\ell=0}^{\varphi} \begin{bmatrix}\varphi\\ \ell\end{bmatrix} q^{2\ell(s-\varphi+\ell)} f^{\{\ell\}}(X,Y;\lambda)*g^{\{\varphi-\ell\}}(X,Y;\lambda-2\ell).$$

Proof. For simplification we shall write $f(X,Y;\lambda),\ g(X,Y;\lambda)$ as $f(Y;\lambda),\ g(Y;\lambda)$. Now by differentiation we have

$$\begin{aligned}
[f(Y;\lambda)*g(Y;\lambda)]^{\{1\}} &= \frac{f\left(q^{-2}Y;\lambda\right)*g\left(q^{-2}Y;\lambda\right)-f(Y;\lambda)*g(Y;\lambda)}{(q^{-2}-1)Y}\\
&= \frac{1}{(q^{-2}-1)Y}\Big\{ f\left(q^{-2}Y;\lambda\right)*g\left(q^{-2}Y;\lambda\right)-f\left(q^{-2}Y;\lambda\right)*g(Y;\lambda)\\
&\qquad + f\left(q^{-2}Y;\lambda\right)*g(Y;\lambda)-f(Y;\lambda)*g(Y;\lambda)\Big\}\\
&= \frac{1}{(q^{-2}-1)Y}\Big\{ f\left(q^{-2}Y;\lambda\right)*\left(g\left(q^{-2}Y;\lambda\right)-g(Y;\lambda)\right)\Big\}\\
&\qquad + \frac{1}{(q^{-2}-1)Y}\Big\{\left(f\left(q^{-2}Y;\lambda\right)-f(Y;\lambda)\right)*g(Y;\lambda)\Big\}\\
&\overset{(3.4.12)}{=} f(Y;\lambda)*\frac{\left(g\left(q^{-2}Y;\lambda\right)-g(Y;\lambda)\right)}{(q^{-2}-1)\,Y}\\
&\qquad \overset{(3.4.11)}{+} q^{2s}\frac{\left(f\left(q^{-2}Y;\lambda\right)-f(Y;\lambda)\right)}{(q^{-2}-1)\,Y}*g(Y;\lambda-2)\\
&= f(Y;\lambda)*g^{\{1\}}(Y;\lambda)+q^{2s}f^{\{1\}}(Y;\lambda)*g(Y;\lambda-2).
\end{aligned}$$

So the initial case holds. Assume the statement holds true for $\varphi=\overline{\varphi}$, i.e.

$$\Big[f(X,Y;\lambda)*g(X,Y;\lambda)\Big]^{\{\overline{\varphi}\}} = \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} q^{2\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}(X,Y;\lambda)*g^{\{\overline{\varphi}-\ell\}}(X,Y;\lambda-2\ell).$$

Now considering $\overline{\varphi}+1$ and for simplicity writing $f(X,Y;\lambda),\ g(X,Y;\lambda)$ as $f(\lambda),\ g(\lambda)$ we have

$$
\begin{aligned}
\Big[f(\lambda) * g(\lambda)\Big]^{\{\overline{\varphi}+1\}} &= \left[\sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} q^{2\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}(\lambda) * g^{\{\overline{\varphi}-\ell\}}(\lambda-2\ell)\right]^{\{1\}} \\
&\overset{(3.4.2)}{=} \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} q^{2\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}(\lambda) * g^{\{\overline{\varphi}-\ell+1\}}(\lambda-2\ell) \\
&\qquad + \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} q^{2\ell(s-\overline{\varphi}+\ell)} q^{2(v-\overline{\varphi}+\ell)} f^{\{\ell+1\}}(\lambda) * g^{\{\overline{\varphi}-\ell\}}(\lambda-2\ell-2) \\
&= \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} q^{2\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}(\lambda) * g^{\{\overline{\varphi}-\ell+1\}}(\lambda-2\ell) \\
&\qquad + \sum_{\ell=1}^{\overline{\varphi}+1} \begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix} q^{2(\ell-1)(s-\overline{\varphi}+\ell-1)} q^{2(s-\overline{\varphi}+(\ell-1))} \\
&\qquad \times f^{\{\ell\}}(\lambda) * g^{\{\overline{\varphi}-\ell+1\}}(\lambda-2\ell) \\
&= f(\lambda) * g^{\{\overline{\varphi}+1\}}(\lambda) + \sum_{\ell=1}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} q^{2\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}(\lambda) * g^{\{\overline{\varphi}-\ell+1\}}(\lambda-2\ell) \\
&\qquad + \begin{bmatrix}\overline{\varphi}\\ \overline{\varphi}\end{bmatrix} q^{2(\overline{\varphi}+1)(s+1)} q^{-2\overline{\varphi}-2} f^{\{\overline{\varphi}+1\}}(\lambda) * g(\lambda-2(\overline{\varphi}+1)) \\
&\qquad + \sum_{\ell=1}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix} q^{2(\ell-1)(s-\overline{\varphi}+\ell-1)} q^{2(s-\overline{\varphi}+(\ell-1))} \\
&\qquad \times f^{\{\ell\}}(\lambda) * g^{\{\overline{\varphi}-\ell+1\}}(\lambda-2\ell) \\
&= f(\lambda) * g^{\{\overline{\varphi}+1\}}(\lambda) + \sum_{\ell=1}^{\overline{\varphi}} \left(\begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} + q^{-2\ell} \begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix} \right) q^{2\ell(s-\overline{\varphi}+\ell)} \\
&\qquad \times f^{\{\ell\}}(\lambda) * g^{\{\overline{\varphi}+1-\ell\}}(\lambda-2\ell) \\
&\qquad + q^{2s(\overline{\varphi}+1)} f^{\{\overline{\varphi}+1\}}(\lambda) * g(\lambda-2(\overline{\varphi}+1)) \\
&\overset{(2.3.30)}{=} f(\lambda) * g^{\{\overline{\varphi}+1-\ell\}}(\lambda) + \sum_{\ell=1}^{\overline{\varphi}} q^{-2\ell} \begin{bmatrix}\overline{\varphi}+1\\ \ell\end{bmatrix} q^{2\ell(s-\overline{\varphi}+\ell)} \\
&\qquad \times f^{\{\ell\}}(\lambda) * g^{\{\overline{\varphi}+1-\ell\}}(\lambda-2\ell) \\
&\qquad + \begin{bmatrix}\overline{\varphi}+1\\ \overline{\varphi}+1\end{bmatrix} q^{2(\overline{\varphi}+1)(s-\overline{\varphi}-1+(\overline{\varphi}+1))} \\
&\qquad \times f^{\{\overline{\varphi}+1\}}(\lambda) * g^{\{\overline{\varphi}+1-(\overline{\varphi}+1)\}}(\lambda-2(\overline{\varphi}+1)) \\
&= \sum_{\ell=0}^{\overline{\varphi}+1} \begin{bmatrix}\overline{\varphi}+1\\ \ell\end{bmatrix} q^{2\ell(s-(\overline{\varphi}+1)+\ell)} f^{\{\ell\}}(\lambda) * g^{\{\overline{\varphi}+1-\ell\}}(\lambda-2\ell)
\end{aligned}
$$

as required. □

3.4.3 Evaluating the Skew-q-Derivative and the Skew-q^{-1}-Derivative

Now we need to introduce some lemmas which yield useful results when developing moments of the skew rank weight distribution. These lemmas are analogous to parts of the proof of [22, Proposition 4], but in more detail.

Lemma 3.4.9. *For $j, \ell \in \mathbb{Z}^+,\ 0 \leq \ell \leq j$ and $X = Y = 1$,*

$$\nu^{[j](\ell)}(1, 1; \lambda) = \beta(j, j)\delta_{j\ell}. \tag{3.4.13}$$

Proof. Consider

$$\nu^{[j](\ell)}(X, Y; \lambda) \overset{(3.4.3)}{=} \beta(j, \ell) \sum_{u=0}^{j-\ell} (-1)^u q^{u(u-1)} \begin{bmatrix} j-\ell \\ u \end{bmatrix} Y^u X^{j-\ell-u}.$$

So

$$\begin{aligned} \nu^{[j](\ell)}(1, 1; \lambda) &= \beta(j, \ell) \sum_{u=0}^{j-\ell} (-1)^u q^{u(u-1)} \begin{bmatrix} j-\ell \\ u \end{bmatrix} \\ &\overset{(2.3.35)}{=} \beta(\ell, \ell) \begin{bmatrix} j \\ \ell \end{bmatrix} \sum_{u=0}^{j-\ell} (-1)^u q^{u(u-1)} \begin{bmatrix} j-\ell \\ u \end{bmatrix} \\ &\overset{(2.3.24)(2.3.25)}{=} \beta(\ell, \ell) \sum_{k=\ell}^{j} (-1)^{k-\ell} q^{\sigma_{k-\ell}} \begin{bmatrix} j \\ k \end{bmatrix} \begin{bmatrix} k \\ \ell \end{bmatrix} \\ &\overset{(2.3.28)}{=} \beta(\ell, \ell)\delta_{\ell j} = \beta(j, j)\delta_{j\ell}. \end{aligned}$$

□

Lemma 3.4.10. *For any homogeneous polynomial, $\rho(X, Y; \lambda)$ and for any $s \geq 0$,*

$$\left(\rho * \mu^{[s]}\right)(1, 1; \lambda) = q^{\lambda s} \rho(1, 1; \lambda). \tag{3.4.14}$$

Proof. Let $\rho(X, Y; \lambda) = \sum_{i=0}^{r} \rho_i(\lambda) Y^i X^{r-i}$, then by Theorem 3.2.4 we have,

$$\mu^{[s]}(X, Y; \lambda) = \sum_{t=0}^{s} \begin{bmatrix} s \\ t \end{bmatrix} \gamma(\lambda, t) Y^t X^{s-t} = \sum_{t=0}^{s} \mu_t^{[s]}(\lambda) Y^t X^{s-t}$$

and using the skew-q-product we have

$$\left(\rho * \mu^{[s]}\right)(X, Y; \lambda) = \sum_{u=0}^{r+s} c_u(\lambda) Y^u X^{(r+s-u)}$$

where

$$c_u(\lambda) = \sum_{i=0}^{u} q^{2is} \rho_i(\lambda) \mu_{u-i}^{[s]}(\lambda - 2i).$$

Then

$$\begin{aligned}\left(\rho * \mu^{[s]}\right)(1,1;\lambda) &= \sum_{u=0}^{r+s} c_u(\lambda) = \sum_{u=0}^{r+s}\sum_{i=0}^{u} q^{2is}\rho_i(\lambda)\mu_{u-i}^{[s]}(\lambda-2i)\\ &= \sum_{j=0}^{r+s} q^{2js}\rho_j(\lambda)\left(\sum_{k=0}^{r+s-j}\mu_k^{[s]}(\lambda-2j)\right)\\ &= \sum_{j=0}^{r} q^{2js}\rho_j(\lambda)\left(\sum_{k=0}^{s}\mu_k^{[s]}(\lambda-2j)\right)\\ &= \sum_{j=0}^{r} q^{2js}\rho_j(\lambda)\left(\sum_{k=0}^{s}\begin{bmatrix}s\\k\end{bmatrix}\gamma(\lambda-2j,k)\right)\\ &\overset{(2.3.27)}{=} \sum_{j=0}^{r} q^{2js}\rho_j(\lambda)q^{(\lambda-2j)s}\\ &= q^{\lambda s}\rho(1,1;\lambda)\end{aligned}$$

since $\rho_j(\lambda)=0$ when $j>r$ and $\mu_k^{[s]}(\lambda-2j)=0$ when $k>s$. □

3.5 Moments of the Skew Rank Distribution

Here we explore the moments of the skew rank distribution of a subgroup of skew-symmetric matrices over $\mathbb{F}_q$ and that of its dual. These are the Gaussian binomial moments of the weight distribution comparable to the binomial moments in the Hamming case which are demonstrated and illustrated well in [41, p131] and for rank metric codes over $\mathbb{F}_{q^m}$ in [22, Prop 4]. Deriving these moments help us evaluate the important parameters of each code. The moments derived from the skew-q-derivative and the skew-q^{-1}-derivative look similar, but the first takes the derivative with respect to X whilst the second takes the derivative with the respect to Y.

3.5.1 Moments derived from the Skew-q-Derivative

Proposition 3.5.1. *For $0 \le \varphi \le n$ and a linear code $\mathscr{C} \subseteq \mathscr{A}_{q,t}$ and its dual $\mathscr{C}^\perp \subseteq \mathscr{A}_{q,t}$ with weight distributions $\boldsymbol{c} = (c_0,\dots,c_n)$ and $\boldsymbol{c'} = (c'_0,\dots,c'_n)$, respectively we have*

$$\sum_{i=0}^{n-\varphi}\begin{bmatrix}n-i\\ \varphi\end{bmatrix}c_i = \frac{1}{|\mathscr{C}^\perp|}q^{m(n-\varphi)}\sum_{i=0}^{\varphi}\begin{bmatrix}n-i\\ n-\varphi\end{bmatrix}c_i^{'}.$$

Proof. We apply Theorem 3.3.4 to $\mathscr{C}^\perp$, giving

$$W_{\mathscr{C}}^{SR}(X,Y) = \frac{1}{|\mathscr{C}^\perp|}\overline{W}_{\mathscr{C}^\perp}^{SR}\left(X+(q^m-1)Y, X-Y\right)$$

or equivalently

$$\begin{aligned}\sum_{i=0}^{n} c_i Y^i X^{n-i} &= \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{n} c_i'\,(X-Y)^{[i]} * [X+(q^m-1)\,Y]^{[n-i]}\\ &= \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{n} c_i'\nu^{[i]}(X,Y;m) * \mu^{[n-i]}(X,Y;m). \qquad (3.5.1)\end{aligned}$$

For each side of Equation (3.5.1), we shall apply the skew-q-derivative φ times and then evaluate at $X=Y=1$.

For the left hand side, we obtain

$$\left(\sum_{i=0}^{n} c_i Y^i X^{n-i}\right)^{(\varphi)} \overset{(3.4.1)}{=} \sum_{i=0}^{n-\varphi} c_i \beta(n-i,\varphi) Y^i X^{(n-i-\varphi)}.$$

Letting $X=Y=1$ then gives

$$\begin{aligned}\sum_{i=0}^{n-\varphi} c_i\beta(n-i,\varphi) &\overset{(2.3.35)}{=} \sum_{i=0}^{n-\varphi} c_i \begin{bmatrix} n-i \\ \varphi \end{bmatrix}\beta(\varphi,\varphi)\\ &= \beta(\varphi,\varphi)\sum_{i=0}^{n-\varphi} c_i \begin{bmatrix} n-i \\ \varphi \end{bmatrix}.\end{aligned}$$

We now move on to the right hand side. For simplicity we write $\mu(X,Y;m)$ as μ and similarly $\nu(X,Y;m)$ as ν. Then by Theorem 3.4.4,

$$\begin{aligned}\left(\frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{n} c_i'\nu^{[i]} * \mu^{[n-i]}\right)^{(\varphi)} &\overset{(3.4.6)}{=} \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{n} c_i' \left(\sum_{\ell=0}^{\varphi}\begin{bmatrix} \varphi \\ \ell \end{bmatrix} q^{2(\varphi-\ell)(i-\ell)}\nu^{[i](\ell)} * \mu^{[n-i](\varphi-\ell)}\right)\\ &= \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{n} c_i'\psi_i(X,Y;m)\end{aligned}$$

where

$$\psi_i(X,Y;m) = \sum_{\ell=0}^{\varphi}\begin{bmatrix} \varphi \\ \ell \end{bmatrix} q^{2(\varphi-\ell)(i-\ell)}\nu^{[i](\ell)}(X,Y;m) * \mu^{[n-i](\varphi-\ell)}(X,Y;m).$$

So with $X = Y = 1$

$$\begin{aligned}
\psi_i(1,1;m) &\overset{(3.4.2)}{=} \sum_{\ell=0}^{\varphi} \begin{bmatrix}\varphi\\ \ell\end{bmatrix} q^{2(\varphi-\ell)(i-\ell)}\beta(n-i,\varphi-\ell)\left(\nu^{[i](\ell)} * \mu^{[n-i-\varphi+\ell]}\right)(1,1;m)\\
&\overset{(3.4.14)}{=} \sum_{\ell=0}^{\varphi} \begin{bmatrix}\varphi\\ \ell\end{bmatrix} q^{2(\varphi-\ell)(i-\ell)}\beta(n-i,\varphi-\ell)q^{m(n-i-(\varphi-\ell))}\nu^{[i](\ell)}(1,1;m)\\
&\overset{(3.4.13)}{=} \sum_{\ell=0}^{\varphi} q^{2(\varphi-\ell)(i-\ell)} \begin{bmatrix}\varphi\\ \ell\end{bmatrix} \beta(n-i,\varphi-\ell)q^{m(n-i-(\varphi-\ell))}\beta(i,i)\delta_{i\ell}\\
&\overset{(2.3.35)}{=} \begin{bmatrix}\varphi\\ i\end{bmatrix}\begin{bmatrix}n-i\\ \varphi-i\end{bmatrix}\beta(\varphi-i,\varphi-i)q^{m(n-\varphi)}\beta(i,i)\\
&\overset{(2.3.36)}{=} \begin{bmatrix}n-i\\ \varphi-i\end{bmatrix} q^{m(n-\varphi)}\beta(\varphi,\varphi).
\end{aligned}$$

Thus

$$\begin{aligned}
\frac{1}{|\mathscr{C}^\perp|}\sum_{i=0}^{n} c_i'\psi_i(1,1;m) &= \frac{1}{|\mathscr{C}^\perp|}\sum_{i=0}^{\varphi} c_i' \begin{bmatrix}n-i\\ \varphi-i\end{bmatrix} q^{m(n-\varphi)}\beta(\varphi,\varphi)\\
&\overset{(2.3.24)}{=} \beta(\varphi,\varphi)\frac{q^{m(n-\varphi)}}{|\mathscr{C}^\perp|}\sum_{i=0}^{\varphi} c_i' \begin{bmatrix}n-i\\ n-\varphi\end{bmatrix}.
\end{aligned}$$

Combining the results for each side, and simplifying, we finally obtain

$$\sum_{i=0}^{n-\varphi} c_i \begin{bmatrix}n-i\\ \varphi\end{bmatrix} = \frac{q^{m(n-\varphi)}}{|\mathscr{C}^\perp|}\sum_{i=0}^{\varphi} c_i' \begin{bmatrix}n-i\\ n-\varphi\end{bmatrix}$$

as required. □

Note. In particular, if $\varphi = 0$ we have

$$\sum_{i=0}^{n} c_i = \frac{q^{mn}}{|\mathscr{C}^\perp|}c_0' = \frac{q^{mn}}{|\mathscr{C}^\perp|}.$$

In other words

$$|\mathscr{C}||\mathscr{C}^\perp| = q^{mn}.$$

We note that $mn = \frac{t(t-1)}{2}$ for skew-symmetric matrices and $q^{\frac{t(t-1)}{2}}$ is the number of skew-symmetric matrices of size $t \times t$. This is the simple fact that the dimensions of a code and that of its dual add up to the dimension of the whole space they belong to.

We can simplify Proposition 3.5.1 if φ is less than the minimum distance of the dual code.

Corollary 3.5.2. *Let d_{SR}' be the minimum skew rank distance of $\mathscr{C}^\perp$. If $0 \le \varphi < d_{SR}'$ then*

$$\sum_{i=0}^{n-\varphi} \begin{bmatrix}n-i\\ \varphi\end{bmatrix} c_i = \frac{1}{|\mathscr{C}^\perp|}q^{m(n-\varphi)}\begin{bmatrix}n\\ \varphi\end{bmatrix}.$$

Proof. We have $c_0' = 1$ and $c_1' = \ldots = c_\varphi' = 0$. □

3.5.2 Moments derived from the Skew-q^{-1}-Derivative

The next proposition relates the moments of the skew rank distribution of a linear code to those of its dual, this time using the skew-q^{-1}-derivative of the MacWilliams Identity for the skew rank association scheme. Before proceeding we first need the following two lemmas.

Lemma 3.5.3. *Let* $\delta(\lambda,\varphi,j)=\sum_{i=0}^{j}\begin{bmatrix} j\\ i\end{bmatrix}(-1)^i q^{2\sigma_i}\gamma(\lambda-2i,\varphi)$*. Then for all* $\lambda\in\mathbb{R},\varphi,j\in\mathbb{Z}$*,*

$$\delta(\lambda,\varphi,j)=\gamma(2\varphi,j)\gamma(\lambda-2j,\varphi-j)q^{j(\lambda-2j)}. \tag{3.5.2}$$

Proof. Initial case: $j=0$.

$$\delta(\lambda,\varphi,0)=\begin{bmatrix} 0\\ 0\end{bmatrix}(-1)^0 q^{2\sigma_0}\gamma(\lambda,\varphi)=\gamma(\lambda,\varphi)=\gamma(2\varphi,0)\gamma(\lambda,\varphi)q^{0(\lambda)}.$$

So the initial case holds. Now assume the case is true for $j=\bar{\jmath}$ and consider the $\bar{\jmath}+1$ case.

$$\begin{aligned}
\delta(\lambda,\varphi,\bar{\jmath}+1)&=\sum_{i=0}^{\bar{\jmath}+1}\begin{bmatrix} \bar{\jmath}+1\\ i\end{bmatrix}(-1)^i q^{2\sigma_i}\gamma(\lambda-2i,\varphi)\\
&\overset{(2.3.30)}{=}\sum_{i=0}^{\bar{\jmath}+1}\left(q^{2i}\begin{bmatrix} \bar{\jmath}\\ i\end{bmatrix}+\begin{bmatrix} \bar{\jmath}\\ i-1\end{bmatrix}\right)(-1)^i q^{2\sigma_i}\gamma(\lambda-2i,\varphi)\\
&=\sum_{i=0}^{\bar{\jmath}}\begin{bmatrix} \bar{\jmath}\\ i\end{bmatrix}(-1)^i q^{2\sigma_i}q^{2i}\gamma(\lambda-2i,\varphi)+\sum_{i=0}^{\bar{\jmath}}\begin{bmatrix} \bar{\jmath}\\ i\end{bmatrix}(-1)^{i+1} q^{2\sigma_{i+1}}\gamma(\lambda-2(i+1),\varphi)\\
&\overset{(3.1.3)}{=}\sum_{i=0}^{\bar{\jmath}}\begin{bmatrix} \bar{\jmath}\\ i\end{bmatrix}(-1)^i q^{2i}q^{2\sigma_i}\left(q^{\lambda-2i}-1\right)q^{2(\varphi-1)}\gamma(\lambda-2i-2,\varphi-1)\\
&\qquad\overset{(3.1.3)}{-}\sum_{i=0}^{\bar{\jmath}}\begin{bmatrix} \bar{\jmath}\\ i\end{bmatrix}(-1)^i q^{2\sigma_{i+1}}\left(q^{\lambda-2i-2}-q^{2(\varphi-1)}\right)\gamma(\lambda-2i-2,\varphi-1)\\
&=\sum_{i=0}^{\bar{\jmath}}\begin{bmatrix} \bar{\jmath}\\ i\end{bmatrix}(-1)^i q^{2\sigma_i}\gamma(\lambda-2i-2,\varphi-1)q^{\lambda-2}\left(q^{2\varphi}-1\right)\\
&=q^{\lambda-2}\left(q^{2\varphi}-1\right)\delta(\lambda-2,\varphi-1,\bar{\jmath})\\
&=q^{\lambda-2}\left(q^{2\varphi}-1\right)\gamma(2(\varphi-1),\bar{\jmath})q^{\bar{\jmath}(\lambda-2\bar{\jmath}-2)}\gamma(\lambda-2-2\bar{\jmath},\varphi-1-\bar{\jmath})\\
&\overset{(3.1.3)}{=}q^{(\bar{\jmath}+1)(\lambda-2(\bar{\jmath}+1))}\gamma(2\varphi,\bar{\jmath}+1)\gamma(\lambda-2(\bar{\jmath}+1),\varphi-(\bar{\jmath}+1)).
\end{aligned}$$

since $\begin{bmatrix} \bar{\jmath}\\ i-1\end{bmatrix}=0$ when $i=0$ and $\begin{bmatrix} \bar{\jmath}\\ i\end{bmatrix}=0$ when $i=\bar{\jmath}+1$. Hence by induction the lemma is proved. □

Lemma 3.5.4. *Let* $\varepsilon(\Lambda,\varphi,i)=\sum_{\ell=0}^{i}\begin{bmatrix} i\\ \ell\end{bmatrix}\begin{bmatrix} \Lambda-i\\ \varphi-\ell\end{bmatrix}q^{2\ell(\Lambda-\varphi)}(-1)^\ell q^{2\sigma_\ell}\gamma(2(\varphi-\ell),i-\ell)$*. Then for all* $\Lambda\in\mathbb{R},\varphi,i\in\mathbb{Z}$*,*

$$\varepsilon(\Lambda,\varphi,i)=(-1)^i q^{2\sigma_i}\begin{bmatrix} \Lambda-i\\ \Lambda-\varphi\end{bmatrix}. \tag{3.5.3}$$

Proof. Initial case $i = 0$,

$$\varepsilon(\Lambda, \varphi, 0) = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \begin{bmatrix} \Lambda \\ \varphi \end{bmatrix} q^0 (-1)^0 q^0 \gamma(2\varphi, 0) = \begin{bmatrix} \Lambda \\ \varphi \end{bmatrix}$$
$$(-1)^0 q^0 \begin{bmatrix} \Lambda \\ \Lambda - \varphi \end{bmatrix} = \begin{bmatrix} \Lambda \\ \varphi \end{bmatrix}.$$

So the initial case holds. Now suppose the case is true when $i = \bar{\imath}$. Then

$$\begin{aligned}
\varepsilon(\Lambda, \varphi, \bar{\imath} + 1) &= \sum_{\ell=0}^{\bar{\imath}+1} \begin{bmatrix} \bar{\imath} + 1 \\ \ell \end{bmatrix} \begin{bmatrix} \Lambda - \bar{\imath} - 1 \\ \varphi - \ell \end{bmatrix} q^{2\ell(\Lambda - \varphi)} (-1)^\ell q^{2\sigma_\ell} \gamma(2(\varphi - \ell), \bar{\imath} + 1 - \ell) \\
&\overset{(2.3.29)}{=} \sum_{\ell=0}^{\bar{\imath}+1} \begin{bmatrix} \bar{\imath} \\ \ell \end{bmatrix} \begin{bmatrix} \Lambda - \bar{\imath} - 1 \\ \varphi - \ell \end{bmatrix} q^{2\ell(\Lambda - \varphi)} (-1)^\ell q^{2\sigma_\ell} \gamma(2(\varphi - \ell), \bar{\imath} + 1 - \ell) \\
&\quad + \sum_{\ell=1}^{\bar{\imath}+1} q^{2(\bar{\imath}+1-\ell)} \begin{bmatrix} \bar{\imath} \\ \ell - 1 \end{bmatrix} \begin{bmatrix} \Lambda - \bar{\imath} - 1 \\ \varphi - \ell \end{bmatrix} q^{2\ell(\Lambda - \varphi)} (-1)^\ell q^{2\sigma_\ell} \gamma(2(\varphi - \ell), \bar{\imath} + 1 - \ell) \\
&= A + B, \quad \text{say.}
\end{aligned}$$

Now

$$\begin{aligned}
A &\overset{(3.1.4)}{=} \left(q^{2\varphi} - q^{2\bar{\imath}}\right) \sum_{\ell=0}^{\bar{\imath}} \begin{bmatrix} \bar{\imath} \\ \ell \end{bmatrix} \begin{bmatrix} \Lambda - \bar{\imath} - 1 \\ \varphi - \ell \end{bmatrix} q^{2\ell(\Lambda - 1 - \varphi)} (-1)^\ell q^{2\sigma_\ell} \gamma(2(\varphi - \ell), \bar{\imath} - \ell) \\
&= \left(q^{2\varphi} - q^{2\bar{\imath}}\right) \varepsilon(\Lambda - 1, \varphi, \bar{\imath}) \\
&= \left(q^{2\varphi} - q^{2\bar{\imath}}\right) (-1)^{\bar{\imath}} q^{2\sigma_{\bar{\imath}}} \begin{bmatrix} \Lambda - \bar{\imath} - 1 \\ \Lambda - 1 - \varphi \end{bmatrix}
\end{aligned}$$

and

$$\begin{aligned}
B &= \sum_{\ell=0}^{\bar{\imath}} q^{2(\bar{\imath} - \ell)} \begin{bmatrix} \bar{\imath} \\ \ell \end{bmatrix} \begin{bmatrix} \Lambda - \bar{\imath} - 1 \\ \varphi - \ell - 1 \end{bmatrix} q^{2(\ell+1)(\Lambda - \varphi)} (-1)^{\ell+1} q^{2\sigma_{\ell+1}} \gamma(2(\varphi - \ell - 1), \bar{\imath} - \ell) \\
&= -q^{2(\bar{\imath} + \Lambda - \varphi)} \varepsilon(\Lambda - 1, \varphi - 1, \bar{\imath}) \\
&= -q^{2(\bar{\imath} + \Lambda - \varphi)} (-1)^{\bar{\imath}} q^{2\sigma_{\bar{\imath}}} \begin{bmatrix} \Lambda - \bar{\imath} - 1 \\ \Lambda - \varphi \end{bmatrix}.
\end{aligned}$$

So

$$\begin{aligned}
\varepsilon(\Lambda, \varphi, \bar{\imath} + 1) = A + B &= (-1)^{\bar{\imath}} q^{2\sigma_{\bar{\imath}}} \left\{ \left(q^{2\varphi} - q^{2\bar{\imath}}\right) \begin{bmatrix} \Lambda - \bar{\imath} - 1 \\ \Lambda - \varphi - 1 \end{bmatrix} - q^{2(\bar{\imath} + \Lambda - \varphi)} \begin{bmatrix} \Lambda - \bar{\imath} - 1 \\ \Lambda - \varphi \end{bmatrix} \right\} \\
&\overset{(2.3.31)}{=} (-1)^{\bar{\imath}+1} q^{2\sigma_{\bar{\imath}}} \left\{ q^{2(\bar{\imath} + \Lambda - \varphi)} \begin{bmatrix} \Lambda - \bar{\imath} - 1 \\ \Lambda - \varphi \end{bmatrix} - \left(q^{2\varphi} - q^{2\bar{\imath}}\right) \frac{\left(q^{2(\Lambda - \varphi)} - 1\right)}{\left(q^{2(\varphi - \bar{\imath})} - 1\right)} \begin{bmatrix} \Lambda - \bar{\imath} - 1 \\ \Lambda - \varphi \end{bmatrix} \right\} \\
&= (-1)^{\bar{\imath}+1} \begin{bmatrix} \Lambda - (\bar{\imath} + 1) \\ \Lambda - \varphi \end{bmatrix} q^{2\sigma_{\bar{\imath}}} \left\{ \frac{q^{2(\bar{\imath} + \Lambda - \varphi)} \left(q^{2(\varphi - \bar{\imath})} - 1\right) - \left(q^{2\varphi} - q^{2\bar{\imath}}\right) \left(q^{2(\Lambda - \varphi)} - 1\right)}{q^{2(\varphi - \bar{\imath})} - 1} \right\} \\
&= (-1)^{\bar{\imath}+1} q^{2\sigma_{\bar{\imath}+1}} \begin{bmatrix} \Lambda - (\bar{\imath} + 1) \\ \Lambda - \varphi \end{bmatrix}
\end{aligned}$$

as required. □

Proposition 3.5.5. *For $0 \leq \varphi \leq n$ and a linear code $\mathscr{C} \subseteq \mathscr{A}_{q,t}$ with dimension k and its dual $\mathscr{C}^{\perp} \subseteq \mathscr{A}_{q,t}$ with weight distributions $\boldsymbol{c} = (c_0, \ldots, c_n)$ and $\boldsymbol{c'} = (c'_0, \ldots, c'_n)$, respectively we have*

$$\sum_{i=\varphi}^{n} q^{2\varphi(n-i)} \begin{bmatrix} i \\ \varphi \end{bmatrix} c_i = q^{k-m\varphi} \sum_{i=0}^{\varphi} (-1)^i q^{2\sigma_i} q^{2i(\varphi-i)} \begin{bmatrix} n-i \\ n-\varphi \end{bmatrix} \gamma(m-2i, \varphi-i) c'_i.$$

Proof. As per Proposition 3.5.1, we apply Theorem 3.3.4 to $\mathscr{C}^{\perp}$ to obtain

$$W_{\mathscr{C}}^{SR}(X,Y) = \frac{1}{|\mathscr{C}^{\perp}|} \overline{W}_{\mathscr{C}^{\perp}}^{SR}\left(X + (q^m-1)Y, X - Y\right)$$

or equivalently

$$\begin{aligned} \sum_{i=0}^{n} c_i Y^i X^{n-i} &= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{n} c'_i \left(X-Y\right)^{[i]} * \left(X + (q^m-1)Y\right)^{[n-i]} \\ &= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{n} c'_i \nu^{[i]}(X,Y;m) * \mu^{[n-i]}(X,Y;m). \qquad (3.5.4) \end{aligned}$$

For each side of Equation (3.5.4), we shall apply the skew-q^{-1}-derivative φ times and then evaluate at $X = Y = 1$.

For the left hand side, we have

$$\begin{aligned} \left(\sum_{i=0}^{n} c_i Y^i X^{n-i}\right)^{\{\varphi\}} &\overset{(3.4.8)}{=} \sum_{i=\varphi}^{n} c_i q^{2\varphi(1-i)+2\sigma_\varphi} \beta(i,\varphi) Y^{i-\varphi} X^{n-i} \qquad (3.5.5) \\ &\overset{(2.3.35)}{=} \sum_{i=\varphi}^{n} c_i q^{2\varphi(1-i)+2\sigma_\varphi} \begin{bmatrix} i \\ \varphi \end{bmatrix} \beta(\varphi,\varphi) Y^{i-\varphi} X^{n-i}. \qquad (3.5.6) \end{aligned}$$

Then using $X = Y = 1$ gives

$$\sum_{i=\varphi}^{n} c_i q^{2\varphi(1-i)+2\sigma_\varphi} \begin{bmatrix} i \\ \varphi \end{bmatrix} \beta(\varphi,\varphi) Y^{i-\varphi} X^{n-i} = \sum_{i=\varphi}^{n} q^{2\varphi(1-i)+2\sigma_\varphi} \beta(\varphi,\varphi) \begin{bmatrix} i \\ \varphi \end{bmatrix} c_i.$$

We now move on to the right hand side. For simplicity we shall write $\mu(X,Y;m)$ as $\mu(m)$ and similarly $\nu(X,Y;m)$ as $\nu(m)$. Then,

$$\begin{aligned} \psi_i(m) &\overset{(3.4.10)(3.4.9)}{=} \sum_{\ell=0}^{\varphi} \begin{bmatrix} \varphi \\ \ell \end{bmatrix} q^{2\ell(n-i-\varphi+\ell)} \left\{(-1)^{\ell} \beta(i,\ell) \nu^{[i-\ell]}(m)\right\} \\ &\quad * \left\{q^{-2\sigma_{\varphi-\ell}} \beta(n-i,\varphi-\ell) \gamma(m-2\ell,\varphi-\ell) \mu^{[n-i-\varphi+\ell]}(m-2\varphi)\right\}. \end{aligned}$$

Now let

$$\Psi(X,Y;m-2\varphi) = \nu^{[i-\ell]}(X,Y;m) * \gamma(m-2\ell,\varphi-\ell) \mu^{[n-i-\varphi+\ell]}(X,Y;m-2\varphi).$$

We apply the skew-q-product, reorder the summations and set $X = Y = 1$ giving

$$
\begin{aligned}
&\Psi(1,1;m-2\varphi)\\
&\quad= \sum_{u=0}^{n-\varphi}\left[\sum_{p=0}^{u} q^{2p(n-i-\varphi+\ell)}\nu_p^{[i-\ell]}(m)\gamma(m-2\ell-2p,\varphi-\ell)\mu_{u-p}^{[n-i-\varphi+\ell]}(m-2\varphi-2p)\right]\\
&\quad= \sum_{r=0}^{i-\ell} q^{2r(n-i-\varphi+\ell)}\nu_r^{[i-\ell]}(m)\gamma(m-2\ell-2r,\varphi-\ell)\left[\sum_{t=0}^{n-i-\varphi+\ell}\mu_t^{[n-i-\varphi+\ell]}(m-2\varphi-2r)\right]\\
&\quad\overset{(2.3.27)}{=} \sum_{r=0}^{i-\ell} q^{2r(n-i-\varphi+\ell)}q^{(m-2\varphi-2r)(n-i-\varphi+\ell)}\nu_r^{[i-\ell]}(m)\gamma(m-2\ell-2r,\varphi-\ell)\\
&\quad\overset{(3.2.6)}{=} q^{(m-2\varphi)(n-i-\varphi+\ell)}\sum_{r=0}^{i-\ell}(-1)^r q^{2\sigma_r}\begin{bmatrix}i-\ell\\ r\end{bmatrix}\gamma(m-2\ell-2r,\varphi-\ell)\\
&\quad= q^{(m-2\varphi)(n-i-\varphi+\ell)}\delta(m-2\ell,\varphi-\ell,i-\ell)\\
&\quad\overset{(3.5.2)}{=} q^{(m-2\varphi)(n-i-\varphi+\ell)}q^{(i-\ell)(m-2i)}\gamma(2(\varphi-\ell),i-\ell)\gamma(m-2i,\varphi-i).
\end{aligned}
$$

Noting that $q^{2\ell(n-i-\varphi+\ell)}q^{-2\sigma_{\varphi-\ell}} = q^{2\ell(n-i)}q^{-2\sigma_\varphi}q^{2\sigma_\ell}$ we get

$$
\begin{aligned}
\psi_i(1,1;m) &= \sum_{\ell=0}^{\varphi}(-1)^\ell\begin{bmatrix}\varphi\\ \ell\end{bmatrix}q^{2\ell(n-i-\varphi+\ell)}q^{-2\sigma_{\varphi-\ell}}\beta(i,\ell)\beta(n-i,\varphi-\ell)\Psi(1,1;m-2\varphi)\\
&\overset{(2.3.36)}{=} q^{-2\sigma_\varphi}\beta(\varphi,\varphi)\sum_{\ell=0}^{\varphi}(-1)^\ell q^{2\ell(n-i)}q^{2\sigma_\ell}\begin{bmatrix}i\\ \ell\end{bmatrix}\begin{bmatrix}n-i\\ \varphi-\ell\end{bmatrix}\Psi(1,1;m-2\varphi).
\end{aligned}
$$

Writing

$$
\begin{aligned}
q^{-2\sigma_\varphi}q^{2\ell(n-i)}q^{(m-2\varphi)(n-\varphi-i+\ell)}q^{(i-\ell)(m-2i)} &= q^{2\sigma_\varphi}q^{2\varphi(1-n)}q^{m(n-\varphi)}q^{2\ell(n-\varphi)}q^{2i(\varphi-i)}\\
&= q^{\theta}q^{2l(n-\varphi)}
\end{aligned}
$$

gives

$$
\begin{aligned}
\psi_i(1,1;m) &= q^\theta\beta(\varphi,\varphi)\gamma(m-2i,\varphi-i)\sum_{\ell=0}^{i}(-1)^\ell q^{2\ell(n-\varphi)}q^{2\sigma_\ell}\begin{bmatrix}i\\ \ell\end{bmatrix}\begin{bmatrix}n-i\\ \varphi-\ell\end{bmatrix}\gamma(2(\varphi-\ell),i-\ell)\\
&\overset{(3.5.3)}{=} (-1)^i q^\theta q^{2\sigma_i}\beta(\varphi,\varphi)\begin{bmatrix}n-i\\ n-\varphi\end{bmatrix}\gamma(m-2i,\varphi-i).
\end{aligned}
$$

Combining both sides, we obtain

$$
\sum_{i=\varphi}^{n} q^{2\varphi(1-i)+2\sigma_\varphi}\beta(\varphi,\varphi)\begin{bmatrix}i\\ \varphi\end{bmatrix}c_i = \frac{1}{|\mathscr{C}^\perp|}\sum_{i=0}^{n}c_i'(-1)^i q^\theta q^{2\sigma_i}\beta(\varphi,\varphi)\begin{bmatrix}n-i\\ n-\varphi\end{bmatrix}\gamma(m-2i,\varphi-i).
$$

Thus

$$
\sum_{i=\varphi}^{n} q^{2\varphi(n-i)}\begin{bmatrix}i\\ \varphi\end{bmatrix}c_i = \frac{q^{m(n-\varphi)}}{|\mathscr{C}^\perp|}\sum_{i=0}^{\varphi}(-1)^i q^{2\sigma_i}q^{2i(\varphi-i)}\begin{bmatrix}n-i\\ n-\varphi\end{bmatrix}\gamma(m-2i,\varphi-i)c_i'.
$$

If $\mathscr{C}$ has dimension k we have

$$|\mathscr{C}| = q^k, \ |\mathscr{C}^\perp| = q^{mn-k},$$

so

$$\frac{q^{m(n-\varphi)}}{|\mathscr{C}^\perp|} = \frac{q^{m(n-\varphi)}}{q^{mn-k}} = q^{k-m\varphi}$$

as required. □

We can simplify Proposition 3.5.5 if φ is less than the minimum distance of the dual code. Also we can introduce the ***dual diameter***, ϱ'_{SR}, defined as the maximum distance between any two codewords of the dual code and simplify Proposition 3.5.5 further.

Corollary 3.5.6. *If* $0 \leq \varphi < d'_{SR}$ *then*

$$\sum_{i=\varphi}^{n} q^{2\varphi(n-i)} \begin{bmatrix} i \\ \varphi \end{bmatrix} c_i = q^{k-m\varphi} \begin{bmatrix} n \\ \varphi \end{bmatrix} \gamma(m, \varphi).$$

For $\varrho'_{SR} < \varphi \leq n$ *then*

$$\sum_{i=0}^{\varphi} (-1)^i q^{2\sigma_i} q^{2i(\varphi-i)} \begin{bmatrix} n-i \\ n-\varphi \end{bmatrix} \gamma(m-2i, \varphi-i) c_i = 0.$$

Proof. First consider $0 \leq \varphi < d'_{SR}$, then $c'_0 = 1$, $c'_1 = \ldots = c'_\varphi = 0$. Also since $\begin{bmatrix} n \\ n-\varphi \end{bmatrix} = \begin{bmatrix} n \\ \varphi \end{bmatrix}$ the first statement holds. Now if $\varrho'_{SR} < \varphi \leq n$ then applying Proposition 3.5.5 to $\mathscr{C}^\perp$ gives

$$\sum_{i=\varphi}^{n} q^{2\varphi(n-i)} \begin{bmatrix} i \\ \varphi \end{bmatrix} c'_i = q^{mn-k-m\varphi} \sum_{i=0}^{\varphi} (-1)^i q^{2\sigma_i} q^{2i(\varphi-i)} \begin{bmatrix} n-i \\ n-\varphi \end{bmatrix} \gamma(m-2i, \varphi-i) c_i.$$

So using $c'_\varphi = \ldots = c'_n = 0$ we get

$$0 = \sum_{i=0}^{\varphi} (-1)^i q^{2\sigma_i} q^{2i(\varphi-i)} \begin{bmatrix} n-i \\ n-\varphi \end{bmatrix} \gamma(m-2i, \varphi-i) c_i$$

as required. □

3.5.3 MSRD Codes

As an application of the MacWilliams Identity, we can derive an alternative proof for the explicit coefficients of the skew rank weight distribution for MSRD codes to that in [12, Theorem 4]. This is analogous to the results for MRD codes presented in [22, Proposition 9].

Firstly a lemma that will be needed.

Lemma 3.5.7. *If $a_0, a_1, \ldots, a_\ell$ and $b_0, b_1, \ldots, b_\ell$ are two sequences of real numbers and if*

$$a_j = \sum_{i=0}^{j} \begin{bmatrix} \ell - i \\ \ell - j \end{bmatrix} b_i$$

for $0 \leq j \leq \ell$, then also for $0 \leq i \leq \ell$ we have,

$$b_i = \sum_{j=0}^{i} (-1)^{i-j} q^{2\sigma_{i-j}} \begin{bmatrix} \ell - j \\ \ell - i \end{bmatrix} a_j.$$

Proof. This result uses the property of skew-q-ary Gaussian coefficients (2.3.28). That is

$$\sum_{k=i}^{j} (-1)^{k-i} q^{2\sigma_{k-i}} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} j \\ k \end{bmatrix} = \delta_{ij}.$$

Then for $0 \leq i \leq \ell$,

$$\begin{aligned}
\sum_{j=0}^{i} (-1)^{i-j} q^{2\sigma_{i-j}} \begin{bmatrix} \ell - j \\ \ell - i \end{bmatrix} a_j &= \sum_{j=0}^{i} (-1)^{i-j} q^{2\sigma_{i-j}} \begin{bmatrix} \ell - j \\ \ell - i \end{bmatrix} \left(\sum_{k=0}^{j} \begin{bmatrix} \ell - k \\ \ell - j \end{bmatrix} b_k \right) \\
&= \sum_{k=0}^{i} \sum_{j=k}^{i} (-1)^{i-j} q^{2\sigma_{i-j}} \begin{bmatrix} \ell - j \\ \ell - i \end{bmatrix} \begin{bmatrix} \ell - k \\ \ell - j \end{bmatrix} b_k \\
&= \sum_{k=0}^{i} b_k \left(\sum_{s=\ell-i}^{\ell-k} (-1)^{i-\ell+s} q^{2\sigma_{i-\ell+s}} \begin{bmatrix} s \\ \ell - i \end{bmatrix} \begin{bmatrix} \ell - k \\ s \end{bmatrix} \right) \\
&\overset{(2.3.28)}{=} \sum_{k=0}^{i} b_k \delta_{ik} \\
&= b_i
\end{aligned}$$

as required. □

The following proposition can be seen to be equivalent to [21, (15)].

Proposition 3.5.8. *Let $\mathscr{C} \subseteq \mathscr{A}_{q,t}$ be a linear MSRD code with weight distribution $\boldsymbol{c} = (c_0, \ldots, c_n)$. Then we have $c_0 = 1$ and for $0 \leq r \leq n - d_{SR}$*

$$c_{d_{SR}+r} = \sum_{i=0}^{r} (-1)^{r-i} q^{2\sigma_{r-i}} \begin{bmatrix} d_{SR} + r \\ d_{SR} + i \end{bmatrix} \begin{bmatrix} n \\ d_{SR} + r \end{bmatrix} \left(\frac{q^{m(d_{SR}+i)}}{|\mathscr{C}^\perp|} - 1 \right).$$

Proof. From Corollary 3.5.2 we have

$$\sum_{i=0}^{n-\varphi} \begin{bmatrix} n - i \\ \varphi \end{bmatrix} c_i = \frac{1}{|\mathscr{C}^\perp|} q^{m(n-\varphi)} \begin{bmatrix} n \\ \varphi \end{bmatrix}$$

for $0 \leq \varphi < d'_{SR}$. Now if a linear code $\mathscr{C}$ is MSRD, with minimum distance d_{SR} then $\mathscr{C}^\perp$ is also MSRD with minimum distance $d'_{SR} = n - d_{SR} + 2$ [12, p35]. So Corollary 3.5.2 holds for $0 \leq \varphi \leq n - d_{SR} = d'_{SR} - 2$. We therefore have $c_0 = 1$ and $c_1 = c_2 = \ldots = c_{d_{SR}-1} = 0$ and setting $\varphi = n - d_{SR} - j$ for $0 \leq j \leq n - d_{SR}$ we get

$$\begin{aligned}\begin{bmatrix} n \\ n-d_{SR}-j \end{bmatrix} + \sum_{i=d_{SR}}^{d_{SR}+j} \begin{bmatrix} n-i \\ n-d_{SR}-j \end{bmatrix} c_i &= \frac{1}{|\mathscr{C}^{\perp}|} q^{m(d_{SR}+j)} \begin{bmatrix} n \\ n-d_{SR}-j \end{bmatrix} \\ \sum_{r=0}^{j} \begin{bmatrix} n-d_{SR}-r \\ n-d_{SR}-j \end{bmatrix} c_{r+d_{SR}} &= \begin{bmatrix} n \\ n-d_{SR}-j \end{bmatrix} \left(\frac{q^{m(d_{SR}+j)}}{|\mathscr{C}^{\perp}|} - 1 \right).\end{aligned}$$

Applying Lemma 3.5.7 with $\ell = n - d_{SR}$ and $b_r = c_{r+d_{SR}}$ then letting

$$a_j = \begin{bmatrix} n \\ n-d_{SR}-j \end{bmatrix} \left(\frac{q^{m(d_{SR}+j)}}{|\mathscr{C}^{\perp}|} - 1 \right)$$

gives

$$\sum_{r=0}^{j} \begin{bmatrix} n-d_{SR}-r \\ n-d_{SR}-j \end{bmatrix} b_r = a_j,$$

so

$$\begin{aligned} b_r = c_{r+d_{SR}} &= \sum_{i=0}^{r} (-1)^{r-i} q^{2\sigma_{r-i}} \begin{bmatrix} n-d_{SR}-i \\ n-d_{SR}-r \end{bmatrix} a_i \\ &= \sum_{i=0}^{r} (-1)^{r-i} q^{2\sigma_{r-i}} \begin{bmatrix} n-d_{SR}-i \\ n-d_{SR}-r \end{bmatrix} \begin{bmatrix} n \\ n-d_{SR}-i \end{bmatrix} \left(\frac{q^{m(d_{SR}+i)}}{|\mathscr{C}^{\perp}|} - 1 \right). \end{aligned}$$

But we have

$$\begin{aligned} \begin{bmatrix} n-d_{SR}-i \\ n-d_{SR}-r \end{bmatrix} \begin{bmatrix} n \\ n-d_{SR}-i \end{bmatrix} &\overset{(2.3.24)}{=} \begin{bmatrix} n-(d_{SR}+i) \\ n-(d_{SR}+r) \end{bmatrix} \begin{bmatrix} n \\ d_{SR}+i \end{bmatrix} \\ &\overset{(2.3.25)}{=} \begin{bmatrix} d_{SR}+r \\ d_{SR}+i \end{bmatrix} \begin{bmatrix} n \\ n-(d_{SR}+r) \end{bmatrix} \\ &\overset{(2.3.24)}{=} \begin{bmatrix} d_{SR}+r \\ d_{SR}+i \end{bmatrix} \begin{bmatrix} n \\ d_{SR}+r \end{bmatrix}. \end{aligned}$$

Therefore

$$c_{r+d_{SR}} = \sum_{i=0}^{r} (-1)^{r-i} q^{2\sigma_{r-i}} \begin{bmatrix} d_{SR}+r \\ d_{SR}+i \end{bmatrix} \begin{bmatrix} n \\ d_{SR}+r \end{bmatrix} \left(\frac{q^{m(d_{SR}+i)}}{|\mathscr{C}^{\perp}|} - 1 \right)$$

as required. □

Note. We note again that $mn = \frac{t(t-1)}{2}$ for skew-symmetric matrices and $|\mathscr{C}||\mathscr{C}^{\perp}| = q^{mn}$ which can be can be used to simplify this to

$$c_{r+d_{SR}} = \sum_{i=0}^{r} (-1)^{r-i} q^{2\sigma_{r-i}} \begin{bmatrix} d_{SR}+r \\ d_{SR}+i \end{bmatrix} \begin{bmatrix} n \\ d_{SR}+r \end{bmatrix} \left(|\mathscr{C}| q^{m(d_{SR}+i-n)} - 1 \right).$$

Chapter 4

The Hermitian Association Scheme

Having sucessfully developed a q-algebra for skew-symmetric matrices to prove the MacWilliams Identity as a functional transform, we now investigate whether a similar process can be applied to the association scheme of Hermitian matrices, once again with the rank metric. We shall call this scheme the Hermitian association scheme.

As before we begin with an overview of what we already know from Section 2.7, followed by some more specific preliminaries in Section 4.1. Section 4.2 introduces yet another form of a q-algebra before identifying two further homogeneous polynomials relevant to this particular space. Again the powers of these polynomials turn out to be the weight enumerator of the set of Hermitian matrices of a given size t. Equipped with these polynomials, which we note are significantly different to the ones identified in the skew rank metric, another explicit form of the Krawtchouk polynomials is found. It is then proven that these polynomials are indeed generalised Krawtchouk polynomials using a different recurrence relation, one used by Schmidt [53, Lemma 7], rather than the relation used by Delsarte [11, (1)]. We later prove that the two recurrence relations are equivalent in Section 5.1.2. Then we have the ability to state and prove the MacWilliams Identity for the Hermitian association scheme as a functional transform.

Following the same structure as Chapter 3, two derivatives on this space are derived analogous to the q-derivative and q^{-1}-derivative for the rank association scheme [22, Definiton 5, 6] and the ones shown in Section 3.4. We can also then find the moments of the Hermitian rank weight distribution. Slightly differently to the skew rank case, when we consider MHRD codes, (Maximum Hermitian Rank Distance codes), we already know that if the minimum distance is even, the Hermitian rank weight distribution of the code is not uniquely determined, so we have to restrict our conclusions to the special case when a code is MHRD and also the minimum distance is odd.

The aim of this, as well as extending the MacWilliams Identity as a functional transform in this setting, is to draw similarities between these methods with a view to potentially generalising the results. In this case, the associated algebra and the relevant homogeneous polynomial have the same form but different parameters. The new Krawtchouk polynomials are then derived in exactly the same fashion. They are compared to known eigenvalues using a recurrence relation, all of which are distinct from the eigenvalues and recurrence relation used in Chapter 3.

4.1 Preliminaries

4.1.1 Parameters

Similar to the skew rank association scheme, let's remind ourselves of some of the notation from Section 2.7 for the b-nary Gaussian coefficients and the b-nary beta function. As we are working with the Hermitian association scheme we set the parameter $b = -q$. So we have

$$
\begin{aligned}
{}_{-q}\begin{bmatrix} x \\ k \end{bmatrix} &= \prod_{i=0}^{k-1} \frac{(-q)^x - (-q)^i}{(-q)^k - (-q)^i} = \prod_{i=0}^{k-1} \frac{b^x - b^i}{b^k - b^i}, \\
\beta_{-q}(x,k) &= \prod_{i=0}^{k-1} {}_{-q}\begin{bmatrix} x-i \\ 1 \end{bmatrix}.
\end{aligned}
$$

To make notation simpler and while there is no ambiguity, in this section we shall write ${}_{-q}\left[\begin{smallmatrix} x \\ k \end{smallmatrix}\right] = \left[\begin{smallmatrix} x \\ k \end{smallmatrix}\right]$ and $\beta_{-q}(x,k) = \beta(x,k)$. We also have that $\sigma_i = \frac{i(i-1)}{2}$ as usual. In addition, in the interest of keeping notation simpler, we shall write b instead of $-q$ throughout this chapter.

As a reminder, we have the eigenvalues of the association scheme, defined by Schmidt [53, (4)] as

$$
P_k(x,t) = (-1)^k \sum_{i=0}^{k} b^{\sigma_{k-i}+ti} \begin{bmatrix} t-i \\ t-k \end{bmatrix} \begin{bmatrix} t-x \\ i \end{bmatrix}.
$$

We state Delsarte's MacWilliams Identity explicitly for Hermitian association schemes.

Theorem 4.1.1. *Let $\mathscr{C} \subseteq \mathscr{H}_{q,t}$ be a code with Hermitian rank weight distribution $\boldsymbol{c} = (c_0, \ldots, c_n)$ and $\mathscr{C}^\perp$ be its dual code with Hermitian rank weight distribution $\boldsymbol{c'} = (c'_0, \ldots, c'_n)$ and the $(n+1) \times (n+1)$ eigenmatrix of the Hermitian association scheme $\boldsymbol{P} = (p_{xk})$, consisting of the eigenvalues $P_k(x,n) = p_{xk}$, then we have*

$$
\boldsymbol{c'} = \frac{1}{|\mathscr{C}|}\boldsymbol{cP}. \tag{4.1.1}
$$

4.1.2 The Negative-q Gamma Function

Again we define another function, this time we call it the negative-q gamma function, to aid us with notation in this association scheme.

Definition 4.1.2. We define the ***Negative-q gamma function*** for $x \in \mathbb{R},\ k \in \mathbb{Z}$ to be

$$\begin{aligned}\gamma'(x,k) &= (-1)^k \prod_{i=0}^{k-1} \left(b^x + b^i\right)\\ &= \prod_{i=0}^{k-1} \left(-b^x - b^i\right).\end{aligned}$$

Theorem 2.7.6 can then be rewritten as below.

Theorem 4.1.3. *The number of Hermitian matrices of order t and Hermitian rank h can be rewritten as*

$$\xi_{t,h} = \begin{bmatrix} t \\ h \end{bmatrix} \gamma'(t,h). \tag{4.1.2}$$

Proof. We have

$$\begin{aligned}\begin{bmatrix} t \\ h \end{bmatrix} \gamma'(t,h) &= (-1)^h \prod_{i=1}^{h} \frac{b^{t-i+1}-1}{b^i-1} \prod_{i=0}^{h-1} \left(b^t + b^i\right)\\ &= (-1)^h \frac{\displaystyle\prod_{i=0}^{h-1} b^{t-i}-1}{\displaystyle\prod_{i=1}^{h} (-1)^i \left(q^i - (-1)^i\right)} \prod_{i=0}^{h-1} \left(b^{t-i}+1\right) b^i\\ &= (-1)^h \frac{\displaystyle\prod_{i=0}^{h-1} b^i \left(b^{2t-2i}-1\right)}{\displaystyle\prod_{i=1}^{h} (-1)^i \left(q^i - (-1)^i\right)}\\ &= (-1)^h b^{\sigma_h} \frac{\displaystyle\prod_{i=0}^{h-1} b^{2t-2i}-1}{\displaystyle\prod_{i=1}^{h} (-1)^i \left(q^i - (-1)^i\right)}\\ &= \frac{(-1)^h (-1)^{\sigma_h} q^{\sigma_h}}{(-1)^{\sigma_{h+1}}} \frac{\displaystyle\prod_{i=0}^{h-1} q^{2t-2i}-1}{\displaystyle\prod_{i=1}^{h} q^i - (-1)^i}\\ &= q^{\sigma_h} \times \frac{\displaystyle\prod_{i=0}^{h-1} q^{2t-2i}-1}{\displaystyle\prod_{i=1}^{h} q^i - (-1)^i}\\ &= \xi_{t,h}.\end{aligned}$$

□

Lemma 4.1.4. *We have the following identities for the negative-q gamma function:*

1.

$$\gamma'(x,k) = b^{\sigma_k} \prod_{i=0}^{k-1} \left(-b^{x-i} - 1\right)$$

2.

$$\gamma'(x,k) = b^{k-1}\big(- b^{x} - 1\big)\gamma'(x-1,k-1) \tag{4.1.3}$$

3.

$$\gamma'(x,k+1) = \left(-b^{x} - b^{k}\right)\gamma'(x,k). \tag{4.1.4}$$

Proof.

(1)

$$\begin{aligned}
\gamma'(x,k) &= \prod_{i=0}^{k-1} \left(-b^{x} - b^{i}\right) \\
&= \left(\prod_{i=0}^{k-1} b^{i}\right) \prod_{i=0}^{k-1} \left(-b^{x-i} - 1\right) \\
&= b^{\sigma_k} \prod_{i=0}^{k-1} \left(-b^{x-i} - 1\right).
\end{aligned}$$

(2)

$$\begin{aligned}
\gamma'(x,k) &= \prod_{i=0}^{k-1} \left(-b^{x} - b^{i}\right) \\
&= \left(-b^{x} - 1\right) \prod_{i=1}^{k-1} \left(-b^{x} - b^{i}\right) \\
&= \left(-b^{x} - 1\right) \prod_{i=1}^{k-1} b\left(-b^{x-1} - b^{i-1}\right) \\
&= \left(-b^{x} - 1\right) b^{k-1} \prod_{i=0}^{k-2} \left(-b^{x-1} - b^{i}\right) \\
&= \left(-b^{x} - 1\right) b^{k-1} \prod_{i=0}^{k-2} \left(-b^{x-1} - b^{i}\right) \\
&= b^{k-1}\left(-b^{x} - 1\right)\gamma'(x-1,k-1).
\end{aligned}$$

(3)

$$\begin{aligned}
\gamma'(x,k+1) &= \prod_{i=0}^{k} \left(-b^{x} - b^{i}\right) \\
&= \left(-b^{x} - b^{k}\right) \prod_{i=0}^{k-1} \left(-b^{x} - b^{i}\right) \\
&= \left(-b^{x} - b^{k}\right)\gamma'(x,k).
\end{aligned}$$

□

4.2 The Negative-q-Algebra

The weight enumerators of any linear code $\mathscr{C} \subseteq \mathscr{H}_{q,t}$ are homogeneous polynomials. We introduce an operation, the negative-q-product, on homogeneous polynomials that will help express the relation between the Hermitian rank weight enumerator of a code and that of its dual. The negative-q-power and negative-q-transform are analogous to those for the rank association scheme [22, Section 3.1] and the skew rank association scheme, as in Section 3.2.

4.2.1 The Negative-q-Product, Negative-q-Power and the Negative-q-Transform

Definition 4.2.1. Let

$$a(X,Y;\lambda) = \sum_{i=0}^{r} a_i(\lambda) Y^i X^{r-i}$$
$$b(X,Y;\lambda) = \sum_{i=0}^{s} b_i(\lambda) Y^i X^{s-i}$$

be two homogeneous polynomials in X and Y with coefficients $a_i(\lambda)$ and $b_i(\lambda)$ respectively, which are real functions of λ that are 0 unless otherwise specified. For example $b_i(\lambda) = 0$ if $i \notin \{0,1,\ldots,s\}$. The ***negative-$q$-product***, $*$, of $a(X,Y;\lambda)$ degree r, and $b(X,Y;\lambda)$ of degree s, is defined as

$$\begin{aligned} c(X,Y;\lambda) &= a(X,Y;\lambda) * b(X,Y;\lambda) & (4.2.1)\\ &= \sum_{u=0}^{r+s} c_u(\lambda) Y^u X^{r+s-u} & (4.2.2)\end{aligned}$$

with

$$c_u(\lambda) = \sum_{i=0}^{u} (-q)^{is} a_i(\lambda) b_{u-i}(\lambda - i).$$

We note that as with the q-product in [22, Lemma 1], the negative-q-product is not commutative or distributive in general. However, as in Chapter 3, if $a(X,Y;\lambda) = a$ is a constant independent of λ, the following property holds:

$$a * b(X,Y;\lambda) = b(X,Y;\lambda) * a = ab(X,Y;\lambda).$$

Another property is that if the degrees of $a(X,Y;\lambda)$ and $c(X,Y;\lambda)$ are the same then,

$$\{a(X,Y;\lambda) + c(X,Y;\lambda)\} * b(X,Y;\lambda) = a(X,Y;\lambda) * b(X,Y;\lambda) + c(X,Y;\lambda) * b(X,Y;\lambda)$$

and

$$a(X,Y;\lambda) * \{b(X,Y;\lambda) + c(X,Y;\lambda)\} = a(X,Y;\lambda) * b(X,Y;\lambda) + a(X,Y;\lambda) * c(X,Y;\lambda).$$

Definition 4.2.2. The ***negative-q-power*** is defined by

$$\begin{cases} a^{[0]}(X,Y;\lambda) = 1 \\ a^{[1]}(X,Y;\lambda) = a(X,Y;\lambda) \\ a^{[k]}(X,Y;\lambda) = a(X,Y;\lambda) * a^{[k-1]}(X,Y;\lambda) \quad \text{for } k \geq 2. \end{cases}$$

Definition 4.2.3 ([22, Definition 4])**.** Let $a(X,Y;\lambda) = \sum_{u=0}^{r} a_i(\lambda) Y^i X^{r-i}$. We define the ***negative-q-transform*** to be the homogeneous polynomial

$$\overline{a}(X,Y;\lambda) = \sum_{i=0}^{r} a_i(\lambda) Y^{[i]} * X^{[r-i]}.$$

4.2.2 Using the Negative-q-Product in the Hermitian Association Scheme

In the theory that follows we consider the following two polynomials. First let

$$\mu(X,Y;\lambda) = X + \left(-b^{\lambda} - 1\right) Y. \tag{4.2.3}$$

The negative-q-powers of $\mu(X,Y;t)$ provide an explicit form for the Hermitian rank weight enumerator of $\mathscr{H}_{q,t}$, the set of Hermitian matrices of order t.

Theorem 4.2.4. *If $\mu(X,Y;\lambda)$ is defined as above, then*

$$\mu^{[k]}(X,Y;\lambda) = \sum_{u=0}^{k} \mu_u(\lambda,k) Y^u X^{k-u} \quad \textit{for } k \geq 1, \tag{4.2.4}$$

where

$$\mu_u(\lambda,k) = \begin{bmatrix} k \\ u \end{bmatrix} \gamma'(\lambda,u).$$

Specifically, the weight enumerators for $\mathscr{H}_{q,t}$, the set of Hermitian matrices of size $t \geq 1$, denoted by Ω_t, is given by

$$\Omega_t = \mu^{[t]}(X,Y;t). \tag{4.2.5}$$

Proof. The proof follows the method of induction. Consider $k = 1$, so

$$\mu^{[1]}(X,Y;\lambda) = \mu(X,Y;\lambda) = X + \left(-b^{\lambda} - 1\right) Y.$$

Then

$$\begin{aligned} \mu_0(\lambda,1) &= 1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \gamma'(\lambda,0) \\ \mu_1(\lambda,1) &= \left(-b^{\lambda} - 1\right) = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \gamma'(\lambda,1). \end{aligned}$$

So

$$\mu_u^{[1]}(\lambda,1)=\begin{bmatrix}1\\u\end{bmatrix}\gamma'(\lambda,u)$$

as required for $k=1$. Now assume the theorem is true for $k\geq 1$. Then

$$\begin{aligned}\mu^{[k+1]}(X,Y;\lambda)&=\mu(X,Y;\lambda)*\mu^{[k]}(X,Y;\lambda)\\&=\left(X+\left(-b^{\lambda}-1\right)Y\right)*\left(\sum_{u=0}^{k}\begin{bmatrix}k\\u\end{bmatrix}\gamma'(\lambda,u)Y^uX^{k-u}\right)\\&=\sum_{i=0}^{k+1}f_i(\lambda)Y^iX^{k+1-i}\end{aligned}$$

where,

$$\begin{aligned}f_i(\lambda)&=\mu_0(\lambda,1)\mu_i(\lambda,k)+b^k\mu_1(\lambda,1)\mu_{i-1}(\lambda-1,k)\\&=\begin{bmatrix}k\\i\end{bmatrix}\gamma'(\lambda,i)+b^k\left(-b^k-1\right)\begin{bmatrix}k\\i-1\end{bmatrix}\gamma'(\lambda-1,i-1)\\&\overset{(2.3.32)}{=}\frac{b^{k-i+1}-1}{b^{k+1}-1}\begin{bmatrix}k+1\\i\end{bmatrix}\gamma'(\lambda,i)\overset{(4.1.3)(2.3.33)}{+}b^k\frac{b^i-1}{b^{k+1}-1}b^{i-1}\begin{bmatrix}k+1\\i\end{bmatrix}\gamma'(\lambda,i)\\&=\gamma'(\lambda,i)\begin{bmatrix}k+1\\i\end{bmatrix}\left(\frac{b^{k-i+1}-1+b^{k-i+1}\left(b^i-1\right)}{b^{k+1}-1}\right)\\&=\gamma'(\lambda,i)\begin{bmatrix}k+1\\i\end{bmatrix}\end{aligned}$$

since for $i\geq 1$ we only need to consider the first two coefficients as when $j\geq 2$ then $\mu_j(\lambda,1)=0$. So it is true for $k+1$. Therefore by induction the first part of the theorem is true. Now consider $\mu^{[t]}(X,Y;t)$, then clearly

$$\begin{aligned}\mu^{[t]}(X,Y;t)&=\sum_{u=0}^{t}\begin{bmatrix}t\\i\end{bmatrix}\gamma'(t,u)Y^uX^{t-u}\\&\overset{(4.1.2)}{=}\sum_{u=0}^{t}\xi_{t,u}Y^uX^{t-u}\overset{(4.2.5)}{=}\Omega_t\end{aligned}$$

as required. □

Second, consider the polynomial

$$\nu(X,Y;\lambda)=X-Y.$$

Theorem 4.2.5. *If $\nu(X,Y;\lambda)$ is as defined above, then for all $k\geq 1$,*

$$\nu^{[k]}(X,Y;\lambda)=\sum_{u=0}^{k}\nu_u(\lambda,j)Y^uX^{k-u}=\sum_{u=0}^{k}(-1)^ub^{\sigma_u}\begin{bmatrix}k\\u\end{bmatrix}Y^uX^{k-u}.\qquad(4.2.6)$$

Proof. We perform induction on k. It is easily checked that the theorem holds for $k=1$.

Now assume the theorem holds for $k \geq 1$. For clarity, $\nu_0(\lambda, 1) = 1$ and $\nu_1(\lambda, 1) = -1$. Then

$$\begin{aligned}\nu^{[k+1]}(X,Y;\lambda) &= \nu(X,Y;\lambda) * \nu^{[k]}(X,Y;\lambda)\\ &= (X-Y) * \left(\sum_{u=0}^{k}(-1)^u b^{\sigma_u}\begin{bmatrix}k\\u\end{bmatrix}Y^u X^{k-u}\right)\\ &= \sum_{i=0}^{k+1} g_i(\lambda)Y^i X^{k+1-i}\end{aligned}$$

where

$$\begin{aligned}g_i(\lambda) &= \sum_{j=0}^{i} b^{jk}\nu_j(\lambda,j)\nu_{i-j}(\lambda-j,k)\\ &= b^0(1)(-1)^i b^{\sigma_i}\begin{bmatrix}k\\i\end{bmatrix} + b^k(-1)(-1)^{i-1}b^{\sigma_{i-1}}\begin{bmatrix}k\\i-1\end{bmatrix}\\ &\overset{(2.3.32)}{=} (-1)^i b^{\sigma_i}\frac{b^{k+1-i}-1}{b^{k+1}-1}\begin{bmatrix}k+1\\i\end{bmatrix} \overset{(2.3.33)}{+} b^k(-1)^i b^{\sigma_{i-1}}\frac{b^i-1}{b^{k+1}-1}\begin{bmatrix}k+1\\i\end{bmatrix}\\ &= (-1)^i b^{\sigma_i}\begin{bmatrix}k+1\\i\end{bmatrix}\left\{\frac{b^{k+1-i}-1}{b^{k+1}-1} + b^k b^{1-i}\frac{b^i-1}{b^{k+1}-1}\right\}\\ &= (-1)^i\frac{b^{\sigma_i}}{b^{k+1}-1}\begin{bmatrix}k+1\\i\end{bmatrix}\left\{b^{k+1-i}-1+b^{k+1}-b^{k+1-i}\right\}\\ &= (-1)^i b^{\sigma_i}\begin{bmatrix}k+1\\i\end{bmatrix}\end{aligned}$$

since if $i \geq 1$ then we only need to consider the first two terms of the sum as when $j \geq 2$ then $\nu_j(\lambda, 1) = 0$, as required. □

4.3 The MacWilliams Identity for the Hermitian Association Scheme

In this section we introduce the negative-q-Krawtchouk polynomials which we then prove are equal to the eigenvalues that are identified in [53, (4)] of the association scheme of Hermitian matrices over $\mathbb{F}_{q^2}$. In this way a new q-analog of the MacWilliams Identity for the Hermitian association scheme is presented and proven by comparison with a traditional form of the identity as given in [12, Theorem 3].

4.3.1 The Negative-q-Krawtchouk Polynomial

In comparison to the eigenvalues defined in Equation (2.7.3), a new set of polynomials is derived, which arise in finding the negative-q-transform of $\mu(X,Y;t)$ and $\nu(X,Y;t)$. We then go on to prove that these new polynomials are indeed the eigenvalues of the association scheme by proving that they are solutions to the recurrence relation used in [53, Lemma 7]. We note here that the recurrence relation used by Delsarte could not be used directly here because the parameters lay outside of the scope of validity. Specifically, q is defined to be strictly greater than or equal to 1 [11, Section 5.1], whereas in this section the equivalent parameter is negative. So instead, the recurrence relation used by Schmidt is the one we use here.

Definition 4.3.1. For $t \in \mathbb{Z}^+,\ x, k \in \{0, 1, \ldots, t\}$ we define the ***Negative-q-Krawtchouk Polynomial*** as

$$C_k(x,t) = \sum_{j=0}^{k} (-1)^j b^{j(t-x)} b^{\sigma_j} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} t-x \\ k-j \end{bmatrix} \gamma'(t-j, k-j). \tag{4.3.1}$$

We first prove that the $C_k(x,t)$ satisfy the recurrence relation (2.7.4) and the initial values in Equations (2.7.5), (2.7.6) and are therefore the eigenvalues of the association scheme.

Proposition 4.3.2. *For all $x, k \in \{0, 1, \ldots, t\}$ we have*

$$C_{k+1}(x+1, t+1) = C_{k+1}(x, t+1) + b^{2t+1-x} C_k(x,t).$$

Proof. We look at all three terms separately. Firstly,

$$\begin{aligned} C_{k+1}(x+1,t+1) &= \sum_{j=0}^{k+1} (-1)^j b^{j(t-x)} b^{\sigma_j} \begin{bmatrix} x+1 \\ j \end{bmatrix} \begin{bmatrix} t-x \\ k+1-j \end{bmatrix} \gamma'(t+1-j, k+1-j) \\ &= C_{k+1}(x+1,t+1)|_{j=k+1} \\ &\quad \overset{(2.3.30)}{+} \sum_{j=0}^{k} (-1)^j b^{j(t-x)} b^{\sigma_j} \left\{ \begin{bmatrix} x \\ j-1 \end{bmatrix} + b^j \begin{bmatrix} x \\ j \end{bmatrix} \right\} \begin{bmatrix} t-x \\ k+1-j \end{bmatrix} \\ &\quad \times \gamma'(t+1-j, k+1-j) \\ &= C_{k+1}(x+1,t+1)|_{j=k+1} \\ &\quad + \sum_{j=0}^{k} (-1)^j b^{j(t-x)} b^{\sigma_j} \begin{bmatrix} x \\ j-1 \end{bmatrix} \begin{bmatrix} t-x \\ k+1-j \end{bmatrix} \gamma'(t+1-j, k+1-j) \end{aligned}$$

(4.3.2)

$$\overset{(4.1.3)}{+} \sum_{j=0}^{k} (-1)^{j+1} b^{j(t-x-1)+k+t+1} b^{\sigma_j} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} t-x \\ k+1-j \end{bmatrix} \gamma'(t-j, k-j)$$

(4.3.3)

$$+ \sum_{j=0}^{k} (-1)^{j+1} b^{j(t-x)+k} b^{\sigma_j} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} t-x \\ k+1-j \end{bmatrix} \gamma'(t-j, k-j) \tag{4.3.4}$$

$$= C_{k+1}(x+1,t+1)|_{j=k+1} + \alpha_1 + \alpha_2 + \alpha_3$$

where $\alpha_1,\ \alpha_2,\ \alpha_3$ represent (4.3.2), (4.3.3), (4.3.4) respectively and for notation $|_{j=k+1}$ means “the term when $j = k+1$”.

Second,

$$\begin{aligned}
C_{k+1}(x,t+1) &= C_{k+1}(x,t+1)|_{j=k+1}\\
&\quad \overset{(4.1.3)}{+} \sum_{j=0}^{k}(-1)^{j+1}b^{l(t-x-1)+t+k+1}b^{\sigma_j}\begin{bmatrix}x\\ j\end{bmatrix}\begin{bmatrix}t+1-x\\ k+1-j\end{bmatrix}\gamma'(t-j,k-j)\\
&\quad + \sum_{j=0}^{k}(-1)^{j+1}b^{l(t-x)+k}b^{\sigma_j}\begin{bmatrix}x\\ j\end{bmatrix}\begin{bmatrix}t+1-x\\ k+1-j\end{bmatrix}\gamma'(t-j,k-j)\\
&= C_{k+1}(x,t+1)|_{j=k+1}\\
&\quad \overset{(2.3.29)}{+} \sum_{j=0}^{k}(-1)^{j+1}b^{j(t-x-2)+2k+t+2}b^{\sigma_j}\begin{bmatrix}x\\ j\end{bmatrix}\begin{bmatrix}t-x\\ k+1-j\end{bmatrix}\gamma'(t-j,k-j) && (4.3.5)\\
&\quad + \sum_{j=0}^{k}(-1)^{j+1}b^{j(t-x-1)+k+t+1}b^{\sigma_j}\begin{bmatrix}x\\ j\end{bmatrix}\begin{bmatrix}t-x\\ k-j\end{bmatrix}\gamma'(t-j,k-j) && (4.3.6)\\
&\quad \overset{(2.3.29)}{+} \sum_{j=0}^{k}(-1)^{j+1}b^{j(t-x-1)+2k+1}b^{\sigma_j}\begin{bmatrix}x\\ j\end{bmatrix}\begin{bmatrix}t-x\\ k+1-j\end{bmatrix}\gamma'(t-j,k-j) && (4.3.7)\\
&\quad + \sum_{j=0}^{k}(-1)^{j+1}b^{j(t-x)+k}b^{\sigma_j}\begin{bmatrix}x\\ j\end{bmatrix}\begin{bmatrix}t-x\\ k-j\end{bmatrix}\gamma'(t-j,k-j) && (4.3.8)\\
&= C_{k+1}(x,t+1)|_{j=k+1} + \beta_1 + \beta_2 + \beta_3 + \beta_4
\end{aligned}$$

where $\beta_1,\ \beta_2,\ \beta_3,\ \beta_4$ represent (4.3.5), (4.3.6), (4.3.7), (4.3.8) respectively. Thus,

$$\begin{aligned}
b^{2t-x+1}C_k(x,t) &= \sum_{j=0}^{k}(-1)^{j}b^{j(t-x)+2t-x+1}b^{\sigma_j}\begin{bmatrix}x\\ j\end{bmatrix}\begin{bmatrix}t-x\\ k-j\end{bmatrix}\gamma'(t-j,k-j)\\
&= \rho_1
\end{aligned}$$

So let $C = C_{k+1}(x+1,t+1) - C_{k+1}(x,t+1) - b^{2t+1-x}C_k(x,t)$. so

$$C = C_{k+1}(x+1,t+1)|_{j=k+1} + \alpha_1 + \alpha_2 + \alpha_3 - C_{k+1}(x,t+1)|_{j=k+1} - \beta_1 - \beta_2 - \beta_3 - \beta_4 - \rho_1.$$

Claim 1: $\alpha_2 - \beta_1 - \beta_2 - \rho_1 = 0$.

$$\begin{aligned}
\alpha_2 - \beta_1 &= \sum_{j=0}^{k}(-1)^{j+1}b^{l(t-x-1)+k+t+1}b^{\sigma_j}\begin{bmatrix}x\\ j\end{bmatrix}\begin{bmatrix}t-x\\ k+1-j\end{bmatrix}\gamma'(t-j,k-j)\left(1-b^{k-j+1}\right)\\
&\overset{(2.3.31)}{=} \sum_{j=0}^{k}(-1)^{j}b^{j(t-x)+t+1}b^{\sigma_j}\begin{bmatrix}x\\ j\end{bmatrix}\begin{bmatrix}t-x\\ k-j\end{bmatrix}\gamma'(t-j,k-j)\left(b^{t-x}-b^{k-j}\right)\\
&= \rho_1 + \beta_2
\end{aligned}$$

Thus $\alpha_2 - \beta_1 - \beta_2 - \rho_1 = 0$.

Claim 2: $\alpha_1+\alpha_3-\beta_3-\beta_4=(-1)^k b^{k(t-x+1)+t-x} b^{\sigma_{k+1}} \begin{bmatrix} x \\ k \end{bmatrix} \gamma'(t-k,0)$.

$$\begin{aligned}
\alpha_3-\beta_3 &= \sum_{j=0}^{k} (-1)^{j+1} b^{j(t-x)+k} b^{\sigma_j} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} t-x \\ k+1-j \end{bmatrix} \gamma'(t-j,k-j)\left(1-b^{k-j+1}\right) \\
&\overset{(2.3.31)}{=} \sum_{j=0}^{k} (-1)^{j} b^{j(t-x+1)} b^{\sigma_j} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} t-x \\ k-j \end{bmatrix} \gamma'(t-j,k-j)\left(b^{t-x}-b^{k-j}\right) \\
&= \sum_{j=0}^{k} (-1)^{j} b^{j(t-x+1)+t-x} b^{\sigma_j} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} t-x \\ k-j \end{bmatrix} \gamma'(t-j,k-j)+\beta_4 \qquad (4.3.9)
\end{aligned}$$

So

$$\begin{aligned}
C &= C_{k+1}(x+1,t+1)|_{j=k+1}-C_{k+1}(x,t+1)|_{j=k+1}+\alpha_1 \\
&\quad +\sum_{j=0}^{k} (-1)^{j} b^{j(t-x+1)+t-x} b^{\sigma_j} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} t-x \\ k-j \end{bmatrix} \gamma'(t-j,k-j) \qquad (4.3.10) \\
&= C_{k+1}(x+1,t+1)|_{j=k+1}-C_{k+1}(x,t+1)|_{j=k+1}+\alpha_1+\rho_2
\end{aligned}$$

where ρ_2 represents the summand in (4.3.10). Now,

$$\alpha_1=\sum_{j=1}^{k} (-1)^{j} b^{j(t-x)} b^{\sigma_j} \begin{bmatrix} x \\ j-1 \end{bmatrix} \begin{bmatrix} t-x \\ k+1-j \end{bmatrix} \gamma'(t+1-j,k+1-j)$$

since the $\begin{bmatrix} x \\ j-1 \end{bmatrix}=0$ when $j=0$. Now let $\ell=j-1,\ j=\ell+1$

$$\begin{aligned}
\alpha_1 &= \sum_{\ell=0}^{k-1} (-1)^{\ell+1} b^{(\ell+1)(t-x)} b^{\sigma_{\ell+1}} \begin{bmatrix} x \\ \ell \end{bmatrix} \begin{bmatrix} t-x \\ k-\ell \end{bmatrix} \gamma'(t-\ell,k-\ell) \\
&= \sum_{j=0}^{k-1} (-1)^{j+1} b^{j(t-x+1)+t-x} b^{\sigma_j} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} t-x \\ k-j \end{bmatrix} \gamma'(t-j,k-j).
\end{aligned}$$

So we have,

$$\begin{aligned}
\rho_2+\alpha_1 &= \sum_{j=0}^{k} (-1)^{j} b^{j(t-x+1)+t-x} b^{\sigma_j} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} t-x \\ k-j \end{bmatrix} \gamma'(t-j,k-j) \\
&\quad +\sum_{j=0}^{k-1} (-1)^{j+1} b^{j(t-x+1)+t-x} b^{\sigma_j} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} t-x \\ k-j \end{bmatrix} \gamma'(t-j,k-j) \\
&= (-1)^k b^{k(t-x+1)+t-x} b^{\sigma_{k+1}} \begin{bmatrix} x \\ k \end{bmatrix} \begin{bmatrix} t-x \\ 0 \end{bmatrix} \gamma'(t-k,0).
\end{aligned}$$

Thus Claim 2 holds. So

$$\begin{aligned}C &= b^{k(t-x)+k+t-x} b^{\sigma_k} \begin{bmatrix} x \\ k \end{bmatrix} \begin{bmatrix} t-x \\ 0 \end{bmatrix} \gamma'(t-k,0) \\ &\quad + (-1)^{k+1} b^{(k+1)(t-x)} b^{\sigma_{k+1}} \begin{bmatrix} x+1 \\ k+1 \end{bmatrix} \begin{bmatrix} t-x \\ 0 \end{bmatrix} \gamma'(t-k,0) \\ &\quad - (-1)^{k+1} b^{(k+1)(t+1-x)} b^{\sigma_{k+1}} \begin{bmatrix} x \\ k+1 \end{bmatrix} \begin{bmatrix} t+1-x \\ 0 \end{bmatrix} \gamma'(t-k,0) \\ &= (-1)^k b^{(k+1)(t-x)} b^{\sigma_{k+1}} \left\{ \begin{bmatrix} x \\ k \end{bmatrix} - \begin{bmatrix} x+1 \\ k+1 \end{bmatrix} + \begin{bmatrix} x \\ k+1 \end{bmatrix} b^{k+1} \right\} \\ &\overset{(2.3.30)}{=} 0.\end{aligned}$$

□

Lemma 4.3.3. *The $C_k(x,t)$ are the eigenvalues of the Hermitian association scheme. In other words,*

$$C_k(x,t) = P_k(x,t). \tag{4.3.11}$$

Proof. The $C_k(x,t)$ satisfy the recurrence relation (2.7.4) and the initial values of the $C_k(x,t)$ are

$$\begin{aligned}C_k(0,t) &= \sum_{j=0}^{k} b^{jt} (-1)^j b^{\sigma_j} \begin{bmatrix} 0 \\ j \end{bmatrix} \begin{bmatrix} t \\ k-j \end{bmatrix} \gamma'(t-j,k-j) \\ &= \begin{bmatrix} t \\ k \end{bmatrix} \gamma'(t,k)\end{aligned}$$

$$\begin{aligned}C_0(x,t) &= (-1)^0 b^0 b^{\sigma_0} \begin{bmatrix} x \\ 0 \end{bmatrix} \begin{bmatrix} t-x \\ 0 \end{bmatrix} \gamma'(t,0) \\ &= 1\end{aligned}$$

□

4.3.2 The MacWilliams Identity for the Hermitian Association Scheme

We now use the negative-q-Krawtchouk polynomials to prove the q-analog form of the MacWilliams Identity for the Hermitian association scheme. The new form below uses a functional transformation of the weight distribution rather than explicit use of the eigenvalues. Notably, the form developed in this paper is similar to the q-analog of the MacWilliams Identity developed in [22] for linear rank metric codes over $\mathbb{F}_{q^m}$ and is similar to the q-analog of the MacWilliams Identity developed in Chapter 3 but differs in the form of the new Krawtchouk polynomial.

Let the Hermitian rank weight enumerator of $\mathscr{C} \subseteq \mathscr{H}_{q,t}$ be

$$W^{HR}_{\mathscr{C}}(X,Y) = \sum_{i=0}^{t} c_i Y^i X^{t-i}$$

and of its dual, $\mathscr{C}^{\perp} \subseteq \mathscr{H}_{q,t}$ be

$$W^{HR}_{\mathscr{C}^{\perp}}(X,Y) = \sum_{i=0}^{t} c'_i Y^i X^{t-i}.$$

Theorem 4.3.4 (The MacWilliams Identity for the Hermitian Association Scheme)**.** *Let $\mathscr{C} \subseteq \mathscr{H}_{q,t}$ be a linear code with weight distribution $\boldsymbol{c} = (c_0, \ldots, c_n)$ and $\mathscr{C}^{\perp} \subseteq \mathscr{H}_{q,t}$ its dual code with weight distribution $\boldsymbol{c'} = (c'_0, \ldots, c'_n)$. Then*

$$W^{HR}_{\mathscr{C}^{\perp}}(X,Y) = \frac{1}{|\mathscr{C}|}\overline{W}^{HR}_{\mathscr{C}}\left(X + (-b^t - 1)Y, X - Y\right).$$

Proof. For $0 \leq i \leq n$ we have

$$\begin{aligned}
&(X-Y)^{[i]} * \left(X + \left(-b^t - 1\right)Y\right)^{[t-i]} \\
&\quad = \left(\nu^{[i]}(X,Y;t)\right) * \left(\mu^{[t-i]}(X,Y;t)\right) \\
&\quad \overset{(4.2.4)(4.2.6)}{=} \left(\sum_{u=0}^{i}(-1)^u b^{\sigma_u}\begin{bmatrix} i \\ u \end{bmatrix} Y^u X^{i-u}\right) * \left(\sum_{j=0}^{t-i}\begin{bmatrix} t-i \\ j \end{bmatrix}\gamma'(t,j)Y^j X^{t-i-j}\right) \\
&\quad \overset{(4.2.1)}{=} \sum_{k=0}^{t}\left(\sum_{\ell=0}^{k}(-1)^{\ell} b^{\ell(t-i)} b^{\sigma_\ell}\begin{bmatrix} i \\ \ell \end{bmatrix}\begin{bmatrix} t-i \\ k-\ell \end{bmatrix}\gamma'(t-\ell, k-\ell)\right) Y^k X^{t-k} \\
&\quad = \sum_{k=0}^{t} C_k(i,t) Y^k X^{t-k} \\
&\quad \overset{(4.3.11)}{=} \sum_{k=0}^{t} P_k(i,t) Y^k X^{t-k}.
\end{aligned}$$

So then we have

$$\begin{aligned}
\frac{1}{|\mathscr{C}|}\overline{W}^{HR}_{\mathscr{C}}\left(X + \left(-b^t - 1\right)Y, X - Y\right) &= \frac{1}{|\mathscr{C}|}\sum_{i=0}^{t} c_i \left(X - Y\right)^{[i]} * \left(X + \left(-b^t - 1\right)Y\right)^{[t-i]} \\
&= \frac{1}{|\mathscr{C}|}\sum_{i=0}^{t} c_i \sum_{k=0}^{t} P_k(i,t) Y^k X^{t-k} \\
&= \sum_{k=0}^{t}\left(\frac{1}{|\mathscr{C}|}\sum_{i=0}^{t} c_i P_k(i,t)\right) Y^k X^{t-k} \\
&\overset{(4.1.1)}{=} \sum_{k=0}^{n} c'_k Y^k X^{t-k} \\
&= W^{HR}_{\mathscr{C}^{\perp}}(X,Y)
\end{aligned}$$

□

In this way we have shown that the MacWilliams Identity for the Hermitian association scheme can be expressed as a q-transform of homogeneous polynomials in a form analogous to the original MacWilliams Identity for the Hamming metric and the q-analogs developed by Gadouleau and Yan [22] for the rank association scheme and in Chapter 3 for the skew rank association scheme.

4.4 The Negative-q-Derivatives

In this section we develop a new negative-q-derivative and negative-q^{-1}-derivative to help analyse the coefficients of Hermitian rank weight enumerators. This is analogous to the q-derivative applied to the rank metric in [22] with the parameter q replaced by $-q = b$.

4.4.1 The Negative-q-Derivative

Definition 4.4.1. For $q \geq 2$, the ***negative-q-derivative*** at $X \neq 0$ for a real-valued function $f(X)$ is defined as

$$f^{(1)}(X) = \frac{f(bX) - f(X)}{(b-1)X}.$$

For $\varphi \geq 0$ we denote the φ^{th} negative-q-derivative (with respect to X) of $f(X,Y;\lambda)$ as $f^{(\varphi)}(X,Y;\lambda)$. The 0^{th} negative-q-derivative of $f(X,Y;\lambda)$ is $f(X,Y;\lambda)$. For any $a \in \mathbb{R}$, $X \neq 0$, and real-valued function $g(X)$,

$$[f(X) + ag(X)]^{(1)} = f^{(1)}(X) + ag^{(1)}(X).$$

Lemma 4.4.2.

1. *For $0 \leq \varphi \leq \ell$, $\varphi \in \mathbb{Z}^+$ and $\ell \geq 0$,*

$$\left(X^{\ell}\right)^{(\varphi)} = \beta(\ell,\varphi)X^{\ell-\varphi}.$$

2. *The φ^{th} negative-q-derivative of $f(X,Y;\lambda) = \sum_{i=0}^{r} f_i(\lambda)Y^iX^{r-i}$ is given by*

$$f^{(\varphi)}(X,Y;\lambda) = \sum_{i=0}^{r-\varphi} f_i(\lambda)\beta(r-i,\varphi)Y^iX^{r-i-\varphi}. \quad (4.4.1)$$

3. *Also,*

$$\mu^{[k](\varphi)}(X,Y;\lambda) = \beta(k,\varphi)\mu^{[k-\varphi]}(X,Y;\lambda) \quad (4.4.2)$$
$$\nu^{[k](\varphi)}(X,Y;\lambda) = \beta(k,\varphi)\nu^{[k-\varphi]}(X,Y;\lambda). \quad (4.4.3)$$

Proof. (1) For $\varphi = 1$ we have

$$\left(X^{\ell}\right)^{(1)} = \frac{(bX)^{\ell} - X^{\ell}}{(b-1)X} = \frac{b^{\ell}-1}{b-1}X^{\ell-1} = \begin{bmatrix}\ell\\1\end{bmatrix}X^{\ell-1} = \beta(\ell,\varphi)X^{\ell-1}.$$

The rest of the proof follows by induction on φ and is omitted.

(2) Now consider $f(X,Y;\lambda) = \sum_{i=0}^{r} f_i(\lambda)Y^iX^{r-i}$. We have,

$$\begin{aligned} f^{(1)}(X,Y;\lambda) &= \left(\sum_{i=0}^{r} f_i(\lambda)Y^iX^{r-i}\right)^{(1)} \\ &= \sum_{i=0}^{r} f_i(\lambda)Y^i\left(X^{r-i}\right)^{(1)} \\ &= \sum_{i=0}^{r-1} f_i(\lambda)\beta(r-i,\varphi)Y^iX^{r-i-1}. \end{aligned}$$

Then the case of $\varphi = 1$ holds. The rest of the proof follows by induction on φ and is omitted.

(3) Now consider $\mu^{[k]} = \sum_{u=0}^{k} \mu_u(\lambda,k)Y^uX^{k-u}$ where $\mu_u(\lambda,k) = \begin{bmatrix}k\\u\end{bmatrix}\gamma'(\lambda,u)$ as in Equation (4.2.4). Then we have

$$\begin{aligned} \mu^{[k](1)}(X,Y;\lambda) &= \left(\sum_{u=0}^{k} \mu_u(\lambda,k)Y^uX^{k-u}\right)^{(1)} \\ &= \sum_{u=0}^{k} \mu_u(\lambda,k)Y^u\left(\frac{(bX)^{k-u} - X^{k-u}}{(b-1)X}\right) \\ &= \sum_{u=0}^{k-1} \frac{b^{(k-u)}-1}{b-1}\begin{bmatrix}k\\u\end{bmatrix}\gamma'(\lambda,u)Y^uX^{k-u-1} \\ &\overset{(2.3.32)}{=} \sum_{u=0}^{k-1} \frac{\left(b^k-1\right)\left(b^{(k-u)}-1\right)}{(b^{(k-u)}-1)(b-1)}\begin{bmatrix}k-1\\u\end{bmatrix}\gamma'(\lambda,u)Y^uX^{k-u-1} \\ &= \left(\frac{b^k-1}{b-1}\right)\mu^{[k-1]}(X,Y;\lambda) \\ &\overset{(2.3.34)}{=} \beta(k,1)\mu^{[k-1]}(X,Y;\lambda). \end{aligned}$$

Then the case of $\varphi = 1$ holds. The statement of the theorem, $\mu^{[k](\varphi)}(X,Y;\lambda) = \beta(k,\varphi)\mu^{[k-\varphi]}(X,Y;\lambda)$, then follows by induction on φ and is omitted.

Now consider $\nu^{[k]} = \sum_{u=0}^{k}(-1)^u b^{\sigma_u}\begin{bmatrix}k\\u\end{bmatrix}Y^uX^{k-u}$ as in Equation (4.2.6). Then we have

$$\begin{aligned}\nu^{[k](1)}(X,Y;\lambda) &= \sum_{u=0}^{k}(-1)^u b^{\sigma_u}\frac{b^{(k-u)}-1}{b-1}\begin{bmatrix}k\\u\end{bmatrix}Y^uX^{k-u-1}\\ &= \sum_{u=0}^{k-1}(-1)^u b^{\sigma_u}\frac{\left(b^k-1\right)\left(b^{(k-u)}-1\right)}{\left(b^{(k-u)}-1\right)(b-1)}\begin{bmatrix}k-1\\u\end{bmatrix}Y^uX^{k-1-u}\\ &= \frac{b^k-1}{b-1}\nu^{[k-1]}(X,Y;\lambda)\\ &= \beta(k,1)\nu^{[k-1]}(X,Y;\lambda).\end{aligned}$$

The statement of the theorem, $\nu^{[k](\varphi)}(X,Y;\lambda) = \beta(k,\varphi)\nu^{[k-\varphi]}(X,Y;\lambda)$, then follows by induction also and is omitted.

□

We now need a few smaller lemmas in order to prove the Leibniz rule for the negative-q-derivative.

Lemma 4.4.3. *Let*

$$\begin{aligned}u\left(X,Y;\lambda\right) &= \sum_{i=0}^{r}u_i(\lambda)Y^iX^{r-i}\\ v\left(X,Y;\lambda\right) &= \sum_{i=0}^{s}v_i(\lambda)Y^iX^{s-i}.\end{aligned}$$

1. If $u_r(\lambda)=0$ *then*

$$\frac{1}{X}\left[u\left(X,Y;\lambda\right) * v\left(X,Y;\lambda\right)\right] = \frac{u\left(X,Y;\lambda\right)}{X} * v\left(X,Y;\lambda\right). \tag{4.4.4}$$

2. If $v_s(\lambda)=0$ *then*

$$\frac{1}{X}\left[u\left(X,Y;\lambda\right) * v\left(X,Y;\lambda\right)\right] = u\left(X,bY;\lambda\right) * \frac{v\left(X,Y;\lambda\right)}{X}. \tag{4.4.5}$$

Proof.

(1) If $u_r(\lambda)=0$,

$$\frac{u\left(X,Y;\lambda\right)}{X} = \sum_{i=0}^{r-1}u_i(\lambda)Y^iX^{r-i-1}.$$

Hence

$$\begin{aligned}\frac{u\left(X,Y;\lambda\right)}{X}*v\left(X,Y;\lambda\right)&=\sum_{k=0}^{r+s-1}\left(\sum_{\ell=0}^{k}b^{\ell s}u_{\ell}(\lambda)v_{k-\ell}(\lambda-\ell)\right)Y^{k}X^{r+s-1-k}\\&=\frac{1}{X}\sum_{k=0}^{r+s-1}\left(\sum_{\ell=0}^{k}b^{\ell s}u_{\ell}(\lambda)v_{k-\ell}(\lambda-\ell)\right)Y^{k}X^{r+s-k}\\&\quad+\frac{1}{X}\sum_{\ell=0}^{r+s}b^{\ell s}u_{\ell}(\lambda)v_{r+s-\ell}(\lambda-\ell)Y^{r+s}X^{0}\\&=\frac{1}{X}\left(u\left(X,Y;\lambda\right)*v\left(X,Y;\lambda\right)\right)\end{aligned}$$

since $v_{r+s-\ell}(\lambda-\ell)=0$ for $0\leq\ell\leq r-1$ and $u_{\ell}(\lambda)=0$ for $r\leq\ell\leq r+s$ so

$$\frac{1}{X}\sum_{\ell=0}^{r+s}b^{\ell s}u_{\ell}(\lambda)v_{r+s-\ell}(\lambda-\ell)Y^{r+s}X^{0}=0.$$

(2) Now if $v_s(\lambda)=0$,

$$\frac{v\left(X,Y;\lambda\right)}{X}=\sum_{i=0}^{s-1}v_{i}(\lambda)Y^{i}X^{s-1-i}.$$

Then

$$\begin{aligned}u\left(X,bY;\lambda\right)*\frac{v\left(X,Y;\lambda\right)}{X}&=\sum_{k=0}^{r+s-1}\left(\sum_{\ell=0}^{k}b^{\ell(s-1)}b^{\ell}u_{\ell}(\lambda)v_{k-\ell}(\lambda-\ell)\right)Y^{k}X^{r+s-1-k}\\&=\sum_{k=0}^{r+s-1}\left(\sum_{\ell=0}^{k}b^{\ell(s-1)}b^{\ell}u_{\ell}(\lambda)v_{k-\ell}(\lambda-\ell)\right)Y^{k}X^{r+s-1-k}\\&\quad+\frac{1}{X}\sum_{\ell=0}^{r+s}b^{\ell s}u_{\ell}(\lambda)v_{r+s-\ell}(\lambda-\ell)Y^{r+s}X^{0}\\&=\frac{1}{X}\left[u(X,Y;\lambda)*v(X,Y;\lambda)\right]\end{aligned}$$

since $v_{r+s-\ell}(\lambda-\ell)=0$ for $0\leq\ell\leq r$ and $u_{\ell}=0$ for $r+1\leq\ell\leq r+s$. □

Theorem 4.4.4 (Leibniz rule for the negative-q-derivative)**.** *For two homogeneous polynomials in X and Y, $f(X,Y;\lambda)$ and $g(X,Y;\lambda)$ with degrees r and s respectively, and for $\varphi\geq 0$, the φ^{th} negative-q-derivative of their negative-q-product is given by*

$$\left[f\left(X,Y;\lambda\right)*g\left(X,Y;\lambda\right)\right]^{(\varphi)}=\sum_{\ell=0}^{\varphi}\begin{bmatrix}\varphi\\ \ell\end{bmatrix}b^{(\varphi-\ell)(r-\ell)}f^{(\ell)}\left(X,Y;\lambda\right)*g^{(\varphi-\ell)}\left(X,Y;\lambda\right). \quad (4.4.6)$$

Proof. For simplification, we shall write $f(X,Y;\lambda)$ as $f(X,Y)$ and similarly $g(X,Y;\lambda)$ as

$g(X,Y)$. Now by differentiation we have

$$\begin{aligned}
[f(X,Y)*g(X,Y)]^{(1)} &= \frac{f(bX,Y)*g(bX,Y)-f(X,Y)*g(X,Y)}{(b-1)X}\\
&= \frac{1}{(b-1)X}\Big\{f(bX,Y)*g(bX,Y)-f(bX,Y)*g(X,Y)\\
&\qquad +f(bX,Y)*g(X,Y)-f(X,Y)*g(X,Y)\Big\}\\
&= \frac{1}{(b-1)X}\left\{f(bX,Y)*(g(bX,Y)-g(X,Y))\right\}\\
&\qquad +\frac{1}{(b-1)X}\Big\{(f(bX,Y)-f(X,Y))*g(X,Y)\Big\}\\
&\overset{(4.4.5)}{=} f(bX,bY)*\left\{\frac{g(bX,Y)-g(X,Y)}{(b-1)X}\right\}\\
&\qquad \overset{(4.4.4)}{+}\left\{\frac{f(bX,Y)-f(X,Y)}{(b-1)X}\right\}*g(X,Y)\\
&= b^r f(X,Y)*g^{(1)}(X,Y)+f^{(1)}(X,Y)*g(X,Y)
\end{aligned}$$

since $f(X,Y)$ is a homogeneous polynomial. So the initial case holds. Assume the statement holds true for $\varphi=\overline{\varphi}$, i.e.

$$[f(X,Y)*g(X,Y)]^{(\overline{\varphi})}=\sum_{\ell=0}^{\overline{\varphi}}\begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix}b^{(\overline{\varphi}-\ell)(r-\ell)}f^{(\ell)}(X,Y)*g^{(\overline{\varphi}-\ell)}(X,Y).$$

Now considering $\overline{\varphi}+1$ and for simplicity writing $f(X,Y;\lambda)$, $g(X,Y;\lambda)$ as f,g we have

$$\begin{aligned}
[f*g]^{(\overline{\varphi}+1)} &= \left[\sum_{\ell=0}^{\overline{\varphi}}\begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix}b^{(\overline{\varphi}-\ell)(r-\ell)}f^{(\ell)}*g^{(\overline{\varphi}-\ell)}\right]^{(1)}\\
&= \sum_{\ell=0}^{\overline{\varphi}}\begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix}b^{(\overline{\varphi}-\ell)(r-\ell)}\left(b^{(r-\ell)}f^{(\ell)}*g^{(\overline{\varphi}-\ell+1)}+f^{(\ell+1)}*g^{(\overline{\varphi}-\ell)}\right)\\
&= \sum_{\ell=0}^{\overline{\varphi}}\begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix}b^{(\overline{\varphi}-\ell+1)(r-\ell)}f^{(\ell)}*g^{(\overline{\varphi}-\ell+1)}\\
&\qquad +\sum_{\ell=1}^{\overline{\varphi}+1}\begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix}b^{(\overline{\varphi}-\ell+1)(r-\ell+1)}f^{(\ell)}*g^{(\overline{\varphi}-\ell+1)}\\
&= \begin{bmatrix}\overline{\varphi}\\ 0\end{bmatrix}b^{(\overline{\varphi}+1)r}f*g^{(\overline{\varphi}+1)}+\sum_{\ell=1}^{\overline{\varphi}}\begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix}b^{(\overline{\varphi}+1-\ell)(r-\ell)}f^{(\ell)}*g^{(\overline{\varphi}-\ell+1)}\\
&\qquad +\begin{bmatrix}\overline{\varphi}\\ \overline{\varphi}\end{bmatrix}b^{(\overline{\varphi}+1-\overline{\varphi}-1)(r-\overline{\varphi}-1+1)}f^{(\overline{\varphi}+1)}*g\\
&\qquad +\sum_{\ell=1}^{\overline{\varphi}}\begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix}b^{(\overline{\varphi}+1-\ell)(r-\ell+1)}f^{(\ell)}*g^{(\overline{\varphi}-\ell+1)}\\
&= b^{(\overline{\varphi}+1)r}f*g^{(\overline{\varphi}+1)}+f^{(\overline{\varphi}+1)}*g+\sum_{\ell=1}^{\overline{\varphi}}\left(\begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix}+b^{(\overline{\varphi}-\ell+1)}\begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix}\right)\\
&\qquad \times b^{(\overline{\varphi}-\ell+1)(r-\ell)}f^{(\ell)}*g^{(\overline{\varphi}-\ell+1)}
\end{aligned}$$

Then applying Equation (2.3.29) yields

$$\begin{aligned}\sum_{\ell=1}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}+1\\ \ell\end{bmatrix} b^{(\overline{\varphi}+1-\ell)(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}+1-\ell)} + \begin{bmatrix}\overline{\varphi}+1\\ 0\end{bmatrix} b^{(\overline{\varphi}+1)(r)} f * g^{(\overline{\varphi}+1)}&\\ + \begin{bmatrix}\overline{\varphi}+1\\ \overline{\varphi}+1\end{bmatrix} b^{(\overline{\varphi}-1-\overline{\varphi}-1)} f^{(\overline{\varphi}+1)} * g&\\ = \sum_{\ell=0}^{\overline{\varphi}+1} \begin{bmatrix}\overline{\varphi}+1\\ \ell\end{bmatrix} b^{(\overline{\varphi}+1-\ell)(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}+1-\ell)}&\end{aligned}$$

as required. □

4.4.2 The Negative-q^{-1}-Derivative

Definition 4.4.5. For $q \geq 2,\ -q = b$, the ***negative-q^{-1}-derivative*** at $Y \neq 0$ for a real-valued function $g(Y)$ is defined as

$$g^{\{1\}}(Y) = \frac{g\left(b^{-1}Y\right) - g(Y)}{(b^{-1}-1)Y}.$$

For $\varphi \geq 0$ we denote the φ^{th} negative-q^{-1}-derivative (with respect to Y) of $g(X,Y;\lambda)$ as $g^{\{\varphi\}}(X,Y;\lambda)$. The 0^{th} negative-q^{-1}-derivative of $g(X,Y;\lambda)$ is $g(X,Y;\lambda)$. For any $a \in \mathbb{R},\ Y \neq 0$ and real-valued function $f(Y)$,

$$[f(Y) + ag(Y)]^{\{1\}} = f^{\{1\}}(Y) + ag^{\{1\}}(Y).$$

Lemma 4.4.6. *1. For $0 \leq \varphi \leq \ell, \varphi \in \mathbb{Z}^+, \ell \geq 0$,*

$$\left(Y^{\ell}\right)^{\{\varphi\}} = b^{\varphi(1-\ell)+\sigma_\varphi}\beta(\ell,\varphi)Y^{\ell-\varphi}.$$

2. The φ^{th} negative-q^{-1}-derivative of $g(X,Y;\lambda) = \sum_{i=0}^{s} g_i(\lambda)Y^iX^{s-i}$ is given by

$$g^{\{\varphi\}}(X,Y;\lambda) = \sum_{i=\varphi}^{s} g_i(\lambda)b^{\varphi(1-i)+\sigma_\varphi}\beta(i,\varphi)Y^{i-\varphi}X^{s-i}. \tag{4.4.7}$$

3. Also,

$$\mu^{[k]\{\varphi\}}(X,Y;\lambda) = b^{-\sigma_\varphi}\beta(k,\varphi)\gamma'(\lambda,\varphi)\mu^{[k-\varphi]}(X,Y;\lambda-\varphi) \tag{4.4.8}$$

$$\nu^{[k]\{\varphi\}}(X,Y;\lambda) = (-1)^{\varphi}\beta(k,\varphi)\nu^{[k-\varphi]}(X,Y;\lambda). \tag{4.4.9}$$

Proof. (1) For $\varphi = 1$ we have

$$\left(Y^{\ell}\right)^{\{1\}} = \frac{\left(b^{-1}Y\right)^{\ell} - Y^{\ell}}{(b^{-1}-1)Y} = \left(\frac{b^{-\ell}-1}{b^{-1}-1}\right)Y^{\ell-1}$$
$$= b^{1-\ell}\beta(\ell,1)Y^{\ell-1}.$$

So the initial case holds. Assume the case for $\varphi = \overline{\varphi}$ holds. Then we have

$$\begin{aligned}
\left(Y^{\ell}\right)^{\{\overline{\varphi}+1\}} &= \left(b^{(\overline{\varphi}(1-\ell)+\sigma_{\overline{\varphi}})}\beta(\ell,\overline{\varphi})Y^{\ell-\overline{\varphi}}\right)^{\{1\}} \\
&= b^{(\overline{\varphi}(1-\ell)+\sigma_{\overline{\varphi}})}\beta(\ell,\overline{\varphi})\frac{b^{-(\ell-\overline{\varphi})}Y^{\ell-\overline{\varphi}} - Y^{\ell-\overline{\varphi}}}{\left(b^{-1}-1\right)Y} \\
&= b^{\overline{\varphi}(1-\ell)+\sigma_{\overline{\varphi}}}\beta(\ell,\varphi)b^{1-(\ell-\overline{\varphi})}\beta(\ell-\overline{\varphi},1)Y^{\ell-\overline{\varphi}-1} \\
&\overset{(2.3.37)}{=} b^{(\overline{\varphi}+1)(1-\ell)+\sigma_{\overline{\varphi}+1}}\beta(\ell,\overline{\varphi}+1)Y^{\ell-(\overline{\varphi}+1)}.
\end{aligned}$$

Thus the statement holds by induction.

(2) Now consider $g(X,Y;\lambda) = \sum\limits_{i=0}^{s} g_i(\lambda)Y^iX^{s-i}$. For $\varphi = 1$ we have

$$g^{\{1\}}\left(X,Y;\lambda\right) = \left(\sum_{i=0}^{s} g_i(\lambda)Y^iX^{s-i}\right)^{\{1\}} = \sum_{i=0}^{s} g_i(\lambda)b^{(-i+1)}\beta(i,1)Y^{i-1}X^{s-i}.$$

As $\beta(i,1) = 0$ when $i = 0$ we have

$$g^{\{1\}}\left(X,Y;\lambda\right) = \sum_{i=1}^{s} g_i(\lambda)b^{(1-i)+\sigma_1}\beta(i,1)Y^{i-1}X^{s-i}.$$

So the initial case holds. Now assume the case holds for $\varphi = \overline{\varphi}$ i.e. $g^{\{\overline{\varphi}\}}\left(X,Y;\lambda\right) = \sum\limits_{i=\overline{\varphi}}^{s} g_i(\lambda)b^{\overline{\varphi}(1-i)+\sigma_{\overline{\varphi}}}\beta(i,\overline{\varphi})Y^{i-\overline{\varphi}}X^{s-i}$. Then we have

$$\begin{aligned}
g^{\{\overline{\varphi}+1\}}\left(X,Y;\lambda\right) &= \left(\sum_{i=\overline{\varphi}}^{s} g_i(\lambda)b^{\overline{\varphi}(1-i)+\sigma_{\overline{\varphi}}}\beta(i,\overline{\varphi})Y^{i-\overline{\varphi}}X^{s-i}\right)^{\{1\}} \\
&= \sum_{i=\overline{\varphi}}^{s} g_i(\lambda)b^{\overline{\varphi}(1-i)+\sigma_{\overline{\varphi}}}\beta(i,\overline{\varphi})b^{-(i-\overline{\varphi}-1)}\beta(i-\overline{\varphi},1)Y^{i-\overline{\varphi}-1}X^{s-i} \\
&\overset{(2.3.34)}{=} \sum_{i=\overline{\varphi}}^{s} g_i(\lambda)b^{(\overline{\varphi}+1)(1-i)+\sigma_{\overline{\varphi}}}\prod_{j=0}^{\overline{\varphi}-1}\frac{\left(b^{i-j}-1\right)\left(b^{i-\overline{\varphi}}-1\right)}{(b-1)(b-1)}Y^{i-\overline{\varphi}-1}X^{s-i} \\
&= \sum_{i=\overline{\varphi}}^{s} g_i(\lambda)b^{(\overline{\varphi}+1)(1-i)+\sigma_{\overline{\varphi}+1}}\beta(i,\overline{\varphi}+1)Y^{i-\overline{\varphi}-1}X^{s-i} \\
&= \sum_{i=\overline{\varphi}+1}^{s} g_i(\lambda)b^{(\overline{\varphi}+1)(1-i)+\sigma_{\overline{\varphi}+1}}\beta(i,\overline{\varphi}+1)Y^{i-\overline{\varphi}-1}X^{s-i}
\end{aligned}$$

since when $i = \overline{\varphi}$, $\beta(\overline{\varphi},\overline{\varphi}+1) = 0$. So by induction Equation (4.4.7) holds.

(3) Now consider $\mu^{[k]}(X,Y;\lambda) = \sum_{u=0}^{k} \mu_u(\lambda,k) Y^u X^{k-u}$ where $\mu_u(\lambda,k) = \begin{bmatrix} k \\ u \end{bmatrix} \gamma'(\lambda,u)$ as in Equation (4.2.4). Then we have

$$\begin{aligned}
\mu^{[k]\{1\}}(X,Y;\lambda) &= \left(\sum_{u=0}^{k} \mu_u(\lambda,k) Y^u X^{k-u} \right)^{\{1\}} \\
&= \sum_{u=0}^{k} \mu_u(\lambda,k) b^{1-u} \beta(u,1) Y^{u-1} X^{k-u} \\
&= \sum_{r=0}^{k-1} \mu_{r+1}(\lambda,k) b^{1-(r+1)} \beta(r+1,1) Y^{r+1-1} X^{k-r-1} \\
&= \sum_{r=0}^{k-1} \begin{bmatrix} k \\ r+1 \end{bmatrix} \gamma'(\lambda,r+1) b^{-r} \beta(r+1,1) Y^r X^{k-1-r} \\
&\overset{(2.3.33)}{=} \sum_{r=0}^{k-1} \begin{bmatrix} k-1 \\ r \end{bmatrix} \frac{\left(b^k-1\right)\left(b^{r+1}-1\right)}{\left(b^{r+1}-1\right)(b-1)} \\
&\qquad \times \left(-b^{\lambda}-1\right) b^r b^{-r} \gamma'(\lambda-1,r) Y^r X^{k-1-r} \\
&= b^{-\sigma_1} \beta(k,1) \gamma'(\lambda,1) \mu^{[k-1]}(X,Y;\lambda-1).
\end{aligned}$$

So the case for $\varphi = 1$ holds. Now assume that the statement holds for $\varphi = \overline{\varphi}$. Then we have

$$\begin{aligned}
\mu^{[k]\{\overline{\varphi}+1\}}(X,Y;\lambda) &= \left[b^{-\sigma_{\overline{\varphi}}} \beta(k,\overline{\varphi}) \gamma'(\lambda,\overline{\varphi}) \mu^{[k-\overline{\varphi}]}(X,Y;\lambda-\overline{\varphi}) \right]^{\{1\}} \\
&= b^{-\sigma_{\overline{\varphi}}} \beta(k,\overline{\varphi}) \gamma'(\lambda,\overline{\varphi}) \left(\sum_{r=0}^{k-\overline{\varphi}} \begin{bmatrix} k-\overline{\varphi} \\ r \end{bmatrix} \gamma'(\lambda-\overline{\varphi},r) Y^r X^{k-\overline{\varphi}-r} \right)^{\{1\}} \\
&= b^{-\sigma_{\overline{\varphi}}} \beta(k,\overline{\varphi}) \gamma'(\lambda,\overline{\varphi}) \sum_{u=0}^{k-\overline{\varphi}-1} \begin{bmatrix} k-\overline{\varphi} \\ u+1 \end{bmatrix} \gamma'(\lambda-\overline{\varphi},u+1) \\
&\qquad \times b^{1-(u+1)} \beta(u+1,1) Y^{u+1-1} X^{k-\overline{\varphi}-u-1} \\
&\overset{(4.1.3)(2.3.34)}{=} b^{-\sigma_{\overline{\varphi}}} \beta(k,\overline{\varphi}) \gamma'(\lambda,\overline{\varphi}) \sum_{u=0}^{k-(\overline{\varphi}+1)} \begin{bmatrix} k-\overline{\varphi}-1 \\ u \end{bmatrix} \frac{\left(b^{k-\overline{\varphi}}-1\right)\left(b^{u+1}-1\right)}{\left(b^{u+1}-1\right)(b-1)} \\
&\qquad \times b^u b^{-u} \left(q^{\lambda-\overline{\varphi}}-1\right) \gamma'(\lambda-(\overline{\varphi}+1),u) Y^u X^{k-(\overline{\varphi}+1)-u} \\
&= b^{-\sigma_{\overline{\varphi}+1}} \gamma'(\lambda,\overline{\varphi}+1) \beta(k,\overline{\varphi}+1) \mu^{[k-(\overline{\varphi}+1)]}(X,Y;\lambda-(\overline{\varphi}+1))
\end{aligned}$$

as required. Now consider $\nu^{[k]}(X,Y;\lambda) = \sum_{u=0}^{k} (-1)^u b^{u(u-1)} \begin{bmatrix} k \\ u \end{bmatrix} Y^u X^{k-u}$ as in Equation

4.2.6. Then we have

$$\begin{aligned}
\nu^{[k]\{1\}}(X,Y;\lambda) &= \left(\sum_{u=0}^{k}(-1)^u b^{\sigma_u}\begin{bmatrix} k \\ u \end{bmatrix} Y^u X^{k-u}\right)^{\{1\}} \\
&= \sum_{r=0}^{k-1}(-1)^{r+1} b^{\sigma_{r+1}} b^{1-(r+1)} \begin{bmatrix} k \\ r+1 \end{bmatrix} \beta(r+1,1) Y^{r+1-1} X^{k-r-1} \\
&\overset{(4.1.3)(2.3.34)}{=} -\sum_{r=0}^{k-1}(-1)^r b^{\sigma_r} b^r b^{-r} \begin{bmatrix} k-1 \\ r \end{bmatrix} \frac{\left(b^k-1\right)\left(b^{r+1}-1\right)}{\left(b^{r+1}-1\right)(b-1)} \beta(r,1) Y^r X^{k-r-1} \\
&= (-1)^1 \beta(k,1) \nu^{[k-1]}(X,Y;\lambda).
\end{aligned}$$

Now assume that the statement holds for $\varphi = \overline{\varphi}$. Then we have

$$\begin{aligned}
\nu^{[k]}(X,Y;\lambda)^{\{\overline{\varphi}+1\}} &= \left[(-1)^{\overline{\varphi}}\beta(k,\overline{\varphi})\nu^{[k-\overline{\varphi}]}(X,Y;\lambda)\right]^{\{1\}} \\
&= (-1)^{\overline{\varphi}}\beta(k,\overline{\varphi}) \sum_{u=1}^{k-\overline{\varphi}} (-1)^u b^{\sigma_u} \begin{bmatrix} k-\overline{\varphi} \\ u \end{bmatrix} \left(Y^u\right)^{\{1\}} X^{k-\overline{\varphi}-u} \\
&= (-1)^{\overline{\varphi}}\beta(k,\overline{\varphi}) \sum_{r=0}^{k-\overline{\varphi}-1} (-1)^{r+1} b^{\sigma_{r+1}} b^{-(r+1)+1} \begin{bmatrix} k-\overline{\varphi} \\ r+1 \end{bmatrix} \\
&\qquad \times \beta(r+1,1) Y^{r+1-1} X^{k-\overline{\varphi}-r-1} \\
&\overset{(2.3.33)}{=} (-1)^{\overline{\varphi}+1}\beta(k,\overline{\varphi}) \sum_{r=0}^{k-\overline{\varphi}-1} (-1)^r b^{\sigma_r} \begin{bmatrix} k-(\overline{\varphi}+1) \\ r \end{bmatrix} \\
&\qquad \times \frac{\left(b^{k-\overline{\varphi}}-1\right)\left(b^{r+1}-1\right)}{\left(b^{r+1}-1\right)(b-1)} Y^r X^{k-\overline{\varphi}-1-r} \\
&= (-1)^{\overline{\varphi}+1}\beta(k,\overline{\varphi}+1)\nu^{[k-(\overline{\varphi}+1)]}(X,Y;\lambda)
\end{aligned}$$

as required. □

Now we need a few smaller lemmas in order to prove the Leibniz rule for the negative-q^{-1}-derivative.

Lemma 4.4.7. *Let*

$$\begin{aligned}
u\left(X,Y;\lambda\right) &= \sum_{i=0}^{r} u_i(\lambda) Y^i X^{r-i} \\
v\left(X,Y;\lambda\right) &= \sum_{i=0}^{s} v_i(\lambda) Y^i X^{s-i}.
\end{aligned}$$

1. *If* $u_0(\lambda) = 0$ *then*

$$\frac{1}{Y}\left[u\left(X,Y;\lambda\right) * v\left(X,Y;\lambda\right)\right] = b^s \frac{u\left(X,Y;\lambda\right)}{Y} * v\left(X,Y;\lambda-1\right). \tag{4.4.10}$$

2. If $v_0(\lambda) = 0$ then

$$\frac{1}{Y}\left[u\left(X,Y;\lambda\right) * v\left(X,Y;\lambda\right)\right] = u\left(X,bY;\lambda\right) * \frac{v\left(X,Y;\lambda\right)}{Y}. \tag{4.4.11}$$

Proof.

(1) Suppose $u_0(\lambda) = 0$. Then

$$\frac{u\left(X,Y;\lambda\right)}{Y} = \sum_{i=0}^{r} u_i(\lambda)Y^{i-1}X^{r-i} = \sum_{i=0}^{r-1} u_{i+1}(\lambda)Y^{i}X^{r-i-1}$$

Hence

$$\begin{aligned} b^s\frac{u\left(X,Y;\lambda\right)}{Y} * v\left(X,Y;\lambda-1\right) &= b^s\sum_{u=0}^{r+s-1}\left(\sum_{\ell=0}^{u} b^{\ell s}u_{\ell+1}(\lambda)v_{u-\ell}(\lambda-\ell-1)\right)Y^uX^{r+s-1-u}\\ &= b^s\sum_{u=0}^{r+s-1}\left(\sum_{i=1}^{u+1} b^{(i-1)s}u_i(\lambda)v_{u-i+1}(\lambda-i)\right)Y^uX^{r+s-1-u}\\ &= b^s\sum_{j=1}^{r+s}\left(\sum_{i=1}^{j} b^{(i-1)s}u_i(\lambda)v_{j-i}(\lambda-i)\right)Y^{j-1}X^{r+s-j}\\ &= \frac{1}{Y}\sum_{j=0}^{r+s}\left(\sum_{i=0}^{j} b^{is}u_i(\lambda)v_{j-i}(\lambda-i)\right)Y^{j}X^{r+s-j}\\ &= \frac{1}{Y}\left(u\left(X,Y;\lambda\right) * v\left(X,Y;\lambda\right)\right) \end{aligned}$$

since when $j = 0$, $\sum_{i=0}^{j} b^{is}u_i(\lambda)v_{j-i}(\lambda-i) = 0$ as $u_0(\lambda) = 0$.

(2) Now if $v_0(\lambda) = 0$, then

$$\begin{aligned} \frac{v\left(X,Y;\lambda\right)}{Y} &= \sum_{j=1}^{s} v_j(\lambda)Y^{j-1}X^{s-j}\\ &= \sum_{i=0}^{s-1} v_{i+1}(\lambda)Y^{i}X^{s-i-1}. \end{aligned}$$

So,

$$\begin{aligned} u\left(X,bY;\lambda\right) * \frac{v\left(X,Y;\lambda\right)}{Y} &= \sum_{u=0}^{r+s-1}\left(\sum_{j=0}^{u} b^{j(s-1)}b^{j}u_j(\lambda)v_{u-j+1}(\lambda-j)\right)Y^uX^{r+s-1-u}\\ &= \frac{1}{Y}\sum_{\ell=1}^{r+s}\left(\sum_{j=0}^{\ell} b^{js}u_j(\lambda)v_{\ell-j}(\lambda-j)\right)Y^{\ell}X^{r+s-\ell}\\ &= \frac{1}{Y}\sum_{\ell=0}^{r+s}\left(\sum_{j=0}^{\ell} b^{js}u_j(\lambda)v_{\ell-j}(\lambda-j)\right)Y^{\ell}X^{r+s-\ell} \end{aligned}$$

since when $j=\ell$, $\displaystyle\sum_{i=0}^{j} b^{is}u_i(\lambda)v_{j-i}(\lambda-i)=0$ as $v_0(\lambda)=0$.

□

Theorem 4.4.8 (Leibniz rule for the negative-q^{-1}-derivative)**.** *For two homogeneous polynomials in Y, $f(X,Y;\lambda)$ and $g(X,Y;\lambda)$ with degrees r and s respectively, for $\varphi\geq 0$, the φ^{th} negative-q^{-1}-derivative of their negative-q-product is given by*

$$[f\left(X,Y;\lambda\right)*g\left(X,Y;\lambda\right)]^{\{\varphi\}}=\sum_{\ell=0}^{\varphi}\begin{bmatrix}\varphi\\ \ell\end{bmatrix}b^{\ell(s-\varphi+\ell)}f^{\{\ell\}}\left(X,Y;\lambda\right)*g^{\{\varphi-\ell\}}\left(X,Y;\lambda-\ell\right). \tag{4.4.12}$$

Proof. For simplification we shall write $f(X,Y;\lambda)$, $g(X,Y;\lambda)$ as $f(Y;\lambda)$, $g(Y;\lambda)$. Now by differentiation we have

$$\begin{aligned}\Big[f\left(Y;\lambda\right)*g\left(Y;\lambda\right)\Big]^{\{1\}} &= \frac{f\left(b^{-1}Y;\lambda\right)*g\left(b^{-1}Y;\lambda\right)-f\left(Y;\lambda\right)*g\left(Y;\lambda\right)}{(b^{-1}-1)Y}\\ &= \frac{1}{(b^{-1}-1)Y}\Big\{f\left(b^{-1}Y;\lambda\right)*g\left(b^{-1}Y;\lambda\right)-f\left(b^{-1}Y;\lambda\right)*g\left(Y;\lambda\right)\\ &\qquad +f\left(b^{-1}Y;\lambda\right)*g\left(Y;\lambda\right)-f\left(Y;\lambda\right)*g\left(Y;\lambda\right)\Big\}\\ &= \frac{1}{(b^{-1}-1)Y}\Big\{f\left(b^{-1}Y;\lambda\right)*\left(g\left(b^{-1}Y;\lambda\right)-g\left(Y;\lambda\right)\right)\Big\}\\ &\qquad +\frac{1}{(b^{-1}-1)Y}\Big\{\left(f\left(b^{-1}Y;\lambda\right)-f\left(Y;\lambda\right)\right)*g\left(Y;\lambda\right)\Big\}\\ &\overset{(4.4.11)}{=} f\left(Y;\lambda\right)*\frac{\left(g\left(b^{-1}Y;\lambda\right)-g\left(Y;\lambda\right)\right)}{\left(b^{-1}-1\right)Y}\\ &\qquad \overset{(4.4.10)}{+} b^{s}\frac{\left(f\left(b^{-1}Y;\lambda\right)-f\left(Y;\lambda\right)\right)}{\left(b^{-1}-1\right)Y}*g\left(Y;\lambda-1\right)\\ &= f\left(Y;\lambda\right)*g^{\{1\}}\left(Y;\lambda\right)+b^{s}f^{\{1\}}\left(Y;\lambda\right)*g\left(Y;\lambda-1\right).\end{aligned}$$

So the initial case holds. Assume the statement holds true for $\varphi=\overline{\varphi}$, i.e.

$$\Big[f\left(X,Y;\lambda\right)*g\left(X,Y;\lambda\right)\Big]^{\{\overline{\varphi}\}}=\sum_{\ell=0}^{\overline{\varphi}}\begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix}b^{\ell(s-\overline{\varphi}+\ell)}f^{\{\ell\}}\left(X,Y;\lambda\right)*g^{\{\overline{\varphi}-\ell\}}\left(X,Y;\lambda-\ell\right).$$

Now considering $\overline{\varphi}+1$ and for simplicity writing $f(X,Y;\lambda)$, $g(X,Y;\lambda)$ as $f(\lambda),g(\lambda)$ we have

$$
\begin{aligned}
&\Big[f\left(\lambda\right) * g\left(\lambda\right)\Big]^{\{\overline{\varphi}+1\}} \\
&= \left[\sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}-\ell\}}\left(\lambda-\ell\right)\right]^{\{1\}} \\
&\overset{(4.2.1)}{=} \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}-\ell+1\}}\left(\lambda-\ell\right) \\
&\qquad + \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{\ell(s-\overline{\varphi}+\ell)} b^{s-\overline{\varphi}+\ell} f^{\{\ell+1\}}\left(\lambda\right) * g^{\{\overline{\varphi}-\ell\}}\left(\lambda-\ell-1\right) \\
&= \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}-\ell+1\}}\left(\lambda-\ell\right) \\
&\qquad + \sum_{\ell=1}^{\overline{\varphi}+1} \begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix} b^{(\ell-1)(s-\overline{\varphi}+\ell-1)} b^{s-\overline{\varphi}+(\ell-1)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}-\ell+1\}}\left(\lambda-\ell\right) \\
&= f\left(\lambda\right) * g^{\{\overline{\varphi}+1\}}\left(\lambda\right) + \sum_{\ell=1}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}-\ell+1\}}\left(\lambda-\ell\right) \\
&\qquad + \sum_{\ell=1}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix} b^{(\ell-1)(s-\overline{\varphi}+\ell-1)} b^{(s-\overline{\varphi}+(\ell-1))} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}-\ell+1\}}\left(\lambda-\ell\right) \\
&\qquad + \begin{bmatrix}\overline{\varphi}\\ \overline{\varphi}\end{bmatrix} b^{(\overline{\varphi}+1)(s+1)} b^{-\overline{\varphi}-1} f^{\{\overline{\varphi}+1\}}\left(\lambda\right) * g\left(\lambda-(\overline{\varphi}+1)\right) \\
&= f\left(\lambda\right) * g^{\{\overline{\varphi}+1\}}\left(\lambda\right) + \sum_{\ell=1}^{\overline{\varphi}} \left(\begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} + b^{-\ell}\begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix}\right) b^{\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}+1-\ell\}}\left(\lambda-\ell\right) \\
&\qquad + b^{s(\overline{\varphi}+1)} f^{\{\overline{\varphi}+1\}}\left(\lambda\right) * g\left(\lambda-(\overline{\varphi}+1)\right) \\
&\overset{(2.3.30)}{=} f\left(\lambda\right) * g^{\{\overline{\varphi}+1\}}\left(\lambda\right) + \sum_{\ell=1}^{\overline{\varphi}} b^{-\ell}\begin{bmatrix}\overline{\varphi}+1\\ \ell\end{bmatrix} b^{\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}+1-\ell\}}\left(\lambda-\ell\right) \\
&\qquad + \begin{bmatrix}\overline{\varphi}+1\\ \overline{\varphi}+1\end{bmatrix} b^{(\overline{\varphi}+1)(s-\overline{\varphi}-1+(\overline{\varphi}+1))} f^{\{\overline{\varphi}+1\}}\left(\lambda\right) * g^{\{\overline{\varphi}+1-(\overline{\varphi}+1)\}}\left(\lambda-(\overline{\varphi}+1)\right) \\
&= \sum_{\ell=0}^{\overline{\varphi}+1} \begin{bmatrix}\overline{\varphi}+1\\ \ell\end{bmatrix} b^{\ell(s-(\overline{\varphi}+1)+\ell)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}+1-\ell\}}\left(\lambda-\ell\right)
\end{aligned}
$$

as required. □

4.4.3 Evaluating the Negative-q-Derivative and the Negative-q^{-1}-Derivative

Here we introduce some lemmas which yield useful results when developing moments of the Hermitian rank weight distribution.

Lemma 4.4.9. *For $j, \ell \in \mathbb{Z}^+$, $0 \leq \ell \leq j$ and $X = Y = 1$,*

$$\nu^{[j](\ell)}(1,1;\lambda) = \beta(j,j)\delta_{j\ell}. \tag{4.4.13}$$

Proof. Consider

$$\nu^{[j](\ell)}(X,Y;\lambda) \overset{(4.4.3)}{=} \beta(j,\ell)\nu^{[j-\ell]}(X,Y;\lambda) = \beta(j,\ell)\sum_{u=0}^{j-\ell}(-1)^u b^{\sigma_u}\begin{bmatrix} j-\ell \\ u \end{bmatrix} Y^u X^{(j-\ell)-u}.$$

So

$$\begin{aligned}
\nu^{[j](\ell)}(1,1;\lambda) &= \beta(j,\ell)\sum_{u=0}^{j-\ell}(-1)^u b^{\sigma_u}\begin{bmatrix} j-\ell \\ u \end{bmatrix} \\
&\overset{(2.3.35)}{=} \beta(\ell,\ell)\begin{bmatrix} j \\ \ell \end{bmatrix}\sum_{u=0}^{j-\ell}(-1)^u b^{\sigma_u}\begin{bmatrix} j-\ell \\ u \end{bmatrix} \\
&\overset{(2.3.24)(2.3.25)}{=} \beta(\ell,\ell)\sum_{k=\ell}^{j}(-1)^{k-\ell} b^{\sigma_{k-\ell}}\begin{bmatrix} j \\ k \end{bmatrix}\begin{bmatrix} k \\ \ell \end{bmatrix} \\
&\overset{(2.3.28)}{=} \beta(\ell,\ell)\delta_{\ell j} = \beta(j,j)\delta_{j\ell}.
\end{aligned}$$

□

Lemma 4.4.10. *For any homogeneous polynomial, $\rho(X,Y;\lambda)$ and for any $s \geq 0$,*

$$\left(\rho * \mu^{[s]}\right)(1,1;\lambda) = (-1)^s b^{\lambda s}\rho(1,1;\lambda). \tag{4.4.14}$$

Proof. Let $\rho(X,Y;\lambda) = \sum_{i=0}^{r}\rho_i(\lambda)Y^i X^{r-i}$. Then by Theorem 4.2.4 we have,

$$\mu^{[s]}(X,Y;\lambda) = \sum_{t=0}^{s}\mu_t^{[s]}(\lambda)Y^t X^{s-t} = \sum_{t=0}^{s}\begin{bmatrix} s \\ t \end{bmatrix}\gamma'(\lambda,t)Y^t X^{s-t}.$$

Thus giving

$$\left(\rho * \mu^{[s]}\right)(X,Y;\lambda) = \sum_{u=0}^{r+s} c_u(\lambda)Y^u X^{(r+s-u)}$$

where

$$c_u(\lambda) = \sum_{i=0}^{u} b^{is}\rho_i(\lambda)\mu_{u-i}^{[s]}(\lambda - i).$$

Then

$$\begin{aligned}
\left(\rho * \mu^{[s]}\right)(1,1;\lambda) = \sum_{u=0}^{r+s} c_u(\lambda) &= \sum_{u=0}^{r+s}\sum_{i=0}^{u} b^{is}\rho_i(\lambda)\mu_{u-i}^{[s]}(\lambda - i)\\
&= \sum_{j=0}^{r+s} b^{js}\rho_j(\lambda)\left(\sum_{k=0}^{r+s-j}\mu_k^{[s]}(\lambda - j)\right)\\
&= \sum_{j=0}^{r} b^{js}\rho_j(\lambda)\left(\sum_{k=0}^{s}\mu_k^{[s]}(\lambda - j)\right)\\
&= \sum_{j=0}^{r} b^{js}\rho_j(\lambda)\left(\sum_{k=0}^{s}\begin{bmatrix}s\\k\end{bmatrix}\gamma'(\lambda - j, k)\right)\\
&\overset{(2.3.27)}{=} \sum_{j=0}^{r} b^{js}\rho_j(\lambda)\left(-b^{\lambda-j}\right)^s\\
&= (-1)^s b^{\lambda s}\rho(1,1;\lambda)
\end{aligned}$$

since $\rho_j(\lambda) = 0$ when $j > r$ and $\mu_k^{[s]}(\lambda - j) = 0$ when $k > s$. □

4.5 Moments of the Hermitian Rank Distribution

Here we explore the moments of the Hermitian rank distribution of a subgroup of Hermitian matrices over $\mathbb{F}_{q^2}$ and that of its dual. Similar results for the Hamming association scheme were derived in [41, p131], for the rank association scheme in [22, Prop 4] and for the skew rank association scheme in Section 3.5.

4.5.1 Moments derived from the Negative-q-Derivative

The following proposition is obtained in the proof by Schmidt [53, Theorem 1], by combining the eigenvalues of the association scheme [53, (5)] with the coefficients of the dual inner distribution [53, (7)]. In this paper an alternative method for deriving the moments is presented using the MacWilliams Identity and the negative-q-derivative.

Proposition 4.5.1. *For $0 \le \varphi \le t$, $-q = b$, and a linear code $\mathscr{C} \subseteq \mathscr{H}_{q,t}$ and its dual $\mathscr{C}^\perp \subseteq \mathscr{H}_{q,t}$ with weight distributions $\boldsymbol{c} = (c_0, \dots, c_t)$ and $\boldsymbol{c'} = (c'_0, \dots, c'_t)$, respectively we have*

$$\sum_{i=0}^{t-\varphi}\begin{bmatrix}t-i\\ \varphi\end{bmatrix} c_i = \frac{1}{|\mathscr{C}^\perp|}\left(-b^t\right)^{t-\varphi}\sum_{i=0}^{\varphi}\begin{bmatrix}t-i\\ t-\varphi\end{bmatrix} c'_i.$$

Proof. We apply Theorem 4.3.4 to $\mathscr{C}^\perp$ to get

$$W_{\mathscr{C}}^{HR}(X,Y) = \frac{1}{|\mathscr{C}^\perp|}\overline{W}_{\mathscr{C}^\perp}^{HR}\left(X + (-b^t - 1)Y, X - Y\right)$$

or equivalently

$$\begin{aligned}\sum_{i=0}^{t} c_i Y^i X^{t-i} &= \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{t} c_i'\,(X-Y)^{[i]} * \left[X+(-b^t-1)Y\right]^{[t-i]}\\ &= \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{t} c_i'\nu^{[i]}(X,Y;t) * \mu^{[t-i]}(X,Y;t). \qquad (4.5.1)\end{aligned}$$

For each side of Equation (4.5.1), we shall apply the negative-q-derivative φ times and then evaluate at $X=Y=1$.

For the LHS, we obtain

$$\left(\sum_{i=0}^{t} c_i Y^i X^{t-i}\right)^{(\varphi)} \overset{(4.4.1)}{=} \sum_{i=0}^{t-\varphi} c_i \beta(t-i,\varphi) Y^i X^{t-i-\varphi}.$$

Setting $X=Y=1$ we then have

$$\begin{aligned}\sum_{i=0}^{t-\varphi} c_i\beta(t-i,\varphi) &\overset{(2.3.35)}{=} \sum_{i=0}^{t-\varphi} c_i \begin{bmatrix} t-i \\ \varphi \end{bmatrix}\beta(\varphi,\varphi)\\ &= \beta(\varphi,\varphi)\sum_{i=0}^{t-\varphi} c_i \begin{bmatrix} t-i \\ \varphi \end{bmatrix}.\end{aligned}$$

We now move on to the RHS. For simplicity we write $\mu(X,Y;t)$ as μ and similarly $\nu(X,Y;n)$ as ν. We have

$$\begin{aligned}\left(\frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{t} c_i'\nu^{[i]} * \mu^{[t-i]}\right)^{(\varphi)} &\overset{(4.4.6)}{=} \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{t} c_i'\left(\sum_{\ell=0}^{\varphi}\begin{bmatrix}\varphi \\ \ell\end{bmatrix} b^{(\varphi-\ell)(i-\ell)}\nu^{[i](\ell)} * \mu^{[t-i](\varphi-\ell)}\right)\\ &= \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{t} c_i'\psi_i(X,Y;t)\end{aligned}$$

where

$$\psi_i(X,Y;t) = \sum_{\ell=0}^{\varphi}\begin{bmatrix}\varphi \\ \ell\end{bmatrix} b^{(\varphi-\ell)(i-\ell)}\nu^{[i](\ell)}(X,Y;t) * \mu^{[t-i](\varphi-\ell)}(X,Y;t).$$

Then with $X=Y=1$,

$$\begin{aligned}\psi_i(1,1;t) &\overset{(4.4.2)}{=} \sum_{\ell=0}^{\varphi}\begin{bmatrix}\varphi \\ \ell\end{bmatrix} b^{(\varphi-\ell)(i-\ell)}\beta(t-i,\varphi-\ell)\left(\nu^{[i](\ell)} * \mu^{[t-i-\varphi+\ell]}\right)(1,1;t)\\ &\overset{(4.4.14)}{=} \sum_{\ell=0}^{\varphi}\begin{bmatrix}\varphi \\ \ell\end{bmatrix} b^{(\varphi-\ell)(i-\ell)}\beta(t-i,\varphi-\ell)\left(-b^t\right)^{t-i-(\varphi-\ell)}\nu^{[i](\ell)}(1,1;t)\\ &\overset{(4.4.13)}{=} \sum_{\ell=0}^{\varphi} b^{(\varphi-\ell)(i-\ell)}\begin{bmatrix}\varphi \\ \ell\end{bmatrix}\beta(t-i,\varphi-\ell)\left(-b^t\right)^{t-i-(\varphi-\ell)}\beta(i,i)\delta_{i\ell}\\ &\overset{(2.3.35)}{=} \begin{bmatrix}\varphi \\ i\end{bmatrix}\begin{bmatrix}t-i \\ \varphi-i\end{bmatrix}\beta(\varphi-i,\varphi-i)\left(-b^t\right)^{t-\varphi}\beta(i,i)\\ &\overset{(2.3.36)}{=} \begin{bmatrix}t-i \\ \varphi-i\end{bmatrix}\left(-b^t\right)^{t-\varphi}\beta(\varphi,\varphi).\end{aligned}$$

So

$$\frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{t} c_i'\psi_i(1,1;t) = \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{\varphi} c_i' \begin{bmatrix} t-i \\ \varphi - i\end{bmatrix} \left(-b^t\right)^{t-\varphi} \beta(\varphi,\varphi)$$
$$\overset{(2.3.24)}{=} \beta(\varphi,\varphi)\frac{1}{|\mathscr{C}^{\perp}|}\left(-b^t\right)^{t-\varphi}\sum_{i=0}^{\varphi} c_i' \begin{bmatrix} t-i \\ t-\varphi\end{bmatrix}.$$

Combining the results for each side, and simplifying, we finally obtain

$$\sum_{i=0}^{t-\varphi} c_i \begin{bmatrix} t-i \\ \varphi \end{bmatrix} = \frac{1}{|\mathscr{C}^{\perp}|}\left(-b^t\right)^{t-\varphi}\sum_{i=0}^{\varphi} c_i' \begin{bmatrix} t-i \\ t-\varphi\end{bmatrix}$$

as required. □

Note. In particular, if $\varphi = 0$ we have

$$\sum_{i=0}^{t} c_i = \frac{\left(-b^t\right)^t}{|\mathscr{C}^{\perp}|} c_0' = \frac{\left(-b^t\right)^t}{|\mathscr{C}^{\perp}|}.$$

In other words

$$|\mathscr{C}||\mathscr{C}^{\perp}| = \left(-b^t\right)^t = (-1)^t(-1)^{t^2}q^{t^2} = q^{t^2}$$

as expected.

We can simplify Proposition 4.5.1 if φ is less than the minimum distance of the dual code.

Corollary 4.5.2. *Let d'_{HR} be the minimum rank distance of $\mathscr{C}^{\perp}$. If $0 \leq \varphi < d'_{HR}$ then*

$$\sum_{i=0}^{t-\varphi} \begin{bmatrix} t-i \\ \varphi \end{bmatrix} c_i = \frac{1}{|\mathscr{C}^{\perp}|}\left(-b^t\right)^{t-\varphi}\begin{bmatrix} t \\ \varphi \end{bmatrix}.$$

Proof. We have $c_0' = 1$ and $c_1' = \ldots = c_\varphi' = 0$. □

4.5.2 Moments Derived from the Negative-q^{-1}-Derivative

The next proposition relates the moments of the negative rank distribution of a linear code to those of its dual, this time using the negative-q^{-1}-derivative of the MacWilliams Identity for the Hermitian rank association scheme. There is a slight difference in the way that these two lemmas are defined compared to the skew rank case (and the rank case presented in [22, Appendix D]). In the skew rank case, $\delta(\lambda,\varphi,j)$ is defined using two gamma functions and a power of q^2. This form was effective there because of the particular formulation of the gamma function, which does not hold in this case. That is, one of the products in Equation (4.5.2) is identical to the gamma function in the skew case, due to the fact that the multiplier of b^φ is 1. In the Hermitian case, the multiplier of b^φ in the gamma function is -1, so the simplification of the product to a gamma function cannot be made. Therefore one of the gamma functions in Lemma 4.5.3 has to be replaced with a more general product.

Lemma 4.5.3. *Let* $\delta(\lambda, \varphi, j) = \sum_{i=0}^{j} \begin{bmatrix} j \\ i \end{bmatrix} (-1)^i b^{\sigma_i} \gamma'(\lambda - i, \varphi)$*. Then for all* $\lambda \in \mathbb{R}, \varphi, j \in \mathbb{Z}$*,*

$$\delta(\lambda, \varphi, j) = (-1)^j \prod_{i=0}^{j-1} \left(b^{\varphi} - b^i\right) \gamma'(\lambda - j, \varphi - j) b^{j(\lambda - j)}. \tag{4.5.2}$$

Proof. We follow the proof by induction. Initial case: $j = 0$.

$$\delta(\lambda, \varphi, 0) = \begin{bmatrix} 0 \\ 0 \end{bmatrix} (-1)^0 b^{\sigma_0} \gamma'(\lambda, \varphi) = \gamma'(\lambda, \varphi) = \gamma'(\lambda, \varphi) q^{0(\lambda)}.$$

So the initial case holds. Now assume it is true for $j = \bar{\jmath}$ and consider the case where $\bar{\jmath} + 1$.

$$\begin{aligned}
\delta(\lambda, \varphi, \bar{\jmath} + 1) &= \sum_{i=0}^{\bar{\jmath}+1} \begin{bmatrix} \bar{\jmath} + 1 \\ i \end{bmatrix} (-1)^i b^{\sigma_i} \gamma'(\lambda - i, \varphi) \\
&\overset{(2.3.30)}{=} \sum_{i=0}^{\bar{\jmath}+1} \left(b^i \begin{bmatrix} \bar{\jmath} \\ i \end{bmatrix} + \begin{bmatrix} \bar{\jmath} \\ i - 1 \end{bmatrix} \right) (-1)^i b^{\sigma_i} \gamma'(\lambda - i, \varphi) \\
&= \sum_{i=0}^{\bar{\jmath}} \begin{bmatrix} \bar{\jmath} \\ i \end{bmatrix} (-1)^i b^{\sigma_i} b^i \gamma'(\lambda - i, \varphi) + \sum_{i=0}^{\bar{\jmath}} \begin{bmatrix} \bar{\jmath} \\ i \end{bmatrix} (-1)^{i+1} b^{\sigma_{i+1}} \gamma'(\lambda - (i+1), \varphi) \\
&\overset{(4.1.3)}{=} \sum_{i=0}^{\bar{\jmath}} \begin{bmatrix} \bar{\jmath} \\ i \end{bmatrix} (-1)^i b^i b^{\sigma_i} \left(-b^{\lambda - i} - 1\right) b^{\varphi - 1} \gamma'(\lambda - i - 1, \varphi - 1) \\
&\qquad \overset{(4.1.4)}{-} \sum_{i=0}^{\bar{\jmath}} \begin{bmatrix} \bar{\jmath} \\ i \end{bmatrix} (-1)^i b^{\sigma_{i+1}} \left(-b^{\lambda - i - 1} - b^{\varphi - 1}\right) \gamma'(\lambda - i - 1, \varphi - 1) \\
&= \sum_{i=0}^{\bar{\jmath}} \begin{bmatrix} \bar{\jmath} \\ i \end{bmatrix} (-1)^i b^{\sigma_i} \gamma'(\lambda - i - 1, \varphi - 1)(-b^{\lambda - 1}) \left(b^{\varphi} - 1\right) \\
&= -b^{\lambda - 1} \left(b^{\varphi} - 1\right) \delta(\lambda - 1, \varphi - 1, \bar{\jmath}) \\
&= -b^{\lambda - 1} \left(b^{\varphi} - 1\right) (-1)^{\bar{\jmath}} \prod_{i=0}^{\bar{\jmath}-1} \left(b^{\varphi - 1} - b^i\right) b^{\bar{\jmath}(\lambda - \bar{\jmath} - 1)} \gamma'(\lambda - \bar{\jmath} - 1, \varphi - \bar{\jmath} - 1) \\
&\overset{(4.1.3)}{=} (-1)^{\bar{\jmath}+1} b^{(\bar{\jmath}+1)(\lambda - (\bar{\jmath}+1))} \prod_{i=0}^{\bar{\jmath}} \left(b^{\varphi} - b^i\right) \gamma'(\lambda - (\bar{\jmath} + 1), \varphi - (\bar{\jmath} + 1))
\end{aligned}$$

since $\begin{bmatrix} \bar{\jmath} \\ i - 1 \end{bmatrix} = 0$ when $i = 0$. Hence by induction the lemma is proved. □

Lemma 4.5.4. *Let* $\varepsilon(\Lambda, \varphi, i) = \sum_{\ell=0}^{i} \begin{bmatrix} i \\ \ell \end{bmatrix} \begin{bmatrix} \Lambda - i \\ \varphi - \ell \end{bmatrix} b^{\ell(\Lambda - \varphi)} (-1)^{\ell} b^{\sigma_{\ell}} \prod_{j=0}^{i-\ell-1} \left(b^{\varphi - \ell} - b^j\right)$*. Then for all* $\Lambda \in \mathbb{R}, \varphi, i \in \mathbb{Z}$*,*

$$\varepsilon(\Lambda, \varphi, i) = (-1)^i b^{\sigma_i} \begin{bmatrix} \Lambda - i \\ \Lambda - \varphi \end{bmatrix}.$$

Proof. We follow the proof by induction. Initial case $i = 0$,

$$\begin{aligned}
\varepsilon(\Lambda, \varphi, 0) = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \begin{bmatrix} \Lambda \\ 0 \end{bmatrix} b^0 (-1)^0 b^0 &= \begin{bmatrix} \Lambda \\ \varphi \end{bmatrix} \\
(-1)^0 b^0 \begin{bmatrix} \Lambda \\ \Lambda - \varphi \end{bmatrix} &\overset{(2.3.24)}{=} \begin{bmatrix} \Lambda \\ \varphi \end{bmatrix}.
\end{aligned}$$

So the initial case holds. Now suppose it is true when $i = \bar{\imath}$. Then

$$\begin{aligned}
\varepsilon(\Lambda, \varphi, \bar{\imath}+1) &= \sum_{\ell=0}^{\bar{\imath}+1} \begin{bmatrix} \bar{\imath}+1 \\ \ell \end{bmatrix} \begin{bmatrix} \Lambda-\bar{\imath}-1 \\ \varphi-\ell \end{bmatrix} b^{\ell(\Lambda-\varphi)} (-1)^{\ell} b^{\sigma_\ell} \prod_{j=0}^{\bar{\imath}-\ell} \left(b^{\varphi-\ell} - b^{j}\right) \\
&\overset{(2.3.29)}{=} \sum_{\ell=0}^{\bar{\imath}+1} \begin{bmatrix} \bar{\imath} \\ \ell \end{bmatrix} \begin{bmatrix} \Lambda-\bar{\imath}-1 \\ \varphi-\ell \end{bmatrix} b^{\ell(\Lambda-\varphi)} (-1)^{\ell} b^{\sigma_\ell} \prod_{j=0}^{\bar{\imath}-\ell} \left(b^{\varphi-\ell} - b^{j}\right) \\
&\quad + \sum_{\ell=1}^{\bar{\imath}+1} b^{(\bar{\imath}+1-\ell)} \begin{bmatrix} \bar{\imath} \\ \ell-1 \end{bmatrix} \begin{bmatrix} \Lambda-\bar{\imath}-1 \\ \varphi-\ell \end{bmatrix} b^{\ell(\Lambda-\varphi)} (-1)^{\ell} b^{\sigma_\ell} \prod_{j=0}^{\bar{\imath}-\ell} \left(b^{\varphi-\ell} - b^{j}\right) \\
&= A + B, \quad \text{say.}
\end{aligned}$$

Now

$$\begin{aligned}
A &= \left(-b^{\varphi} - b^{\bar{\imath}}\right) \sum_{\ell=0}^{\bar{\imath}} \begin{bmatrix} \bar{\imath} \\ \ell \end{bmatrix} \begin{bmatrix} \Lambda-\bar{\imath}-1 \\ \varphi-\ell \end{bmatrix} b^{\ell(\Lambda-1-\varphi)} (-1)^{\ell} b^{\sigma_\ell} \prod_{j=0}^{\bar{\imath}-\ell-1} \left(b^{\varphi-\ell} - b^{j}\right) \\
&= \left(-b^{\varphi} - b^{\bar{\imath}}\right) \varepsilon(\Lambda-1, \varphi, \bar{\imath}) \\
&= \left(-b^{\varphi} - b^{\bar{\imath}}\right) (-1)^{\bar{\imath}} b^{\sigma_{\bar{\imath}}} \begin{bmatrix} \Lambda-\bar{\imath}-1 \\ \Lambda-1-\varphi \end{bmatrix}
\end{aligned}$$

and

$$\begin{aligned}
B &= \sum_{\ell=0}^{\bar{\imath}} b^{(\bar{\imath}-\ell)} \begin{bmatrix} \bar{\imath} \\ \ell \end{bmatrix} \begin{bmatrix} \Lambda-\bar{\imath}-1 \\ \varphi-\ell-1 \end{bmatrix} b^{(\ell+1)(\Lambda-\varphi)} (-1)^{\ell+1} b^{\sigma_{\ell+1}} \prod_{j=0}^{\bar{\imath}-\ell-1} \left(b^{\varphi-\ell-1} - b^{j}\right) \\
&= -b^{(\bar{\imath}+\Lambda-\varphi)} \varepsilon(\Lambda-1, \varphi-1, \bar{\imath}) \\
&= -b^{(\bar{\imath}+\Lambda-\varphi)} (-1)^{\bar{\imath}} b^{\sigma_{\bar{\imath}}} \begin{bmatrix} \Lambda-\bar{\imath}-1 \\ \Lambda-\varphi \end{bmatrix}.
\end{aligned}$$

So

$$\begin{aligned}
\varepsilon(\Lambda, \varphi, \bar{\imath}+1) &= A + B \\
&= (-1)^{\bar{\imath}} b^{\sigma_{\bar{\imath}}} \left\{ \left(b^{\varphi} - b^{\bar{\imath}}\right) \begin{bmatrix} \Lambda-\bar{\imath}-1 \\ \Lambda-1-\varphi \end{bmatrix} - b^{(\bar{\imath}+n-\varphi)} \begin{bmatrix} \Lambda-\bar{\imath}-1 \\ \Lambda-\varphi \end{bmatrix} \right\} \\
&\overset{(2.3.31)}{=} (-1)^{\bar{\imath}+1} b^{\sigma_{\bar{\imath}}} \left\{ b^{\bar{\imath}+n-\varphi} \begin{bmatrix} \Lambda-\bar{\imath}-1 \\ \Lambda-\varphi \end{bmatrix} - \left(b^{\varphi} - b^{\bar{\imath}}\right) \frac{\left(b^{\Lambda-\varphi}-1\right)}{\left(b^{\varphi-\bar{\imath}}-1\right)} \begin{bmatrix} \Lambda-\bar{\imath}-1 \\ \Lambda-\varphi \end{bmatrix} \right\} \\
&= (-1)^{\bar{\imath}+1} \begin{bmatrix} \Lambda-(\bar{\imath}+1) \\ \Lambda-\varphi \end{bmatrix} b^{\sigma_{\bar{\imath}}} \left\{ \frac{b^{\bar{\imath}+n-\varphi}\left(b^{\varphi-\bar{\imath}}-1\right) - \left(b^{\varphi} - b^{\bar{\imath}}\right)\left(b^{\Lambda-\varphi}-1\right)}{\left(b^{\varphi-\bar{\imath}}-1\right)} \right\} \\
&= (-1)^{\bar{\imath}+1} b^{\sigma_{\bar{\imath}+1}} \begin{bmatrix} \Lambda-(\bar{\imath}+1) \\ \Lambda-\varphi \end{bmatrix}
\end{aligned}$$

as required. □

Proposition 4.5.5. *For $0 \leq \varphi \leq t$ and a linear code $\mathscr{C} \subseteq \mathscr{H}_{q,t}$ with dimension k and its dual $\mathscr{C}^{\perp} \subseteq \mathscr{H}_{q,t}$ with weight distributions $\mathbf{c} = (c_0, \ldots, c_n)$ and $\mathbf{c'} = (c'_0, \ldots, c'_n)$, respectively* *we have*

$$\sum_{i=\varphi}^{t} b^{\varphi(t-i)} \begin{bmatrix} i \\ \varphi \end{bmatrix} c_i = \frac{1}{|\mathscr{C}^{\perp}|} \left(-b^t\right)^{t-\varphi} \sum_{i=0}^{\varphi} (-1)^i b^{\sigma_i} b^{i(\varphi-i)} \begin{bmatrix} t-i \\ t-\varphi \end{bmatrix} \gamma'(t-i, \varphi-i) c'_i.$$

Proof. As in Proposition 4.5.1, we apply Theorem 4.3.4 to $\mathscr{C}^{\perp}$ to obtain

$$W_{\mathscr{C}}^{HR}(X,Y) = \frac{1}{|\mathscr{C}^{\perp}|} \overline{W}_{\mathscr{C}^{\perp}}^{HR} \left(X + (-b^t - 1)Y, X - Y\right)$$

or equivalently

$$\begin{aligned} \sum_{i=0}^{t} c_i Y^i X^{t-i} &= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{t} c'_i \left(X - Y\right)^{[i]} * \left(X + (-b^t - 1)Y\right)^{[t-i]} \\ &= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{t} c'_i \nu^{[i]}(X,Y;t) * \mu^{[t-i]}(X,Y;t). \end{aligned} \tag{4.5.3}$$

For each side of Equation (4.5.3), we shall apply the negative-q^{-1}-derivative φ times and then evaluate at $X = Y = 1$. i.e.

$$\left(\sum_{i=0}^{t} c_i Y^i X^{t-i}\right)^{\{\varphi\}} = \left(\frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{t} c'_i \nu^{[i]}(X,Y;t) * \mu^{[t-i]}(X,Y;t)\right)^{\{\varphi\}}. \tag{4.5.4}$$

For the LHS, we obtain

$$\begin{aligned} \left(\sum_{i=0}^{t} c_i Y^i X^{t-i}\right)^{\{\varphi\}} &= \sum_{i=\varphi}^{t} c_i b^{\varphi(1-i)+\sigma_{\varphi}} \beta(i,\varphi) Y^{i-\varphi} X^{t-i} \\ &\overset{(2.3.35)}{=} \sum_{i=\varphi}^{t} c_i b^{\varphi(1-i)+\sigma_{\varphi}} \begin{bmatrix} i \\ \varphi \end{bmatrix} \beta(\varphi,\varphi) Y^{i-\varphi} X^{t-i} \end{aligned} \tag{4.5.5}$$

Then using $X = Y = 1$ gives

$$\sum_{i=\varphi}^{t} c_i b^{\varphi(1-i)+\sigma_{\varphi}} \begin{bmatrix} i \\ \varphi \end{bmatrix} \beta(\varphi,\varphi) Y^{i-\varphi} X^{t-i} = \sum_{i=\varphi}^{t} b^{\varphi(1-i)+\sigma_{\varphi}} \beta(\varphi,\varphi) \begin{bmatrix} i \\ \varphi \end{bmatrix} c_i. \tag{4.5.6}$$

We now move on to the RHS, for simplicity writing $\mu(X,Y;t)$ as $\mu(t)$ and $\nu(X,Y;t)$ as $\nu(t)$. We have

$$\left(\frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{t} c'_i \nu^{[i]}(t) * \mu^{[t-i]}(t)\right)^{\{\varphi\}} \tag{4.5.7}$$

$$\overset{(4.4.12)}{=} \frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{t} c'_i \left(\sum_{\ell=0}^{\varphi} \begin{bmatrix} \varphi \\ \ell \end{bmatrix} b^{\ell(t-i-\varphi+\ell)} \nu^{[i]\{\ell\}}(t) * \mu^{[t-i]\{\varphi-\ell\}}(t-\ell)\right)$$

$$= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{n} c'_i \psi_i(t) \tag{4.5.8}$$

say. Then

$$\begin{aligned}\psi_i(t) &\overset{(4.4.9)(4.4.8)}{=} \sum_{\ell=0}^{\varphi} \begin{bmatrix}\varphi\\ \ell\end{bmatrix} b^{\ell(t-i-\varphi+\ell)} \left\{(-1)^{\ell}\beta(i,\ell)\nu^{[i-\ell]}(t)\right\}\\ &\qquad * \left\{b^{-\sigma_{\varphi-\ell}}\beta(t-i,\varphi-\ell)\gamma'(t-\ell,\varphi-\ell)\mu^{[t-i-\varphi+\ell]}(t-\varphi)\right\}.\end{aligned}$$

Now let

$$\Psi(X,Y;t-\varphi) = \nu^{[i-\ell]}(X,Y;t) * \gamma'(t-\ell,\varphi-\ell)\mu^{[t-i-\varphi+\ell]}(X,Y;t-\varphi).$$

Then we apply the negative-q-product, reorder the summations and set $X = Y = 1$ which gives

$$\begin{aligned}&\Psi(1,1;t-\varphi)\\ &\quad= \sum_{u=0}^{t-\varphi}\left[\sum_{p=0}^{u} b^{p(t-i-\varphi+\ell)}\nu_p^{[i-\ell]}(t)\gamma'(t-\ell-p,\varphi-\ell)\mu_{u-p}^{[t-i-\varphi+\ell]}(t-\varphi-p)\right]\\ &\quad= \sum_{r=0}^{i-\ell} b^{r(t-i-\varphi+\ell)}\nu_r^{[i-\ell]}(t)\gamma'(t-\ell-r,\varphi-\ell)\left[\sum_{w=0}^{t-i-\varphi+\ell}\mu_w^{[t-i-\varphi+\ell]}(t-\varphi-r)\right]\\ &\quad\overset{(2.3.27)}{=} \sum_{r=0}^{i-\ell} b^{r(t-i-\varphi+\ell)}(-1)^{t-i-\varphi+\ell}b^{(t-\varphi-r)(t-i-\varphi+\ell)}\nu_r^{[i-\ell]}(t)\gamma'(t-\ell-r,\varphi-\ell)\\ &\quad= (-1)^{t-i-\varphi+\ell}b^{(t-\varphi)(t-i-\varphi+\ell)}\sum_{r=0}^{i-\ell}(-1)^r b^{\sigma_r}\begin{bmatrix}i-\ell\\ r\end{bmatrix}\gamma'(t-\ell-r,\varphi-\ell)\\ &\quad= (-1)^{t-i-\varphi+\ell}b^{(t-\varphi)(t-i-\varphi+\ell)}\delta(t-\ell,\varphi-\ell,i-\ell)\\ &\quad\overset{(4.5.2)}{=} (-1)^{t-i-\varphi+\ell}b^{(t-\varphi)(t-i-\varphi+\ell)}(-1)^{i-\ell}b^{(i-\ell)(t-i)}\prod_{j=0}^{i-\ell-1}\left(b^{\varphi-\ell}-b^j\right)\gamma'(t-i,\varphi-i)\\ &\quad= (-1)^{t-\varphi}b^{(t-\varphi)(t-i-\varphi+\ell)}b^{(i-\ell)(t-i)}\prod_{j=0}^{i-\ell-1}\left(b^{\varphi-\ell}-b^j\right)\gamma'(t-i,\varphi-i).\end{aligned}$$

Noting that $b^{\ell(t-i-\varphi+\ell)}b^{-\sigma_{\varphi-\ell}} = b^{\ell(t-i)}b^{-\sigma_\varphi}b^{\sigma_\ell}$ gives

$$\begin{aligned}\psi_i(1,1;t) &= \sum_{\ell=0}^{\varphi}(-1)^{\ell}\begin{bmatrix}\varphi\\ \ell\end{bmatrix}b^{\ell(t-i-\varphi+\ell)}b^{-\sigma_{\varphi-\ell}}\beta(i,\ell)\beta(t-i,\varphi-\ell)\Psi(1,1;t-\varphi)\\ &\overset{(2.3.36)}{=} b^{-\sigma_\varphi}\beta(\varphi,\varphi)\sum_{\ell=0}^{\varphi}(-1)^{\ell}b^{\ell(t-i)}b^{\sigma_\ell}\begin{bmatrix}i\\ \ell\end{bmatrix}\begin{bmatrix}t-i\\ \varphi-\ell\end{bmatrix}\Psi(1,1;t-\varphi).\end{aligned}$$

Writing that

$$\begin{aligned}b^{-\sigma_\varphi}b^{\ell(t-i)}b^{(t-\varphi)(t-\varphi-i+\ell)}b^{(i-\ell)(t-i)} &= b^{\sigma_\varphi}b^{\varphi(1-t)}b^{t(t-\varphi)}b^{\ell(t-\varphi)}b^{i(\varphi-i)} &(4.5.9)\\ &= b^{\theta}b^{\ell(t-\varphi)} &(4.5.10)\end{aligned}$$

gives

$$\begin{aligned}\psi_i(1,1;t) &= (-1)^{t-\varphi} b^{\theta} \beta(\varphi,\varphi)\gamma'(t-i,\varphi-i) \sum_{\ell=0}^{i} (-1)^{\ell} b^{\ell(t-\varphi)} b^{\sigma_\ell} \begin{bmatrix} i \\ \ell \end{bmatrix} \begin{bmatrix} t-i \\ \varphi-\ell \end{bmatrix} \prod_{j=0}^{i-\ell-1} \left(b^{\varphi-\ell} - b^{j}\right) \\ &= (-1)^{t-\varphi}(-1)^{i} b^{\theta} b^{\sigma_i} \beta(\varphi,\varphi) \begin{bmatrix} t-i \\ t-\varphi \end{bmatrix} \gamma'(t-i,\varphi-i) \qquad (4.5.11)\end{aligned}$$

by Lemma 4.5.4.

Substituting the results from (4.5.6), (4.5.8) and (4.5.11) we have

$$\sum_{i=\varphi}^{t} b^{\varphi(1-i)+\sigma_\varphi} \beta(\varphi,\varphi) \begin{bmatrix} i \\ \varphi \end{bmatrix} c_i = \frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{t} c'_i (-1)^{t-\varphi+i} b^{\theta} b^{\sigma_i} \beta(\varphi,\varphi) \begin{bmatrix} t-i \\ t-\varphi \end{bmatrix} \gamma'(t-i,\varphi-i).$$

Thus cancelling and rearranging gives,

$$\sum_{i=\varphi}^{t} b^{\varphi(t-i)} \begin{bmatrix} i \\ \varphi \end{bmatrix} c_i = \frac{\left(-b^{t}\right)^{t-\varphi}}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{\varphi} (-1)^{i} b^{\sigma_i} b^{i(\varphi-i)} \begin{bmatrix} t-i \\ t-\varphi \end{bmatrix} \gamma'(t-i,\varphi-i) c'_i$$

as required. □

We can simplify Proposition 4.5.5 if φ is less than the minimum distance of the dual code. Also we can introduce the ***dual diameter***, ϱ'_R, defined as the maximum distance between any two codewords of the dual code and simplify Proposition 4.5.5 further.

Corollary 4.5.6. *If* $0 \leq \varphi < d'_{HR}$ *then*

$$\sum_{i=\varphi}^{t} b^{\varphi(t-i)} \begin{bmatrix} i \\ \varphi \end{bmatrix} c_i = \frac{1}{|\mathscr{C}^{\perp}|} \left(-b^{t}\right)^{t-\varphi} \begin{bmatrix} t \\ \varphi \end{bmatrix} \gamma'(t,\varphi).$$

For $\varrho'_R < \varphi \leq t$ *then*

$$\sum_{i=0}^{\varphi} (-1)^{i} b^{\sigma_i} b^{i(\varphi-i)} \begin{bmatrix} t-i \\ t-\varphi \end{bmatrix} \gamma'(t-i,\varphi-i) c_i = 0.$$

Proof. First consider $0 \leq \varphi < d'_{HR}$, then $c'_0 = 1$, $c'_1 = \ldots = c'_\varphi = 0$. Also since $\begin{bmatrix} t \\ t-\varphi \end{bmatrix} = \begin{bmatrix} t \\ \varphi \end{bmatrix}$ the statement holds. Now if $\varrho'_R < \varphi \leq n$ then applying Proposition 4.5.5 to $\mathscr{C}^{\perp}$ gives

$$\sum_{i=\varphi}^{t} b^{\varphi(t-i)} \begin{bmatrix} i \\ \varphi \end{bmatrix} c'_i = \frac{1}{|\mathscr{C}|} \left(-b^{t}\right)^{t-\varphi} \sum_{i=0}^{\varphi} (-1)^{i} b^{\sigma_i} b^{i(\varphi-i)} \begin{bmatrix} t-i \\ t-\varphi \end{bmatrix} \gamma'(t-i,\varphi-i) c_i.$$

So using $c'_\varphi = \ldots = c'_t = 0$ we have

$$0 = \sum_{i=0}^{\varphi} (-1)^{i} b^{\sigma_i} b^{i(\varphi-i)} \begin{bmatrix} t-i \\ t-\varphi \end{bmatrix} \gamma'(t-i,\varphi-i) c_i$$

as required. □

4.5.3 MHRD Codes

As an application for the MacWilliams Identity, we can derive an alternative proof for the explicit coefficients of the Hermitian rank weight distribution for some MHRD codes to that in [53, Theorem 3]. This is analogous to the results for MRD codes presented in [22, Proposition 9] and Proposition 3.5.8. Firstly a lemma, analogous to the rank and skew rank cases, that will be needed.

Lemma 4.5.7. *If $a_0, a_1, \dots, a_\ell$ and $b_0, b_1, \dots, b_\ell$ are two sequences of real numbers and if*

$$a_j = \sum_{i=0}^{j} \begin{bmatrix} \ell - i \\ \ell - j \end{bmatrix} b_i$$

for $0 \leq j \leq \ell$, then also for $0 \leq i \leq \ell$ we have,

$$b_i = \sum_{j=0}^{i} (-1)^{i-j} b^{\sigma_{i-j}} \begin{bmatrix} \ell - j \\ \ell - i \end{bmatrix} a_j.$$

Proof. For $0 \leq i \leq \ell$,

$$\begin{aligned}
\sum_{j=0}^{i} (-1)^{i-j} b^{\sigma_{i-j}} \begin{bmatrix} \ell - j \\ \ell - i \end{bmatrix} a_j &= \sum_{j=0}^{i} (-1)^{i-j} b^{\sigma_{i-j}} \begin{bmatrix} \ell - j \\ \ell - i \end{bmatrix} \left(\sum_{k=0}^{j} \begin{bmatrix} \ell - k \\ \ell - j \end{bmatrix} b_k \right) \\
&= \sum_{k=0}^{i} \sum_{j=k}^{i} (-1)^{i-j} b^{\sigma_{i-j}} \begin{bmatrix} \ell - j \\ \ell - i \end{bmatrix} \begin{bmatrix} \ell - k \\ \ell - j \end{bmatrix} b_k \\
&= \sum_{k=0}^{i} b_k \left(\sum_{s=\ell-i}^{\ell-k} (-1)^{i-\ell+s} b^{\sigma_{i-\ell+s}} \begin{bmatrix} s \\ \ell - i \end{bmatrix} \begin{bmatrix} \ell - k \\ s \end{bmatrix} \right) \\
&\overset{(2.3.28)}{=} \sum_{k=0}^{i} b_k \delta_{ik} \\
&= b_i
\end{aligned}$$

as required. □

Before we write our next proposition, we shall explain a similar proposition presented by Schmidt [53, Theorem 3]. Theorem 3 states that if a code, $\mathscr{C}$, has minimum distance d_{HR}, and its dual, $\mathscr{C}^\perp$, has minimum distance at least $t - d_{HR} + 1$, then the weight distribution is uniquely determined by its parameters. Moreoever, if d_{HR} is odd and the code $\mathscr{C}$ meets the Singleton bound, i.e. $|\mathscr{C}| = q^{t(t-d_{HR}+1)}$ (2.7.1) then, by [53, Theorem 1], $\mathscr{C}^\perp$ has minimum distance at least $t - d_{HR} + 2$ and the conditions for [53] Theorem 3 are met. However, if d_{HR} is even and $\mathscr{C}$ meets the Singleton bound, the weight distribution cannot necessarily be determined uniquely by its parameters and Schmidt provides a counterexample to show this. Consequently the following proposition looks specifically at codes which are MHRD, i.e. meets the Singleton bound, with minimum distance, d_{HR}, odd. We can then use [53, Theorem 1] and Corollary 4.5.2 to derive the unique weight distribution of the code as a function of its parameters equivalent to [53, Theorem 3].

Proposition 4.5.8. *Let $\mathscr{C} \subseteq \mathscr{H}_{q,t}$ be a linear MHRD code with weight distribution $\boldsymbol{c} = (c_0, \dots, c_t)$ and minimum distance d_{HR} odd. Then we have $c_0 = 1$ and for $0 \le r \le t - d_{HR}$,*

$$c_{r+d_{HR}} = \sum_{i=0}^{r} (-1)^{r-i} b^{\sigma_{r-i}} \begin{bmatrix} d_{HR}+r \\ d_{HR}+i \end{bmatrix} \begin{bmatrix} t \\ d_{HR}+r \end{bmatrix} \left(\frac{(-b^t)^{d_{HR}+i}}{|\mathscr{C}^\perp|} - 1 \right).$$

Proof. From Corollary 4.5.2, for $0 \le \varphi < d'_{HR}$ we have

$$\sum_{i=0}^{t-\varphi} \begin{bmatrix} t-i \\ \varphi \end{bmatrix} c_i = \frac{1}{|\mathscr{C}^\perp|} \left(-b^t\right)^{t-\varphi} \begin{bmatrix} t \\ \varphi \end{bmatrix}.$$

Now if a linear code $\mathscr{C}$ is MHRD, with minimum distance d_{HR} odd, then $\mathscr{C}^\perp$ is also MHRD with minimum distance $d'_{HR} = t - d_{HR} + 2$ by [53, Theorem 1]. So Corollary 4.5.2 holds for $0 \le \varphi \le t - d_{HR} = d'_{HR} - 2$. We therefore have $c_0 = 1$ and $c_1 = c_2 = \ldots = c_{d_{HR}-1} = 0$ and setting $\varphi = t - d_{HR} - j$ for $0 \le j \le t - d_{HR}$ gives

$$\begin{bmatrix} t \\ t-d_{HR}-j \end{bmatrix} + \sum_{i=d_{HR}}^{d_{HR}+j} \begin{bmatrix} t-i \\ t-d_{HR}-j \end{bmatrix} c_i = \frac{1}{|\mathscr{C}^\perp|} \left(-b^t\right)^{d_{HR}+j} \begin{bmatrix} t \\ t-d_{HR}-j \end{bmatrix}$$

$$\sum_{r=0}^{j} \begin{bmatrix} t-d_{HR}-r \\ t-d_{HR}-j \end{bmatrix} c_{r+d_{HR}} = \begin{bmatrix} t \\ t-d_{HR}-j \end{bmatrix} \left(\frac{(-b^t)^{d_{HR}+j}}{|\mathscr{C}^\perp|} - 1 \right).$$

Applying Lemma 4.5.7 with $\ell = t - d_{HR}$ and $b_r = c_{r+d_{HR}}$ then setting

$$a_j = \begin{bmatrix} t \\ t-d_{HR}-j \end{bmatrix} \left(\frac{(-b^t)^{d_{HR}+j}}{|\mathscr{C}^\perp|} - 1 \right)$$

gives

$$\sum_{r=0}^{j} \begin{bmatrix} t-d_{HR}-r \\ t-d_{HR}-j \end{bmatrix} b_r = a_j$$

and so

$$\begin{aligned} b_r = c_{r+d_{HR}} &= \sum_{i=0}^{r} (-1)^{r-i} b^{\sigma_{r-i}} \begin{bmatrix} t-d_{HR}-i \\ t-d_{HR}-r \end{bmatrix} a_i \\ &= \sum_{i=0}^{r} (-1)^{r-i} b^{\sigma_{r-i}} \begin{bmatrix} t-d_{HR}-i \\ t-d_{HR}-r \end{bmatrix} \begin{bmatrix} t \\ t-d_{HR}-i \end{bmatrix} \left(\frac{(-b^t)^{d_{HR}+i}}{|\mathscr{C}^\perp|} - 1 \right). \end{aligned}$$

But we have

$$\begin{aligned} \begin{bmatrix} t-d_{HR}-i \\ t-d_{HR}-r \end{bmatrix} \begin{bmatrix} t \\ t-d_{HR}-i \end{bmatrix} &\overset{(2.3.24)}{=} \begin{bmatrix} t-(d_{HR}+i) \\ t-(d_{HR}+r) \end{bmatrix} \begin{bmatrix} t \\ d_{HR}+i \end{bmatrix} \\ &\overset{(2.3.25)}{=} \begin{bmatrix} d_{HR}+r \\ d_{HR}+i \end{bmatrix} \begin{bmatrix} t \\ t-(d_{HR}+r) \end{bmatrix} \\ &\overset{(2.3.24)}{=} \begin{bmatrix} d_{HR}+r \\ d_{HR}+i \end{bmatrix} \begin{bmatrix} t \\ d_{HR}+r \end{bmatrix}. \end{aligned}$$

Therefore

$$c_{r+d_{HR}} = \sum_{i=0}^{r} (-1)^{r-i} b^{\sigma_{r-i}} \begin{bmatrix} d_{HR}+r \\ d_{HR}+i \end{bmatrix} \begin{bmatrix} t \\ d_{HR}+r \end{bmatrix} \left(\frac{(-b^t)^{d_{HR}+i}}{|\mathscr{C}^{\perp}|} - 1 \right)$$

as required. □

Chapter 5

The Generalised MacWilliams Identity as a Functional Transform

We have successfully extended a q-algebra for each of the skew rank and the Hermitian association schemes from the q-algebra for the rank association scheme by Gadouleau and Yan [22, Section 3.1]. We now explore ways in which the theory that has been studied could be generalised with a view to applying it to a wider group of metric association schemes. The association schemes that have been studied so far are all formally self dual metric association schemes with eigenvalues that satisfy Delsarte's recurrence relation with specific initial values. We will call any association scheme with these characteristics a Krawtchouk association scheme.

We summarise the results for each association scheme. From that we develop a theory that encompasses the four classes of association schemes studied in this thesis.

This chapter is arranged as follows. Section 5.1 presents a summary of results from the q-algebra approach for the individual metrics, summarised in Tables 5.1.1 and 5.1.2. Section 5.2 recaps some of the already known theory of association schemes and proposes a general gamma function which arises from a component of the solutions to the recurrence relation. It is interesting to note here that once these functions are introduced, we can then write the valencies of Krawtchouk association schemes in a neat and compact form, that depends only on its parameters and not the particular structure of the underlying space. The remaining sections follow a similar pattern to those in Chapter 3 and Chapter 4. Section 5.3 is the generalised q-algebra that we have called the b-algebra. Here we introduce the b-product, b-power and b-transform, as well as what we call the "fundamental polynomials". These polynomials are a generalisation of the homogeneous polynomials presented in the previous chapters and once again, if we take the b-power of one of these polynomials then we can find the weight enumerator of the whole space dependent only on the parameters of the association scheme.

In Section 5.4 a generalised polynomial that we call the b-Krawtchouk polynomial is proposed and shown to represent the eigenvalues of a relevant association scheme. The recurrence relation that it satisfies is an extension of the relation defined in [11, (1)] to include the Hermitian association scheme case where the parameter $b = -q$. Using these tools the MacWilliams Identity is proven as a generalised functional transform that applies to all the schemes we have studied and potentially to a wider class of self dual metric association schemes that have eigenvalues that satisfy the recurrence relation with a specific set of initial values.

Since the theory for the q-derivatives, skew-q-derivatives and the negative-q-derivatives are all analogous to one another, it was relatively straightforward to find analogous b-derivatives which are presented in Section 5.5. This then takes us on nicely to our final Section, 5.6, where we calculate the moments of the weight distribution of these association scheme highlighting the special case when we have a code and its dual both being maximal.

Chapter 5 is a late addition to this thesis. The earlier chapters represent significant advances in the development of the MacWilliams Identity as a functional transform. While documenting these developments a new challenge was identified, which is how, if at all, these theories might be unified. The difficulties involved identifying the relevant characteristics of each association scheme, including how the dual of a code can be defined in general. In particular, it was also difficult to see how their distinct parameters could be blended together to build a general form for the gamma function, for the relevant q-algebra and, crucially, for the fundamental polynomials.

5.1 More of the Individual Association Schemes

Now, to be able to confirm our expectations that we are able to generalise the theory outlined in the previous two chapters, we need to check some results in the other schemes. Specifically, to confirm that the recurrence relation defined by Delsarte [11, (1)] is consistent with the ones used by Gadouleau and Yan [22, Appendix C] and Schmidt [53, Lemma 7].

5.1.1 The Rank Association Scheme

As we have the majority of the theory for the rank metric already, we need to explain why the recurrence relation in [22, (C.1)] is equivalent to the more general recurrence relation in [11, (1)].

The recurrence relation stated in [22] is as follows,

$$P_{k+1}(x+1; m+1, n+1) = q^{k+1} P_{k+1}(x; m, n) - q^k P_k(x; m, n)$$

which at a glance of it looks identical to the recurrence relation presented in [11] below

$$P_{k+1}(x+1, n+1) = q^{k+1} P_{k+1}(x, n) - q^k P_k(x, n)$$

but with an extra parameter in each term. In fact these recurrence relations are indeed the same but the reasoning isn't as obvious. In the case of $\mathbb{F}_q^{m\times n}$, bilinear forms in Delsarte notation, there are two parameters m and n. In order to maintain a constant power of q, as specified by Delsarte [11, Section 5.1 (ii)], we will see in our later analysis that this equates to $m - n$ being a constant. Therefore, as n increases so must m.

Although not their main method of proof, Gadouleau and Yan do also show that the rank-Krawtchouk polynomials are indeed the generalised Krawtchouk polynomials by satisfying the recurrence relation above [22, Appendix C], so we do not need to restate the MacWilliams Identity for the rank metric as we now have all the information we need.

5.1.2 The Hermitian Association Scheme

We note that substituting the parameters $b = -q$ into the recurrence relation in [11, (1)] yields the same formula as Schmidt [53, Lemma 7] despite the parameters lying outside the bounds of the definition given by Delsarte. For the following proposition we take the b-nary Gaussian coefficients as defined in Equation (4.1), the negative-q-gamma function as defined in Definition 4.1.2 and the eigenvalues of the association scheme, $C_k(x, n)$ as defined in Equation (4.3.1).

Proposition 5.1.1. *For $b = -q \in \mathbb{R}$, $b \neq 0$, $x, k \in \{0, \ldots, n\}$ the recurrence relation from [53, Lemma 7],*

$$C_{k+1}(x+1, n+1) = C_{k+1}(x, n+1) + b^{2n+1-x} C_k(x, n)$$

has the same solutions as the recurrence relation from [11, (1)],

$$C_{k+1}(x+1, n+1) = b^{k+1} C_{k+1}(x, n) - b^k C_k(x, n)$$

where $C_k(x, n)$ are the eigenvalues of the association scheme of Hermitian matrices.

Proof. We show that

$$C_{k+1}(x, n+1) + b^{2n+1-x} C_k(x, n) = b^{k+1} C_{k+1}(x, n) - b^k C_k(x, n).$$

Let $\alpha_1 = b^{k+1} C_{k+1}(x, n)$ and $\alpha_2 = b^k C_k(x, n)$ and also let $\beta_1 = C_{k+1}(x, n+1)$ and $\beta_2 =$

$b^{2n+1-x}C_k(x,n)$. Then using the eigenvalues defined in (4.3.1) we have,

$$\begin{aligned}
\alpha_1 &= b^{k+1}\sum_{j=0}^{k+1}(-1)^j b^{j(n-x)} b^{\sigma_j}\begin{bmatrix}x\\j\end{bmatrix}\begin{bmatrix}n-x\\k+1-j\end{bmatrix}\gamma'(n-j,k+1-j)\\
\alpha_2 &= b^{k}\sum_{j=0}^{k}(-1)^j b^{j(n-x)} b^{\sigma_j}\begin{bmatrix}x\\j\end{bmatrix}\begin{bmatrix}n-x\\k-j\end{bmatrix}\gamma'(n-j,k-j)\\
\beta_1 &= \sum_{j=0}^{k+1}(-1)^j b^{j(n+1-x)} b^{\sigma_j}\begin{bmatrix}x\\j\end{bmatrix}\begin{bmatrix}n+1-x\\k+1-j\end{bmatrix}\gamma'(n+1-j,k+1-j)\\
\beta_2 &= b^{2n+1-x}\sum_{j=0}^{k}(-1)^j b^{j(n-x)} b^{\sigma_j}\begin{bmatrix}x\\j\end{bmatrix}\begin{bmatrix}n-x\\k-j\end{bmatrix}\gamma'(n-j,k-j).
\end{aligned}$$

Consider $\alpha_1|_{j=k+1}$ and $\beta_1|_{j=k+1}$. Then,

$$\begin{aligned}
\alpha_1|_{j=k+1} &= b^{k+1}(-1)^{k+1} b^{(k+1)(n-x)} b^{\sigma_{k+1}}\begin{bmatrix}x\\k+1\end{bmatrix}\begin{bmatrix}n-x\\0\end{bmatrix}\gamma'(n-k+1,0)\\
\beta_1|_{j=k+1} &= (-1)^{k+1} b^{(k+1)(n+1-x)} b^{\sigma_{k+1}}\begin{bmatrix}x\\k+1\end{bmatrix}\begin{bmatrix}n+1-x\\0\end{bmatrix}\gamma'(n+1-k-1,0)
\end{aligned}$$

since $\gamma'(x,0)=1$ for any $x \in \mathbb{R}$. So $\alpha_1|_{j=k+1} = \beta_1|_{j=k+1}$. Now rearranging α_1 and β_1 we have

$$\begin{aligned}
\alpha_1 &= b^{k+1}\sum_{j=0}^{k+1}(-1)^j b^{j(n-x)} b^{\sigma_j}\begin{bmatrix}x\\j\end{bmatrix}\begin{bmatrix}n-x\\k+1-j\end{bmatrix}\gamma'(n-j,k+1-j)\\
&\overset{(2.3.31)(4.1.4)}{=} \sum_{j=0}^{k}(-1)^j b^{j(n-x)+1} b^{\sigma_j}\begin{bmatrix}x\\j\end{bmatrix}\frac{b^{n-x-k+j}-1}{b^{k+1-j}-1}\begin{bmatrix}n-x\\k-j\end{bmatrix}\left(-b^{n-j}-b^{k-j}\right)\gamma'(n-j,k-j)\\
&\qquad + \alpha_1|_{j=k+1}\\
\beta_1 &= \sum_{j=0}^{k+1}(-1)^j b^{j(n+1-x)} b^{\sigma_j}\begin{bmatrix}x\\j\end{bmatrix}\begin{bmatrix}n+1-x\\k+1-j\end{bmatrix}\gamma'(n+1-j,k+1-j)\\
&\overset{(2.3.33)(4.1.3)}{=} \sum_{j=0}^{k}(-1)^j b^{j(n+1-x)} b^{\sigma_j}\begin{bmatrix}x\\j\end{bmatrix}\frac{b^{n+1-x}-1}{b^{k+1-j}-1}\begin{bmatrix}n-x\\k-j\end{bmatrix} b^{k-j}\left(-b^{n+1-j}-1\right)\gamma'(n-j,k-j)\\
&\qquad + \beta_1|_{j=k+1}.
\end{aligned}$$

Now let $C = \alpha_1 - \alpha_2 - \beta_1 - \beta_2$. Then

$$\begin{aligned}
\alpha_1 - \alpha_2 - \beta_1 - \beta_2 = \sum_{j=0}^{k}&(-1)^j b^{j(n-x)} \beta^{\sigma_j}\begin{bmatrix}x\\j\end{bmatrix}\begin{bmatrix}n-x\\k-j\end{bmatrix}\gamma'(n-j,k-j)\\
&\times\Bigg(b^{k+1}\left(-b^{n-j}-b^{k-j}\right)\frac{\left(b^{n-x-(k-j)}-1\right)}{b^{k+1-j}-1} - b^k\\
&- b^j b^{k-j}\left(-b^{n+1-j}-1\right)\frac{b^{n+1-x}-1}{b^{k+1-j}-1} - b^{2n+1-x}\Bigg)\\
&+ \alpha_1|_{j=k+1} - \beta_1|_{j=k+1}.
\end{aligned}$$

But

$$\begin{aligned}
b^{k+1}\left(-b^{n-j}-b^{k-j}\right)&\frac{\left(b^{n-x-(k-j)}-1\right)}{b^{k+1-j}-1}-b^{k}-b^{j}b^{k-j}\left(-b^{n+1-j}-1\right)\frac{\left(b^{n+1-x}-1\right)}{b^{k+1-j}-1}-b^{2n+1-x}\\
&=\frac{b^{k}}{b^{k+1-k}-1}\Bigg(b^{k+1}\left(-b^{n-j+1}-b^{k-j+1}\right)\left(b^{n-x-k+j}-1\right)\\
&\qquad\times\left(-b^{n+1-j}-1\right)\left(b^{n+1-x}-1\right)\Bigg)-b^{k}-b^{2n+1-x-k}\\
&=\frac{b^{k}}{b^{k+1-k}-1}\Big(-b^{2n+1-k-x}-b^{n-x+1}+b^{n-j+1}\\
&\qquad+b^{k-j+1}+b^{2n+2-x-j}-b^{n+1-j}+b^{n+1-x}-b^{k+1-j}+1\\
&\qquad-1-b^{2n+1-x+1-j}+b^{2n+1-x-k}\Big)\\
&=0.
\end{aligned}$$

Therefore $C=0$, and $\alpha_1-\alpha_2=\beta_1+\beta_2$. Therefore the recurrence relations have the same solutions. □

5.1.3 The Overview

To summarise the results obtained so far in this thesis, Table 5.1.2 highlights the features we need in each association scheme. At a glance there are evident similarities but significant differences. For each case we have listed the associated metric, the number of classes in the relevant association scheme, the underlying space, the homogeneous polynomial used in the MacWilliams Identity, the "fundamental polynomial", the known eigenvalues of the scheme and its valencies. In all cases q is a power of a prime. The final row is the accumulation of the results from analysing the ways in which the differences can be assimilated in a general theory. The other table, Table 5.1.1, details the allocation of the general parameters identified for each case. The analysis that led to these conclusions is outlined in the rest of this chapter.

Name	b	c	λ	cb^{λ}
Hamming	1	q	n	q
Bilinear Gabidulin	q	q^{m-n}	n	q^{m}
Skew	q^2	t odd - q, t even - q^{-1}	n	cq^{2n}
Hermitian	$-q$	-1	t	$-(-q)^t$

Table 5.1.1: Proposed generalised parameters

Name	Metric	Class	Space	Fundamental Polynomial	Eigenvalues	Valencies v_s
Hamming length n	Hamming	n	$\mathbb{F}_q^n$	$X+(q-1)Y$	$\sum_{j=0}^{k}(-1)^j\binom{x}{j}\binom{n-x}{k-j}(q-1)^{k-j}$	$\binom{n}{s}(q-1)^s$
Bilinear $m\times n,\ m\geq n$ Gabudulin $m\times n$	Rank	n n	$\mathbb{F}_q^{m\times n}$ $\mathbb{F}_{q^m}^n$	$X+(q^m-1)\,Y$	$\sum_{j=0}^{k}(-1)^j q^{j(n-x)}q^{\sigma_j}\ {}_{q}\begin{bmatrix}x\\j\end{bmatrix}\ {}_{q}\begin{bmatrix}n-x\\k-j\end{bmatrix}\alpha(n-j,k-j)$	${}_{q}\begin{bmatrix}n\\s\end{bmatrix}\alpha(m,s)$
Skew $t\times t$, $n=\left\lfloor\frac{t}{2}\right\rfloor$, $m=\frac{t(t-1)}{2n}$	Skew Rank	n	$\mathbb{F}_q^{t\times t}$	t odd, $X+\left(q^{2n+1}-1\right)Y$ t even, $X+\left(q^{2n-1}-1\right)Y$	$\sum_{j=0}^{k}(-1)^j q^{2j(n-x)}q^{j(j-1)}\ {}_{q^2}\begin{bmatrix}x\\j\end{bmatrix}\ {}_{q^2}\begin{bmatrix}n-x\\k-j\end{bmatrix}\gamma(m-2j,k-j)$	${}_{q^2}\begin{bmatrix}n\\s\end{bmatrix}\gamma(m,s)$
Hermitian $t\times t$	Rank	t	$\mathbb{F}_{q^2}^{t\times t}$	$X+(-(-q)^t-1)\,Y$	$\sum_{j=0}^{k}(-1)^j(-q)^{j(t-x)}(-q)^{\sigma_j}\ {}_{-q}\begin{bmatrix}x\\j\end{bmatrix}\ {}_{-q}\begin{bmatrix}t-x\\k-j\end{bmatrix}\gamma'(t-j,k-j)$	${}_{-q}\begin{bmatrix}t\\s\end{bmatrix}\gamma'(t,s)$
Krawtchouk A-S.	-	n	$\mathscr{X}$	$X+(cb^n-1)\,Y$	$\sum_{j=0}^{k}(-1)^j b^{j(n-x)}b^{\sigma_j}\ {}_{b}\begin{bmatrix}x\\j\end{bmatrix}\ {}_{b}\begin{bmatrix}n-x\\k-j\end{bmatrix}\gamma_{b,c}(n-j,k-j)$	${}_{b}\begin{bmatrix}n\\s\end{bmatrix}\gamma_{b,c}(n,s)$

Table 5.1.2: An overview of key parameters and results

5.2 Preliminaries

Since we are considering the more general idea of metric schemes (and therefore P-polynomial schemes) we don't specify the details of any codes and spaces they are in, but rather consider parameters of their association schemes. So as before in Definition 2.3.1, we have a finite set $\mathscr{X}$ of v points and $n+1$ relations forming a symmetric association scheme with n classes. In this chapter we are only considering metric schemes which are self dual, i.e. when there is an ordering of the relations as in Definition 2.3.6 and the eigenmatrices P and Q coincide, and also only considering those with eigenvalues that satisfy Delsarte's recurrence relation [11, (1)] with specific initial values.

5.2.1 b-nary Identities

We begin by rewriting here the generalised b-nary identities that we will be using, plus a new important generalised gamma function which we have developed using a comparison of the earlier gamma functions and alpha function.

Definition 5.2.1. For $x, k \in \mathbb{Z}^+$, $b \in \mathbb{R}$, $b \neq 1$ the ***b*-nary Gaussian coefficients** are defined as

$$ {}_b\begin{bmatrix} x \\ k \end{bmatrix} = \prod_{i=0}^{k-1} \frac{b^x - b^i}{b^k - b^i} $$

with

$$ {}_b\begin{bmatrix} x \\ 0 \end{bmatrix} = 1. $$

Again we note that, as in Section 2.3.1, for the Hamming metric when we want to take $b = 1$, this definition would be undefined. So we take the limit $b \to 1$, leaving us with the usual binomial coefficients.

Also note for ease we also define $\sigma_i = \frac{i(i-1)}{2}$ for $i \geq 0$ and we write ${}_b\left[\begin{smallmatrix} x \\ k \end{smallmatrix}\right]$ as $\left[\begin{smallmatrix} x \\ k \end{smallmatrix}\right]$. Here are some identities relating to the b-nary Gaussian coefficients which are useful in simplifying notation, and can be used for different values of b from [12]. For $b \in \mathbb{R}$, $b \neq 1$, $x, i, j, k \in \mathbb{Z}^+$, $y \in \mathbb{R}$ we have

$$ \begin{bmatrix} x \\ k \end{bmatrix} \begin{bmatrix} x \\ k \end{bmatrix} = \begin{bmatrix} x \\ x-k \end{bmatrix} \tag{5.2.1} $$

$$ \begin{bmatrix} x \\ i \end{bmatrix} \begin{bmatrix} x-i \\ k \end{bmatrix} = \begin{bmatrix} x \\ k \end{bmatrix} \begin{bmatrix} x-k \\ i \end{bmatrix} \tag{5.2.2} $$

$$ \prod_{i=0}^{x-1} \left(y - b^i\right) = \sum_{k=0}^{x} (-1)^{x-k} b^{\binom{x-k}{2}} \begin{bmatrix} x \\ k \end{bmatrix} y^k \tag{5.2.3} $$

$$ \sum_{k=0}^{x} \begin{bmatrix} x \\ k \end{bmatrix} \prod_{i=0}^{k-1} \left(y - b^i\right) = y^x \tag{5.2.4} $$

$$ \sum_{k=i}^{j} (-1)^{k-i} b^{\sigma_{k-i}} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} j \\ k \end{bmatrix} = \delta_{ij}. \tag{5.2.5} $$

The following identities are each used in the rest of this paper but can be shown trivially to be equal.

$$\begin{aligned}\begin{bmatrix}x\\k\end{bmatrix} &= \begin{bmatrix}x-1\\k\end{bmatrix} + b^{x-k}\begin{bmatrix}x-1\\k-1\end{bmatrix} && (5.2.6)\\ &= \begin{bmatrix}x-1\\k-1\end{bmatrix} + b^{k}\begin{bmatrix}x-1\\k\end{bmatrix} && (5.2.7)\\ &= \frac{b^{x-k+1}-1}{b^k-1}\begin{bmatrix}x\\k-1\end{bmatrix} && (5.2.8)\\ &= \frac{b^x-1}{b^{x-k}-1}\begin{bmatrix}x-1\\k\end{bmatrix} && (5.2.9)\\ &= \frac{b^x-1}{b^k-1}\begin{bmatrix}x-1\\k-1\end{bmatrix}. && (5.2.10)\end{aligned}$$

Definition 5.2.2. We define a ***b-nary Beta function*** for $x, b \in \mathbb{R}$, $b \neq 1$, $k \in \mathbb{Z}^+$, as

$$\beta_b(x,k) = \prod_{i=0}^{k-1}\begin{bmatrix}x-i\\1\end{bmatrix}. \tag{5.2.11}$$

Similar to the b-nary Gaussian coefficients, in the Hamming case when we want to use $b = 1$ we take the limit as $b \to 1$ instead.

Lemma 5.2.3. *We have for all $x \in \mathbb{R}$, $k \in \mathbb{Z}^+$,*

1. $$\beta_b(x,k) = \begin{bmatrix}x\\k\end{bmatrix}\beta_b(k,k), \tag{5.2.12}$$

2. $$\beta_b(x,x) = \begin{bmatrix}x\\k\end{bmatrix}\beta_b(k,k)\beta_b(x-k,x-k), \tag{5.2.13}$$

3. $$\beta_b(x,k)\beta_b(x-k,1) = \beta_b(x,k+1). \tag{5.2.14}$$

To aid us in notation, we define a new b-nary gamma function, which is a component of the expression derived from setting $x = 0$ in the generalised Krawtchouk polynomials (2.3.38).

Definition 5.2.4. We define the ***b-nary gamma function*** for $x, b, c \in \mathbb{R}$, $k \in \mathbb{Z}^+$, $cb > 1$, to be

$$\gamma_{b,c}(x,k) = \prod_{i=0}^{k-1}\left(cb^x - b^i\right).$$

Lemma 5.2.5. *We have the following identities for the b-nary Gamma function:*

1. $$\gamma_{b,c}(x,k) = b^{\sigma_k}\prod_{i=0}^{k-1}\left(cb^{x-i} - 1\right) \tag{5.2.15}$$

2. $$\gamma_{b,c}(x+1,k+1) = \left(cb^{x+1} - 1\right)b^k\gamma_{b,c}(x,k) \tag{5.2.16}$$

3.

$$\gamma_{b,c}(x,k+1) = \left(cb^x - b^k\right)\gamma_{b,c}(x,k). \tag{5.2.17}$$

Proof.

(1)

$$\begin{aligned}
\gamma_{b,c}(x,k) &= \prod_{i=0}^{k-1}\left(cb^x - b^i\right)\\
&= \left(\prod_{i=0}^{k-1} b^i\right)\prod_{i=0}^{k-1}\left(cb^{x-i} - 1\right)\\
&= b^{\sigma_k}\prod_{i=0}^{k-1}\left(cb^{x-i} - 1\right).
\end{aligned}$$

(2)

$$\begin{aligned}
\gamma_{b,c}(x+1,k+1) &= \prod_{i=0}^{k}\left(cb^{x+1} - b^i\right)\\
&= \left(cb^{x+1} - 1\right)\prod_{i=1}^{k}\left(cb^{x+1} - b^i\right)\\
&= \left(cb^{x+1} - 1\right)\prod_{i=1}^{k} b\left(cb^{x} - b^{i-1}\right)\\
&= \left(cb^{x+1} - 1\right) b^k\prod_{i=0}^{k-1}\left(cb^{x} - b^{i}\right)\\
&= \left(cb^{x+1} - 1\right) b^k\gamma_{b,c}(x,k).
\end{aligned}$$

(3)

$$\begin{aligned}
\gamma_{b,c}(x,k+1) &= \prod_{i=0}^{k}\left(cb^x - b^i\right)\\
&= \left(cb^x - b^k\right)\prod_{i=0}^{k-1}\left(cb^x - b^i\right)\\
&= \left(cb^x - b^k\right)\gamma_{b,c}(x,k).
\end{aligned}$$

□

Note. The b-nary beta and b-nary gamma functions are new expressions which have been developed to unify the following theories in Hamming, rank, skew rank and Hermitian association schemes.

5.2.2 Recurrence relation

Below is the recurrence relation we will use to define our set of association schemes. The recurrence relation, for $b \in \mathbb{R}$, $b \neq 0$ $n \in \mathbb{Z}^+$ and $x, k \in \{0, 1, \ldots, n\}$ is

$$F_{k+1}(x+1, n+1) = b^{k+1} F_{k+1}(x, n) - b^k F_k(x, n) \tag{5.2.18}$$

for any function $F_k(x, n)$. It is noted that in using this recurrence we have slightly extended the ranges of the parameters to encompass all of the association schemes studied in this thesis. A proof that this recurrence relation is valid for the case of the Hermitian association scheme, for which the values of b lie outside the range specified by Delsarte, is shown in Proposition 5.1.1.

We can now define the set of the association schemes that we want to consider in this chapter.

Definition 5.2.6. For an $(\mathscr{X}, R)$ n-class formally self dual metric translation association scheme with defined parameters $b, c \in \mathbb{R}$ we say it is a ***Krawtchouk association scheme*** if the eigenvalues, $P_k(x, n)$, for $x, k \in \{0, 1, \ldots, n\}$ satisfy the recurrence relation

$$P_{k+1}(x+1, n+1) = b^{k+1} P_{k+1}(x, n) - b^k P_k(x, n)$$

with specific initial values

$$P_k(0, n) = \begin{bmatrix} n \\ k \end{bmatrix} \gamma_{b,c}(n, k) \tag{5.2.19}$$

$$P_0(x, n) = 1. \tag{5.2.20}$$

In fact, we can find a new set of polynomials which satisfy the recurrence relation with these initial values and therefore are the eigenvalues of the Krawtchouk association schemes.

5.2.3 The b-Krawtchouk Polynomials

Definition 5.2.7. For an n-class Krawtchouk association scheme where $x, k \in \{0, 1, \ldots, n\}$, $b \in \mathbb{R}$, $b \neq 0$, we define the ***the b-Krawtchouk Polynomial*** as

$$C_k(x, n; b, c) = \sum_{j=0}^{k} (-1)^j b^{j(n-x)} b^{\sigma_j} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k-j \end{bmatrix} \gamma_{b,c}(n-j, k-j).$$

For simplicity we shall write $C_k(x, n; b, c)$ as $C_k(x, n)$ since b and c pertain to the underlying structure of the space are being worked in and are therefore constants. The way these polynomials arise will be explained in Section 5.3. We first prove that the $C_k(x, n)$ satisfy the recurrence relation (5.2.18) and the initial values (5.2.19), (5.2.20) and therefore are the eigenvalues of the Krawtchouk association schemes.

Proposition 5.2.8. *For $b, c \in \mathbb{R}$, $b \neq 0$, $cb > 1$ and for all $x, k \in \{0, \dots, n\}$ we have*

$$C_{k+1}(x+1, n+1) = b^{k+1} C_{k+1}(x, n) - b^k C_k(x, n). \tag{5.2.21}$$

Proof. We look at all three terms sequentially. First, noting that $\begin{bmatrix} x \\ j-1 \end{bmatrix} = 0$ when $j = 0$,

$$\begin{aligned}
&C_{k+1}(x+1, n+1) \\
&\quad = \sum_{j=0}^{k+1} (-1)^j b^{j(n-x)} b^{\sigma_j} \begin{bmatrix} x+1 \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k+1-j \end{bmatrix} \gamma_{b,c}\,(n+1-j, k+1-j) \\
&\quad = C_{k+1}(x+1, n+1)\big|_{j=k+1} \\
&\qquad \overset{(5.2.7)}{+} \sum_{j=0}^{k} (-1)^j b^{j(n-x)+\sigma_j} \left\{ \begin{bmatrix} x \\ j-1 \end{bmatrix} + b^j \begin{bmatrix} x \\ j \end{bmatrix} \right\} \begin{bmatrix} n-x \\ k+1-j \end{bmatrix} \gamma_{b,c}\,(n+1-j, k+1-j)
\end{aligned}$$

$$= C_{k+1}(x+1, n+1)\big|_{j=k+1} \tag{5.2.22}$$

$$+ \sum_{j=1}^{k} (-1)^j b^{j(n-x)+\sigma_j} \begin{bmatrix} x \\ j-1 \end{bmatrix} \begin{bmatrix} n-x \\ k+1-j \end{bmatrix} \gamma_{b,c}(n+1-j, k+1-j) \tag{5.2.23}$$

$$\overset{(5.2.16)}{+} \sum_{j=0}^{k} (-1)^j c b^{j(n-x)+\sigma_j+n+1+k-j} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k+1-j \end{bmatrix} \gamma_{b,c}\,(n-j, k-j) \tag{5.2.24}$$

$$- \sum_{j=0}^{k} (-1)^j b^{j(n-x)+\sigma_j+k} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k+1-j \end{bmatrix} \gamma_{b,c}(n-j, k-j) \tag{5.2.25}$$

$$= C_{k+1}(x+1, n+1)\big|_{j=k+1} + \alpha_1 + \alpha_2 + \alpha_3$$

where α_1, α_2, α_3 represent summands (5.2.23), (5.2.24), (5.2.25) respectively and for notation, $|_{j=k+1}$ means "the term when $j = k+1$".

Second,

$$\begin{aligned}
b^{k+1} C_{k+1}(x, n) &= \sum_{j=0}^{k+1} (-1)^j b^{k+1} b^{j(n-x)} b^{\sigma_j} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k+1-j \end{bmatrix} \gamma_{b,c}(n-j, k+1-j) \\
&= b^{k+1}\ C_{k+1}(x, n)\big|_{j=k+1} \\
&\qquad \overset{(5.2.17)}{+} \sum_{j=0}^{k} (-1)^j c b^{j(n-x)+\sigma_j+n+1+k-j} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k+1-j \end{bmatrix} \gamma_{b,c}(n-j, k-j) \\
&\qquad - \sum_{j=0}^{k} (-1)^j b^{j(n-x)+\sigma_j+k+k-j+1} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k+1-j \end{bmatrix} \gamma_{b,c}(n-j, k-j)
\end{aligned} \tag{5.2.26}$$

$$= b^{k+1}\ C_{k+1}(x, n)\big|_{j=k+1} + \alpha_2 + \beta_1.$$

Where β_1 represents the summand (5.2.26). Third,

$$\begin{aligned} b^k C_k(x,n) &= \sum_{j=0}^{k} (-1)^j b^{j(n-x)+\sigma_j+k} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k-j \end{bmatrix} \gamma_{b,c}(n-j,k-j), \\ &= \rho, \text{ say.} \end{aligned}$$

So let $C = C_{k+1}(x+1,n+1) - b^{k+1}C_{k+1}(x,n) + b^k C_k(x,n)$. We have,

$$C = \alpha_1 + \alpha_3 - \beta_1 + \rho + C_{k+1}(x+1,n+1)\big|_{j=k+1} - b^{k+1}\, C_{k+1}(x,n)\big|_{j=k+1}.$$

Consider $\alpha_3 - \beta_1 + \rho$. Then

$$\begin{aligned} \alpha_3 - \beta_1 &= \sum_{j=0}^{k} (-1)^{j+1} b^{j(n-x)+\sigma_j+k} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k+1-j \end{bmatrix} \gamma_{b,c}(n-j,k-j) \left(1 - b^{k-j+1}\right) \\ &\overset{(5.2.8)}{=} \sum_{j=0}^{k} (-1)^{j+1} b^{j(n-x)+\sigma_j+k} \left(1 - b^{k-j+1}\right) \begin{bmatrix} x \\ j \end{bmatrix} \\ &\qquad \times \frac{b^{(n-x)-(k-j)} - 1}{b^{k+1-j} - 1} \begin{bmatrix} n-x \\ k-j \end{bmatrix} \gamma_{b,c}(n-j,k-j) \\ &= \sum_{j=0}^{k} (-1)^j b^{(j+1)(n-x)+\sigma_{j+1}} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k-j \end{bmatrix} \gamma_{b,c}(n-j,k-j) \qquad (5.2.27) \\ &\qquad - \sum_{j=0}^{k} (-1)^j b^{j(n-x)+\sigma_j+k} \begin{bmatrix} x \\ j \end{bmatrix} \begin{bmatrix} n-x \\ k-j \end{bmatrix} \gamma_{b,c}(n-j,k-j) \\ &= \tau - \rho, \end{aligned}$$

where τ represents the summand in (5.2.27). Thus,

$$C = \alpha_1 + \tau + C_{k+1}(x+1,n+1)\big|_{j=k+1} - b^{k+1}\, C_{k+1}(x,n)\big|_{j=k+1}.$$

Now,

$$\begin{aligned} &C_{k+1}\ (x+1,n+1)\big|_{j=k+1} - b^{k+1}\, C_{k+1}(x,n)\big|_{j=k+1} \\ &\quad = (-1)^{k+1} b^{(k+1)(n-x)} b^{\sigma_{k+1}} \left\{ \begin{bmatrix} x+1 \\ k+1 \end{bmatrix} - b^{k+1} \begin{bmatrix} x \\ k+1 \end{bmatrix} \right\} \\ &\quad \overset{(5.2.7)}{=} (-1)^{k+1} b^{(k+1)(n-x)} b^{\sigma_{k+1}} \begin{bmatrix} x \\ k \end{bmatrix} \\ &\quad = -\tau|_{j=k} \end{aligned}$$

Now consider α_1.

$$\begin{aligned}
\alpha_1 &= \sum_{j=1}^{k}(-1)^j b^{j(n-x)+\sigma_j}\begin{bmatrix} x \\ j-1\end{bmatrix}\begin{bmatrix} n-x \\ k+1-j\end{bmatrix}\gamma_{b,c}(n+1-j,k+1-j) \\
&= \sum_{j=0}^{k-1}(-1)^{j+1} b^{(j+1)(n-x)+\sigma_{j+1}}\begin{bmatrix} x \\ j\end{bmatrix}\begin{bmatrix} n-x \\ k-j\end{bmatrix}\gamma_{b,c}(n-j,k-j) \\
&= -\tau + \tau|_{j=k}.
\end{aligned}$$

Thus $C = 0$ and so the $C_k(x,n)$ satisfy the recurrence relation (5.2.18). □

Lemma 5.2.9. *The $C_k(x,n)$ are the eigenvalues of the Krawtchouk association scheme. In other words,*

$$C_k(x,n) = P_k(x,n). \tag{5.2.28}$$

Proof. The $C_k(x,n)$ satisfy the recurrence relation (5.2.21) and the initial values of the $C_k(x,n)$ are

$$\begin{aligned}
C_k(0,n) &= \sum_{j=0}^{k}(-1)^j b^{jn} b^{\sigma_j}\begin{bmatrix} 0 \\ j\end{bmatrix}\begin{bmatrix} n \\ k-j\end{bmatrix}\gamma_{b,c}(n-j,k-j) \\
&= \begin{bmatrix} n \\ k\end{bmatrix}\gamma_{b,c}(n,k)
\end{aligned}$$

as $\begin{bmatrix} 0 \\ j\end{bmatrix} = 0$ unless $j = 0$ and

$$\begin{aligned}
C_0(x,n) &= (-1)^0 b^0 b^0 \begin{bmatrix} x \\ 0\end{bmatrix}\begin{bmatrix} n-x \\ 0\end{bmatrix}\gamma_{b,c}(n,0) \\
&= 1
\end{aligned}$$

as required. □

We note that this form for the eigenvalues is distinct from the three forms presented in [11, Section 5.1].

Example 5.2.10. Consider the association scheme of skew-symmetric matrices with $t = 4$, then $n = 2$ and $m = 3$. We let the 3 forms presented in [11, Section 5.1], starting with Equation (15), be $P_k(x,n)$, $Q_k(x,n)$ and $R_k(x,n)$ in the order they appear in the paper. Then looking term by term we have the resulting Table 5.2.1 for $k = 1$ and $x = 1$.

Eigenvalues	$j=0$	$j=1$	$\sum_{j=0}^{1}$
$C_1(1,2)$	q^3-1	$-q^2$	q^3-q^2-1
$P_1(1,2)$	$-q^2-1$	q^3	q^3-q^2-1
$Q_1(1,2)$	q^3-q^2	-1	q^3-q^2-1
$R_1(1,2)$	$\left(q^2+1\right)\left(q^3-1\right)$	$-q^5$	q^3-q^2-1

Table 5.2.1: Components of the eigenvalues for $C_k(x,n)$ compared to others

We can clearly see in this example that the sum of the terms is the same, but the individual components cannot be equated on a term by term basis.

5.2.4 Weight Functions

Given that we are only working with translation association schemes where the set of points $\mathscr{X}$ is a vector space, we can always attribute a weight function for that scheme since we will always have a distance between points and a 0 element. Mathematically speaking, if we let $(\mathscr{X},R)$ be an n-class translation scheme, we say that if x,y are n distance apart, then $(x,y)\in R_n$. Since $\mathscr{X}$ is a vector space, then $x-y,0\in\mathscr{X}$. Consequently, since x,y are distance n apart, then $(x-y,0)\in R_n$ also.

Definition 5.2.11. For an $(\mathscr{X},R)$ n-class Krawtchouk association scheme and $x\in\mathscr{X}$, we define the ***scheme weight*** of x to be ω if and only if $(x,0)\in R_\omega$.

Definition 5.2.12. For an $(\mathscr{X},R)$ n-class Krawtchouk association scheme, and for all $x\in\mathscr{X}$ of weight ω, the ***scheme weight function*** of x, denoted $f_S(x)$, is defined as the homogeneous polynomial

$$f_S(x)=Y^\omega X^{n-\omega}.$$

Now let $\mathscr{C}\subseteq\mathscr{X}$ be a code. Suppose there are c_i codewords in $\mathscr{C}$ with weight i for $0\leq i\leq n$. Then the ***scheme weight enumerator*** of $\mathscr{C}$, denoted $W_{\mathscr{C}}^S(X,Y)$, is defined as,

$$W_{\mathscr{C}}^S(X,Y)=\sum_{\zeta\in\mathscr{C}}f_S(\zeta)=\sum_{i=0}^{n}c_iY^iX^{n-i}.$$

The $(n+1)$-tuple, $\boldsymbol{c}=(c_0,\ldots,c_n)$ of coefficients of the weight enumerator is called the ***scheme weight distribution*** of the code $\mathscr{C}$.

We note that since we are only working with metric association schemes, we can always define the ***minimum distance*** of a code $\mathscr{C}$. Denoted $d_S(\mathscr{C})$ or d_S, it is simply the minimum distance between all possible pairs of codewords in $\mathscr{C}$, dependent on the metric being used.

In previous chapters we have looked at counting the number of elements of a particular weight in the overall space individually using a combinatorial approach. In contrast here we use the valencies of the association scheme to identify those values in general.

Theorem 5.2.13. *For $b, c \in \mathbb{R}$, $b \in \mathbb{R}$, $b \neq 1$, $cb > 1$ the number of elements, $x \in \mathscr{X}$ with weight ω in an $(\mathscr{X}, R)$ n-class Krawtchouk association scheme is*

$$\xi_{n,\omega} = \begin{bmatrix} n \\ \omega \end{bmatrix} \gamma_{b,c}(n, \omega). \tag{5.2.29}$$

Proof. The number of elements of weight ω, is the ω^{th} valency of the Krawtchouk association scheme. Since the ω^{th} valency is the initial value $P_\omega(0, n)$, the statement is proved. □

A direct consequence of this is the ability to find the scheme weight enumerator of $\mathscr{X}$, denoted Ω_n, as

$$\Omega_n = \sum_{i=0}^{n} \xi_{n,i} Y^i X^{n-i}. \tag{5.2.30}$$

As a reminder, we rewrite the MacWilliams Identity, Theorem 2.3.15, formulated by Delsarte [8, (6.9)]. We note that in this chapter we are only considering formally self dual association schemes, i.e. when the eigenmatrices P and Q are the same.

Theorem 5.2.14 (The MacWilliams Identity for Association Schemes)**.** *Let $(\mathscr{X}, R)$ be an n-class Krawtchouk association scheme with dual n-class Krawthouck association scheme $(\mathscr{X}, R')$. For a pair of dual subgroups $X, X' \subseteq \mathscr{X}$, let $\boldsymbol{c} = (c_0, \ldots, c_n)$ be the inner distribution of X and $\boldsymbol{c'} = (c'_0, \ldots c'_n)$ be the inner distribution of X'. If P and Q are the eigenmatrices of $(\mathscr{X}, R)$ then*

$$|X|\boldsymbol{c'} = \boldsymbol{c}Q$$
$$|X'|\boldsymbol{c} = \boldsymbol{c'}P.$$

5.3 The b-Algebra

As seen from the individual association schemes, the weight enumerators of any linear code $\mathscr{C} \subseteq \mathscr{X}$ are homogeneous polynomials. We can now generalise the various "q-algebras" into a succinct b-algebra, which can be used in all settings. This helps us express the relations between the weight enumerator of a code and the weight enumerator of the code's dual.

5.3.1 The b-Product, b-Power and b-Transform

Definition 5.3.1. Let

$$a(X, Y; \lambda) = \sum_{i=0}^{r} a_i(\lambda) Y^i X^{r-i}$$
$$b(X, Y; \lambda) = \sum_{i=0}^{s} b_i(\lambda) Y^i X^{s-i}$$

be two homogeneous polynomials in X and Y with coefficients $a_i(\lambda)$ and $b_i(\lambda)$ respectively, which are real functions of λ and are 0 unless otherwise specified. For example $b_i(\lambda) = 0$ if

$i \notin \{0, 1, \ldots, s\}$. The b-***product***, $*$, of $a(X, Y; \lambda)$ and $b(X, Y; \lambda)$ is defined as

$$\begin{aligned} c(X, Y; \lambda) &= a(X, Y; \lambda) * b(X, Y; \lambda) \qquad (5.3.1) \\ &= \sum_{u=0}^{r+s} c_u(\lambda) Y^u X^{r+s-u} \qquad (5.3.2) \end{aligned}$$

with

$$c_u(\lambda) = \sum_{i=0}^{u} b^{is} a_i(\lambda) b_{u-i}(\lambda - i).$$

We note that as with the q-product in [22, Lemma 1], the b-product is not commutative or distributive in general. However, if $a(X, Y; \lambda) = a$ is a constant independent of λ, the following two properties holds:

$$a * b(X, Y; \lambda) = b(X, Y; \lambda) * a = ab(X, Y; \lambda).$$

Separately if the degree of $a(X, Y; \lambda)$ and $c(X, Y; \lambda)$ are the same then,

$$\begin{aligned} \Big(a(X, Y; \lambda) + c(X, Y; \lambda)\Big) * b(X, Y; \lambda) = a(X, Y; \lambda) * b(X, Y; \lambda) \\ + c(X, Y; \lambda) * b(X, Y; \lambda) \end{aligned}$$

and

$$\begin{aligned} b(X, Y; \lambda) * \Big(a(X, Y; \lambda) + c(X, Y; \lambda)\Big) = b(X, Y; \lambda) * a(X, Y; \lambda) \\ + b(X, Y; \lambda) * c(X, Y; \lambda). \end{aligned}$$

Definition 5.3.2. For $a(X, Y; \lambda) = \sum_{i=0}^{r} a_i(\lambda) Y^i X^{r-i}$ the b-***power*** is defined by

$$\begin{aligned} &a^{[0]}(X, Y; \lambda) = 1 \\ &a^{[1]}(X, Y; \lambda) = a(X, Y; \lambda) \\ &a^{[k]}(X, Y; \lambda) = a(X, Y; \lambda) * a^{[k-1]}(X, Y; \lambda) \quad \text{for } k \geq 2. \end{aligned}$$

Definition 5.3.3 ([22, Definition 4])**.** Let $a(X, Y; \lambda) = \sum_{u=0}^{r} a_i(\lambda) Y^i X^{r-i}$. We define the b-***transform*** to be the homogeneous polynomial

$$\overline{a}(X, Y; \lambda) = \sum_{i=0}^{r} a_i(\lambda) Y^{[i]} * X^{[r-i]}.$$

5.3.2 Fundamental Polynomials

We can now also generalise what we call the “fundamental polynomials” which is one of the key tools used in proving the MacWilliams Identity previously in each setting. Let

$$\mu(X,Y;\lambda) = X + \left(cb^{\lambda} - 1\right) Y \tag{5.3.3}$$

where b and c are constants related to the space under consideration. The b-powers of $\mu(X,Y;n)$ provide an explicit form for the weight enumerator of $(\mathscr{X}, R)$, the Krawtchouk association scheme with n classes.

Theorem 5.3.4. *If $\mu(X,Y;\lambda)$ is as defined above, then*

$$\mu^{[k]}(X,Y;\lambda) = \sum_{u=0}^{k} \mu_u(\lambda,k) Y^u X^{k-u} \quad \textit{for } k \geq 1, \tag{5.3.4}$$

where

$$\mu_u(\lambda,k) = \begin{bmatrix} k \\ u \end{bmatrix} \gamma_{b,c}(\lambda,u).$$

Specifically, the weight enumerators for $(\mathscr{X}, R)$, the n-class Krawtchouk association scheme, denoted by Ω_n, is given by

$$\Omega_n = \mu^{[n]}(X,Y;n).$$

Proof. The proof follows the method of induction. Consider $k = 1$, so

$$\mu^{[1]}(X,Y;\lambda) = \mu(X,Y;\lambda) = X + \left(cb^{\lambda} - 1\right) Y.$$

Then

$$\mu_0(\lambda,1) = 1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \gamma_{b,c}(\lambda,0)$$
$$\mu_1(\lambda,1) = \left(cb^{\lambda} - 1\right) = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \gamma_{b,c}(\lambda,1).$$

So

$$\mu_u(\lambda,1) = \begin{bmatrix} 1 \\ u \end{bmatrix} \gamma_{b,c}(\lambda,u)$$

and

$$\Omega_1 = \sum_{i=0}^{1} \begin{bmatrix} 1 \\ u \end{bmatrix} \gamma_{b,c}(\lambda,u) Y^i X^{1-i} = \mu^{[1]}(X,Y;1)$$

as required for $k = 1$. Now assume the theorem is true for $k \geq 1$. Then

$$\begin{aligned}\mu^{[k+1]}(X, Y; \lambda) &= \mu(X, Y; \lambda) * \mu^{[k]}(X, Y; \lambda)\\ &= \left(X + \left(cb^{\lambda} - 1\right) Y\right) * \left(\sum_{u=0}^{k} \begin{bmatrix} k \\ u \end{bmatrix} \gamma_{b,c}(\lambda, u) Y^u X^{k-u}\right)\\ &= \sum_{i=0}^{k+1} f_i(\lambda) Y^i X^{k+1-i}\end{aligned}$$

where,

$$\begin{aligned}f_i(\lambda) &= \sum_{j=0}^{i} b^{jk} \mu_j(\lambda, 1) \mu_{i-j}(\lambda - j, k)\\ &= \mu_0(\lambda, 1)\mu_i(\lambda, k) + b^k \mu_1(\lambda, 1)\mu_{i-1}(\lambda - 1, k)\\ &= \begin{bmatrix} k \\ i \end{bmatrix} \gamma_{b,c}(\lambda, i) + b^k \left(cb^{\lambda} - 1\right) \begin{bmatrix} k \\ i-1 \end{bmatrix} \gamma_{b,c}(\lambda - 1, i - 1)\\ &\overset{(5.2.16)(5.2.9)(5.2.10)}{=} \frac{b^{k-i+1} - 1}{b^{k+1} - 1} \begin{bmatrix} k+1 \\ i \end{bmatrix} \gamma_{b,c}(\lambda, i) + b^k \frac{b^i - 1}{b^{k+1} - 1} b^{1-i} \begin{bmatrix} k+1 \\ i \end{bmatrix} \gamma_{b,c}(\lambda, i)\\ &= \gamma_{b,c}(\lambda, i) \begin{bmatrix} k+1 \\ i \end{bmatrix} \left(\frac{b^{k-i+1} - 1 + b^{k-i+1}\left(b^i - 1\right)}{b^{k+1} - 1}\right)\\ &= \gamma_{b,c}(\lambda, i) \begin{bmatrix} k+1 \\ i \end{bmatrix}\end{aligned}$$

since for $i \geq 1$ we only need to consider the first two coefficients as when $j \geq 2$ then $\mu_j(\lambda, 1) = \left[\begin{smallmatrix} 1 \\ j \end{smallmatrix}\right] \gamma(\lambda, j) = 0$ since $\left[\begin{smallmatrix} 1 \\ j \end{smallmatrix}\right] = 0$ when $j \geq 2$. So it is true for $k + 1$. Therefore by induction the first part of the theorem is true. Now consider $\mu^{[n]}(X, Y; n)$, then clearly

$$\begin{aligned}\mu^{[n]}(X, Y; n) &= \sum_{u=0}^{n} \begin{bmatrix} n \\ u \end{bmatrix} \gamma_{b,c}(n, u) Y^u X^{n-u}\\ &\overset{(5.2.29)}{=} \sum_{u=0}^{n} \xi_{n,u} Y^u X^{n-u} \overset{(5.2.30)}{=} \Omega_n\end{aligned}$$

as required. □

Now for the other fundamental polynomial. Interestingly we let $\nu(X, Y; \lambda) = X - Y$, which is the exact same polynomial in all the cases previously studied.

Theorem 5.3.5. *For all $k \geq 1$,*

$$\nu^{[k]}(X, Y; \lambda) = \sum_{u=0}^{k} \nu_u(\lambda, k) Y^u X^{k-u} \tag{5.3.5}$$

where

$$\nu_u(\lambda, k) = (-1)^u b^{\sigma_u} \begin{bmatrix} k \\ u \end{bmatrix}.$$

Proof. We perform induction on k. For $k = 1$ we have

$$\nu^{[1]}(X, Y; \lambda) = \nu(X, Y; \lambda) = X - Y.$$

Clearly we also have

$$(-1)^0 b^{\sigma_0} \begin{bmatrix} 1 \\ 0 \end{bmatrix} Y^0 X^1 + (-1)^1 b^{\sigma_1} \begin{bmatrix} 1 \\ 1 \end{bmatrix} Y^1 X^0 = X - Y$$

as required. Now assume the theorem holds for $k \geq 1$.

$$\begin{aligned} \nu^{[k+1]}(X, Y; \lambda) &= \nu(X, Y; \lambda) * \nu^{[k]}(X, Y; \lambda) \\ &= (X - Y) * \left(\sum_{u=0}^{k} (-1)^u b^{\sigma_u} \begin{bmatrix} k \\ u \end{bmatrix} Y^u X^{k-u} \right) \\ &= \sum_{i=0}^{k+1} g_i(\lambda) Y^i X^{k+1-i} \end{aligned}$$

where

$$\begin{aligned} g_i(\lambda) &= \sum_{j=0}^{i} b^{jk} \nu_j(\lambda, 1) \nu_{i-j}(\lambda - j, k) \\ &= b^0(1)(-1)^i b^{\sigma_i} \begin{bmatrix} k \\ i \end{bmatrix} + b^k(-1)(-1)^{i-1} b^{\sigma_{i-1}} \begin{bmatrix} k \\ i-1 \end{bmatrix} \\ &\overset{(5.2.9)(5.2.10)}{=} (-1)^i b^{\sigma_i} \frac{b^{k+1-i} - 1}{b^{k+1} - 1} \begin{bmatrix} k+1 \\ i \end{bmatrix} + b^k (-1)^i b^{\sigma_{i-1}} \frac{b^i - 1}{b^{k+1} - 1} \begin{bmatrix} k+1 \\ i \end{bmatrix} \\ &= (-1)^i b^{\sigma_i} \begin{bmatrix} k+1 \\ i \end{bmatrix} \left\{ \frac{b^{k+1-i} - 1}{b^{k+1} - 1} + b^k b^{1-i} \frac{b^i - 1}{b^{k+1} - 1} \right\} \\ &= (-1)^i \frac{b^{\sigma_i}}{b^{k+1} - 1} \begin{bmatrix} k+1 \\ i \end{bmatrix} \left\{ b^{k+1-i} - 1 + b^{k+1} - b^{k+1-i} \right\} \\ &= (-1)^i b^{\sigma_i} \begin{bmatrix} k+1 \\ i \end{bmatrix} \end{aligned}$$

since for $i \geq 1$ we only need to consider the first two coefficients as when $j \geq 2$ then $\nu_j(\lambda, 1) = 0$ as since $\left[\begin{smallmatrix} 1 \\ j \end{smallmatrix}\right] = 0$ when $j \geq 2$, thus the statement holds. □

5.4 The Generalised MacWilliams Identity

We can now begin to put the final pieces of the puzzle together to be able to state and prove the MacWilliams Identity for a n-class Krawtchouk association scheme. Since we have proven that the $C_k(x, n)$ are also eigenvalues of the Krawtchouk association scheme, we can then invoke Delsarte's MacWilliams Identity (Theorem 2.3.15) in the proof of our functional transform version.

5.4.1 Generalised MacWilliams Identity

As a reminder from Section 2.3.3, since we are considering Krawtchouk association schemes where $\mathscr{X}$ is a finite abelian group and so we can define an inner product on the space $\mathscr{X}$ [3, p72]. Then we can define for any subgroup (code), $\mathscr{C}$, of $\mathscr{X}$, a dual subgroup (dual code), $\mathscr{C}^{\perp}$ such that

$$\mathscr{C}^{\perp} = \Big\{ x \in \mathscr{X} \mid \langle x, y \rangle = 0 \ \forall \ y \in \mathscr{C} \Big\}.$$

Finally, the one we've been waiting for, we can write a generalised MacWilliams Identity as a functional transform for an $(\mathscr{X}, R)$ n-class Krawtchouk association scheme. Let the weight enumerator of $\mathscr{C} \subseteq \mathscr{X}$ be,

$$W^S_{\mathscr{C}}(X,Y) = \sum_{i=0}^{n} c_i Y^i X^{n-i}$$

and of its dual, $\mathscr{C}^{\perp} \subseteq \mathscr{X}$ be

$$W^S_{\mathscr{C}^{\perp}}(X,Y) = \sum_{i=0}^{n} c'_i Y^i X^{n-i}.$$

Theorem 5.4.1 (The MacWilliams Identity for an n-class Krawtchouk Association Scheme)**.** *Let $\mathscr{C} \subseteq \mathscr{X}$ be an linear $[n,k,d_S]$-code, with weight distribution $\boldsymbol{c} = (c_0, \dots, c_n)$ and $\mathscr{C}^{\perp} \subseteq \mathscr{X}$ its dual code, with weight distribution $\boldsymbol{c'} = (c'_0, \dots, c'_n)$. Then*

$$W^S_{\mathscr{C}^{\perp}}(X,Y) = \frac{1}{|\mathscr{C}|} \overline{W}^S_{\mathscr{C}} \left(X + (cb^n - 1)Y, X - Y\right) \tag{5.4.1}$$

$$= \frac{1}{|\mathscr{C}|} \sum_{i=0}^{n} c_i (X-Y)^{[i]} * \left(X + (cb^n - 1)\, Y\right)^{[n-i]}. \tag{5.4.2}$$

Proof. For $0 \leq i \leq n$ we have

$$\begin{aligned}
&(X-Y)^{[i]} * \left(X + (cb^n - 1)\, Y\right)^{[n-i]} \\
&\quad = \Big(\nu^{[i]}(X,Y;n)\Big) * \Big(\mu^{[n-i]}(X,Y;n)\Big) \\
&\quad \overset{(5.3.4)(5.3.5)}{=} \left(\sum_{u=0}^{i} (-1)^u b^{\sigma_u} \begin{bmatrix} i \\ u \end{bmatrix} Y^u X^{i-u} \right) * \left(\sum_{j=0}^{n-i} \begin{bmatrix} n-i \\ j \end{bmatrix} \gamma_{b,c}(n,j) Y^j X^{n-i-j} \right) \\
&\quad \overset{(5.3.1)}{=} \sum_{k=0}^{t} \left(\sum_{\ell=0}^{k} (-1)^{\ell} b^{\ell(n-x)} b^{\sigma_\ell} \begin{bmatrix} x \\ \ell \end{bmatrix} \begin{bmatrix} n-x \\ k-\ell \end{bmatrix} \gamma_{b,c}(n-\ell, k-\ell) \right) Y^k X^{n-k} \\
&\quad = \sum_{k=0}^{n} C_k(i,n) Y^k X^{n-k}.
\end{aligned}$$

So then we have

$$\begin{aligned}\frac{1}{|\mathscr{C}|}\overline{W}^S_{\mathscr{C}}\left(X+\left(cb^n-1\right)Y, X-Y\right) &= \frac{1}{|\mathscr{C}|}\sum_{i=0}^{n} c_i \left(X-Y\right)^{[i]} * \left(X+\left(cb^n-1\right)Y\right)^{[n-i]}\\ &= \frac{1}{|\mathscr{C}|}\sum_{i=0}^{n} c_i \sum_{k=0}^{n} C_k(i,n) Y^k X^{n-k}\\ &= \sum_{k=0}^{n}\left(\frac{1}{|\mathscr{C}|}\sum_{i=0}^{n} c_i C_k(i,n)\right) Y^k X^{n-k}\\ &\overset{(5.2.14)}{=} \sum_{k=0}^{n} c'_k Y^k X^{n-k}\\ &= W^S_{\mathscr{C}^\perp}(X,Y).\end{aligned}$$

□

5.5 The b-Derivatives

In this section we develop a derivative. It should be clear that this section essentially reworks Section 4.4 with a more general b-algebra.

5.5.1 The b-Derivative

To begin with, we consider the derivative with respect to X.

Definition 5.5.1. For $b \neq 1$, the ***b-derivative*** at $X \neq 0$ for a real-valued function $f(X)$ is defined as

$$f^{(1)}(X) = \frac{f(bX) - f(X)}{(b-1)X}.$$

For $\varphi \geq 0$ we denote the φ^{th} b-derivative (with respect to X) of $f(X,Y;\lambda)$ as $f^{(\varphi)}(X,Y;\lambda)$. The 0^{th} b-derivative of $f(X,Y;\lambda)$ is $f(X,Y;\lambda)$. For any $a \in \mathbb{R}$, $X \neq 0$, and real-valued function $g(X)$,

$$\Big[f(X) + ag(X)\Big]^{(1)} = f^{(1)}(X) + ag^{(1)}(X).$$

Once again for the Hamming metric we take the formal definition of a derivative and take the limit of the function as $b \to 1$. That is, let $b = 1+h$, $h \in \mathbb{R}$, then the derivative becomes,

$$f^{(1)}(X) = \lim_{h\to 0}\frac{f((1+h)X) - f(X)}{hX}$$

and so converts into the derivative in the usual sense of polynomials [41, Problems (5), p98].

Now we have the definition of a derivative we can demonstrate some important results for homogeneous polynomials in general and the fundamental polynomials in particular.

Lemma 5.5.2.

1. *For* $0 \leq \varphi \leq \ell$, $\varphi \in \mathbb{Z}^+$ *and* $\ell \geq 0$,

$$\left(X^{\ell}\right)^{(\varphi)} = \beta_b(\ell, \varphi) X^{\ell-\varphi}.$$

2. *The* φ^{th} *b-derivative of* $f(X, Y; \lambda) = \sum_{i=0}^{r} f_i(\lambda) Y^i X^{r-i}$ *is given by*

$$f^{(\varphi)}\left(X, Y; \lambda\right) = \sum_{i=0}^{r-\varphi} f_i(\lambda) \beta_b(r-i, \varphi) Y^i X^{r-i-\varphi}. \tag{5.5.1}$$

3. *Also,*

$$\mu^{[k](\varphi)}(X, Y; \lambda) = \beta_b(k, \varphi) \mu^{[k-\varphi]}(X, Y; \lambda) \tag{5.5.2}$$

$$\nu^{[k](\varphi)}(X, Y; \lambda) = \beta_b(k, \varphi) \nu^{[k-\varphi]}(X, Y; \lambda). \tag{5.5.3}$$

Proof.

(1) For $\varphi = 1$ we have

$$\left(X^{\ell}\right)^{(1)} = \frac{(bX)^{\ell} - X^{\ell}}{(b-1)X} = \frac{b^{\ell} - 1}{b-1} X^{\ell-1} = \begin{bmatrix} \ell \\ 1 \end{bmatrix} X^{\ell-1} = \beta_b(\ell, \varphi) X^{\ell-1}.$$

The rest of the proof follows by induction on φ and is omitted.

(2) Now consider $f(X, Y; \lambda) = \sum_{i=0}^{r} f_i(\lambda) Y^i X^{r-i}$. We have,

$$\begin{aligned} f^{(1)}\left(X, Y; \lambda\right) &= \left(\sum_{i=0}^{r} f_i(\lambda) Y^i X^{r-i}\right)^{(1)} \\ &= \sum_{i=0}^{r} f_i(\lambda) Y^i \left(X^{r-i}\right)^{(1)} \\ &= \sum_{i=0}^{r-1} f_i(\lambda) \beta_b(r-i, \varphi) Y^i X^{r-i-1}. \end{aligned}$$

So the initial case holds. The rest of the proof follows by induction on φ and is omitted.

(3) Now consider $\mu^{[k]}(X, Y; \lambda) = \sum_{u=0}^{k} \mu_u(\lambda, k) Y^u X^{k-u}$ where $\mu_u(\lambda, k) = \begin{bmatrix} k \\ u \end{bmatrix} \gamma_{b,c}(\lambda, u)$ as

in Theorem 5.3.4. Then we have

$$\begin{aligned}
\mu^{[k](1)}(X,Y;\lambda) &= \left(\sum_{u=0}^{k}\mu_u(\lambda,k)Y^uX^{k-u}\right)^{(1)}\\
&= \sum_{u=0}^{k}\mu_u(\lambda,k)Y^u\left(\frac{(bX)^{k-u}-X^{k-u}}{(b-1)X}\right)\\
&= \sum_{u=0}^{k-1}\frac{b^{k-u}-1}{b-1}\begin{bmatrix}k\\u\end{bmatrix}\gamma_{b,c}(\lambda,u)Y^uX^{k-u-1}\\
&\overset{(5.2.9)}{=} \sum_{u=0}^{k-1}\frac{(b^k-1)\left(b^{k-u}-1\right)}{(b^{k-u}-1)(b-1)}\begin{bmatrix}k-1\\u\end{bmatrix}\gamma_{b,c}(\lambda,u)Y^uX^{k-u-1}\\
&= \left(\frac{b^k-1}{b-1}\right)\mu^{[k-1]}(X,Y;\lambda)\\
&\overset{(5.2.11)}{=} \beta_b(k,1)\mu^{[k-1]}(X,Y;\lambda)
\end{aligned}$$

So $\mu^{[k](\varphi)}(X,Y;\lambda)=\beta_b(k,\varphi)\mu^{[k-\varphi]}(X,Y;\lambda)$ follows by induction on φ and is omitted. Now consider $\nu^{[k]}(X,Y;\lambda)=\sum_{u=0}^{k}(-1)^ub^{\sigma_u}\begin{bmatrix}k\\u\end{bmatrix}Y^uX^{k-u}$ as in Theorem 5.3.5. Then we have

$$\begin{aligned}
\nu^{[k](1)}(X,Y;\lambda) &= \sum_{u=0}^{k}(-1)^ub^{\sigma_u}\frac{b^{k-u}-1}{b-1}\begin{bmatrix}k\\u\end{bmatrix}Y^uX^{k-u-1}\\
&\overset{(5.2.9)}{=} \sum_{u=0}^{k-1}(-1)^ub^{\sigma_u}\frac{\left(b^k-1\right)\left(b^{k-u}-1\right)}{\left(b^{k-u}-1\right)(b-1)}\begin{bmatrix}k-1\\u\end{bmatrix}Y^uX^{k-1-u}\\
&= \frac{b^k-1}{b-1}\nu^{[k-1]}(X,Y;\lambda)\\
&\overset{(5.2.11)}{=} \beta_b(k,1)\nu^{[k-1]}(X,Y;\lambda).
\end{aligned}$$

So the initial case holds. Thus $\nu^{[k](\varphi)}(X,Y;\lambda)=\beta_b(k,\varphi)\nu^{[k-\varphi]}(X,Y;\lambda)$ follows by induction also and is omitted.

□

We now need a few smaller lemmas in order to prove the Leibniz rule for the b-derivative.

Lemma 5.5.3. *Let*

$$\begin{aligned}
u\left(X,Y;\lambda\right) &= \sum_{i=0}^{r}u_i(\lambda)Y^iX^{r-i}\\
v\left(X,Y;\lambda\right) &= \sum_{i=0}^{s}v_i(\lambda)Y^iX^{s-i}.
\end{aligned}$$

1. *If* $u_r(\lambda)=0$ *then*

$$\frac{1}{X}\Big[u\left(X,Y;\lambda\right)*v\left(X,Y;\lambda\right)\Big]=\frac{u\left(X,Y;\lambda\right)}{X}*v\left(X,Y;\lambda\right). \tag{5.5.4}$$

2. If $v_s(\lambda) = 0$ then

$$\frac{1}{X}\Big[u\left(X, Y; \lambda\right) * v\left(X, Y; \lambda\right)\Big] = u\left(X, bY; \lambda\right) * \frac{v\left(X, Y; \lambda\right)}{X}. \tag{5.5.5}$$

Proof. (1) If $u_r(\lambda) = 0$,

$$\frac{u\left(X, Y; \lambda\right)}{X} = \sum_{i=0}^{r-1} u_i(\lambda) Y^i X^{r-i-1}.$$

Hence

$$\begin{aligned}
\frac{u\left(X, Y; \lambda\right)}{X} * v\left(X, Y; \lambda\right) &= \sum_{k=0}^{r+s-1}\left(\sum_{\ell=0}^{k} b^{\ell s} u_\ell(\lambda) v_{k-\ell}(\lambda - \ell)\right) Y^k X^{r+s-1-k} \\
&= \frac{1}{X}\sum_{k=0}^{r+s-1}\left(\sum_{\ell=0}^{k} b^{\ell s} u_\ell(\lambda) v_{k-\ell}(\lambda - \ell)\right) Y^k X^{r+s-k} \\
&\quad + \frac{1}{X}\sum_{\ell=0}^{r+s} b^{\ell s} u_\ell(\lambda) v_{r+s-\ell}(\lambda - \ell) Y^{r+s} X^0 \\
&= \frac{1}{X}\left(u\left(X, Y; \lambda\right) * v\left(X, Y; \lambda\right)\right)
\end{aligned}$$

since $v_{r+s-\ell}(\lambda - \ell) = 0$ for $0 \leq \ell \leq r-1$ and $u_\ell(\lambda) = 0$ for $r \leq \ell \leq r+s$. So

$$\frac{1}{X}\sum_{\ell=0}^{r+s} b^{\ell s} u_\ell(\lambda) v_{r+s-\ell}(\lambda - \ell) Y^{r+s} X^0 = 0.$$

(2) Now if $v_s(\lambda) = 0$,

$$\frac{v\left(X, Y; \lambda\right)}{X} = \sum_{i=0}^{s-1} v_i(\lambda) Y^i X^{s-1-i}.$$

Then

$$\begin{aligned}
u\left(X, bY; \lambda\right) * \frac{v\left(X, Y; \lambda\right)}{X} &= \sum_{k=0}^{r+s-1}\left(\sum_{\ell=0}^{k} b^{\ell(s-1)} b^{\ell} u_\ell(\lambda) v_{k-\ell}(\lambda - \ell)\right) Y^k X^{r+s-1-k} \\
&= \sum_{k=0}^{r+s-1}\left(\sum_{\ell=0}^{k} b^{\ell(s-1)} b^{\ell} u_\ell(\lambda) v_{k-\ell}(\lambda - \ell)\right) Y^k X^{r+s-1-k} \\
&\quad + \frac{1}{X}\sum_{\ell=0}^{r+s} b^{\ell s} u_\ell(\lambda) v_{r+s-\ell}(\lambda - \ell) Y^{r+s} X^0 \\
&= \frac{1}{X}\left[u(X, Y; \lambda) * v(X, Y; \lambda)\right]
\end{aligned}$$

since $v_{r+s-\ell}(\lambda - \ell) = 0$ for $0 \leq \ell \leq r$ and $u_\ell = 0$ for $r+1 \leq \ell \leq r+s$. □

Theorem 5.5.4 (Leibniz rule for the b-derivative)**.** *For two homogeneous polynomials in X and Y, $f(X, Y; \lambda)$ and $g(X, Y; \lambda)$ with degrees r and s respectively, the φ^{th} (for $\varphi \geq 0$) b-derivative of their b-product is given by*

$$\Big[f\left(X, Y; \lambda\right) * g\left(X, Y; \lambda\right)\Big]^{(\varphi)} = \sum_{\ell=0}^{\varphi} \begin{bmatrix}\varphi \\ \ell\end{bmatrix} b^{(\varphi-\ell)(r-\ell)} f^{(\ell)}\left(X, Y; \lambda\right) * g^{(\varphi-\ell)}\left(X, Y; \lambda\right). \tag{5.5.6}$$

Proof. For simplification, we shall write $f(X,Y;\lambda)$ as $f(X,Y)$ and similarly $g(X,Y;\lambda)$ as $g(X,Y)$. Now by differentiation we have

$$\begin{aligned}
\Big[f\left(X,Y\right)*g\left(X,Y\right)\Big]^{(1)} &= \frac{f\left(bX,Y\right)*g\left(bX,Y\right)-f\left(X,Y\right)*g\left(X,Y\right)}{(b-1)X}\\
&= \frac{1}{(b-1)X}\Big\{f\left(bX,Y\right)*g\left(bX,Y\right)-f\left(bX,Y\right)*g\left(X,Y\right)\\
&\qquad +f\left(bX,Y\right)*g\left(X,Y\right)-f\left(X,Y\right)*g\left(X,Y\right)\Big\}\\
&= \frac{1}{(b-1)X}\Big\{f\left(bX,Y\right)*\left(g\left(bX,Y\right)-g\left(X,Y\right)\right)\Big\}\\
&\qquad +\frac{1}{(b-1)X}\Big\{\left(f\left(bX,Y\right)-f\left(X,Y\right)\right)*g\left(X,Y\right)\Big\}\\
&\overset{(5.5.5)}{=} f\left(bX,bY\right)*\left\{\frac{g\left(bX,Y\right)-g\left(X,Y\right)}{(b-1)X}\right\}\\
&\qquad \overset{(5.5.4)}{+}\left\{\frac{f\left(bX,Y\right)-f\left(X,Y\right)}{(b-1)X}\right\}*g\left(X,Y\right)\\
&= b^{r}f\left(X,Y\right)*g^{(1)}\left(X,Y\right)+f^{(1)}\left(X,Y\right)*g\left(X,Y\right)
\end{aligned}$$

since $g(X,Y)$ has the same degree of $g(bX,Y)$ and similarly, $f(X,Y)$ has the same degree as $f(bX,Y)$. So the initial case holds. Assume the statement holds true for $\varphi=\overline{\varphi}$, i.e.

$$\Big[f\left(X,Y\right)*g\left(X,Y\right)\Big]^{(\overline{\varphi})} = \sum_{\ell=0}^{\overline{\varphi}}\begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix}b^{(\overline{\varphi}-\ell)(r-\ell)}f^{(\ell)}\left(X,Y\right)*g^{(\overline{\varphi}-\ell)}\left(X,Y\right).$$

Now considering $\overline{\varphi}+1$ and for simplicity we write $f(X,Y;\lambda),\ g(X,Y;\lambda)$ as f,g we have

$$\begin{aligned}
\Big[f*g\Big]^{(\overline{\varphi}+1)} &= \left[\sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{(\overline{\varphi}-\ell)(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}-\ell)}\right]^{(1)} \\
&= \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{(\overline{\varphi}-\ell)(r-\ell)} \Big[f^{(\ell)} * g^{(\overline{\varphi}-\ell)}\Big]^{(1)} \\
&= \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{(\overline{\varphi}-\ell)(r-\ell)} \Big(b^{(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}-\ell+1)} + f^{(\ell+1)} * g^{(\overline{\varphi}-\ell)}\Big) \\
&= \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{(\overline{\varphi}-\ell+1)(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}-\ell+1)} \\
&\qquad + \sum_{\ell=1}^{\overline{\varphi}+1} \begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix} b^{(\overline{\varphi}-\ell+1)(r-\ell+1)} f^{(\ell)} * g^{(\overline{\varphi}-\ell+1)} \\
&= \begin{bmatrix}\overline{\varphi}\\ 0\end{bmatrix} b^{(\overline{\varphi}+1)r} f * g^{(\overline{\varphi}+1)} + \sum_{\ell=1}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{(\overline{\varphi}+1-\ell)(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}-\ell+1)} \\
&\qquad + \begin{bmatrix}\overline{\varphi}\\ \overline{\varphi}\end{bmatrix} b^{(\overline{\varphi}+1-\overline{\varphi}-1)(r-\overline{\varphi}-1+1)} f^{(\overline{\varphi}+1)} * g \\
&\qquad + \sum_{\ell=1}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix} b^{(\overline{\varphi}+1-\ell)(r-\ell+1)} f^{(\ell)} * g^{(\overline{\varphi}-\ell+1)} \\
&= b^{(\overline{\varphi}+1)r} f * g^{(\overline{\varphi}+1)} + f^{(\overline{\varphi}+1)} * g \\
&\qquad + \sum_{\ell=1}^{\overline{\varphi}} \left(\begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} + b^{(\overline{\varphi}-\ell+1)} \begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix}\right) b^{(\overline{\varphi}-\ell+1)(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}-\ell+1)} \\
&\overset{(5.2.6)}{=} \sum_{\ell=1}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}+1\\ \ell\end{bmatrix} b^{(\overline{\varphi}+1-\ell)(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}+1-\ell)} + \begin{bmatrix}\overline{\varphi}+1\\ 0\end{bmatrix} b^{(\overline{\varphi}+1)(r)} f * g^{(\overline{\varphi}+1)} \\
&\qquad + \begin{bmatrix}\overline{\varphi}+1\\ \overline{\varphi}+1\end{bmatrix} b^{(\overline{\varphi}-1-\overline{\varphi}-1)} f^{(\overline{\varphi}+1)} * g \\
&= \sum_{\ell=0}^{\overline{\varphi}+1} \begin{bmatrix}\overline{\varphi}+1\\ \ell\end{bmatrix} b^{(\overline{\varphi}+1-\ell)(r-\ell)} f^{(\ell)} * g^{(\overline{\varphi}+1-\ell)}.
\end{aligned}$$

□

5.5.2 The b^{-1}-Derivative

Essentially, since the b-derivative finds a derivative with respect to X it is natural to identify a comparable b^{-1}-derivative which can be used to develop a derivative with respect to Y.

Definition 5.5.5. For $b \neq 1$, the b^{-1}***-derivative*** at $Y \neq 0$ for a real-valued function $g(Y)$ is defined as

$$g^{\{1\}}(Y) = \frac{g\left(b^{-1}Y\right) - g(Y)}{(b^{-1}-1)Y}.$$

For $\varphi \geq 0$ we denote the φ^{th} b^{-1}-derivative (with respect to Y) of $g(X,Y;\lambda)$ as $g^{\{\varphi\}}(X,Y;\lambda)$. The 0^{th} b^{-1}-derivative of $g(X,Y;\lambda)$ is $g(X,Y;\lambda)$. For any $a \in \mathbb{R},\ Y \neq 0$ and real-valued function $f(Y)$,

$$\Big[f(Y)+ag(Y)\Big]^{\{1\}}=f^{\{1\}}(Y)+ag^{\{1\}}(Y).$$

Again for the Hamming metric, we take the formal definition of a derivative and take the limit of the function as $b\to 1$, i.e. let $b^{-1}=1+h$, $h\in\mathbb{R}$. Then the derivative becomes,

$$g^{\{1\}}(Y)=\lim_{h\to 0}\frac{g((1+h)Y)-g(Y)}{hY}$$

and so again converts into the derivative in the usual sense of polynomials [41, Problems (5), p98] with respect to Y.

Similar to the b-derivative, since we have the definition of a derivative now with respect to Y we can demonstrate some important results for homogeneous polynomials in general and the fundamental polynomials in particular.

Lemma 5.5.6.

1. *For* $0\le\varphi\le\ell$, $\varphi\in\mathbb{Z}^+$ *and* $\ell\ge 0$,

$$\left(Y^{\ell}\right)^{\{\varphi\}}=b^{\varphi(1-\ell)+\sigma_\varphi}\beta_b(\ell,\varphi)Y^{\ell-\varphi}.$$

2. *The* φ^{th} b^{-1}*-derivative of* $g(X,Y;\lambda)=\sum_{i=0}^{s}g_i(\lambda)Y^iX^{s-i}$ *is given by*

$$g^{\{\varphi\}}\left(X,Y;\lambda\right)=\sum_{i=\varphi}^{s}g_i(\lambda)b^{\varphi(1-i)+\sigma_\varphi}\beta_b(i,\varphi)Y^{i-\varphi}X^{s-i}. \tag{5.5.7}$$

3. *Also,*

$$\mu^{[k]\{\varphi\}}(X,Y;\lambda)=b^{-\sigma_\varphi}\beta_b(k,\varphi)\gamma_{b,c}(\lambda,\varphi)\mu^{[k-\varphi]}(X,Y;\lambda-\varphi) \tag{5.5.8}$$

$$\nu^{[k]\{\varphi\}}(X,Y;\lambda)=(-1)^{\varphi}\beta_b(k,\varphi)\nu^{[k-\varphi]}(X,Y;\lambda). \tag{5.5.9}$$

Proof.

(1) For $\varphi=1$ we have

$$\begin{aligned}\left(Y^{\ell}\right)^{\{1\}}=\frac{\left(b^{-1}Y\right)^{\ell}-Y^{\ell}}{(b^{-1}-1)Y}&=\left(\frac{b^{-\ell}-1}{b^{-1}-1}\right)Y^{\ell-1}\\&=\frac{bb^{-\ell}\left(1-b^{\ell}\right)}{1-b}Y^{\ell-1}\\&=b^{1-\ell}\beta_b(\ell,1)Y^{\ell-1}.\end{aligned}$$

So the initial case holds. Assume the case for $\varphi = \overline{\varphi}$ holds. Then we have

$$\begin{aligned}
\left(Y^{\ell}\right)^{\{\overline{\varphi}+1\}} &= \left(b^{\overline{\varphi}(1-\ell)+\sigma_{\overline{\varphi}}}\beta_b(\ell,\overline{\varphi})Y^{\ell-\overline{\varphi}}\right)^{\{1\}} \\
&= b^{\overline{\varphi}(1-\ell)+\sigma_{\overline{\varphi}}}\beta_b(\ell,\overline{\varphi})\frac{b^{-(\ell-\overline{\varphi})}Y^{\ell-\overline{\varphi}} - Y^{\ell-\overline{\varphi}}}{\left(b^{-1}-1\right)Y} \\
&= b^{\overline{\varphi}(1-\ell)+\sigma_{\overline{\varphi}}}\beta_b(\ell,\varphi)b^{1-(\ell-\overline{\varphi})}\beta_b(\ell-\overline{\varphi},1)Y^{\ell-\overline{\varphi}-1} \\
&\overset{(5.2.14)}{=} b^{(\overline{\varphi}+1)(1-\ell)+\sigma_{\overline{\varphi}+1}}\beta_b(\ell,\overline{\varphi}+1)Y^{\ell-(\overline{\varphi}+1)}.
\end{aligned}$$

Thus the statement holds by induction.

(2) Now consider $g(X,Y;\lambda) = \sum_{i=0}^{s} g_i(\lambda)Y^iX^{s-i}$. For $\varphi = 1$ we have

$$\begin{aligned}
g^{\{1\}}\left(X,Y;\lambda\right) &= \left(\sum_{i=0}^{s} g_i(\lambda)Y^iX^{s-i}\right)^{\{1\}} \\
&= \sum_{i=0}^{s} g_i(\lambda)\left(Y^i\right)^{\{1\}}X^{s-i} \\
&= \sum_{i=0}^{s} g_i(\lambda)b^{-i+1}\beta_b(i,1)Y^{i-1}X^{s-i}.
\end{aligned}$$

As $\beta_b(i,1) = 0$ when $i = 0$ and $\sigma_1 = 0$ then we have

$$g^{\{1\}}\left(X,Y;\lambda\right) = \sum_{i=1}^{s} g_i(\lambda)b^{1-i+\sigma_1}\beta_b(i,1)Y^{i-1}X^{s-i}.$$

So the initial case holds. Now assume the case holds for $\varphi = \overline{\varphi}$ i.e.

$$g^{\{\overline{\varphi}\}}\left(X,Y;\lambda\right) = \sum_{i=\overline{\varphi}}^{s} g_i(\lambda)b^{\overline{\varphi}(1-i)+\sigma_{\overline{\varphi}}}\beta_b(i,\overline{\varphi})Y^{i-\overline{\varphi}}X^{s-i}.$$

Then we have

$$\begin{aligned}
g^{\{\overline{\varphi}+1\}}\left(X,Y;\lambda\right) &= \left(\sum_{i=\overline{\varphi}}^{s} g_i(\lambda)b^{\overline{\varphi}(1-i)+\sigma_{\overline{\varphi}}}\beta_b(i,\overline{\varphi})Y^{i-\overline{\varphi}}\right)^{\{1\}} X^{s-i} \\
&= \sum_{i=\overline{\varphi}}^{s} g_i(\lambda)b^{\overline{\varphi}(1-i)+\sigma_{\overline{\varphi}}}\beta_b(i,\overline{\varphi})b^{-(i-\overline{\varphi}-1)}\beta_b(i-\overline{\varphi},1)Y^{i-\overline{\varphi}-1}X^{s-i} \\
&\overset{(5.2.11)}{=} \sum_{i=\overline{\varphi}}^{s} g_i(\lambda)b^{(\overline{\varphi}+1)(1-i)+\sigma_{\overline{\varphi}}}\prod_{j=0}^{\overline{\varphi}-1}\frac{\left(b^{i-j}-1\right)\left(b^{i-\overline{\varphi}}-1\right)}{(b-1)(b-1)}Y^{i-\overline{\varphi}-1}X^{s-i} \\
&= \sum_{i=\overline{\varphi}}^{s} g_i(\lambda)b^{(\overline{\varphi}+1)(1-i)+\sigma_{\overline{\varphi}+1}}\beta_b(i,\overline{\varphi}+1)Y^{i-\overline{\varphi}-1}X^{s-i} \\
&= \sum_{i=\overline{\varphi}+1}^{s} g_i(\lambda)b^{(\overline{\varphi}+1)(1-i)+\sigma_{\overline{\varphi}+1}}\beta_b(i,\overline{\varphi}+1)Y^{i-\overline{\varphi}-1}X^{s-i}
\end{aligned}$$

since when $i = \overline{\varphi}$, $\beta_b(\overline{\varphi},\overline{\varphi}+1) = 0$. So by induction Equation (5.5.7) holds.

(3) Now consider $\mu^{[k]}(X,Y;\lambda)=\sum_{u=0}^{k}\mu_u(\lambda,k)Y^uX^{k-u}$ where $\mu_u(\lambda,k)=\begin{bmatrix}k\\u\end{bmatrix}\gamma_{b,c}(\lambda,u)$ as in Theorem 5.3.4. Then we have

$$\begin{aligned}
\mu^{[k]\{1\}}(X,Y;\lambda) &= \left(\sum_{u=0}^{k}\mu_u(\lambda,k)Y^uX^{k-u}\right)^{\{1\}}\\
&\overset{(5.5.7)}{=} \sum_{u=1}^{k}\mu_u(\lambda,k)b^{1-u}\beta_b(u,1)Y^{u-1}X^{k-u}\\
&= \sum_{r=0}^{k-1}\mu_{r+1}(\lambda,k)b^{1-(r+1)}\beta_b(r+1,1)Y^{r+1-1}X^{k-r-1}\\
&= \sum_{r=0}^{k-1}\begin{bmatrix}k\\r+1\end{bmatrix}\gamma_{b,c}(\lambda,r+1)b^{-r}\beta_b(r+1,1)Y^rX^{k-1-r}\\
&\overset{(5.2.16)(5.2.10)}{=} \sum_{r=0}^{k-1}\begin{bmatrix}k-1\\r\end{bmatrix}\frac{b^k-1}{b^{r+1}-1}\left(cb^{\lambda}-1\right)b^rb^{-r}\gamma_{b,c}(\lambda-1,r)\\
&\qquad\times\beta_b(r+1,1)Y^rX^{k-1-r}\\
&= b^{-\sigma_1}\beta_b(k,1)\gamma_{b,c}(\lambda,1)\mu^{[k-1]}(X,Y;\lambda-1).
\end{aligned}$$

Now assume that the statement holds for $\varphi=\overline{\varphi}$. Then we have

$$\begin{aligned}
\mu^{[k]\{\overline{\varphi}+1\}}(X,Y;\lambda) &= \left[b^{-\sigma_{\overline{\varphi}}}\beta_b(k,\overline{\varphi})\gamma_{b,c}(\lambda,\overline{\varphi})\mu^{[k-\overline{\varphi}]}(X,Y;\lambda-\overline{\varphi})\right]^{\{1\}}\\
&= b^{-\sigma_{\overline{\varphi}}}\beta_b(k,\overline{\varphi})\gamma_{b,c}(\lambda,\overline{\varphi})\left(\sum_{r=0}^{k-\overline{\varphi}}\begin{bmatrix}k-\overline{\varphi}\\r\end{bmatrix}\gamma_{b,c}(\lambda-\overline{\varphi},r)Y^rX^{k-\overline{\varphi}-r}\right)^{\{1\}}\\
&= b^{-\sigma_{\overline{\varphi}}}\beta_b(k,\overline{\varphi})\gamma_{b,c}(\lambda,\overline{\varphi})\sum_{r=1}^{k-\overline{\varphi}}\begin{bmatrix}k-\overline{\varphi}\\r\end{bmatrix}\gamma_{b,c}(\lambda-\overline{\varphi},r)\left(Y^r\right)^{\{1\}}X^{k-\overline{\varphi}-r}\\
&= b^{-\sigma_{\overline{\varphi}}}\beta_b(k,\overline{\varphi})\gamma_{b,c}(\lambda,\overline{\varphi})\sum_{u=0}^{k-\overline{\varphi}-1}\begin{bmatrix}k-\overline{\varphi}\\u+1\end{bmatrix}\gamma_{b,c}(\lambda-\overline{\varphi},u+1)b^{1-(u+1)}\\
&\qquad\times\beta_b(u+1,1)Y^{u+1-1}X^{k-\overline{\varphi}-u-1}\\
&\overset{(5.2.16)(5.2.10)}{=} b^{-\sigma_{\overline{\varphi}}}\beta_b(k,\overline{\varphi})\gamma_{b,c}(\lambda,\overline{\varphi})\sum_{u=0}^{k-(\overline{\varphi}+1)}\begin{bmatrix}k-\overline{\varphi}-1\\u\end{bmatrix}\\
&\qquad\times\frac{\left(b^{k-\overline{\varphi}}-1\right)\left(b^{u+1}-1\right)}{\left(b^{u+1}-1\right)(b-1)}b^ub^{-u}\\
&\qquad\times\left(cb^{\lambda-\overline{\varphi}}-1\right)\gamma_{b,c}(\lambda-(\overline{\varphi}+1),u)Y^uX^{k-(\overline{\varphi}+1)-u}\\
&= b^{-\sigma_{\overline{\varphi}}}b^{-\overline{\varphi}}\gamma_{b,c}(\lambda,\overline{\varphi}+1)\beta_b(k,\overline{\varphi}+1)\mu^{[k-(\overline{\varphi}+1)]}(X,Y;\lambda-(\overline{\varphi}+1))\\
&= b^{-\sigma_{\overline{\varphi}+1}}\gamma_{b,c}(\lambda,\overline{\varphi}+1)\beta_b(k,\overline{\varphi}+1)\mu^{[k-(\overline{\varphi}+1)]}(X,Y;\lambda-(\overline{\varphi}+1)).
\end{aligned}$$

As required. Now consider $\nu^{[k]}(X,Y;\lambda)=\sum_{u=0}^{k}(-1)^ub^{u(u-1)}\begin{bmatrix}k\\u\end{bmatrix}Y^uX^{k-u}$ as defined in

Theorem 5.3.5. Then we have

$$\begin{aligned}
\nu^{[k]\{1\}}(X,Y;\lambda) &= \left(\sum_{u=0}^{k}(-1)^u b^{\sigma_u}\begin{bmatrix}k\\u\end{bmatrix}Y^u X^{k-u}\right)^{\{1\}}\\
&= \sum_{r=0}^{k-1}(-1)^{r+1}b^{\sigma_{r+1}}b^{1-(r+1)}\begin{bmatrix}k\\r+1\end{bmatrix}\beta_b(r+1,1)Y^{r+1-1}X^{k-r-1}\\
&\overset{(5.2.11)}{=} -\sum_{r=0}^{k-1}(-1)^r b^{\sigma_r}b^r b^{-r}\begin{bmatrix}k-1\\r\end{bmatrix}\frac{\left(b^k-1\right)\left(b^{r+1}-1\right)}{\left(b^{r+1}-1\right)(b-1)}Y^r X^{k-r-1}\\
&= (-1)^1\beta_b(k,1)\nu^{[k-1]}(X,Y;\lambda).
\end{aligned}$$

Now assume that the statement holds for $\varphi=\overline{\varphi}$. Then we have

$$\begin{aligned}
\nu^{[k]}(X,Y;\lambda)^{\{\overline{\varphi}+1\}} &= \left[(-1)^{\overline{\varphi}}\beta_b(k,\overline{\varphi})\nu^{[k-\overline{\varphi}]}(X,Y;\lambda)\right]^{\{1\}}\\
&= (-1)^{\overline{\varphi}}\beta_b(k,\overline{\varphi})\sum_{u=1}^{k-\overline{\varphi}}(-1)^u b^{\sigma_u}\begin{bmatrix}k-\overline{\varphi}\\u\end{bmatrix}\left(Y^u\right)^{\{1\}}X^{k-\overline{\varphi}-u}\\
&= (-1)^{\overline{\varphi}}\beta_b(k,\overline{\varphi})\sum_{r=0}^{k-\overline{\varphi}-1}(-1)^{r+1}b^{\sigma_{r+1}}b^{-(r+1)+1}\begin{bmatrix}k-\overline{\varphi}\\r+1\end{bmatrix}\\
&\qquad\times\beta_b(r+1,1)Y^{r+1-1}X^{k-\overline{\varphi}-r-1}\\
&\overset{(5.2.10)}{=} (-1)^{\overline{\varphi}+1}\beta_b(k,\overline{\varphi})\sum_{r=0}^{k-\overline{\varphi}-1}(-1)^r b^{\sigma_r}\begin{bmatrix}k-\overline{\varphi}-1\\r\end{bmatrix}\\
&\qquad\times\frac{\left(b^{k-\overline{\varphi}}-1\right)\left(b^{r+1}-1\right)}{\left(b^{r+1}-1\right)(b-1)}Y^r X^{k-\overline{\varphi}-1-r}\\
&= (-1)^{\overline{\varphi}+1}\beta_b(k,\overline{\varphi}+1)\nu^{[k-(\overline{\varphi}+1)]}(X,Y;\lambda).
\end{aligned}$$

as required.

□

Now we need a few smaller lemmas in order to prove the Leibniz rule for the b^{-1}-derivative.

Lemma 5.5.7. *Let*

$$\begin{aligned}
u\left(X,Y;\lambda\right) &= \sum_{i=0}^{r}u_i(\lambda)Y^iX^{r-i}\\
v\left(X,Y;\lambda\right) &= \sum_{i=0}^{s}v_i(\lambda)Y^iX^{s-i}.
\end{aligned}$$

1. *If* $u_0(\lambda)=0$ *then*

$$\frac{1}{Y}\Big[u\left(X,Y;\lambda\right)*v\left(X,Y;\lambda\right)\Big]=b^s\frac{u\left(X,Y;\lambda\right)}{Y}*v\left(X,Y;\lambda-1\right). \tag{5.5.10}$$

2. If $v_0(\lambda) = 0$ then

$$\frac{1}{Y}\Big[u\left(X,Y;\lambda\right) * v\left(X,Y;\lambda\right)\Big] = u\left(X,bY;\lambda\right) * \frac{v\left(X,Y;\lambda\right)}{Y}. \tag{5.5.11}$$

Proof.

(1) Suppose $u_0(\lambda) = 0$. Then

$$\frac{u\left(X,Y;\lambda\right)}{Y} = \sum_{i=0}^{r} u_i(\lambda)Y^{i-1}X^{r-i} = \sum_{i=0}^{r-1} u_{i+1}(\lambda)Y^{i}X^{r-i-1}$$

Hence

$$\begin{aligned} b^s\frac{u\left(X,Y;\lambda\right)}{Y} &* v\left(X,Y;\lambda-1\right) \\ &= b^s\sum_{u=0}^{r+s-1}\left(\sum_{\ell=0}^{u} b^{\ell s}u_{\ell+1}(\lambda)v_{u-\ell}(\lambda-\ell-1)\right)Y^uX^{r+s-1-u} \\ &= b^s\sum_{u=0}^{r+s-1}\left(\sum_{i=1}^{u+1} b^{(i-1)s}u_{i}(\lambda)v_{u-i+1}(\lambda-i)\right)Y^uX^{r+s-1-u} \\ &= b^s\sum_{j=1}^{r+s}\left(\sum_{i=1}^{j} b^{(i-1)s}u_{i}(\lambda)v_{j-i}(\lambda-i)\right)Y^{j-1}X^{r+s-j} \\ &= \frac{1}{Y}\sum_{j=0}^{r+s}\left(\sum_{i=0}^{j} b^{is}u_{i}(\lambda)v_{j-i}(\lambda-i)\right)Y^{j}X^{r+s-j} \\ &= \frac{1}{Y}\left(u\left(X,Y;\lambda\right) * v\left(X,Y;\lambda\right)\right) \end{aligned}$$

since when $j = 0$, $\sum_{i=0}^{j} b^{is}u_i(\lambda)v_{j-i}(\lambda-i) = 0$ as $u_0(\lambda) = 0$.

(2) Now if $v_0(\lambda) = 0$, then

$$\begin{aligned} \frac{v\left(X,Y;\lambda\right)}{Y} &= \sum_{j=1}^{s} v_j(\lambda)Y^{j-1}X^{s-j} \\ &= \sum_{i=0}^{s-1} v_{i+1}(\lambda)Y^{i}X^{s-i-1}. \end{aligned}$$

So,

$$\begin{aligned}
u\left(X,bY;\lambda\right)*\frac{v\left(X,Y;\lambda\right)}{Y} &= \sum_{u=0}^{r+s-1}\left(\sum_{j=0}^{u} b^{j(s-1)}b^{j}u_j(\lambda)v_{u-j+1}(\lambda-j)\right)Y^{u}X^{r+s-1-u}\\
&=\sum_{\ell=1}^{r+s}\left(\sum_{j=0}^{\ell-1} b^{js}u_j(\lambda)v_{\ell-j}(\lambda-j)\right)Y^{\ell-1}X^{r+s-\ell}\\
&=\frac{1}{Y}\sum_{\ell=1}^{r+s}\left(\sum_{j=0}^{\ell} b^{js}u_j(\lambda)v_{\ell-j}(\lambda-j)\right)Y^{\ell}X^{r+s-\ell}\\
&=\frac{1}{Y}\sum_{\ell=0}^{r+s}\left(\sum_{j=0}^{\ell} b^{js}u_j(\lambda)v_{\ell-j}(\lambda-j)\right)Y^{\ell}X^{r+s-\ell}\\
&=\frac{1}{Y}\left(u\left(X,Y;\lambda\right)*v\left(X,Y;\lambda\right)\right)
\end{aligned}$$

since when $j=\ell$, $\sum_{i=0}^{j} b^{is}u_i(\lambda)v_{j-i}(\lambda-i)=0$ as $v_0(\lambda)=0$.

□

Theorem 5.5.8 (Leibniz rule for the b^{-1}-derivative)**.** *For two homogeneous polynomials in Y, $f(X,Y;\lambda)$ and $g(X,Y;\lambda)$ with degrees r and s respectively, the φ^{th} (for $\varphi\geq 0$) b^{-1}-derivative of their b-product is given by*

$$\Big[f\left(X,Y;\lambda\right)*g\left(X,Y;\lambda\right)\Big]^{\{\varphi\}}=\sum_{\ell=0}^{\varphi}\begin{bmatrix}\varphi\\ \ell\end{bmatrix}b^{\ell(s-\varphi+\ell)}f^{\{\ell\}}\left(X,Y;\lambda\right)*g^{\{\varphi-\ell\}}\left(X,Y;\lambda-\ell\right). \tag{5.5.12}$$

Proof. For simplification we shall write $f(X,Y;\lambda),\ g(X,Y;\lambda)$ as $f(Y;\lambda),\ g(Y;\lambda)$. Now by differentiation we have

$$\begin{aligned}
\Big[f\left(Y;\lambda\right)*g\left(Y;\lambda\right)\Big]^{\{1\}} &= \frac{f\left(b^{-1}Y;\lambda\right)*g\left(b^{-1}Y;\lambda\right)-f\left(Y;\lambda\right)*g\left(Y;\lambda\right)}{(b^{-1}-1)Y}\\
&=\frac{1}{(b^{-1}-1)Y}\Big\{f\left(b^{-1}Y;\lambda\right)*g\left(b^{-1}Y;\lambda\right)-f\left(b^{-1}Y;\lambda\right)*g\left(Y;\lambda\right)\\
&\qquad+f\left(b^{-1}Y;\lambda\right)*g\left(Y;\lambda\right)-f\left(Y;\lambda\right)*g\left(Y;\lambda\right)\Big\}\\
&=\frac{1}{(b^{-1}-1)Y}\Big\{f\left(b^{-1}Y;\lambda\right)*\left(g\left(b^{-1}Y;\lambda\right)-g\left(Y;\lambda\right)\right)\Big\}\\
&\qquad+\frac{1}{(b^{-1}-1)Y}\Big\{\left(f\left(b^{-1}Y;\lambda\right)-f\left(Y;\lambda\right)\right)*g\left(Y;\lambda\right)\Big\}\\
&\overset{(5.5.11)}{=} f\left(Y;\lambda\right)*\frac{\left(g\left(b^{-1}Y;\lambda\right)-g\left(Y;\lambda\right)\right)}{\left(b^{-1}-1\right)Y}\\
&\qquad\overset{(5.5.10)}{+}\ b^{s}\frac{\left(f\left(b^{-1}Y;\lambda\right)-f\left(Y;\lambda\right)\right)}{\left(b^{-1}-1\right)Y}*g\left(Y;\lambda-1\right)\\
&=f\left(Y;\lambda\right)*g^{\{1\}}\left(Y;\lambda\right)+b^{s}f^{\{1\}}\left(Y;\lambda\right)*g\left(Y;\lambda-1\right).
\end{aligned} \tag{5.5.13}$$

since $g(Y;\lambda)$ has the same degree as $g(b^{-1}Y;\lambda)$ and similarly, $f(Y;\lambda)$ has the same degree as $f(b^{-1}Y;\lambda)$. So the initial case holds. Assume the statement holds true for $\varphi = \overline{\varphi}$, i.e.

$$\Big[f\left(X,Y;\lambda\right) * g\left(X,Y;\lambda\right)\Big]^{\{\overline{\varphi}\}} = \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}\left(X,Y;\lambda\right) * g^{\{\overline{\varphi}-\ell\}}\left(X,Y;\lambda-\ell\right).$$

Now considering $\overline{\varphi}+1$ and for simplicity we write $f(X,Y;\lambda),\ g(X,Y;\lambda)$ as $f(\lambda), g(\lambda)$ we have

$$\begin{aligned}
\Big[f\left(\lambda\right) * g\left(\lambda\right)\Big]^{\{\overline{\varphi}+1\}} &= \left[\sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}-\ell\}}\left(\lambda-\ell\right)\right]^{\{1\}} \\
&\overset{(5.5.13)}{=} \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}-\ell+1\}}\left(\lambda-\ell\right) \\
&\qquad + \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{\ell(s-\overline{\varphi}+\ell)} b^{s-\overline{\varphi}+\ell} f^{\{\ell+1\}}\left(\lambda\right) * g^{\{\overline{\varphi}-\ell\}}\left(\lambda-\ell-1\right) \\
&= \sum_{\ell=0}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}-\ell+1\}}\left(\lambda-\ell\right) \\
&\qquad + \sum_{\ell=1}^{\overline{\varphi}+1} \begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix} b^{(\ell-1)(s-\overline{\varphi}+\ell-1)} b^{s-\overline{\varphi}+(\ell-1)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}-\ell+1\}}\left(\lambda-\ell\right) \\
&= f\left(\lambda\right) * g^{\{\overline{\varphi}+1\}}\left(\lambda\right) + \sum_{\ell=1}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} b^{\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}-\ell+1\}}\left(\lambda-\ell\right) \\
&\qquad + \sum_{\ell=1}^{\overline{\varphi}} \begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix} b^{(\ell-1)(s-\overline{\varphi}+\ell-1)} b^{(s-\overline{\varphi}+(\ell-1))} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}-\ell+1\}}\left(\lambda-\ell\right) \\
&\qquad + \begin{bmatrix}\overline{\varphi}\\ \overline{\varphi}\end{bmatrix} b^{(\overline{\varphi}+1)(s+1)} b^{-\overline{\varphi}-1} f^{\{\overline{\varphi}+1\}}\left(\lambda\right) * g\left(\lambda-\left(\overline{\varphi}+1\right)\right) \\
&= f\left(\lambda\right) * g^{\{\overline{\varphi}+1\}}\left(\lambda\right) + \sum_{\ell=1}^{\overline{\varphi}} \left(\begin{bmatrix}\overline{\varphi}\\ \ell\end{bmatrix} + b^{-\ell}\begin{bmatrix}\overline{\varphi}\\ \ell-1\end{bmatrix}\right) \\
&\qquad \times b^{\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}+1-\ell\}}\left(\lambda-\ell\right) \\
&\qquad + b^{s(\overline{\varphi}+1)} f^{\{\overline{\varphi}+1\}}\left(\lambda\right) * g\left(\lambda-\left(\overline{\varphi}+1\right)\right) \\
&\overset{(5.2.7)}{=} f\left(\lambda\right) * g^{\{\overline{\varphi}+1\}}\left(\lambda\right) + \sum_{\ell=1}^{\overline{\varphi}} b^{-\ell} \begin{bmatrix}\overline{\varphi}+1\\ \ell\end{bmatrix} b^{\ell(s-\overline{\varphi}+\ell)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}+1-\ell\}}\left(\lambda-\ell\right) \\
&\qquad + \begin{bmatrix}\overline{\varphi}+1\\ \overline{\varphi}+1\end{bmatrix} b^{(\overline{\varphi}+1)(s-\overline{\varphi}-1+(\overline{\varphi}+1))} f^{\{\overline{\varphi}+1\}}\left(\lambda\right) * g^{\{\overline{\varphi}+1-(\overline{\varphi}+1)\}}\left(\lambda-\left(\overline{\varphi}+1\right)\right) \\
&= \sum_{\ell=0}^{\overline{\varphi}+1} \begin{bmatrix}\overline{\varphi}+1\\ \ell\end{bmatrix} b^{\ell(s-(\overline{\varphi}+1)+\ell)} f^{\{\ell\}}\left(\lambda\right) * g^{\{\overline{\varphi}+1-\ell\}}\left(\lambda-\ell\right)
\end{aligned}$$

as required. □

5.5.3 Evaluating the b-Derivative and the b^{-1}-Derivative

At this point we need to introduce a couple of lemmas which yield useful results when developing moments of the weight distribution.

Lemma 5.5.9. *For $j, \ell \in \mathbb{Z}^+$, $0 \leq \ell \leq j$ and $X = Y = 1$,*

$$\nu^{[j](\ell)}(1,1;\lambda) = \beta_b(j,j)\delta_{j\ell}. \tag{5.5.14}$$

Proof. Consider

$$\nu^{[j](\ell)}(X,Y;\lambda) \overset{(5.5.3)}{=} \beta_b(j,\ell)\nu^{[j-\ell]}(X,Y;\lambda) = \beta_b(j,\ell)\sum_{u=0}^{j-\ell}(-1)^u b^{\sigma_u}\begin{bmatrix} j-\ell \\ u \end{bmatrix} Y^u X^{(j-\ell)-u}.$$

So

$$\begin{aligned}
\nu^{[j](\ell)}(1,1;\lambda) &= \beta_b(j,\ell)\sum_{u=0}^{j-\ell}(-1)^u b^{\sigma_u}\begin{bmatrix} j-\ell \\ u \end{bmatrix} \\
&\overset{(5.2.12)}{=} \beta_b(\ell,\ell)\begin{bmatrix} j \\ \ell \end{bmatrix}\sum_{u=0}^{j-\ell}(-1)^u b^{\sigma_u}\begin{bmatrix} j-\ell \\ u \end{bmatrix} \\
&\overset{(5.2.1)(5.2.2)}{=} \beta_b(\ell,\ell)\sum_{k=\ell}^{j}(-1)^{k-\ell} b^{\sigma_{k-\ell}}\begin{bmatrix} j \\ k \end{bmatrix}\begin{bmatrix} k \\ \ell \end{bmatrix} \\
&\overset{(5.2.5)}{=} \beta_b(\ell,\ell)\delta_{\ell j} = \beta_b(j,j)\delta_{j\ell}.
\end{aligned}$$

□

Lemma 5.5.10. *For any homogeneous polynomial, $\rho(X,Y;\lambda)$ and for any $s \geq 0$,*

$$\left(\rho * \mu^{[s]}\right)(1,1;\lambda) = \left(cb^{\lambda}\right)^s \rho(1,1;\lambda). \tag{5.5.15}$$

Proof. Let $\rho(X,Y;\lambda) = \sum_{i=0}^{r}\rho_i(\lambda)Y^iX^{r-i}$, then from Theorem 5.3.4

$$\mu^{[s]}(X,Y;\lambda) = \sum_{t=0}^{s}\mu_t^{[s]}(\lambda)Y^tX^{s-t} = \sum_{t=0}^{s}\begin{bmatrix} s \\ t \end{bmatrix}\gamma_{b,c}(\lambda,t)Y^tX^{s-t}$$

and

$$\left(\rho * \mu^{[s]}\right)(X,Y;\lambda) = \sum_{u=0}^{r+s}c_u(\lambda)Y^uX^{(r+s-u)}$$

where

$$c_u(\lambda) = \sum_{i=0}^{u} b^{is}\rho_i(\lambda)\mu_{u-i}^{[s]}(\lambda - i).$$

Then,

$$\begin{aligned}
\left(\rho * \mu^{[s]}\right)(1,1;\lambda) &= \sum_{u=0}^{r+s} c_u(\lambda) \\
&= \sum_{u=0}^{r+s}\sum_{i=0}^{u} b^{is}\rho_i(\lambda)\mu^{[s]}_{u-i}(\lambda - i) \\
&= \sum_{j=0}^{r+s} b^{js}\rho_j(\lambda)\left(\sum_{k=0}^{r+s-j}\mu^{[s]}_k(\lambda - j)\right) \\
&= \sum_{j=0}^{r} b^{js}\rho_j(\lambda)\left(\sum_{k=0}^{s}\mu^{[s]}_k(\lambda - j)\right) \\
&= \sum_{j=0}^{r} b^{js}\rho_j(\lambda)\left(\sum_{k=0}^{s}\begin{bmatrix} s \\ k \end{bmatrix}\gamma_{b,c}(\lambda - j, k)\right) \\
&\overset{(5.2.4)}{=} \sum_{j=0}^{r} b^{js}\rho_j(\lambda)\left(cb^{\lambda - j}\right)^s \\
&= \left(cb^{\lambda}\right)^s \rho(1,1;\lambda)
\end{aligned}$$

since $\rho_j(\lambda) = 0$ when $j > r$ and $\mu^{[s]}_k(\lambda - j) = 0$ when $k > s$. □

5.6 The b-Moments of the Weight Distribution

This final section develops a theory of b-moments analogous to Section 3.5 and Section 4.5 and as before produces comparable formulas to the binomial moments in the Hamming case. Again the moments derived from the b-derivative and the b^{-1}-derivative are not exactly the same, as the first is using the derivative with respect to X and the other is using the derivative with respect to Y.

5.6.1 Moments derived from the b-Derivative

In the first case we consider the moments of the weight distribution with respect to X.

Proposition 5.6.1. *For an $(\mathscr{X}, R)$ n-class Krawtchouk association scheme, $0 \leq \varphi \leq n$, and a linear code $\mathscr{C} \subseteq \mathscr{X}$, and its dual $\mathscr{C}^\perp \subseteq \mathscr{X}$ with weight distributions $\boldsymbol{c} = (c_0, \ldots, c_n)$ and $\boldsymbol{c'} = (c'_0, \ldots, c'_n)$ respectively we have*

$$\sum_{i=0}^{n-\varphi}\begin{bmatrix} n-i \\ \varphi \end{bmatrix} c_i = \frac{1}{|\mathscr{C}^\perp|}\left(cb^n\right)^{n-\varphi}\sum_{i=0}^{\varphi}\begin{bmatrix} n-i \\ n-\varphi \end{bmatrix} c'_i.$$

Proof. We apply Theorem 5.4.1 to $\mathscr{C}^\perp$ to get

$$W^S_{\mathscr{C}}(X,Y) = \frac{1}{|\mathscr{C}^\perp|}\overline{W}^S_{\mathscr{C}^\perp}\left(X + (cb^n - 1)Y, X - Y\right)$$

or equivalently

$$\begin{aligned}\sum_{i=0}^{n} c_i Y^i X^{n-i} &= \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{n} c_i'\,(X-Y)^{[i]} * [X+(cb^n-1)Y]^{[n-i]}\\ &= \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{n} c_i'\nu^{[i]}(X,Y;n) * \mu^{[n-i]}(X,Y;n). \qquad (5.6.1)\end{aligned}$$

For each side of Equation (5.6.1), we shall apply the b-derivative φ times and then evaluate at $X=Y=1$.

For the left hand side, we obtain

$$\left(\sum_{i=0}^{n} c_i Y^i X^{n-i}\right)^{(\varphi)} \overset{(5.5.1)}{=} \sum_{i=0}^{n-\varphi} c_i \beta_b(n-i,\varphi) Y^i X^{n-i-\varphi}.$$

Setting $X=Y=1$ we then have

$$\begin{aligned}\sum_{i=0}^{n-\varphi} c_i\beta_b(n-i,\varphi) &\overset{(5.2.12)}{=} \sum_{i=0}^{n-\varphi} c_i \begin{bmatrix} n-i\\ \varphi\end{bmatrix}\beta_b(\varphi,\varphi)\\ &= \beta_b(\varphi,\varphi)\sum_{i=0}^{n-\varphi} c_i\begin{bmatrix} n-i\\ \varphi\end{bmatrix}.\end{aligned}$$

We now move on to the right hand side. For simplicity we write $\mu(X,Y;n)$ as μ and similarly $\nu(X,Y;n)$ as ν. We have

$$\begin{aligned}\left(\frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{n} c_i'\nu^{[i]} * \mu^{[n-i]}\right)^{(\varphi)} &\overset{(5.5.6)}{=} \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{n} c_i'\left(\sum_{\ell=0}^{\varphi}\begin{bmatrix}\varphi\\ \ell\end{bmatrix} b^{(\varphi-\ell)(i-\ell)}\nu^{[i](\ell)} * \mu^{[n-i](\varphi-\ell)}\right)\\ &= \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{n} c_i'\psi_i(X,Y;n)\end{aligned}$$

where

$$\psi_i(X,Y;n) = \sum_{\ell=0}^{\varphi}\begin{bmatrix}\varphi\\ \ell\end{bmatrix} b^{(\varphi-\ell)(i-\ell)}\nu^{[i](\ell)}(X,Y;n) * \mu^{[n-i](\varphi-\ell)}(X,Y;n).$$

Then with $X=Y=1$,

$$\begin{aligned}\psi_i(1,1;n) &\overset{(5.5.2)}{=} \sum_{\ell=0}^{\varphi}\begin{bmatrix}\varphi\\ \ell\end{bmatrix} b^{(\varphi-\ell)(i-\ell)}\beta_b(n-i,\varphi-\ell)\left(\nu^{[i](\ell)} * \mu^{[n-i-\varphi+\ell]}\right)(1,1;n)\\ &\overset{(5.5.15)}{=} \sum_{\ell=0}^{\varphi}\begin{bmatrix}\varphi\\ \ell\end{bmatrix} b^{(\varphi-\ell)(i-\ell)}\beta_b(n-i,\varphi-\ell)\,(cb^n)^{n-i-(\varphi-\ell)}\,\nu^{[i](\ell)}(1,1;n)\\ &\overset{(5.5.14)}{=} \sum_{\ell=0}^{\varphi} b^{(\varphi-\ell)(i-\ell)}\begin{bmatrix}\varphi\\ \ell\end{bmatrix}\beta_b(n-i,\varphi-\ell)\,(cb^n)^{n-i-(\varphi-\ell)}\,\beta_b(i,i)\delta_{i\ell}\\ &\overset{(5.2.12)}{=} \begin{bmatrix}\varphi\\ i\end{bmatrix}\begin{bmatrix}n-i\\ \varphi-1\end{bmatrix}\beta_b(\varphi-i,\varphi-i)\,(cb^n)^{n-\varphi}\,\beta_b(i,i)\\ &\overset{(5.2.13)}{=} \begin{bmatrix}n-i\\ \varphi-i\end{bmatrix}(cb^n)^{n-\varphi}\,\beta_b(\varphi,\varphi).\end{aligned}$$

So

$$\frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{n} c_i'\psi_i(1,1;n) = \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{\varphi} c_i' \begin{bmatrix} n-i \\ \varphi - i \end{bmatrix} (cb^n)^{n-\varphi}\, \beta_b(\varphi,\varphi)$$
$$\overset{(5.2.1)}{=} \beta_b(\varphi,\varphi)\frac{1}{|\mathscr{C}^{\perp}|}(cb^n)^{n-\varphi}\sum_{i=0}^{\varphi} c_i'\begin{bmatrix} n-i \\ n-\varphi \end{bmatrix}.$$

Combining the results for each side, and simplifying, we finally obtain

$$\sum_{i=0}^{n-\varphi} c_i \begin{bmatrix} n-i \\ \varphi \end{bmatrix} = \frac{1}{|\mathscr{C}^{\perp}|}(cb^n)^{n-\varphi}\sum_{i=0}^{\varphi} c_i'\begin{bmatrix} n-i \\ n-\varphi \end{bmatrix}$$

as required. □

Note. In particular, if $\varphi = 0$ we have

$$\sum_{i=0}^{n} c_i = \frac{(cb^n)^n}{|\mathscr{C}^{\perp}|}c_0' = \frac{(cb^n)^n}{|\mathscr{C}^{\perp}|}.$$

We can simplify Proposition 5.6.1 if φ is less than the minimum distance of the dual code.

Corollary 5.6.2. *Let d_S' be the minimum distance of $\mathscr{C}^{\perp}$. If $0 \le \varphi < d_S'$ then*

$$\sum_{i=0}^{n-\varphi} \begin{bmatrix} n-i \\ \varphi \end{bmatrix} c_i = \frac{1}{|\mathscr{C}^{\perp}|}(cb^n)^{n-\varphi}\begin{bmatrix} n \\ \varphi \end{bmatrix}.$$

Proof. We have $c_0' = 1$ and $c_1' = \ldots = c_{\varphi}' = 0$. □

5.6.2 Moments derived from the b^{-1}-Derivative

The next proposition once again relates the moments of the weight distribution of a linear code to those of its dual, this time using the b^{-1}-derivative of the MacWilliams Identity for a Krawtchouk association scheme. As is the case for the Hermitian association scheme, we must adapt the definition of $\delta(\lambda,\varphi,j)$ in Lemma 5.6.3 to make this definition applicable to all values of the parameter c found in Table 5.1.1.

Lemma 5.6.3. *Let $\delta(\lambda,\varphi,j) = \sum_{i=0}^{j}(-1)^i \begin{bmatrix} j \\ i \end{bmatrix} b^{\sigma_i}\gamma_{b,c}(\lambda - i,\varphi)$. Then for all $\lambda \in \mathbb{R}, \varphi, j \in \mathbb{Z}$,*

$$\delta(\lambda,\varphi,j) = \prod_{i=0}^{j-1}\left(b^{\varphi} - b^i\right)\gamma_{b,c}(\lambda - j,\varphi - j)\left(cb^{\lambda - j}\right)^j. \qquad (5.6.2)$$

Proof. Initial case: $j = 0$.

$$\delta(\lambda,\varphi,0) = \begin{bmatrix} 0 \\ 0 \end{bmatrix}(-1)^0 b^{\sigma_0}\gamma_{b,c}(\lambda,\varphi) = \gamma_{b,c}(\lambda,\varphi) = (\lambda,\varphi)\left(cb^{0(\lambda)}\right).$$

So the initial case holds. Now assume the case is true for $j = \bar{\jmath}$ and consider the $\bar{\jmath}+1$ case.

$$
\begin{aligned}
\delta(\lambda, \varphi, \bar{\jmath}+1) &= \sum_{i=0}^{\bar{\jmath}+1} \begin{bmatrix} \bar{\jmath}+1 \\ i \end{bmatrix} (-1)^i b^{\sigma_i} \gamma_{b,c}(\lambda - i, \varphi) \\
&\overset{(5.2.7)}{=} \sum_{i=0}^{\bar{\jmath}+1} \left(b^i \begin{bmatrix} \bar{\jmath} \\ i \end{bmatrix} + \begin{bmatrix} \bar{\jmath} \\ i-1 \end{bmatrix} \right) (-1)^i b^{\sigma_i} \gamma_{b,c}(\lambda - i, \varphi) \\
&= \sum_{i=0}^{\bar{\jmath}} \begin{bmatrix} \bar{\jmath} \\ i \end{bmatrix} (-1)^i b^{\sigma_i} b^i \gamma_{b,c}(\lambda - i, \varphi) + \sum_{i=0}^{\bar{\jmath}} \begin{bmatrix} \bar{\jmath} \\ i \end{bmatrix} (-1)^{i+1} b^{\sigma_{i+1}} \gamma_{b,c}(\lambda - (i+1), \varphi) \\
&\overset{(5.2.16)}{=} \sum_{i=0}^{\bar{\jmath}} \begin{bmatrix} \bar{\jmath} \\ i \end{bmatrix} (-1)^i b^i b^{\sigma_i} \left(c b^{\lambda - i} - 1 \right) b^{\varphi - 1} \gamma_{b,c}(\lambda - i - 1, \varphi - 1) \\
&\qquad \overset{(5.2.17)}{-} \sum_{i=0}^{\bar{\jmath}} \begin{bmatrix} \bar{\jmath} \\ i \end{bmatrix} (-1)^i b^{\sigma_{i+1}} \left(c b^{\lambda - i - 1} - b^{\varphi - 1} \right) \gamma_{b,c}(\lambda - i - 1, \varphi - 1) \\
&= \sum_{i=0}^{\bar{\jmath}} \begin{bmatrix} \bar{\jmath} \\ i \end{bmatrix} (-1)^i b^{\sigma_i} \gamma_{b,c}(\lambda - i - 1, \varphi - 1) (c b^{\lambda - 1}) \left(b^{\varphi} - 1 \right) \\
&= c b^{\lambda - 1} \left(b^{\varphi} - 1 \right) \delta(\lambda - 1, \varphi - 1, \bar{\jmath}) \\
&= c b^{\lambda - 1} \left(b^{\varphi} - 1 \right) \prod_{i=0}^{\bar{\jmath}-1} \left(b^{\varphi - 1} - b^i \right) c^{\bar{\jmath}} b^{\bar{\jmath}(\lambda - \bar{\jmath} - 1)} \gamma_{b,c}(\lambda - \bar{\jmath} - 1, \varphi - \bar{\jmath} - 1) \\
&= \left(b^{\varphi} - 1 \right) \prod_{i=0}^{\bar{\jmath}-1} \left(b^{\varphi - 1} - b^i \right) (c b^{\lambda - 1}) c^{\bar{\jmath}} b^{\bar{\jmath}(\lambda - (\bar{\jmath}+1))} \gamma_{b,c}(\lambda - (\bar{\jmath}+1), \varphi - (\bar{\jmath}+1)) \\
&= \left(c b^{\lambda - (\bar{\jmath}+1)} \right)^{(\bar{\jmath}+1)} \prod_{i=0}^{\bar{\jmath}} \left(b^{\varphi} - b^i \right) \gamma_{b,c}(\lambda - (\bar{\jmath}+1), \varphi - (\bar{\jmath}+1))
\end{aligned}
$$

since $\begin{bmatrix} \bar{\jmath} \\ i-1 \end{bmatrix} = 0$ when $i = 0$. Hence by induction the lemma is proved. □

Lemma 5.6.4. *Let* $\varepsilon(\Lambda, \varphi, i) = \sum_{\ell=0}^{i} \begin{bmatrix} i \\ \ell \end{bmatrix} \begin{bmatrix} \Lambda - i \\ \varphi - \ell \end{bmatrix} b^{\ell(\Lambda - \varphi)} (-1)^{\ell} b^{\sigma_\ell} \prod_{j=0}^{i-\ell-1} \left(b^{\varphi - \ell} - b^j \right)$*. Then for all* $\Lambda \in \mathbb{R}, \varphi, i \in \mathbb{Z}$*,*

$$\varepsilon(\Lambda, \varphi, i) = (-1)^i b^{\sigma_i} \begin{bmatrix} \Lambda - i \\ \Lambda - \varphi \end{bmatrix}. \tag{5.6.3}$$

Proof. Initial case $i = 0$,

$$\varepsilon(\Lambda, \varphi, 0) = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \begin{bmatrix} \Lambda \\ \varphi \end{bmatrix} b^0 (-1)^0 b^0 = \begin{bmatrix} \Lambda \\ \varphi \end{bmatrix} (-1)^0 b^0 \begin{bmatrix} \Lambda \\ \Lambda - \varphi \end{bmatrix} = \begin{bmatrix} \Lambda \\ \varphi \end{bmatrix}.$$

So the initial case holds. Now suppose the case is true when $i = \bar{\imath}$. Then

$$\begin{aligned}
\varepsilon(\Lambda,\varphi,\bar{\imath}+1) &= \sum_{\ell=0}^{\bar{\imath}+1} \begin{bmatrix}\bar{\imath}+1\\ \ell\end{bmatrix}\begin{bmatrix}\Lambda-\bar{\imath}-1\\ \varphi-\ell\end{bmatrix} b^{\ell(\Lambda-\varphi)}(-1)^{\ell} b^{\sigma_\ell}\prod_{j=0}^{\bar{\imath}-\ell}\left(b^{\varphi-\ell}-b^{j}\right)\\
&\overset{(5.2.6)}{=} \sum_{\ell=0}^{\bar{\imath}+1} \begin{bmatrix}\bar{\imath}\\ \ell\end{bmatrix}\begin{bmatrix}\Lambda-\bar{\imath}-1\\ \varphi-\ell\end{bmatrix} b^{\ell(\Lambda-\varphi)}(-1)^{\ell} b^{\sigma_\ell}\prod_{j=0}^{\bar{\imath}-\ell}\left(b^{\varphi-\ell}-b^{j}\right)\\
&\qquad + \sum_{\ell=1}^{\bar{\imath}+1} b^{(\bar{\imath}+1-\ell)}\begin{bmatrix}\bar{\imath}\\ \ell-1\end{bmatrix}\begin{bmatrix}\Lambda-\bar{\imath}-1\\ \varphi-\ell\end{bmatrix} b^{\ell(\Lambda-\varphi)}(-1)^{\ell} b^{\sigma_\ell}\prod_{j=0}^{\bar{\imath}-\ell}\left(b^{\varphi-\ell}-b^{j}\right)\\
&= A+B, \quad \text{say.}
\end{aligned}$$

Now

$$\begin{aligned}
A &= \left(b^{\varphi}-b^{\bar{\imath}}\right)\sum_{\ell=0}^{\bar{\imath}} \begin{bmatrix}\bar{\imath}\\ \ell\end{bmatrix}\begin{bmatrix}\Lambda-\bar{\imath}-1\\ \varphi-\ell\end{bmatrix} b^{\ell(\Lambda-1-\varphi)}(-1)^{\ell} b^{\sigma_\ell}\prod_{j=0}^{\bar{\imath}-\ell}\left(b^{\varphi-\ell}-b^{j}\right)\\
&= \left(b^{\varphi}-b^{\bar{\imath}}\right)\varepsilon(\Lambda-1,\varphi,\bar{\imath})\\
&= \left(b^{\varphi}-b^{\bar{\imath}}\right)(-1)^{\bar{\imath}} b^{\sigma_{\bar{\imath}}}\begin{bmatrix}\Lambda-\bar{\imath}-1\\ \Lambda-1-\varphi\end{bmatrix}
\end{aligned}$$

and

$$\begin{aligned}
B &= \sum_{\ell=0}^{\bar{\imath}} b^{(\bar{\imath}-\ell)}\begin{bmatrix}\bar{\imath}\\ \ell\end{bmatrix}\begin{bmatrix}\Lambda-\bar{\imath}-1\\ \varphi-\ell-1\end{bmatrix} b^{(\ell+1)(\Lambda-\varphi)}(-1)^{\ell+1} b^{\sigma_{\ell+1}}\prod_{j=0}^{\bar{\imath}-\ell-1}\left(b^{\varphi-\ell-1}-b^{j}\right)\\
&= -b^{(\bar{\imath}+\Lambda-\varphi)}\varepsilon(\Lambda-1,\varphi-1,\bar{\imath})\\
&= -b^{(\bar{\imath}+\Lambda-\varphi)}(-1)^{\bar{\imath}} b^{\sigma_{\bar{\imath}}}\begin{bmatrix}\Lambda-\bar{\imath}-1\\ \Lambda-\varphi\end{bmatrix}.
\end{aligned}$$

So

$$\begin{aligned}
\varepsilon(\Lambda,\varphi,\bar{\imath}+1) &= A+B\\
&= (-1)^{\bar{\imath}} b^{\sigma_{\bar{\imath}}}\left\{\left(b^{\varphi}-b^{\bar{\imath}}\right)\begin{bmatrix}\Lambda-\bar{\imath}-1\\ \Lambda-1-\varphi\end{bmatrix} - b^{(\bar{\imath}+\Lambda-\varphi)}\begin{bmatrix}\Lambda-\bar{\imath}-1\\ \Lambda-\varphi\end{bmatrix}\right\}\\
&\overset{(5.2.8)}{=} (-1)^{\bar{\imath}+1} b^{\sigma_{\bar{\imath}}}\left\{b^{\bar{\imath}+\Lambda-\varphi}\begin{bmatrix}\Lambda-\bar{\imath}-1\\ \Lambda-\varphi\end{bmatrix} - \left(b^{\varphi}-b^{\bar{\imath}}\right)\frac{\left(b^{\Lambda-\varphi}-1\right)}{\left(b^{\varphi-\bar{\imath}}-1\right)}\begin{bmatrix}\Lambda-\bar{\imath}-1\\ \Lambda-\varphi\end{bmatrix}\right\}\\
&= (-1)^{\bar{\imath}+1}\begin{bmatrix}\Lambda-(\bar{\imath}+1)\\ \Lambda-\varphi\end{bmatrix} b^{\sigma_{\bar{\imath}}}\left\{\frac{b^{\bar{\imath}+\Lambda-\varphi}\left(b^{\varphi-\bar{\imath}}-1\right)-\left(b^{\varphi}-b^{\bar{\imath}}\right)\left(b^{\Lambda-\varphi}-1\right)}{\left(b^{\varphi-\bar{\imath}}-1\right)}\right\}\\
&= (-1)^{\bar{\imath}+1} b^{\sigma_{\bar{\imath}+1}}\begin{bmatrix}\Lambda-(\bar{\imath}+1)\\ \Lambda-\varphi\end{bmatrix}
\end{aligned}$$

as required. □

Proposition 5.6.5. *For an $(\mathscr{X},R)$ n-class Krawtchouk association scheme, $0\le\varphi\le n$ and a linear code $\mathscr{C}\subseteq\mathscr{X}$ and its dual $\mathscr{C}^{\perp}\subseteq\mathscr{X}$ with weight distributions $\boldsymbol{c}=(c_0,\ldots,c_n)$ and*

$\boldsymbol{c'} = (c'_0, \ldots, c'_n)$ *respectively we have*

$$\sum_{i=\varphi}^{n} b^{\varphi(n-i)} \begin{bmatrix} i \\ \varphi \end{bmatrix} c_i = \frac{1}{|\mathscr{C}^{\perp}|} (cb^n)^{n-\varphi} \sum_{i=0}^{\varphi} (-1)^i b^{\sigma_i} b^{i(\varphi-i)} \begin{bmatrix} n-i \\ n-\varphi \end{bmatrix} \gamma_{b,c}(n-i, \varphi-i) c'_i.$$

Proof. As per Proposition 5.6.1, we apply Theorem 5.4.1 to $\mathscr{C}^{\perp}$ to obtain

$$W^S_{\mathscr{C}}(X,Y) = \frac{1}{|\mathscr{C}^{\perp}|} \overline{W}^S_{\mathscr{C}^{\perp}} (X + (cb^n - 1)Y, X - Y)$$

or equivalently

$$\begin{aligned} \sum_{i=0}^{n} c_i Y^i X^{n-i} &= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{n} c'_i (X-Y)^{[i]} * (X + (cb^n - 1)Y)^{[n-i]} \\ &= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{n} c'_i \nu^{[i]}(X,Y;n) * \mu^{[n-i]}(X,Y;n). \end{aligned} \tag{5.6.4}$$

For each side of Equation (5.6.4), we shall apply the b^{-1}-derivative φ times and then evaluate at $X = Y = 1$. i.e.

$$\left(\sum_{i=0}^{n} c_i Y^i X^{n-i} \right)^{\{\varphi\}} = \left(\frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{n} c'_i \nu^{[i]}(X,Y;n) * \mu^{[n-i]}(X,Y;n) \right)^{\{\varphi\}}. \tag{5.6.5}$$

For the left hand side, we obtain

$$\begin{aligned} \left(\sum_{i=0}^{n} c_i Y^i X^{n-i} \right)^{\{\varphi\}} &= \sum_{i=\varphi}^{n} c_i b^{\varphi(1-i)+\sigma_\varphi} \beta_b(i,\varphi) Y^{i-\varphi} X^{n-i} \\ &\overset{(5.2.12)}{=} \sum_{i=\varphi}^{n} c_i b^{\varphi(1-i)+\sigma_\varphi} \begin{bmatrix} i \\ \varphi \end{bmatrix} \beta_b(\varphi,\varphi) Y^{i-\varphi} X^{n-i}. \end{aligned} \tag{5.6.6}$$

Then using $X = Y = 1$ gives

$$\sum_{i=\varphi}^{n} c_i b^{\varphi(1-i)+\sigma_\varphi} \begin{bmatrix} i \\ \varphi \end{bmatrix} \beta_b(\varphi,\varphi) Y^{i-\varphi} X^{n-i} = \sum_{i=\varphi}^{n} b^{\varphi(1-i)+\sigma_\varphi} \beta_b(\varphi,\varphi) \begin{bmatrix} i \\ \varphi \end{bmatrix} c_i. \tag{5.6.7}$$

We now move on to the right hand side. For simplicity we shall write $\mu(X,Y;n)$ as $\mu(n)$ and similarly $\nu(X,Y;n)$ as $\nu(n)$. We have,

$$\left(\frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{n} c'_i \nu^{[i]}(n) * \mu^{[n-i]}(n) \right)^{\{\varphi\}} \tag{5.6.8}$$

$$\overset{(5.5.12)}{=} \frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{n} c'_i \left(\sum_{\ell=0}^{\varphi} \begin{bmatrix} \varphi \\ \ell \end{bmatrix} b^{\ell(n-i-\varphi+\ell)} \nu^{[i]\{\ell\}}(n) * \mu^{[n-i]\{\varphi-\ell\}}(n-\ell) \right) \tag{5.6.9}$$

$$= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{i=0}^{n} c'_i \psi_i(n) \tag{5.6.10}$$

say. Then,

$$\begin{aligned}\psi_i(n) \overset{(5.5.9)(5.5.8)}{=} & \sum_{\ell=0}^{\varphi} \begin{bmatrix}\varphi\\ \ell\end{bmatrix} b^{\ell(n-i-\varphi+\ell)} \left\{(-1)^{\ell}\beta_b(i,\ell)\nu^{[i-\ell]}(n)\right\} \\ & * \left\{b^{-\sigma_{\varphi-\ell}}\beta_b(n-i,\varphi-\ell)\gamma_{b,c}(n-\ell,\varphi-\ell)\mu^{[n-i-\varphi+\ell]}(n-\varphi)\right\}.\end{aligned}$$

Now let

$$\Psi(X,Y;n-\varphi) = \nu^{[i-\ell]}(X,Y;n) * \gamma_{b,c}(n-\ell,\varphi-\ell)\mu^{[n-i-\varphi+\ell]}(X,Y;n-\varphi).$$

Then we apply the b-product, reorder the summations and set $X = Y = 1$ to obtain

$$\begin{aligned}&\Psi(1,1;n-\varphi) \\ &\quad = \sum_{u=0}^{n-\varphi}\left[\sum_{p=0}^{u} b^{p(n-i-\varphi+\ell)}\nu_p^{[i-\ell]}(n)\gamma_{b,c}(n-\ell-p,\varphi-\ell)\mu_{u-p}^{[n-i-\varphi+\ell]}(n-\varphi-p)\right] \\ &\quad = \sum_{r=0}^{i-\ell} b^{r(n-i-\varphi+\ell)}\nu_r^{[i-\ell]}(n)\gamma_{b,c}(n-\ell-r,\varphi-\ell)\left[\sum_{w=0}^{n-i-\varphi+\ell}\mu_w^{[n-i-\varphi+\ell]}(n-\varphi-r)\right] \\ &\quad \overset{(5.2.4)}{=} \sum_{r=0}^{i-\ell} b^{r(n-i-\varphi+\ell)}\left(cb^{n-\varphi-r}\right)^{(n-i-\varphi+\ell)}\nu_r^{[i-\ell]}(n)\gamma_{b,c}(n-\ell-r,\varphi-\ell) \\ &\quad = \left(cb^{n-\varphi}\right)^{n-i-\varphi+\ell}\sum_{r=0}^{i-\ell}(-1)^r b^{\sigma_r}\begin{bmatrix}i-\ell\\ r\end{bmatrix}\gamma_{b,c}(n-\ell-r,\varphi-\ell) \\ &\quad = \left(cb^{n-\varphi}\right)^{n-i-\varphi+\ell}\delta(n-\ell,\varphi-\ell,i-\ell) \\ &\quad \overset{(5.6.2)}{=} \left(cb^{n-\varphi}\right)^{n-i-\varphi+\ell}\left(cb^{n-i}\right)^{i-\ell}\prod_{j=0}^{i-\ell-1}\left(b^{\varphi-\ell}-b^j\right)\gamma_{b,c}(n-i,\varphi-i) \\ &\quad = c^{n-\varphi}b^{(n-\varphi)(n-i-\varphi+\ell)}b^{(i-\ell)(n-i)}\prod_{j=0}^{i-\ell-1}\left(b^{\varphi-\ell}-b^j\right)\gamma_{b,c}(n-i,\varphi-i).\end{aligned}$$

Noting that $b^{\ell(n-i-\varphi+\ell)}b^{-\sigma_{\varphi-\ell}} = b^{\ell(n-i)}b^{-\sigma_\varphi}b^{\sigma_\ell}$ we get

$$\begin{aligned}\psi_i(1,1;n) &= \sum_{\ell=0}^{\varphi}(-1)^{\ell}\begin{bmatrix}\varphi\\ \ell\end{bmatrix}b^{\ell(n-i-\varphi+\ell)}b^{-\sigma_{\varphi-\ell}}\beta_b(i,\ell)\beta_b(n-i,\varphi-\ell)\Psi(1,1;n-\varphi) \\ &\overset{(5.2.13)}{=} \sum_{\ell=0}^{\varphi}(-1)^{\ell}\begin{bmatrix}\varphi\\ \ell\end{bmatrix}b^{\ell(n-i-\varphi+\ell)}b^{-\sigma_{\varphi-\ell}}\begin{bmatrix}i\\ \ell\end{bmatrix}\beta_b(\ell,\ell) \\ &\qquad\times\begin{bmatrix}n-i\\ \varphi-\ell\end{bmatrix}\beta_b(\varphi-\ell,\varphi-\ell)\Psi(1,1;n-\varphi) \\ &\overset{(5.2.13)}{=} b^{-\sigma_\varphi}\beta_b(\varphi,\varphi)\sum_{\ell=0}^{i}(-1)^{\ell}b^{\ell(n-i)}b^{\sigma_\ell}\begin{bmatrix}i\\ \ell\end{bmatrix}\begin{bmatrix}n-i\\ \varphi-\ell\end{bmatrix}\Psi(1,1;n-\varphi).\end{aligned}$$

Writing that

$$\begin{aligned}b^{-\sigma_\varphi}b^{\ell(n-i)}b^{(n-\varphi)(n-\varphi-i+\ell)}b^{(i-\ell)(n-i)} &= b^{\sigma_\varphi}b^{\varphi(1-n)}b^{n(n-\varphi)}b^{\ell(n-\varphi)}b^{i(\varphi-i)} \\ &= b^{\theta}b^{\ell(n-\varphi)}\end{aligned}$$

we get

$$\psi_i(1,1;n) = c^{n-\varphi}b^{\theta}\beta_b(\varphi,\varphi)\gamma_{b,c}(n-i,\varphi-i)\sum_{\ell=0}^{i}(-1)^{\ell}b^{\ell(n-\varphi)}b^{\sigma_\ell}\begin{bmatrix} i \\ \ell \end{bmatrix}\begin{bmatrix} n-i \\ \varphi-\ell \end{bmatrix}\prod_{j=0}^{i-\ell-1}\left(b^{\varphi-\ell}-b^{j}\right)$$

$$\overset{(5.6.3)}{=} c^{n-\varphi}b^{\theta}b^{\sigma_i}\beta_b(\varphi,\varphi)\begin{bmatrix} n-i \\ n-\varphi \end{bmatrix}\gamma_{b,c}(n-i,\varphi-i). \qquad (5.6.11)$$

Substituting the results from (5.6.7), (5.6.10) and (5.6.11) we have

$$\sum_{i=\varphi}^{n} b^{\varphi(1-i)+\sigma_\varphi}\beta_b(\varphi,\varphi)\begin{bmatrix} i \\ \varphi \end{bmatrix}c_i = \frac{1}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{n} c_i'(-1)^i c^{n-\varphi}b^{\theta}b^{\sigma_i}\beta_b(\varphi,\varphi)\begin{bmatrix} n-i \\ n-\varphi \end{bmatrix}\gamma_{b,c}(n-i,\varphi-i).$$

Thus cancelling and rearranging gives,

$$\sum_{i=\varphi}^{n} b^{\varphi(n-i)}\begin{bmatrix} i \\ \varphi \end{bmatrix}c_i = \frac{(cb^n)^{n-\varphi}}{|\mathscr{C}^{\perp}|}\sum_{i=0}^{\varphi}(-1)^i b^{\sigma_i}b^{i(\varphi-i)}\begin{bmatrix} n-i \\ n-\varphi \end{bmatrix}\gamma_{b,c}(n-i,\varphi-i)c_i'$$

as required. □

We can simplify Proposition 5.6.5 if φ is less than the minimum distance of the dual code. Also we can introduce the ***dual diameter***, ϱ_S', defined as the maximum distance between any two codewords of the dual code and simplify Proposition 5.6.5 further.

Corollary 5.6.6. *If $0 \le \varphi < d_S'$ then*

$$\sum_{i=\varphi}^{n} b^{\varphi(n-i)}\begin{bmatrix} i \\ \varphi \end{bmatrix}c_i = \frac{1}{|\mathscr{C}^{\perp}|}\left(cb^n\right)^{n-\varphi}\begin{bmatrix} n \\ \varphi \end{bmatrix}\gamma_{b,c}(n,\varphi).$$

For $\varrho_S' < \varphi \le n$ then

$$\sum_{i=0}^{\varphi}(-1)^i b^{\sigma_i}b^{i(\varphi-i)}\begin{bmatrix} n-i \\ n-\varphi \end{bmatrix}\gamma_{b,c}(n-i,\varphi-i)c_i = 0.$$

Explicitly for the Hamming association scheme, when $b = 1$ and $c = q$ we have for $\varrho_S' < \varphi \le n$,

$$\sum_{i=0}^{\varphi}(-1)^i\binom{n-i}{n-\varphi}(q-1)^{\varphi-i}c_i = 0.$$

Moreover for $\varphi = n$,

$$\sum_{i=0}^{n}(-1)^i(q-1)^{n-i}c_i = 0.$$

Proof. First consider $0 \le \varphi < d_S'$, then $c_0' = 1$, $c_1' = \ldots = c_\varphi' = 0$. Also since $\begin{bmatrix} n \\ n-\varphi \end{bmatrix} = \begin{bmatrix} n \\ \varphi \end{bmatrix}$ the statement holds. Now if $\varrho_S' < \varphi \le n$ then applying Proposition 5.6.5 to $\mathscr{C}^{\perp}$ gives

$$\sum_{i=\varphi}^{n} b^{\varphi(n-i)}\begin{bmatrix} i \\ \varphi \end{bmatrix}c_i' = \frac{1}{|\mathscr{C}|}\left(cb^n\right)^{n-\varphi}\sum_{i=0}^{\varphi}(-1)^i b^{\sigma_i}b^{i(\varphi-i)}\begin{bmatrix} n-i \\ n-\varphi \end{bmatrix}\gamma_{b,c}(n-i,\varphi-i)c_i.$$

So using $c'_\varphi = \ldots = c'_n = 0$ we get

$$0 = \sum_{i=0}^{\varphi} (-1)^i b^{\sigma_i} b^{i(\varphi - i)} \begin{bmatrix} n-i \\ n-\varphi \end{bmatrix} \gamma_{b,c}(n-i, \varphi - i) c_i$$

as required. For the Hamming association scheme, we use that $b = 1$, $c = q$ and the b-nary Gaussian coefficients become the usual binomal coefficients and we have immediately

$$0 = \sum_{i=0}^{\varphi} (-1)^i \binom{n-i}{n-\varphi} (q-1)^{\varphi - i} c_i.$$

Moreover when $\varphi = n$,

$$\sum_{i=0}^{n} (-1)^i \binom{n-i}{0} (q-1)^{\varphi - i} c_i = \sum_{i=0}^{n} (-1)^i c_i = 0.$$

□

5.6.3 Maximum Distance Codes in the Association Scheme

As an application for the MacWilliams Identity, we can derive an explicit form of the coefficients of the weight distribution for an $(\mathscr{X}, R)$ n-class association scheme for maximal distance codes. This generalises the results for MDS codes [41, Theorem 6, Chapter 11], MRD codes [22, Proposition 9], MSRD codes in Section 3.5.3 and MHRD codes in Section 4.5.3.

Firstly a lemma that will be needed.

Lemma 5.6.7. *If $x_0, x_1, \ldots, x_\ell$ and $y_0, y_1, \ldots, y_\ell$ are two sequences of real numbers and if*

$$x_j = \sum_{i=0}^{j} \begin{bmatrix} \ell - i \\ \ell - j \end{bmatrix} y_i$$

for $0 \leq j \leq \ell$, then

$$y_i = \sum_{j=0}^{i} (-1)^{i-j} b^{\sigma_{i-j}} \begin{bmatrix} \ell - j \\ \ell - i \end{bmatrix} x_j$$

for $0 \leq i \leq \ell$.

Proof. For $0 \leq i \leq \ell$,

$$\begin{aligned}\sum_{j=0}^{i}(-1)^{i-j}b^{\sigma_{i-j}}\begin{bmatrix}\ell-j\\ \ell-i\end{bmatrix}x_j &= \sum_{j=0}^{i}(-1)^{i-j}b^{\sigma_{i-j}}\begin{bmatrix}\ell-j\\ \ell-i\end{bmatrix}\left(\sum_{k=0}^{j}\begin{bmatrix}\ell-k\\ \ell-j\end{bmatrix}y_k\right)\\ &= \sum_{k=0}^{i}\sum_{j=k}^{i}(-1)^{i-j}b^{\sigma_{i-j}}\begin{bmatrix}\ell-j\\ \ell-i\end{bmatrix}\begin{bmatrix}\ell-k\\ \ell-j\end{bmatrix}y_k\\ &= \sum_{k=0}^{i}y_k\left(\sum_{s=\ell-i}^{\ell-k}(-1)^{i-\ell+s}b^{\sigma_{i-\ell+s}}\begin{bmatrix}s\\ \ell-i\end{bmatrix}\begin{bmatrix}\ell-k\\ s\end{bmatrix}\right)\\ &\overset{(5.2.5)}{=} \sum_{k=0}^{i}y_k\delta_{ik}\\ &= y_i\end{aligned}$$

as required. □

Before going any further we need some restrictions on the codes we consider to be able to use the following proposition. We are only considering $(\mathscr{X}, R)$ n-class Krawtchouk association schemes. From there we are restricted to linear codes $\mathscr{C} \subseteq \mathscr{X}$ with minimum distance d_S and their dual codes $\mathscr{C}^{\perp} \subseteq \mathscr{X}$ with minimum distance d'_S such that $d_S + d'_S = n + 2$. This restriction is necessary since the "first pair of universal bounds" [13, Section IV.F] is met in equality if and only if $d_S + d'_S = n + 2$. We call codes that meet these bounds ***maximal*** codes. More details on these "universal bounds", which are the equivalent Singleton bounds, for any P-polynomial scheme can be found in [13, Section IV.F].

Proposition 5.6.8. *For an $(\mathscr{X}, R)$ n-class Krawtchouk association scheme let $\mathscr{C} \subseteq \mathscr{X}$ be a maximal linear code with weight distribution $\mathbf{c} = (c_0, \ldots, c_n)$ and minimum distance d_S. Let the dual of $\mathscr{C}$ be the maximal linear code $\mathscr{C}^{\perp}$ with minimum distance $d'_S = n - d_S + 2$. Then we have $c_0 = 1$ and for $0 \leq \omega \leq n - d_S$,*

$$c_{d_S+\omega} = \sum_{i=0}^{\omega}(-1)^{\omega-i}b^{\sigma_{\omega-i}}\begin{bmatrix}d_S+\omega\\ d_S+i\end{bmatrix}\begin{bmatrix}n\\ d_S+\omega\end{bmatrix}\left(\frac{cb^{n(d_S+i)}}{|\mathscr{C}^{\perp}|}-1\right).$$

Proof. Now from Corollary 5.6.2 we have

$$\sum_{i=0}^{n-\varphi}\begin{bmatrix}n-i\\ \varphi\end{bmatrix}c_i = \frac{1}{|\mathscr{C}^{\perp}|}\left(cb^n\right)^{n-\varphi}\begin{bmatrix}n\\ \varphi\end{bmatrix}$$

for $0 \leq \varphi < d'_S$. Now since we have a linear code $\mathscr{C}$ which is maximal, with minimum distance d_S and we have $\mathscr{C}^{\perp}$ which is also maximal with minimum distance $d'_S = n - d_S + 2$, Corollary 5.6.2 holds for $0 \leq \varphi \leq n - d_S = d'_S - 2$. We therefore have $c_0 = 1$ and $c_1 = c_2 = \ldots = c_{d_S-1} = 0$ and setting $\varphi = n - d_S - j$ for $0 \leq j \leq n - d_S$ we obtain

$$\begin{aligned}\begin{bmatrix} n \\ n-d_S-j\end{bmatrix} + \sum_{i=d_S}^{d_S+j} \begin{bmatrix} n-i \\ n-d_S-j\end{bmatrix} c_i &= \frac{1}{|\mathscr{C}^\perp|}\left(cb^n\right)^{d_S+j}\begin{bmatrix} n \\ n-d_S-j\end{bmatrix} \\ \sum_{\omega=0}^{j}\begin{bmatrix} n-d_S-\omega \\ n-d_S-j\end{bmatrix} c_{\omega+d_S} &= \begin{bmatrix} n \\ n-d_S-j\end{bmatrix}\left(\frac{\left(cb^n\right)^{d_S+j}}{|\mathscr{C}^\perp|}-1\right).\end{aligned}$$

Applying Lemma 5.6.7 with $\ell = n-d_S$ and $b_\omega = c_{\omega+d_S}$ then setting

$$a_j = \begin{bmatrix} n \\ n-d_S-j\end{bmatrix}\left(\frac{\left(cb^n\right)^{d_S+j}}{|\mathscr{C}^\perp|}-1\right)$$

gives

$$\sum_{\omega=0}^{j}\begin{bmatrix} n-d_S-\omega \\ n-d_S-j\end{bmatrix} b_\omega = a_j$$

and so

$$\begin{aligned} b_\omega = c_{\omega+d_S} &= \sum_{i=0}^{\omega}(-1)^{\omega-i}b^{\sigma_{\omega-i}}\begin{bmatrix} n-d_S-i \\ n-d_S-\omega\end{bmatrix} a_i \\ &= \sum_{i=0}^{\omega}(-1)^{\omega-i}b^{\sigma_{\omega-i}}\begin{bmatrix} n-d_S-i \\ n-d_S-\omega\end{bmatrix}\begin{bmatrix} n \\ n-d_S-i\end{bmatrix}\left(\frac{\left(cb^n\right)^{d_S+i}}{|\mathscr{C}^\perp|}-1\right).\end{aligned}$$

But we have

$$\begin{aligned}\begin{bmatrix} n-d_S-i \\ n-d_S-\omega\end{bmatrix}\begin{bmatrix} n \\ n-d_S-i\end{bmatrix} &\overset{(5.2.1)}{=} \begin{bmatrix} n-(d_S+i) \\ n-(d_S+\omega)\end{bmatrix}\begin{bmatrix} n \\ d_S+i\end{bmatrix} \\ &\overset{(5.2.2)}{=} \begin{bmatrix} d_S+\omega \\ d_S+i\end{bmatrix}\begin{bmatrix} n \\ n-(d_S+\omega)\end{bmatrix} \\ &\overset{(5.2.1)}{=} \begin{bmatrix} d_S+\omega \\ d_S+i\end{bmatrix}\begin{bmatrix} n \\ d_S+\omega\end{bmatrix}.\end{aligned}$$

Therefore

$$c_{\omega+d_S} = \sum_{i=0}^{\omega}(-1)^{\omega-i}q^{2\sigma_{\omega-i}}\begin{bmatrix} d_S+\omega \\ d_S+i\end{bmatrix}\begin{bmatrix} n \\ d_S+\omega\end{bmatrix}\left(\frac{q^{m(d_S+i)}}{|\mathscr{C}^\perp|}-1\right)$$

as required. □

Chapter 6

Conclusions and Future Work

6.1 Summary

This thesis begins by introducing key concepts of association schemes and reviews the literature on the Hamming and rank association schemes studied by MacWilliams [41], Delsarte [9] and Gadouleau and Yan [22]. Specifically the MacWilliams Identity in its various forms and the idea of a q-algebra is presented. Chapter 2 also details some key algebraic functions, namely the b-nary Gaussian coefficients and their properties and a new b-nary beta function both of which contribute heavily to the simplification of the subsequent analysis. The Hamming scheme, being the most researched to date, is used as the primary example to show key concepts of association schemes applied to coding theory. For instance, for the binary Hamming scheme, shown in Figure 2.4.3, the visualisation as a cube is relatively easy to comprehend. After the well known MacWilliams Identity is introduced for the Hamming scheme, immediately the binomial moments of the Hamming weight distribution are stated and proved. Finally the concept of maximal codes, useful for their optimal performance, is introduced and a proposition stated in [41, Theorem 6, Chapter 11], based on the length, dimension and minimum distance of the code only, is proved. The existing results for the rank association scheme, studied by Gadouleau and Yan [22], skew rank association scheme, studied by Delsarte [12] and the Hermitian association scheme studied by Schmidt [53] are also outlined in a similar fashion. The main result highlighted in the rank association scheme is the MacWilliams Identity as a functional transform. Although it appears to be very similar to the functional transform in the Hamming case, the way that these two identities was initially proved are very different.

Using the concepts in Gadouleau and Yan [22], which had been applied to the rank association scheme, we adapt the methods to the different association scheme with skew-symmetric matrices. The first hurdle to jump is the q-algebra from the rank association scheme to one that could be applied in this setting and also create a new gamma function. Gadouleau and

Yan [22] introduced two homogeneous polynomials which were used in the proof of their MacWilliams Identity. However, this proof relied on identifying maximal subgroups of a code and the specific properties of matrices with the rank metric which could not be transferred to skew-symmetric matrices in general. Instead, we identify two new homogeneous polynomials, similar to those in the rank case, use them to generate the eigenvalues of the association scheme and then apply Delsarte's MacWilliams Identity [8, (6.9)] to prove our new MacWilliams Identity as a functional transform. We go on to use the new MacWilliams Identity, along with some skew-q-derivatives to derive new results for the moments of the skew rank distribution with respect to X and with respect to Y. We conclude in this chapter that, similar to the Hamming and rank association schemes, maximal codes with the skew rank metric can be explicitly determined by their length, dimension and minimum distance only.

To test the applicability of these new methods to another association scheme, the Hermitian association scheme is investigated. Once again we have to define the building blocks of a relevant q-algebra and gamma function to start our journey. Similar to the skew rank association scheme, new homogeneous polynomials have to be found that could be used to generate the eigenvalues of this association scheme. We use a different recurrence relation from the one in Chapter 3 [11, (1)], provided by Schmidt [53, Lemma 7], to prove that our newly generated polynomial does indeed represent the eigenvalues of this association scheme, because the parameters lay outside the valid range quoted by Delsarte [11]. Once we have all this in place we then can successfully state and prove the MacWilliams Identity as a functional transform for the Hermitian association scheme. Next we formulate the moments of this association scheme using the new MacWilliams Identity and the negative-q-derivatives. The lemmas used to support the proof of these moments are not directly transferable from the rank and skew rank association schemes. The extension to maximal codes is a lot more involved due to the nature of Hermitian matrices. The difficulty arises because when the minimum distance of a code is even, the weight distribution of a maximal (MHRD) code is not always uniquely determined.

In writing up these two chapters a clear pattern emerges. So as an addition to this thesis, Chapter 5 is written to unify the results for the four association schemes studied. Although the similarities between these association schemes are clear, the way to formulate a uniform theory is much less obvious. The first problem to solve is to show that in the Hermitian association scheme, the solutions to the recurrence relation used in Chapter 4 are also solutions to the recurrence relation used by Delsarte [11, (1)], applied in Chapter 3, with the specific parameter of $b = -q$. The next problem is to harmonise the different gamma and alpha functions and the definition of the b-algebra. The general gamma function can be related back to a component of the specific initial values of the solutions to the recurrence relation by Delsarte, which in turn offers a compact expression for the valencies of the association scheme. The next issue is to amalgamate the homogeneous polynomials used to generate the eigenvalues of each scheme into two “fundamental polynomials” and to seek the parameters that achieve that amalgamation.

In conclusion this thesis develops a way of obtaining the MacWilliams Identity as a functional transform for self dual metric translation association schemes whose eigenvalues satisfy a recurrence relation with specific initial values, which we have called Krawtchouk association schemes. In addition we generate the eigenvalues for these association schemes using two fundamental polynomials from the parameters of the association scheme.

6.2 Extensions of work

As already mentioned, we have shown for the specific case of the Hermitian association scheme that the solutions to the recurrence relation by Delsarte [11, (1)] coincide with the solutions to the recurrence relation used by Schmidt [53, Lemma 7]. So we can conjecture that the validity of the range of parameters, b, for the recurrence relation established by Delsarte [11, (1)] can be extended to any value of $b \in \mathbb{R}$, $b \neq 0$. If confirmed this would be one basis for extending the theory presented in this paper further.

One objective for the future is to apply these MacWilliams Identities and their moments to find explicit new codes and implement them. One further is to take this initial generalisation (of the MacWilliams Identity and its related moments) for the four association schemes studied in this thesis as an inspiration for applying it to a broader set of association schemes.

For the latter, we can first consider the Eberlein polynomials, also studied by Delsarte in [11, Section 5.2]. He finds that these polynomials satisfy the same recurrence relation heavily used in this thesis, whilst also noting that once again they give the eigenvalues of a particular family of association schemes with specified initial values. The family he identified is the Johnson scheme and its q-analog, the Grassmann graphs highlighted pink in Table 6.2.2. We ask, can we adapt the theory developed here in this thesis to find an equivalent set of fundamental polynomials that generate the eigenvalues for these association schemes?

One immediate difference to the schemes studied in this thesis, is even though the Johnson scheme is a P-polynomial scheme, the eigenmatrices P and Q are not equal, i.e. the Johnson scheme is not self dual. We suspect that this can be accommodated. The MacWilliams Identity formulated by Delsarte [8, (6.9)] for any association scheme can still be applied, but in terms of a functional transform, we may be able to relate the inner distribution with the outer distribution rather than a code and its dual.

The other scheme to extend the theory to is the association scheme of symmetric matrices, and its associated quadratic forms graph highlighted in blue in Table 6.2.2. In theory since the eigenvalues of this association scheme are proven by Stanton [61] to be Krawtchouk polynomials, it should be relatively straightforward to check and apply the theory to this case. Saying that, there are additional complexities because the associated distance regular graph is not distance transitive [3, Table 6.2] [17]. We can also note here that quadratic and symmetric forms are closely linked and studied extensively by Schmidt [54].

6.2.1 Further extensions to other classes of association schemes

Below in Table 6.2.2 is a summary table taken from [3, Table 6.1] which has a list of "distance transitive" graphs with classical parameters, and also graphs with classical parameters which are not distance transitive. These have the potential to have the theory presented in this paper extended to them. The graphs highlighted in purple are those related to the Krawtchouk association schemes studied in this thesis. In terms of notation we follow what is presented by Brouwer, the "classical parameters". That is, d is the diameter, i.e. the number of classes; b is the basis of the Gaussian binomials used and $\beta + 1$ is our cb^n, noted in Table 5.1.1. All the association schemes studied in this thesis are formally self dual, (defined in Section 2.3.2) so we have not needed to introduce the final parameter $\alpha + 1$ as these schemes have $b = \alpha + 1$. The reason Table 6.2.2 is included is to give an indication of the potential scope for expanding this approach to other similar association schemes so it is not critical to understand all the details. For more details including definitions of the graphs and their parameters see [3, Table 6.1]. It is defined for self dual graphs with classical parameters that m is either $m = n = 2d + 1$ or $m + 1 = n = 2d$ and for those which are not distance transitive we have m is either $m = n = 2d - 1$ or $m - 1 = n = 2d$.

Graphs with classical parameters [3, Table 6.1]				
Name	d	b	$\alpha+1$	$\beta+1$
Johnson graph $J(n,d)$, $n \geq 2d$	d	1	2	$n-d+1$
Grassmann graph $n \geq 2d$	d	q	$q+1$	$\begin{bmatrix} n-d+1 \\ 1 \end{bmatrix}$
Dual polar graph $e \in \left\{0, \frac{1}{2}, 1, \frac{3}{2}, 2\right\}$	d	q	1	q^e+1
$U(2d,r)$	d	$-r$	$\frac{1+r^2}{1-r}$	$\frac{1-(-r)^{d+1}}{1-r}$
Half dual polar graph $D_{n,n}(q)$	d	q^2	${}_q\begin{bmatrix} 3 \\ 1 \end{bmatrix}$	${}_q\begin{bmatrix} m+1 \\ 1 \end{bmatrix}$
Exceptional Lie graph $E_{7,7}(q)$	3	q^4	${}_q\begin{bmatrix} 5 \\ 1 \end{bmatrix}$	${}_q\begin{bmatrix} 10 \\ 1 \end{bmatrix}$
Gosset graph $E_7(1)$	3	1	5	10
Triality graph ${}^3D_{4,2}(q)$	3	$-q$	$\frac{1}{1-q}$	${}_q\begin{bmatrix} 3 \\ 1 \end{bmatrix}$
Witt graph M_{24}	3	-2	-3	11
Witt graph M_{23}	3	-2	-1	6
Halved cube $\frac{1}{2}H(n,2)$	d	1	3	$m+1$
Self dual graphs with classical parameters [3, Table 6.1]				
Hamming graph $H(d,n)$	d	1	1	n
Bilinear forms graph $n \geq d$	d	q	q	q^n
Alternating forms graph	d	q^2	q^2	q^m
Hermitian forms graph $q = r^2$	d	$-r$	$-r$	$-(-r)^d$
Affine $E_6(q)$ graph	3	q^4	q^4	q^9
Extended ternary Golay code graph	3	-2	-2	9
Graphs with classical parameters but not distance transitive [3, Table 6.2]				
Pseudo $D_m(q)$ graphs	d	q	1	2
Dist. 1-or-2 in simpletic dual polar graph	d	q^2	${}_q\begin{bmatrix} 3 \\ 1 \end{bmatrix}$	${}_q\begin{bmatrix} m+1 \\ 1 \end{bmatrix}$
Doob graph	d	1	1	4
Quadratic forms graphs	d	q^2	q^2	q^m

Table 6.2.2: Classical parameters of some distance regular graphs

6.2.2 Sidel'nikov's Theorem

In the Hamming scheme, the power moments of the weight distribution of an $[n, k, d_H]$-code, $\mathscr{C}$, agree with those of the binomial distribution up to the minimum distance of its dual code, $\mathscr{C}^{\perp}$. About 50 years ago in 1971, Sidel'nikov [58] proved this in the case of binary codes and Delsarte later extended this to other finite fields [10, Lemma 4] with the Hamming metric. As the dual distance increases, the deviation of this curve from a normal distribution decreases. Figure 6.2.1 shows an example of the graph of the weight distribution of a ternary code with the Hamming metric.

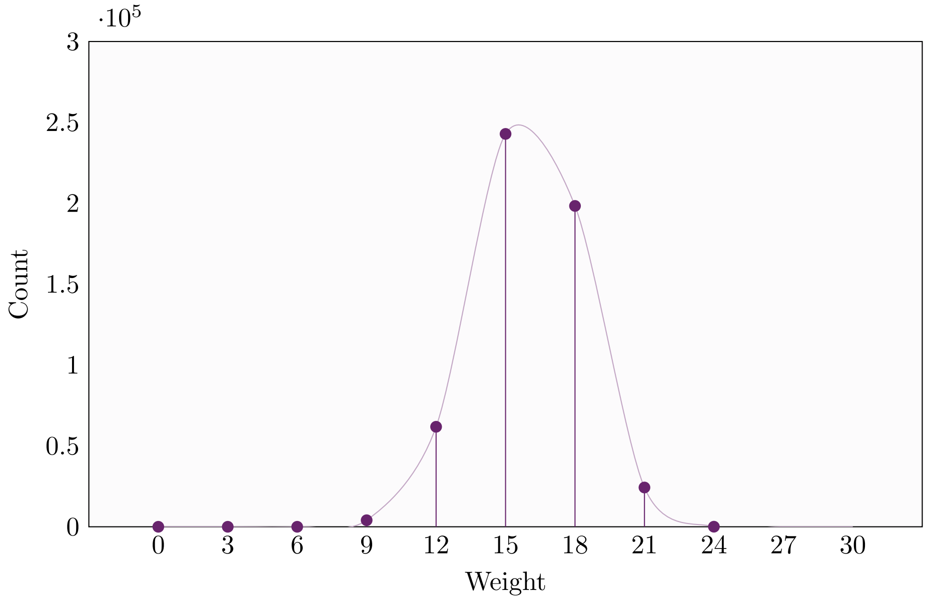

Figure 6.2.1: Weight distribution of ternary $[24, 12, 9]$ quadratic residue code

The core ideas used in the proof by Delsarte are that the power moments agree up to the dual distance, and if they do agree, then the distributions are "close".

In this thesis we have developed a good understanding of the binomial moments thanks to the MacWilliams Identity as a functional transform. The natural question then is can we follow Sidel'nikov's strategy, replacing the central moments with the binomial moments. Moreover if this can be done, there is the possibility of extending this idea to all Krawtchouk association schemes. The scaling of any resulting graphs may need to be adjusted such as by use of the logarithmic scales due to the b-algebra used in this thesis.

Another idea to explore is finding the power moments of the association schemes studied in this thesis and then finding a probability distribution whose moments agree up to the dual distance. The power moments for the Hamming association scheme are derived in [41, Problems (7), Chapter 5] using an operator $y\left(\frac{d}{dy}\right)$ instead of differentiating with respect to y. We question what the q-analog of this would be and whether it does indeed produce the power moments of each association scheme.

6.3 Conclusion

There is an accelerating need for increasingly secure digital communications and storage.

Contributions to this can be made by deploying strategies such as “crypto-segmentation” (where different coding algorithms are used for different segments of data) and “crypto-agility” (where algorithms and keys are changed with high frequency). But alongside these we are compelled to find and implement algorithms that are not only much more secure but also continue to be practical on a day to day basis.

Error correcting codes can play a significant role in that range of coding algorithms. The weight distribution of an error correcting code is one critical set of data that helps to evaluate its effectiveness. For non-trivial codes, the weight distribution can be hard to find and the MacWilliams Identity as a functional transform has been an invaluable tool for achieving that for many years. This research has extended the range of codes for which the MacWilliams Identity can be used in the form of a functional transform. It has specifically extended it to codes based on skew-symmetric and Hermitian matrices over finite fields. Moreover, it has then proven a general theory that covers these and other previously known examples into a common and consistent form. The theory has drawn heavily on the parallel between codes and the known properties of certain classes of association schemes.

Appendix A

Extra Examples

A.1 Example Codes in the Hamming Metric

Four small codes are explored in this section, illustrated in Tables A.1.1 and A.1.2 and are all based on the binary alphabet. As they are small, they can be listed in full and this helps to illustrate an overall view on the type of codes we work with. For more details including the parity check matrix definition see [41, Chapter 1]

Name of code	Example A	Example B
Message words	$(0,0),(0,1),(1,0),(1,1)$	$(0,0),(0,1),(1,0),(1,1)$
Space	$\mathbb{F}_2^3$	$\mathbb{F}_2^4$
Parity Check Rules	$x_3 = x_1 + x_2$	$x_3 = x_1$ and $x_2 = x_4$
Parity Check Matrix PCM	$\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$
Generator Matrix G	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$
Code $\mathscr{C}$	$(0,0,0)$ $(0,1,1)$ $(1,0,1)$ $(1,1,0)$	$(0,0,0,0)$ $(0,1,0,1)$ $(1,0,1,0)$ $(1,1,1,1)$
Weights $\xi_{n,i}$	1 of weight 0, 3 of weight 2	1 of weight 0, 2 of weight 2, 1 of weight 4
Weight Enumerator Ω_n	$X^3 + 3XY^2$	$X^4 + 2X^2Y^2 + Y^4$
Minimum Distance d_H	2	2
Max # of errors that can be corrected	$\left\lfloor \frac{d_H - 1}{2} \right\rfloor = 0$	$\left\lfloor \frac{d_H - 1}{2} \right\rfloor = 0$
$[n, k, d_H]$-code	$[3, 2, 2]$-code	$[4, 2, 2]$-code
Dual Code $\mathscr{C}^\perp$	$(0,0,0)$ $(1,1,1)$	$(0,0,0,0)$ $(1,0,1,0)$ $(0,1,0,1)$ $(1,1,1,1)$
Dimension of Dual	1	2

Table A.1.1: Two codes, in $\mathbb{F}_2^3$ and $\mathbb{F}_2^4$

Name of code	Hamming (7,4) Code	Extended Hamming (8,4) Code
Message words	The 16 message words in $\mathbb{F}_2^4$, of the form $\{x_1, x_2, x_3, x_4\}$	Same as Hamming (7,4) Code.
Space	$\mathbb{F}_2^7$	$\mathbb{F}_2^8$
Parity Check Rules	$x_5 = x_1+x_3+x_4$, $x_6 = x_1+x_2+x_3$, $x_7 = x_2 + x_3 + x_4$.	As for Hamming (7, 4) plus $x_8 = x_1 + x_2 + \cdots + x_7$
Parity Check Matrix PCM	$\begin{pmatrix} 1&0&1&1&1&0&0 \\ 1&1&1&0&0&1&0 \\ 0&1&1&1&0&0&1 \end{pmatrix}$	$\begin{pmatrix} 1&0&1&1&1&0&0&0 \\ 1&1&1&0&0&1&0&0 \\ 0&1&1&1&0&0&1&0 \\ 1&1&0&1&0&0&0&1 \end{pmatrix}$
Generator Matrix G	$\begin{pmatrix} 1&0&0&0&1&1&0 \\ 0&1&0&0&0&1&1 \\ 0&0&1&0&1&1&1 \\ 0&0&0&1&1&0&1 \end{pmatrix}$	$\begin{pmatrix} 1&0&0&0&1&1&0&1 \\ 0&1&0&0&0&1&1&1 \\ 0&0&1&0&1&1&1&0 \\ 0&0&0&1&1&0&1&1 \end{pmatrix}$
Code $\mathscr{C}$	$(0,0,0,0,0,0,0)$ $(0,0,0,1,1,0,1)$ $(0,0,1,0,1,1,1)$ $(0,0,1,1,0,1,0)$ $(0,1,0,0,0,1,1)$ $(0,1,0,1,1,1,0)$ $(0,1,1,0,1,0,0)$ $(0,1,1,1,0,0,1)$ $(1,0,0,0,1,1,0)$ $(1,0,0,1,0,1,1)$ $(1,0,1,0,0,0,1)$ $(1,0,1,1,1,0,0)$ $(1,1,0,0,1,0,1)$ $(1,1,0,1,0,0,0)$ $(1,1,1,0,0,1,0)$ $(1,1,1,1,1,1,1)$	$(0,0,0,0,0,0,0,0)$ $(0,0,0,1,1,0,1,1)$ $(0,0,1,0,1,1,1,0)$ $(0,0,1,1,0,1,0,1)$ $(0,1,0,0,0,1,1,1)$ $(0,1,0,1,1,1,0,0)$ $(0,1,1,0,1,0,0,1)$ $(0,1,1,1,0,0,1,0)$ $(1,0,0,0,1,1,0,1)$ $(1,0,0,1,0,1,1,0)$ $(1,0,1,0,0,0,1,1)$ $(1,0,1,1,1,0,0,0)$ $(1,1,0,0,1,0,1,0)$ $(1,1,0,1,0,0,0,1)$ $(1,1,1,0,0,1,0,0)$ $(1,1,1,1,1,1,1,1)$
Weights $\xi_{n,i}$	1 of weight 0, 7 of weight 3, 7 of weight 4 , 1 of weight 7	1 of weight 0, 14 of weight 4, 1 of weight 8
Weight Enumerator Ω_n	$X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7$	$X^8 + 14X^4Y^4 + Y^8$
Minimum Distance d_H	3	4
Max # of errors that can be corrected	$\left\lfloor \frac{d_H-1}{2} \right\rfloor = 1$	$\left\lfloor \frac{d_H-1}{2} \right\rfloor = 1$
$[n, k, d_H]$-code	$[7, 4, 3]$-code	$[8, 4, 4]$-code
Dual Code $\mathscr{C}^\perp$	$(0,0,0,0,0,0,0)$ $(0,1,1,1,0,0,1)$ $(1,1,1,0,0,1,0)$ $(1,0,0,1,0,1,1)$ $(1,0,1,1,1,0,0)$ $(1,1,0,0,1,0,1)$ $(0,1,0,1,1,1,0)$ $(0,0,1,0,1,1,1)$	$(0,0,0,0,0,0,0,0)$ $(0,0,0,1,1,0,1,1)$ $(0,0,1,0,1,1,1,0)$ $(0,0,1,1,0,1,0,1)$ $(0,1,0,0,0,1,1,1)$ $(0,1,0,1,1,1,0,0)$ $(0,1,1,0,1,0,0,1)$ $(0,1,1,1,0,0,1,0)$ $(1,0,0,0,1,1,0,1)$ $(1,0,0,1,0,1,1,0)$ $(1,0,1,0,0,0,1,1)$ $(1,0,1,1,1,0,0,0)$ $(1,1,0,0,1,0,1,0)$ $(1,1,0,1,0,0,0,1)$ $(1,1,1,0,0,1,0,0)$ $(1,1,1,1,1,1,1,1)$
Dimension of Dual	3	2

Table A.1.2: The Hamming (7,4) code and the Extended Hamming (8,4) code.

A.2 The coefficients for the skew rank weight enumerator Ω_6

The coefficients for the skew rank weight enumerator, Ω_6, are found explicitly below using Equation (2.6.3). We have,

$$\xi_{6,0} = 1$$

$$m = 6,\ s = 1 \quad \xi_{6,1} = \frac{q^0\left(q^{6-0}-1\right)\left(q^{6-0}-1\right)}{\left(q^2-2\right)} = \frac{\left(q^6-1\right)\left(q^5-1\right)}{\left(q^2-1\right)}$$

$$= \left(1+q^2+q^4\right)\left(q^5-1\right),$$

$$m = 6,\ s = 2 \quad \xi_{6,2} = \frac{q^{2(1)}\left(q^6-1\right)\left(q^5-1\right)\cancel{\left(q^4-1\right)}\left(q^3-1\right)}{\left(q^2-1\right)\cancel{\left(q^4-1\right)}}$$

$$q^2\left(q^5-1\right)\left(q^3-1\right)\left(1+q^2+q^4\right)$$

$$m = 6,\ s = 3 \quad \xi_{6,3} = \frac{q^6\cancel{\left(q^6-1\right)}\left(q^5-1\right)\cancel{\left(q^4-1\right)}\left(q^3-1\right)\cancel{\left(q^2-1\right)}\left(q-1\right)}{\cancel{\left(q^2-1\right)}\cancel{\left(q^4-1\right)}\cancel{\left(q^6-1\right)}},$$

$$= q^6\left(q^5-1\right)\left(q^4-q^3-q+1\right).$$

So we can add to the Table 2.6.7 and produce Table A.2.1 below.

$t \times t$	Total	Skew Rank Weight			
		$\xi_{t,0}$	$\xi_{t,1}$	$\xi_{t,2}$	$\xi_{t,3}$
1×1	1	1	-	-	-
2×2	q	1	$q-1$	-	-
3×3	q^3	1	q^3-1	-	-
4×4	q^6	1	$\left(q^2+1\right)\left(q^3-1\right)$	$q^2\left(q^3-1\right)\left(q-1\right)$	-
6×6	q^{15}	1	$\left(1+q^2+q^4\right)\left(q^5-1\right)$	$q^2\left(q^5-1\right)\left(q^3-1\right)\left(1+q^2+q^4\right)$	$q^6\left(q^5-1\right)\left(q^4-q^3-q+1\right)$
$t \times t$	$q^{\frac{t(t-1)}{2}}$	1	See Carlitz Formula (2.6.3)		

Table A.2.1: Coefficents of the skew rank weight enumerator for small matrices in $\mathscr{A}_{q,t}$.

From this we derive the skew rank weight enumerator, Ω_6:

$$\begin{aligned}\Omega_6 = 1 \times X^3Y^0 & \\ & + \left(1+q^2+q^4\right)\left(q^5-1\right)X^2Y^1 \\ & + q^2\left(q^5-1\right)\left(q^3-1\right)\left(1+q^2+q^4\right)X^1Y^2 \\ & + q^6\left(q^5-1\right)\left(q^4-q^3-q+1\right)X^0Y^3 \\ = X^3 + \left(1+q^2+q^4\right)\left(q^5-1\right)X^2Y^1 & \\ & + q^2\left(q^5-1\right)\left(q^3-1\right)\left(1+q^2+q^4\right)X^1Y^2 + q^6\left(q^5-1\right)\left(q^4-q^3-q+1\right)Y^3\end{aligned}$$

A.3 The Canonical form

If the skew rank of a skew-symmetric matrix, $\boldsymbol{A}$ is s with $0 \leq s \leq n$, say, then $\boldsymbol{A}$ is congruent to the canonical $t \times t$ matrix [5, (3.1)],

$$\begin{pmatrix} E_2 & & & & \\ & E_2 & & & \\ & & \ddots & & \\ & & & E_2 & \\ & & & & \mathcal{O}_{t-2s} \end{pmatrix}$$

where $E_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\mathcal{O}_{t-2s}$ is the zero matrix of order $t-2s$. As an example we find the number of matrices in the dual of diag $\{E_2, \mathcal{O}_2\}$, the canonical 4×4 matrix of skew rank 1. Clearly any matrix $\boldsymbol{B} \in \mathscr{A}_{q,4}$ with $b_{12} = 0$ is in this dual, so there are q^5 such matrices in total. So we want to find the number of B_2 such that $\langle \text{diag}\{E_2, \mathcal{O}_2\}, B_2 \rangle = 1$. That is

$$\left\langle \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & b_{12} & b_{13} & b_{14} \\ -b_{12} & 0 & b_{23} & b_{24} \\ -b_{13} & -b_{23} & 0 & b_{34} \\ -b_{14} & -b_{24} & -b_{34} & 0 \end{pmatrix} \right\rangle = 1.$$

Using row reduction, Table A.3.1 below can be found showing the number of these matrices broken down by skew rank.

Skew Rank	0	1	2	TOTAL
$b_{13} \neq 0$	0	$q^3(q-1)$	$q^3(q-1)^2$	$q^4(q-1)$
$b_{13} = 0$ $b_{14} \neq 0$	0	$q^2(q-1)$ $(b_{23} \neq 0)$	$q^2(q-1)^2$ $(b_{23} = 0)$	$q^3(q-1)$
$b_{13} = 0$ $b_{14} = 0$ $b_{23} \neq 0$	0	$q^2(q-1)$	0	$q^2(q-1)$
$b_{13} = 0$, $b_{14} = 0$ $b_{23} = 0$, $b_{24} = 0$ $b_{34} \neq 0$	0	$(q-1)$	0	$(q-1)$
$b_{13} = 0$, $b_{14} = 0$ $b_{23} = 0$, $b_{24} = 0$ $b_{34} = 0$	1	0	0	1
$b_{13} = 0$, $b_{14} = 0$ $b_{23} = 0$, $b_{24} \neq 0$	0	$q(q-1)$	0	$q(q-1)$
TOTAL	1	$q^4 + q^3 - q^2 - 1$	$q^5 - q^4 - q^3 + q^2$	q^5

Table A.3.1: Skew ranks of 4×4 skew-symmetric matrices in the dual of diag$\{E_2, \mathcal{O}_2\}$.

This analysis was explored as it offered a potential route to count the coefficients of the weight enumerator of the dual of a space spanned by a single matrix.

Nomenclature

The next list describes several symbols that have been used within the body of the document. The symbols have been sorted into relevant chapter groups, although some notations which span the latter chapters have been included in Association Schemes Notation and Krawtchouk Association Schemes only. These notations can be adapted using the appropriate b parameter.

Association Schemes Notation

$[n,k,d]$	Code of dimension k, words of length n, with minimum distance d
$\boldsymbol{c}$	Inner distribution
$\mathscr{B}$	The Bose-Mesner algebra
$\mathscr{C}$	Code
$\mathscr{C}^{\perp}$	Dual code
$\mathscr{X}$	Set of finite points
${}_b\begin{bmatrix}x\\k\end{bmatrix}$	b-nary Gaussian coefficient
${}_b\binom{x}{k}$	Binomial coefficient
$\psi(i)$	Multiplicity of $p_k(i)$
σ_i	Shorthand for $\frac{i(i-1)}{2}$
c_{ijk}	Intersection numbers
$d(x,y)$	Distance function d
D_i	The adjaceny matrix
E	Set of edges
E_i	Idempotent matrix

G	A graph
J	The all 1's matrix
P	Eigenmatrix
$p_k(i)$	Eigenvalues
$P_k(x,n)$	Generalised Krawtchouk polynomial
Q	Dual Eigenmatrix
$q_k(i)$	Dual eigenvalues
R	Set of relations
R_i	i^{th} relation
V	Set of vertices
v	Number of points in $\mathscr{X}$
v_i	Valency of $q_k(i)$
$\beta_b(x,k)$	b-nary Beta function

Hamming Scheme Notation

$\cdot$	Vector scalar product
$\mathbb{F}_q^n$	Finite field of dimension n over q where q is a power of a prime
$B_r(a)$	Ball of radius r about a point a
d_H	Hamming distance
w	Hamming weight
$W_{\mathscr{C}}^H(X,Y)$	Hamming weight enumerator of X and Y
MDS	Maximum Distance Separable

Krawtchouk Association Scheme Notation

(φ)	Differentiation with respect to X
$*$	b-product
$\delta(\lambda,\varphi,j)$	Separate function for moments
$\mu(X,Y;\lambda)$	First fundamental polynomial
$\nu(X,Y;\lambda)$	Second fundamental polynomial
$\overline{a}(X,Y;\lambda)$	b-transform of a polynomial $a(X,y;\lambda)$

$\{\varphi\}$ Differentiation with respect to Y

$a^{[i]}(X, Y; \lambda)$ b-power of a polynomial $a(X, Y; \lambda)$

$C_{k+1}(x, t)$ b-Krawtchouk Polynomial

Number sets

$\mathbb{C}$ Complex numbers

$\mathbb{Z}^+$ Set of positive integers

Rank Scheme Notation

$\alpha(x, k)$ Alpha function

$\boldsymbol{A}$ Matrix of size $m \times n$

$\mathbb{F}_q^{m\times n}$ Finite field of dimension $m \times n$ over q where q is a power of a prime

$\Omega_{m,n}$ Rank weight enumerator of $\mathbb{F}_q^{m\times n}$

$\xi_{m,n,r}$ Number of matrices of size $m \times n$ of rank r

d_R Minimum rank weight

$R(\mathbf{A})$ Rank weight of matrix $\boldsymbol{A}$

$Tr(\boldsymbol{A})$ Trace of $\boldsymbol{A}$

$W^R_{\mathscr{C}}(X, Y)$ Rank weight enumerator

MRD Maximum rank distance

Skew Rank Scheme Notation

$\gamma(x, k)$ Gamma function

$\mathscr{A}_{q,t}$ Set of skew-symmetric matrices of size t with entries in the field $\mathbb{F}_q$

Ω_t Skew rank weight enumerator of $\mathscr{A}_{q,t}$

$\xi_{t,s}$ Number of skew-symmetric matrices of size $t \times t$ of skew rank s

d_{SR} Minimum skew rank distance

$SR(\boldsymbol{A})$ Skew rank of a matrix $\boldsymbol{A}$

$W^{SR}_{\mathscr{C}}(X, Y)$ Skew rank weight distribution of $\mathscr{C}$

MSRD Maximum skew rank distance

Hermitian Rank Scheme Notation

$\boldsymbol{H}^\dagger$ Conjugate transpose of $\boldsymbol{H}$

$\gamma'(x,k)$	Negative Gamma function
$\mathscr{H}_{q,t}$	Set of Hermitian matrices of size $t \times t$ over $\mathbb{F}_{q^2}$
Ω_t	Hermitian rank weight enumerator of $\mathscr{H}_{q,t}$
$\overline{x}$	Conjugate of $x \in \mathbb{F}_{q^2}$
d_{HR}	Minimum Hermitian rank distance
$W_{\mathscr{C}}^{HR}(X,Y)$	Hermitian rank weight distribution of $\mathscr{C}$
MHRD	Maximum Hermitian rank distance

Bibliography

[1] R.C. Bose and D.M. Mesner. 'On Linear Associative Algebras Corresponding to Association Schemes of Partially Balanced Designs'. In: *The Annals of Mathematical Statistics* 30.1 (1959), pp. 21–38.

[2] R.C. Bose and K. Nair. 'Partially Balanced Incomplete Block Designs'. In: *Sankhya* 4 (1939), pp. 337–372.

[3] A.E. Brouwer, A.M. Cohen and A. Neumaier. *Distance-Regular Graphs.* Springer Berlin, Heidelberg, 2012.

[4] E. Burlekamp. 'Goppa Codes'. In: *IEEE Transactions on Information Theory* 19.5 (1973), pp. 590–592.

[5] L. Carlitz. 'Representations by Skew Forms in a Finite Field'. In: *Archiv der Mathematik* 5 (1954), pp. 19–31.

[6] L. Carltiz and J.H. Hodges. 'Representations by Hermitian Forms in a Finite Field'. In: *Duke Mathematical Journal* 22.3 (1955), pp. 393–405.

[7] E. Castelow. *Biography of Mary Queen of Scots.* URL: https://www.historic-uk.com/HistoryUK/HistoryofScotland/Mary-Queen-of-Scots/.

[8] P. Delsarte. *An Algebraic Approach to the Association Schemes of Coding Theory.* Philips Journal of Research / Supplement. N.V. Philips' Gloeilampenfabrieken, 1973.

[9] P. Delsarte. 'Bilinear Forms over a Finite Field, with Applications to Coding Theory'. In: *Journal of Combinatorial Theory, Series A* 25.3 (1978), pp. 226–241.

[10] P. Delsarte. 'Distance Distribution over Hamming Spaces'. In: *Philips Research Reports* 30 (1 1975), pp. 1–8.

[11] P. Delsarte. 'Properties and Applications of the Recurrence $F(i+1,k+1,n+1) = q^{k+1}F(i,k+1,n)-q^kF(i,k,n)$'. In: *SIAM Journal on Applied Mathematics* 31.2 (1976), pp. 262–270.

[12] P. Delsarte and J.M. Goethals. 'Alternating Bilinear Forms over $GF(q)$'. In: *Journal of Combinatorial Theory, Series A* 19.1 (1975), pp. 26–50.

[13] P. Delsarte and V.I. Levenshtein. ‘Association Schemes and Coding Theory’. In: *IEEE Transactions on Information Theory* 44.6 (1998), pp. 2477–2504.

[14] W. Diffe and M. Hellman. ‘New Directions in Cryptography’. In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654.

[15] J-G Dumas, R. Gow and J. Sheekey. ‘Rank Properties of Subspaces of Symmetric and Hermitian Matrices over Finite Fields’. In: *Finite Fields and Their Applications* 17 (2011), pp. 504–520.

[16] Barker. E and Dang. Q. *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance.* URL: `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf`.

[17] Y. Egawa. ‘Association Schemes of Quadratic Forms’. In: *Journal of Combinatorial Theory.* Series A 38 (1985), pp. 1–14.

[18] E. Gabidulin. ‘A Brief Survey of Metrics in Coding Theory’. In: *Mathematics of Distances and Applications* 66 (2012).

[19] E. Gabidulin. ‘Optimal Codes Correcting Lattice-Pattern Errors’. In: *Problems of Information Transmission* 21.2 (1985), pp. 3–11.

[20] E. Gabidulin. ‘Rank-metric Codes and Applications’. In: *Moscow Inst. Phys. Technol., State Univ., Dolgoprudny, Russia* (2011). URL: `http://iitp.ru/upload/content/839/Gabidulin.pdf`.

[21] E. Gabidulin. ‘Theory of Codes with Maximum Rank Distance’. In: *Problemy Peredachi Informatsii* 21.1 (1985), pp. 3–16.

[22] M. Gadouleau and Z. Yan. ‘MacWilliams Identity for Codes with the Rank Metric’. In: *EURASIP Journal on Wireless Communications and Networking* 2008.1 (2008).

[23] F.R. Gantmacher and J.L. Brenner. *Applications of the Theory of Matrices.* Dover Books on Mathematics. Dover Publications, 2005.

[24] GhostVault. *The Story of Cryptography: History.* 2023. URL: `https://ghostvolt.com/articles/cryptography_history.html`.

[25] A.M. Gleason. ‘Weight Polynomials of Self-Dual Codes and the MacWilliams Identities’. In: *Congres International de Mathematiques* 3 (1970), pp. 211–215.

[26] M. Golay. ‘Notes on Digital Coding’. In: *Proceedings IRE* 37 (1949), p. 657.

[27] R. Gow et al. ‘Constant Rank-Distance Sets of Hermitian Matrices and Partial Spreads in Hermitian Polar Spaces’. In: *Electronic Journal of Combinatorics* 21 (2012).

[28] D. Grant and M. Varanasi. ‘Duality Theory for Space-Time Codes over Finite Fields’. In: *Advances in Mathematics of Communications* 2 (2008).

[29] D. Grant and M. Varanasi. ‘Weight Enumerators and a MacWilliams-type Identity for Space-Time Rank Codes over Finite Fields’. In: pp. 2137–2146.

[30] R.W. Hamming. ‘Error Detecting and Error Correcting Codes’. In: *Bell System Technical Journal* 29.2 (1950), pp. 147–160.

[31] Muslim Heritage. *Al-Khalil ibn Ahmad.* 2020. URL: https://muslimheritage.com/people/scholars/al-khalil-ibn-ahmad/.

[32] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes.* Cambridge University Press, 2003.

[33] NASA JPL. Feb. 1979. URL: https://images.nasa.gov/details/ARC-1979-A79-7029.

[34] D. Khan. *The Codebreakers: The Story of Secret Writing.* New American Library, 1973.

[35] N. Koblitz. ‘Elliptic Curve Cryptosystems’. In: *Mathematics of Computation* 48 (1987), pp. 203–209.

[36] P. Lefèvre, P. Carré and P. Gaborit. ‘Application of Rank Metric Codes in Digital Image Watermarking’. In: *Signal Processing: Image Communication* 74 (2019), pp. 119–128.

[37] P. Loidreau. ‘A New Rank Metric Codes Based Encryption Scheme’. In: *International Workshop on Post-Quantum Cryptography.* Springer. 2017, pp. 3–17.

[38] F.J MacWilliams. ‘A Theorem on the Distribution of Weights in a Systematic Code’. In: *Bell Syst. Tech. J.* 42 (1963), pp. 79–94.

[39] F.J. MacWilliams. ‘A Theorem on the Distribution of Weights in a Systematic Code’. In: *Bell System Technical Journal* 42.1 (1963), pp. 79–94.

[40] F.J. MacWilliams. ‘Orthogonal Matrices over Finite Fields’. In: *The American Mathematical Monthly* 76.2 (1969), pp. 152–164.

[41] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes.* Mathematical Studies. Elsevier Science, 1977.

[42] V. M. Mano, E. A. Martins and L. A. Vieira. ‘Some Results on the Krein Parameters of an Association Scheme’. In: *Dynamics, Games and Science.* Springer International Publishing, 2015, pp. 441–454.

[43] R.J. McEliece. ‘A Public-Key Cryptosystem based on Algebraic Coding Theory’. In: *Deep Space Network Progress Report* 44 (1978), pp. 114–116.

[44] V. S. Miller. ‘Use of Elliptic Curves in Cryptography’. In: *Advances in Cryptology — CRYPTO ’85 Proceedings.* Ed. by H. C. Williams. Springer Berlin Heidelberg, 1986.

[45] D. Moody. *The 2nd Round of the NIST PQC Standardization Process.* URL: https://csrc.nist.gov/CSRC/media/Presentations/the-2nd-round-of-the-nist-pqc-standardization-proc/images-media/moody-opening-remarks.pdf.

[46] A&E Television Networks. *Julius Ceaser.* 2009. URL: https://www.history.com/topics/ancient-rome/julius-caesar.

[47] NIST. *Post-Quantum Cryptography Standardization.* URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization.

[48] A.V. Ourivski and E. Gabidulin. 'Column Scrambler for the GPT Cryptosystem'. In: *Discrete Applied Mathematics* 128.1 (2003). International Workshop on Coding and Cryptography (WCC2001)., pp. 207–221. URL: http://www.sciencedirect.com/science/article/pii/S0166218X02004468..

[49] Bletchley Park. *Enigma.* URL: https://bletchleypark.org.uk/our-story/enigma/.

[50] V. Pless. *Introduction to the Theory of Error-Correcting Codes.* A Wiley-Interscience publication. Wiley, 1989.

[51] A. Ravagnani. *Rank-Metric Codes and their Duality Theory.* 2015. arXiv: 1410.1333 [cs.IT].

[52] R. Rivest, A. Shamir and L. Adleman. 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems'. In: *Communications of the ACM* 21.2 (1978).

[53] K-U. Schmidt. 'Hermitian Rank Distance Codes'. In: *Designs, Codes and Cryptography* 86 (2018), pp. 1469–1481.

[54] K-U. Schmidt. 'Quadratic and Symmetric Bilinear Forms over Finite Fields and their Association Schemes'. In: *Algebraic Combinatorics* 3 (2020), pp. 161–189.

[55] M. Shi, O. Rioul and P. Solé. 'Designs in Finite Metric Spaces: A Probabilistic Approach'. In: *Graphs and Combinatorics* (2021), pp. 1654–1667.

[56] P. Shor. 'Algorithms for Quantum Computation: Discrete Logarithms and Factoring'. In: *IEEE Comput. Soc. Press* (1994).

[57] P. W. Shor. 'Algorithms for Quantum Computation: Discrete Logarithms and Factoring'. In: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science.* SFCS '94. USA: IEEE Computer Society, 1994, pp. 124–134.

[58] V. Sidel'nikov. 'Weight Specturm of Binary Bose-Chauduri-Hocquenghem codes'. In: *Problemy Peredachi Informatsii* 7 (1 1971), pp. 14–22.

[59] H. Sidhpurwala. *A Brief History of Cryptography.* 2023. URL: https://www.redhat.com/en/blog/brief-history-cryptography#.

[60] W. Stallings. *Cryptography and Network Security: Principles and Practice.* Prentice Hall, 1999.

[61] D. Stanton. 'A partially Ordered Set and q-Krawtchouk Polynomials'. In: *Journal of Combinatorial Theory, Series A* 30.3 (1981), pp. 276–284.

[62] D. Stanton. 'Some q-Krawtchouk Polynomials on Chevalley Groups'. In: *American Journal of Mathematics* 102.4 (1980), pp. 625–662.

[63] Thales. *A Brief History of Encryption (and Cryptography)*. 2023. URL: `https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption`.

[64] A. Thorup and D. Laksov. 'Counting Matrices with Coordinates in Finite Fields and of Fixed Rank'. In: *Mathematica Scandinavica* 74 (1994), pp. 19–33.

[65] Denso Wave. *QR Code® Development Story*. URL: `https://www.denso-wave.com/en/technology/vol1.html`.