Projective Space Codes for the Injection Metric

by

Azadeh Khaleghi

A thesis submitted in conformity with the requirements
for the degree of Master of Applied Science,
The Edward S. Rogers Sr. Department of
Electrical & Computer Engineering,
University of Toronto

Abstract

Projective Space Codes for the Injection Metric

Azadeh Khaleghi

Master of Applied Science

The Edward S. Rogers Sr. Department of Electrical & Computer Engineering

University of Toronto

2009

In the context of error control in random linear network coding, it is useful to construct codes that comprise well-separated collections of subspaces of a vector space over a finite field.

This thesis concerns the construction of non-constant-dimension projective space codes for adversarial error-correction in random linear network coding. The metric used is the so-called injection distance introduced by Silva and Kschischang, which perfectly reflects the adversarial nature of the channel.

A Gilbert-Varshamov-type bound for such codes is derived and its asymptotic behavior is analysed. It is shown that in the limit as the ambient space dimension approaches infinity, the Gilbert-Varshamov bound on the size of non-constant-dimension codes behaves similar to the Gilbert-Varshamov bound on the size of constant-dimension codes contained within the largest Grassmannians in the projective space.

Using the code-construction framework of Etzion and Silberstein, new non-constant-dimension codes are constructed; these codes contain more codewords than comparable codes designed for the subspace metric. To our knowledge this work is the first to address the construction of non-constant-dimension codes designed for the injection metric.

... in loving memory of my father,
without whom, success is as tasteless as a grain of sand ...

Acknowledgements

I wish to express my most sincere gratitude to my supervisor, Professor Frank R. Kschischang, for his inspiring supervision throughout the course of this research work. He, with his patience, insight and extensive knowledge of the field has guided me in all aspects of my graduate studies, and has helped me mature as a researcher.

I would like to thank Professor Raviraj Adve, Professor Amr Helmy, and Professor Konstantinos N. Plataniotis, the committee members of my thesis defense, for their valuable comments.

Additionally, I would like to thank my colleagues at the University of Toronto, and especially the members of FRK group for providing a joyful research environment. I specifically thank Danilo Silva for all the fruitful discussions throughout the course of preparing this thesis.

Finally, and most importantly, I am grateful to my loving parents and to my brother and best friend Khashyar, for their unconditional love and support throughout my life. I am forever indebted to them for all that they have done for me and for all the sacrifices they have made. If not for them, I would not be who I am now. To them I dedicate this dissertation.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Network Coding

Network coding was first introduced by Ahlswede et al. in 2000 [1], and has since received considerable amount of attention. The main idea behind network coding is to allow for the mixing of data at intermediate network nodes. The motivation behind this notion is best described through an example. Consider two cars traveling on independent paths that merge at an intersection. Clearly, it is not possible for both cars to pass through the merging point simultaneously. Hence, the only way would be for them to travel sequentially.

Now imagine that this intersection point is part of a communication network through which *"information packets"* travel instead of *"cars"*. In this case a traditional network would also form a queue for the data packets being transmitted, completely disregarding the fact that, unlike cars, data packets can undergo mathematical operations.

Figure 1.1(a) is an example of a simple network in which a node acts as a bottleneck. There is a single source and two destinations, both of which are interested in bits A and B produced at the source. Each link in the network has capacity to transmit a single bit at a time. In a traditional routing scheme, two transmissions are required at the min-cut in order for both receivers to recover both bits A and B.

On the other hand, if mixing the data at intermediate nodes is allowed, then the centre link no longer acts as a bottleneck since the XOR of bits A and B may be transmitted as shown in Figure 1.1(b) . Thus each destination node will receive one of the two bits along with their XOR, and is able to recover both bits. In particular, one receiver receives A and $A \oplus B$, and is therefore able to recover $B = A \oplus (A \oplus B)$. Similarly another receiver

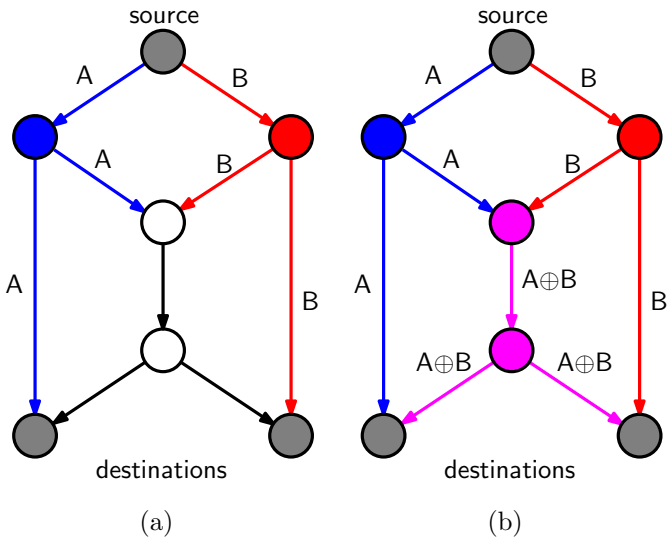

Figure 1.1: (a) With routing alone, v acts as a bottleneck. (b) With network coding $A \oplus B$ is transmitted to both receivers simultaneously.

is able to recover $A = B \oplus (A \oplus B)$. This simple example, known as the *"butterfly network"* [1], illustrates that network coding can result in an increase of throughput in a communication network. A transmission scenario similar to that of Figure 1.1 in which there exist a source and multiple destinations all interested in all of the source packets is regarded as *"multicast transmission"*.

In a communication network that uses network coding the output of an intermediate node at its outgoing links is a function f of its incoming packets. A natural question that arises is: *"What would be a suitable and practical choice for f?"*. A network may benefit from network coding only if the operations performed at intermediate nodes are feasible. This requires the design of f and its decoder to be simple enough so that the network complexity and the implementation costs are not increased to a prohibitive level.

In *"linear network coding"* [2, 3] f is constrained to be linear with respect to a finite field, requiring the intermediate nodes to transmit linear combinations of their incoming packets at their outgoing links. The fundamental benefit of this linearity constraint is the simplicity of coding operations, allowing network coding to be more practical. It is shown in [2] that for a sufficiently large packet size, linear network coding achieves multicast capacity.

The coefficients of the linear operations at the intermediate nodes may either be determined by a central authority, or at random. In the latter case, each node outputs a *random* linear combination of its incoming packets and the network is said to be using

"random linear network coding" [4, 5]. In [5] Ho. et al. show that for sufficiently large packet size random linear network coding also achieves multicast capacity.

Even in cases where throughput is not increased, random linear network coding may still be desirable as it simplifies the operation. Such a distributed approach is beneficial in that it allows for a decentralized operation that is also robust to dynamic network changes or link failures.

1.2 Linear Network Coding Channel

Consider a communication network represented as a directed graph with a single source multicasting information to a number of destination nodes. Packets are vectors of length n over a finite field $\mathbb{F}_q$. A message to be transmitted by the source is a matrix $X \in \mathbb{F}_q^{m\times n}$ composed of m packets $X_1,\ X_2, \cdots, X_m \in \mathbb{F}_q^n$ as its rows. Transmission through each link connecting one node to another in the network is assumed to be error-free.

An intermediate node transmits an $\mathbb{F}_q$-linear combination of its incoming packets. It is then easy to observe that every received packet is a linear combination of the source packets. Let $Y \in \mathbb{F}_q^{N\times n}$ be a received matrix composed of a set of N received packets $Y_1,\ Y_2, \cdots, Y_N$ at a destination node. Then

$$Y = \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_N \end{bmatrix} = AX, \tag{1.1}$$

where $A \in \mathbb{F}_q^{N\times m}$ is the transfer matrix of the network from the source to that destination node. Clearly if A is invertible then it is possible to recover X. In this case the network code is said to be *"feasible"*. It is shown in [5] that a random network code is feasible with high probability provided that the field size q is sufficiently large.

In the case of random linear network coding, the transfer matrices are not predetermined as their entries are chosen independently and uniformly at random. In order to inform the destination nodes about the specific transfer matrices produced, typically an identity matrix is prepended to X. This way the random coefficients are recorded as the packets traverse through the network [5, 6].

So far we have assumed that packets are transmitted without error. This assumption is valid only if the links are truly error-free and the nodes fully comply with the

transmission protocol. However, this may not necessarily be the case in a real network.

Consider a packet $P_{u\to v}$ to be transmitted from u to v. The link $u \to v$ from u to v may or may not be error-free in a real network. Thus v can be modeled to have received $P'_{u\to v} = P_{u\to v} + E_{u\to v}$, where $E_{u\to v} \in \mathbb{F}_q^n$ is an error packet injected in link $u \to v$. If $E_{u\to v} = 0$ then no error has occurred on $u \to v$.

Let $\mathcal{L}$ be the total number of links in the network. The error packets $E_1,\ E_2, \cdots, E_{|\mathcal{L}|}$ injected in each link may be stacked in a matrix,

$$E = \begin{bmatrix} E_1 \\ E_2 \\ \vdots \\ E_{\mathcal{L}} \end{bmatrix}.$$

Note that E_i with $i \in 1, 2, \cdots |\mathcal{L}|$ may be zero denoting that link i is error-free. By linearity of the network we obtain the following model for the linear network coding channel with additive errors:

$$Y = AX + BE, \tag{1.2}$$

where $B \in \mathbb{F}_q^{N\times|\mathcal{L}|}$ is the transfer matrix corresponding to the linear transformation applied to the error packets.

1.3 Error Control in Network Coding

The problem of error-correction in random network coding has recently become an active area of research [7–12]. The main motivation for this problem is the phenomenon of error-propagation in the network. Since the received packets are linear combinations of packets inserted at intermediate nodes, the system is very sensitive to transmission errors. Indeed, as illustrated in Figure 1.3, even a single corrupt packet, when combined with other packets in the network may render the entire transmission useless. Unfortunately, the error-correcting capability of any classical code designed for the Hamming metric may be overpowered by error-propagation in network coding. Thus, appropriate coding techniques based on more suitable distance metrics must be devised.

As described in the previous section, an error may occur in a network if the links are not guaranteed to be error free, or that the nodes do not fully comply with the network topology. The former corresponds to a random error model while the latter relates to

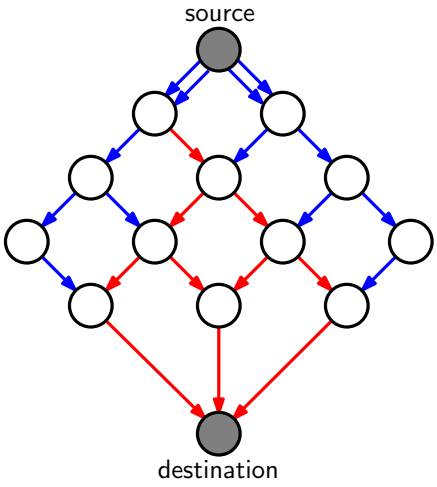

Figure 1.2: Phenomenon of Error-Propagation in Network Coding

an adversarial error model. An adversary is a malicious node that may inject erroneous packets at some or all of its outgoing links. The corrupt packets injected by an adversary cannot possibly be rejected in the lower layers. Thus the effect of an adversary must be detected in the application layer. Our focus in this thesis is on adversarial error-correction in random linear network coding. In particular we assume that the network links are error-free, while there may exist malicious nodes in the network.

Fundamental limits for adversarial error-control in network coding were first devised in [13–17] under a deterministic network coding model. The main drawback of these constructions is their requirement for the field and packet sizes to be arbitrarily large. Kötter and Kschischang showed in [11,18] that due to the vector-space preserving nature of linear network coding, subspace coding is a suitable choice for error-correction in random linear network coding. In particular they observed that under ideal circumstances the space spanned by the source packets is the same as that spanned by the received packets. Thus a message may be encoded at the transmitter in a ***vector-space*** as opposed to a ***vector***, the choice of which is conveyed via transmission of a set of spanning vectors for the space. As the generators of the input space traverse through the network, such disturbances as "insertions" and "deletions" of dimensions are applied by the channel. The degree of dissimilarity between the transmitted and the received space is captured in a metric called the "subspace distance". The received subspace is decoded to the original transmitted space using a minimum subspace distance decoder. The term "*subspace coding*" comes from the fact that the input and output alphabet are subspaces of a vector space over a finite field.

Our code construction in Chapter 4 is motivated by the work of Etzion and Silberstein in [19]. Etzion and Silberstein extended the work of Kötter and Kschischang, introducing a class of codes called "Ferrers Diagram Lifted Rank-Metric Codes" which have a slightly higher rate than those presented in [12]. A detailed review of this work is presented in Section 4.1.

In an adversarial channel any disturbance induced by the channel (i.e. injection and deletion of dimensions) is produced via injection of packets by an adversary. When the insertion and deletion of dimensions as modeled by Kötter and Kschischang is translated to the number of packets injected in the network, only decoding guarantees can be obtained for the minimum subspace distance decoder. In [20] a new metric called the *"injection distance"* is introduced which fully captures the error-correcting capability of a subspace code designed for the random network coding channel. Injection distance is closely related to but different than the subspace distance and measures the amount of effort required by an adversary to transform one subspace to another. In the case of non-constant-dimension codes, the minimum injection distance decoder is shown to correct more errors than a minimum distance decoder associated with the subspace distance.

1.4 Contributions

In this thesis we focus on bounds and constructions of subspace codes designed for the injection distance. This choice of distance metric is the main parameter that distinguishes our work from the existing literature on subspace codes constructed for random linear network coding. Note that almost all existing bounds and constructions are based on the subspace distance. Moreover, with the exception of [19], the existing schemes are designed to construct codes of constant dimension as opposed to non-constant-dimension codes. The question has been lingering however as to how much a performance gain non-constant-dimension codes can achieve as compared to constat-dimension codes. In this work, we address the construction of non-constant-dimension projective space codes. In particular,

- we derive the size of a hypothetical sphere of a fixed radius centred at a subspace in a projective space;
- we derive a Gilbert-Varshamov-type bound on the size of non-constant-dimension subspace codes designed for the injection distance, and analyze its asymptotic be-

haviour as the ambient space dimension approaches infinity;

- using the code-construction framework of Etzion and Silberstein [19], we construct new non-constant-dimension codes. In particular we propose an algorithm for partitioning the projective space via asymmetric codes; we also provide a general construction of the Ferrers Diagram Rank-Metric Codes as subcodes of linear Maximum-Rank-Distance (MRD) codes. Our codes contain more codewords than comparable codes designed for the subspace distance. Moreover, our codes contain the codes of [19] as a special case.

Part of the results in this thesis has been published in [21].

1.5 Outline

The remainder of the thesis is organized as follows:. In Chapter 2 we establish the notation used in this thesis and review mathematical preliminaries on projective spaces. We also briefly review the theory of rank-metric codes, as part of our code construction presented in Chapter 4 is based on these codes. In Chapter 3 we present a Gilbert-Varshamov-type bound on the size of projective space codes separated via a minimum injection distance. In Chapter 4, we describe our construction scheme, and present numerical results, providing comparison with the existing constructions. In Chapter 5 we provide our conclusions and suggestions for future work.

Chapter 2

Preliminaries

The aim of this chapter is to review the necessary mathematical background and establish the notation used in this thesis. We start with notations in Section 2.1. In Section 2.2 we review the projective space and Grassmannian. Finally, Section 2.6 reviews the basic theory of rank-metric codes, which is used in our construction of projective space codes introduced in Chapter 4.

2.1 Notation

Let $q \geq 2$ be a power of a prime. In this thesis, all vectors and matrices are defined over the finite field $\mathbb{F}_q$, unless otherwise mentioned. We denote by $\mathbb{F}_q^{m\times n}$, the set of all $m \times n$ matrices over $\mathbb{F}_q$. The linear span of a set of k vectors $v_1, \ldots, v_k$ is denoted by $\langle\{v_1, \ldots, v_k\}\rangle$, and the row-space of a matrix $X \in \mathbb{F}_q^{m\times n}$ by $\langle X\rangle$.

Let v be a vector. The i^{th} entry of v is denoted by v_i and the number of non-zero elements of v is denoted by $wt(v)$. We define the support set of v, denoted $\text{supp}(v)$ to be the set of indices corresponding to the non-zero entries of v. For a matrix $X \in \mathbb{F}_q^{m\times n}$ and a set $\mathcal{S} \subseteq \{1, \ldots, m\}$, we denote by $X_\mathcal{S}$ the submatrix of X consisting of the rows indexed by $\mathcal{S}$ (in increasing order). If $v = (v_1, v_2, \cdots, v_n)$ is a binary vector we denote its logical complement by $\bar{v} = (\bar{v}_1, \bar{v}_2, \cdots, \bar{v}_n)$, where $\bar{0} = 1$ and $\bar{1} = 0$.

Let x and y be two binary vectors of length n. We denote the number of positions $i \in \{0, 1, 2, \cdots, n\}$ where x_i is one and y_i is zero by $N(x, y)$, their Hamming distance by $d_H(x, y)$ and the logical AND operation between x and y by $\wedge$.

The $m \times n$ all-zero matrix and the $k \times k$ identity matrix are denoted by $\mathbf{0}_{m\times n}$ and $I_{k\times k}$ respectively. The row (column) rank of a matrix $X \in \mathbb{F}_q^{m\times n}$ is the maximum number of

rows (columns) of X that are linearly independent. As the row and the column rank of X are always equal, we may simply regard them as the rank of X, denoted $\operatorname{rank} X$. We denote the row-space of a matrix X by $\langle X \rangle$.

Let P be a logical statement. We define the function $\mathbf{I}(P)$, to take on a value of 1 if P is true, and 0 otherwise.

2.2 Projective Spaces

Definition 2.2.1. *Let $\mathbb{F}_q$ be a finite field with q elements and let V be an n-dimensional vector space over $\mathbb{F}_q$. The set of all subspaces of V forms a Projective Space $\mathcal{P}_q^n$ of order n over $\mathbb{F}_q$.*

Definition 2.2.2. *Let $\mathbb{F}_q$ be a finite field with q elements and let V be an n-dimensional vector space over $\mathbb{F}_q$. For a non-negative integer $k \leq n$ the set of all k-dimensional subspaces of V, denoted $\mathcal{G}(n,k)$ is called a Grassmannian.*

Thus $\mathcal{P}_q^n$ can be viewed as a union of the Grassmannian for all $k \leq n$, i.e.,

$$\mathcal{P}_q^n = \bigcup_{k=0}^{n} \mathcal{G}(n,k).$$

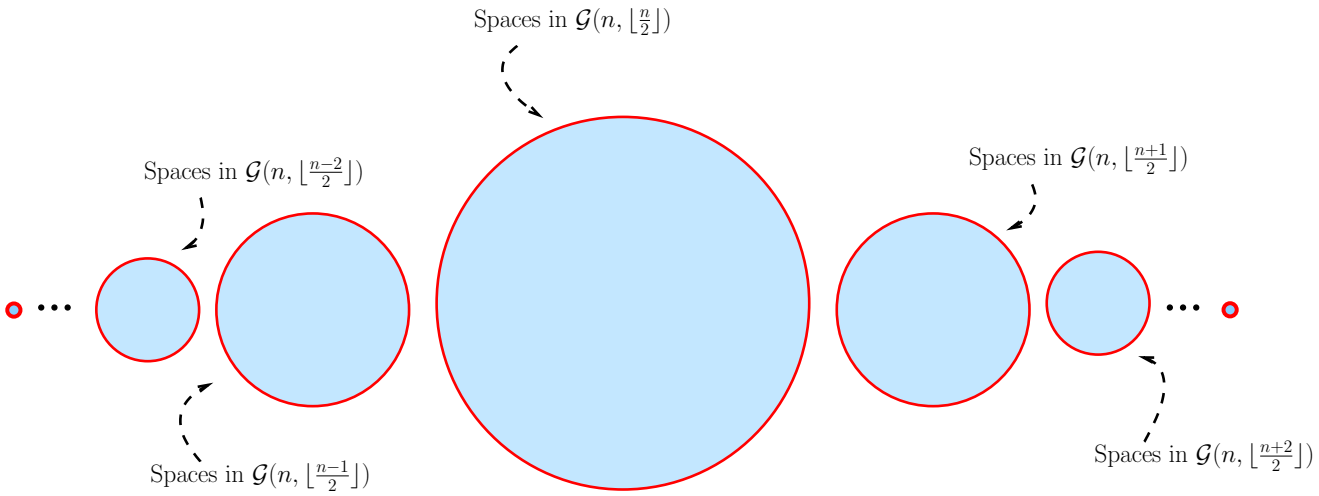

Figure 2.1: $\mathcal{P}_q^n$ viewed as a union of Grassmannian

A k-dimensional vector space V in $\mathcal{P}_q^n$ can be viewed as the row-space of a $k \times n$ generator matrix over $\mathbb{F}_q$, whose rows form a basis for V. Such a matrix is not unique, as any set

of k linearly independent vectors in V can form a basis and hence a generator matrix for V. However, exactly one such matrix is in Reduced Row Echelon Form (RREF). Hence every k-dimensional vector space V in $\mathcal{P}_q^n$ arises *uniquely* as the row-space of a $k \times n$ matrix in RREF. We denote by $RRE(M)$ the Reduced Row Echelon Form of M. Recall that if $M' = RRE(M)$, then M' satisfies the following three properties:

1. The first nonzero entry (or leading coefficient) of every row of $RRE(M')$ is **1**.
2. Every leading coefficient is the *only* nonzero entry in its column,
3. The leading coefficient of every row appears strictly to the right of that of the row above it.

Example 2.2.1. *For example* $M_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$ *and* $M_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$ *are in RREF, while* $M_3 = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$ *is not.*

Let r be an arbitrary row of $X = RRE(M)$. The first nonzero entry of r is regarded as its **leading coefficient**. Notice that since X is in RREF, if the leading coefficient of r does not appear as its first entry, it must be preceded by a number of zeros. We regard the zero entries preceding the leading coefficient of r as **terminal zeros**. We will use this terminology regarding matrices in RREF to describe the code constructions in Chapter 4.

Definition 2.2.3. *Let U and V be two subspaces in $\mathcal{P}_q^n$. The intersection*

$$U \cap V = \langle \{u : u \in U \text{ and } u \in V\} \rangle$$

is the largest vector space in $\mathcal{P}_q^n$ that is contained in both U and V.

Definition 2.2.4. *Let U and V be two subspaces in $\mathcal{P}_q^n$. The sum-space*

$$U + V = \{u + v : u \in U, v \; in V\}$$

is the smallest vector space in $\mathcal{P}_q^n$ that contains both U and V.

For two space U and V we have

$$\dim(U + V) = \dim U + \dim V - \dim (U \cap V).$$

Definition 2.2.5. *Let n and k be two non-negative integers, with $k \leq n$. The q-ary Gaussian coefficient (or the q-binomial coefficient) is defined as*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \triangleq \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} \tag{2.1}$$

Note that $\begin{bmatrix} n \\ n \end{bmatrix}_q = \begin{bmatrix} n \\ 0 \end{bmatrix}_q = 0$.

Theorem 2.2.1 ([22])**.** *The Gaussian coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_q$ *gives the number of distinct k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_q$.*

For convenience, we omit the parameter q, and will denote $\begin{bmatrix} n \\ k \end{bmatrix}_q$ by $\begin{bmatrix} n \\ k \end{bmatrix}$ in the rest of the thesis.

Lemma 2.2.1. *Let V be a k-dimensional vector space in $\mathcal{P}_q^n$, and let W be a fixed l-dimensional subspace of V. The number of m-spaces in $\mathcal{P}_q^n$ whose intersection with V is W is given by, $N(n,k,m,l) = q^{(k-l)(m-l)} \begin{bmatrix} n-k \\ m-l \end{bmatrix}$.*

Proof. We may extend W to an $(l+1)$-space $U_1 \in \mathcal{P}_q^n$ such that $U_1 \cap V = W$ in $\dfrac{q^n-q^k}{q^m-q^l}$ ways. To see this observe that we can adjoin to W any of the $q^n - q^k$ vectors not in V to construct U_1. However, by this procedure any potential m-space containing U_1 will arise exactly $q^m - q^l$ times. Similarly, we can construct an $(l+2)$-space U_2, with $U_2 \cap V = W$ in $\dfrac{q^n-q^{k+1}}{q^m-q^{l+1}}$ ways: we can adjoin to the sum-space $(W+U_1)$ any of the $q^n - q^{k+1}$ vectors that are not in the (U_1+V). However, again any m-spaces containing U_2 arises exactly $q^m - q^{l+1}$ times. Following this counting procedure recursively we obtain,

$$\begin{aligned} N &= \left(\frac{q^n-q^k}{q^m-q^l}\right)\left(\frac{q^n-q^{k+1}}{q^m-q^{l+1}}\right)\cdots\left(\frac{q^n-q^{k+m-l+1}}{q^m-q^{m-1}}\right) \\ &= q^{(k-l)(m-l)}\left(\frac{q^{n-k}-1}{q^{m-l}-1}\right)\left(\frac{q^{n-k-1}-1}{q^{m-l-1}-1}\right)\cdots\left(\frac{q^{n-k-m+l-1}-1}{q-1}\right) \\ &= q^{(k-l)(m-l)}\begin{bmatrix} n-k \\ m-l \end{bmatrix} \end{aligned}$$

□

Lemma 2.2.2. *Let V be a k-dimensional vector space in $\mathcal{P}_q^n$. The total number of m-spaces that intersect V in some l-space is given by,*

$$q^{(k-l)(m-l)}\begin{bmatrix} k \\ l \end{bmatrix}\begin{bmatrix} n-k \\ m-l \end{bmatrix}$$

Proof. Follows directly from Theorem 2.2.1 and Lemma 2.2.1. □

2.3 Metrics on Projective Spaces

Just as in classical coding theory, a notion of distance is required to quantify the distinction between codewords. In this thesis we are concerned with codes over projective spaces, hence we discuss distance metrics defined on projective spaces.

Let U and V be two distinct subspaces in $\mathcal{P}_q^n$. Although U and V are assumed to be distinct, their intersection $U \cap V$ need not be empty, however they must necessarily be different in at least a single dimension. The *subspace distance* proposed by Kötter and Kschischang in [11] captures the degree of such dissimilarity between two spaces.

Definition 2.3.1 ([11])**.** *The subspace distance between subspaces U and V in $\mathcal{P}_q^n$ is defined as follows:*

$$\begin{aligned} d_{\mathrm{S}}(U,V) &\triangleq \dim(U+V) - \dim(U \cap V) \\ &= \dim U + \dim V - 2\dim(U \cap V) \\ &= \dim(U+V) - \dim U - \dim V. \end{aligned} \tag{2.2}$$

Theorem 2.3.1 ([11])**.** *The subspace distance $d_{\mathrm{S}}(\cdot,\cdot)$ is a metric.*

Definition 2.3.2 ([20])**.** *The injection distance between two subspaces U and V in $\mathcal{P}_q^n$ is defined as follows:*

$$\begin{aligned} d_{\mathrm{I}}(U,V) &\triangleq \max\{\dim U, \dim V\} - \dim(U \cap V) \\ &= \dim(U+V) - \dim(U \cap V) \\ &= \frac{1}{2} d_{\mathrm{S}}(U,V) + \frac{1}{2} |\dim U - \dim V| \end{aligned} \tag{2.3}$$

The injection distance measures the minimum number of packet injections required for U and V to be transformed to one another. Note that if $\dim U = \dim V$ then $d_{\mathrm{I}}(U,V)$ and $d_{\mathrm{S}}(U,V)$ are equal up to scale. The minimum injection and subspace distance of a set $\Omega \subseteq \mathcal{P}_q^n$ are denoted $d_{\mathrm{I}}(\Omega)$ and $d_{\mathrm{S}}(\Omega)$ respectively.

Theorem 2.3.2 ([20])**.** *The injection distance $d_{\mathrm{I}}(\cdot,\cdot)$ is a metric.*

Let Ω be a set and δ a metric defined on Ω. We define the minimum distance of a subset $\Omega' \subseteq \Omega$ as follows:

$$\delta(\Omega') = \min_{\substack{\alpha,\beta \in \Omega' \\ \alpha \neq \beta}} \delta(\alpha,\beta) \tag{2.4}$$

In particular, let $\mathcal{S} \subseteq \mathcal{P}_q(n)$ be a set of subspaces in $\mathcal{P}_q(n)$. The minimum injection distance of $\mathcal{S}$, denoted $d_{\mathrm{I}}(\mathcal{S})$ and $d_{\mathrm{S}}(\mathcal{S})$ are defined by Equation 2.4, with Ω replaced with $\mathcal{P}_q(n)$, Ω' with $\mathcal{S}$, and δ replaced with d_{I} and d_{S} respectively.

2.4 Codes Over Projective Spaces

Having defined metrics over $\mathcal{P}_q^n$ we are now ready to formally define projective space codes. A code over $\mathcal{P}_q^n$ is a collection of subspaces $U \in \mathcal{P}_q^n$ with a prescribed minimum distance. We distinguish between codes designed for the subspace distance and those designed for the injection distance by using the following notation:

Definition 2.4.1. *A code $\mathcal{C} \subseteq \mathcal{P}_q^n$ is an $(n, d)_{d_\mathrm{S}}$ code over $\mathcal{P}_q^n$ if $d_\mathrm{S}(\mathcal{C}) = d$, i.e.*

$$\text{for all } U,\ V \in \mathcal{C},\ U \neq V\ d_\mathrm{S}(U, V) \geq d$$

Theorem 2.4.1 ([11])**.** *An $(n, d)_{d_\mathrm{S}}$ code $\mathcal{C}$ can correct any t error packets if $d_\mathrm{S}(\mathcal{C}) > 4t$.*

Definition 2.4.2. *A code $\mathcal{C} \subseteq \mathcal{P}_q^n$ is an $(n, d)_{d_\mathrm{I}}$ code over $\mathcal{P}_q^n$ if $d_\mathrm{I}(\mathcal{C}) = d$, i.e.*

$$\text{for all } U,\ V \in \mathcal{C},\ U \neq V\ d_\mathrm{I}(U, V) \geq d$$

Theorem 2.4.2 ([20])**.** *An $(n, d)_{d_\mathrm{I}}$ code $\mathcal{C}$ can correct any t error packets* ***if and only if*** *$d_\mathrm{I}(\mathcal{C}) > 2t$.*

Definition 2.4.3. *An $(n, d)_{d_\mathrm{I}}$ projective space code $\mathcal{C}$ is an (n, d, k) constant-dimension code if $\mathcal{C} \subseteq \mathcal{G}(n, k)$ for some $k \in \{0, 1, \cdots, n\}$.*

Throughout this thesis, we denote by $A_q(n, d, k)$ the maximum size of an (n, d, k) code in $\mathcal{G}_q(n, k)$. Similarly $A_q^\mathrm{S}(n, d)$ and $A_q(n, d)$ denote the maximum size of an $(n, d)_{d_\mathrm{S}}$ and $(n, d)_{d_\mathrm{I}}$ code in $\mathcal{P}_q(n)$ respectively.

Let $\Omega \subseteq \mathcal{P}_q(n)$ be an $(n, d)_{d_\mathrm{S}}$ code, and assume that there exists a channel which maps an input code $U \in \Omega$ to some subspace $V \in \mathcal{P}_q(n)$. Let $U \in \Omega$ be transmitted and $V \in \mathcal{P}_q(n)$ received. A minimum subspace distance decoder for Ω computes $\hat{U}$ according to the following decoding rule:

$$\hat{U} = \operatorname*{argmin}_{U \in \Omega} d_\mathrm{S}(U, V)$$

Similarly, if Ω is an $(n, d)_{d_\mathrm{I}}$ code, then a minimum injection decoder computes $\hat{U}$ according to $\hat{U} = \operatorname*{argmin}_{U \in \Omega} d_\mathrm{I}(U, V)$.

An example by [20] examines a situation where a subspace code designed for the injection distance may be desirable over one designed for the subspace distance in an adversarial channel.

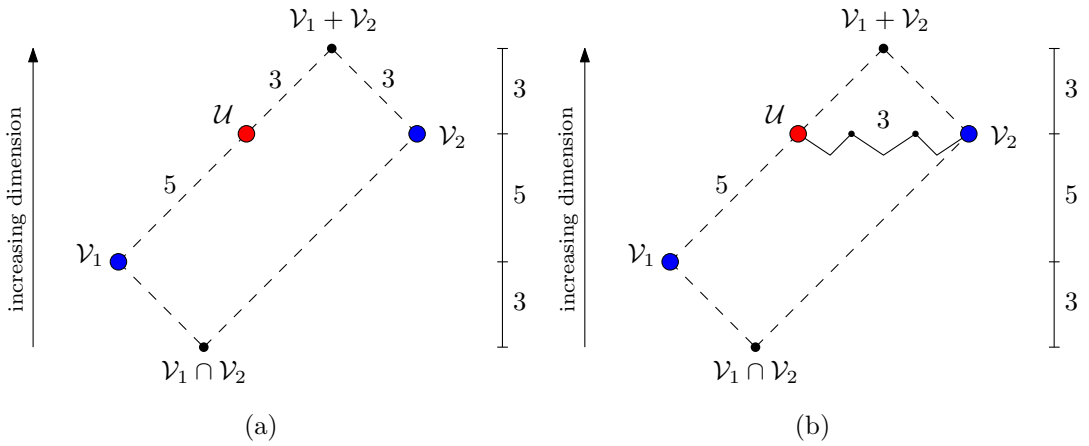

Figure 2.2: Lattice of Subspaces in Example 2.4.1: Two spaces are joined with a dashed line if one is a subspace of the other.(a) A minimum-d_{S}-decoder decodes to $\mathcal{V}_1$. (b) A minimum-d_{I}-decoder decodes to $\mathcal{V}_2$

Example 2.4.1. *Imagine a simple codebook with codewords $\mathcal{V}_1$ and $\mathcal{V}_2$. Assume that $\mathcal{U} \in \mathcal{P}_q(n)$ is received, as shown in Figure 2.4. A minimum-d_{S}-decoder decodes to $\mathcal{V}_1$ as $d_{\mathrm{S}}(\mathcal{U}, \mathcal{V}_1) = 5 < d_{\mathrm{S}}(\mathcal{U}, \mathcal{V}_2) = 6$. A minimum-$d_{\mathrm{I}}$-decoder on the other hand decodes to $\mathcal{V}_2$ as $d_{\mathrm{I}}(\mathcal{U}, \mathcal{V}_2) = 3 < d_{\mathrm{I}}(\mathcal{U}, \mathcal{V}_1) = 5$.*

Notice that the subspace distance treats insertions and deletions of dimensions symmetrically. However, as shown in Example 2.4.1 it is possible that the injection of a single packet causes a replacement of dimension which captures erasure of a dimension and insertion of another. More specifically, in the above example it is possible to transform $\mathcal{V}_2$ to $\mathcal{U}$ by injection of three packets, each of which replaces a dimension in $\mathcal{V}_2$. A minimum-d_{I}-decoder explains a received subspace with as few packet-injections as possible, thus arriving at the solution that minimizes the number of packet errors injected by an adversary.

2.5 Generalized Gilbert-Varshamov Bound for a General Metric Space

Let Ω be a set and δ a metric defined on Ω. Let $C \subseteq \Omega$ be a code of minimum distance at least d in Ω. The general derivation of the Gilbert-Varshamov bound can be described algorithmically as follows:

1. Initialize C to the emptyset, set $i = 1$ and lable all elements in Ω as "non-excluded".

2. While there are non-excluded points in Ω, do the following:

   (a) Select some non-excluded element $c_i \in \Omega$ (at random, for exmaple).

   (b) Add c_i to the code, i.e. replace C with $C \cup \{c_i\}$.

   (c) Mark c_i and all elements in Ω within distance $d-1$ from c_i as excluded.

   (d) set i to $i+1$.

Upon termination of the above algorithm C contains a collection of codewords whose minimum distance is at least d. Let $\mathcal{B}_\alpha(t) \triangleq \{\beta \in \Omega : \delta(\alpha, \beta) \leq t\}$ be a sphere of radius t centered at α in Ω. We have the following union bound:

$$\sum_{c \in C} |\mathcal{B}_c(d-1)| \geq |\Omega|, \tag{2.5}$$

If the size of a sphere in Ω depends merely on its radius, then we can simply factor out the sphere sizes from the summation in Equation 2.5 and obtain a lower bound on $|\mathcal{C}|$.

For example, in classical coding theory, the distance metric used is the familiar Hamming distance and the code alphabet forms a homogeneous space (i.e. Hamming space) in which the sphere sizes are independent of their centres. Due to the homogeneity of the Hamming space, derivation of the classical Gilbert-Varshamov bound is rather simple. Irrespective of its centre, the size of a Hamming sphere of radius t in $\mathbb{F}_q^n$ is given by $\sum_{j=0}^{t} \binom{n}{j} (q-1)^j$. In this case, we obtain the Gilbert-Varshamov bound from Equation 2.5:

$$|C| \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{j} (q-1)^j}.$$

Now assume that Ω is not a homogenous space in the sense that spheres of the same radius in Ω are not all of the samse size. In this case the above approach may not be suitable for the derivation of a Gilbart-Varshamov bound for codes over Ω.

In [23] Tolhuizen extends the general idea of Gilbert-Varshamov bound to such spaces. Let $\overline{B}(t) \triangleq \frac{1}{|\Omega|} \sum_{\alpha \in \Omega} |\mathcal{B}_\alpha(t)|$ denote the average size of a sphere of radius t in Ω. Tolhuizen showed in [23] that the maximum size of a code $C \subseteq \Omega$ of minimum distance d is at least $\frac{|\Omega|}{|\overline{B}(d-1)|}$.

We use this result in Section 3.3 to obtain a Gilbert-Varshamov bound on $A_q(n, d)$. Therefore, in this section we provide a detailed review of this general method. First, we need the following definition and theorem from extremal graph-theory:

Definition 2.5.1 (k-Clique in a Graph [24])**.** *Let $G = (\mathcal{V}, \mathcal{E})$ be an undirected graph. A subset $\mathcal{V}' \subseteq \mathcal{V}$ of cardinality k is said to form a k-clique if there exists an edge between every pair of vertices in $\mathcal{V}'$.*

Theorem 2.5.1 (Túran's Theorem [24])**.** *If a graph $G = (\mathcal{V}, \mathcal{E})$ on n-vertices has no k-clique, with $k \geq 3$, then*

$$|\mathcal{E}| \leq (1 - \frac{1}{k-1})\frac{n^2}{2}$$

In order to construct a code $\mathcal{C}$ of minimum distance $\delta(\mathcal{C}) = d$ in Ω we may first construct a graph G with vertex set $\mathcal{V} = \Omega$, in which two vertices x and y are adjacent if and only if $\delta(x, y) \geq d$. The induced subgraph is a code in Ω with minimum distance d. Thus designing a code of cardinality k in $\mathcal{P}_q(n)$ is equivalent to finding a k-clique in G. Let $\mathcal{E}$ denote the edge set of G. We have

$$|\mathcal{E}| = \frac{1}{2}\sum_{x\in\Omega}(|\Omega| - |\mathcal{B}_x(d-1)|)$$

where, the factor of $\frac{1}{2}$ is due to the symmetric property of $\delta(\cdot, \cdot)$.

Let $\overline{B}(d-1) = \frac{1}{|\Omega|}\sum_{X\in\Omega}|\mathcal{B}_x(d-1)|$ denote the average sphere size in Ω. Then,

$$\begin{aligned} |\mathcal{E}| &= \frac{1}{2}\sum_{x\in\Omega}(|\mathcal{P}_q(n)| - |\mathcal{B}_x(d-1)|) \\ &= \frac{1}{2}|\mathcal{P}_q(n)|\,(|\Omega| - \overline{B}(d-1)). \end{aligned} \tag{2.6}$$

Now, by Turan's Theorem, in order to have a code of cardinality k and minimum distance d, $|\mathcal{E}|$ must satisfy $|\mathcal{E}| > \frac{k-2}{k-1}\frac{|\Omega|^2}{2}$. Substituting $|\mathcal{E}|$ with Equation 2.6 we must have $k < 1 + \frac{|\Omega|}{\overline{B}(d-1)}$. Thus, for a code $\mathcal{C}$ of maximum size in Ω we have,

$$\begin{aligned} |\mathcal{C}| &\geq \frac{|\Omega|}{\overline{B}(d-1)} \\ &= \frac{|\Omega|^2}{\sum_{x\in\Omega}|\mathcal{B}_x(d-1)|} \end{aligned}$$

2.6 Rank-Metric Codes

Let X and Y be two matrices in $\mathbb{F}_q^{m\times n}$. The *rank distance* between X and Y, denoted $d_R(X, Y)$ is defined as

$$d_R(X, Y) \triangleq \text{rank}(Y - X) \tag{2.7}$$

As shown in [25] the rank distance is indeed a *metric*. In particular it satisfies the triangle inequality, due to the following familiar property of matrices:

$$\text{for all } X,\ Y \in \mathbb{F}_q^{m\times n}\ \operatorname{rank}(X+Y) \leq \operatorname{rank} X + \operatorname{rank} Y$$

Thus $\mathbb{F}_q^{m\times n}$ is a metric-space. A *rank-metric code* $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ is a matrix code used in the context of the rank metric. The *minimum rank distance* of $\mathcal{C}$, denoted $d_R(\mathcal{C})$, is the minimum rank distance between all pairs of distinct codewords in $\mathcal{C}$, i.e.

$$d_R(\mathcal{C}) \triangleq \min_{x\neq y\in C} \operatorname{rank}(x-y) \tag{2.8}$$

There exists a rich coding theory for rank-metric codes that is analogous to the classical coding theory in the Hamming space. In particular, the following theorem due to [25] gives a Singleton-type bound for rank metric codes.

Theorem 2.6.1. *Every rank metric code $\mathcal{C}$ must satisfy*

$$\log_q |\mathcal{C}| \ \leq\ \max\{m,n\}(\min\{m,n\} - d + 1) \tag{2.9}$$

A rank metric code achieving the bound of Theorem 2.6.1 with equality is said to be a Maximum-Rank-Distance (MRD) code. MRD codes are known to exist for all choice of parameters q, m, n and $d \leq \min\{m,n\}$.

Let $\mathbb{F}_q$ be a field with q elements, where $q \geq 2$ is a power of a prime. Let $\mathbb{F}_{q^m}$ with $m \geq 1$ be an extension of $\mathbb{F}_q$. Since $\mathbb{F}_{q^m}$ can also be regarded as an m-dimensional vector space over $\mathbb{F}_q$, for any basis of $\mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$ an element of $\mathbb{F}_{q^m}$ can be expanded to a vector of length m over $\mathbb{F}_q$. Thus the rank of a vector $v = (v_1, v_2, \cdots, v_n) \in \mathbb{F}_{q^m}^n$ is the rank of the $m \times n$ matrix obtained by expanding each entry of v to an $m \times 1$ column vector over $\mathbb{F}_q$. In this context, a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ can simply be regarded as a block code of length n over $\mathbb{F}_{q^m}$. Gabidulin codes, presented by Gabidulin [25] are an important class of MRD codes, which are the analogues of the Generalized Reed-Solomon codes designed for the rank metric.

Let $q \geq 2$ be a power of a prime and let $g_1, g_2, \cdots g_n \in \mathbb{F}_{q^m}$ with $m \geq 1$ be linearly independent over the base field $\mathbb{F}_q$. A *Gabidulin* code with minimum rank distance $d_R(\mathcal{G}) = d$ is a rank metric code that has as its generator matrix,

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{[k-1]} & g_2^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix} \tag{2.10}$$

where $[i] = q^i$. Similarly, its parity check matrix has the form,

$$H = \begin{pmatrix} h_1 & h_2 & \cdots & h_n \\ h_1^{[1]} & h_2^{[1]} & \cdots & h_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ h_1^{[k-1]} & h_2^{[k-1]} & \cdots & h_n^{[k-1]} \end{pmatrix} \tag{2.11}$$

where $h_1, \cdots, h_n \in \mathbb{F}_{q^m}$ are linearly independent over $\mathbb{F}_q$ and $k = \log |\mathcal{G}|$. Efficient polynomial-time decoding algorithms exist that correct errors of rank up to $\left\lfloor \frac{d-1}{2} \right\rfloor$; see [26] and references therein.

Chapter 3

Bounds on the Parameters of Projective Space Codes

In this chapter we derive a generalized Gilbert-Varshamov-type bound on the size of $(n, d)_{d_\mathrm{I}}$ codes. We start in Section 3.1 with the formulation of spheres in any metric space and in particular in $\mathcal{P}_q(n)$. We also review the existing Gilbert-Varshamov-type bounds on the size of (n, d, k) and $(n, d)_{d_\mathrm{S}}$ codes. In Section 3.2 we derive the size of a sphere in $\mathcal{P}_q(n)$, where d_I is used as a measure of distance. In Section 3.3, we present our derivation of the generalized Gilbert-Varshamov-type bound the size of $(n, d)_{d_\mathrm{I}}$ codes. For completeness, a survey on existing bounds on the size of constant-dimension (n, d, k) subspace codes, as well as non-constant-dimension $(n, d)_{d_\mathrm{S}}$ codes is included in Appendix B.

3.1 Background and Related Work

3.1.1 Spheres in $\mathcal{P}_q(n)$

Let Ω be a set and δ a metric defined on Ω. A sphere (ball) of radius t centred at α is defined as the set of all elements in Ω at a distance *at most* t from α, i.e.

$$\mathcal{B}_\alpha(t) \triangleq \{\beta \in \Omega : \delta(\alpha, \beta) \leq t\}.$$

As discussed in Section 2.2, a projective space $\mathcal{P}_q(n)$ of order n forms metric spaces $(\mathcal{P}_q(n), d_\mathrm{I})$ and $(\mathcal{P}_q(n), d_\mathrm{S})$ with respect to $d_\mathrm{I}(\cdot, \cdot)$ and $d_\mathrm{S}(\cdot, \cdot)$ respectively. Thus spheres centred at a subspace $V \in \mathcal{P}_q(n)$, may be defined in both metric spaces $(\mathcal{P}_q(n), d_\mathrm{S})$ and $(\mathcal{P}_q(n), d_\mathrm{I})$. We denote a sphere of radius t centred at some $V \in (\mathcal{P}_q(n), d_\mathrm{I})$ by $\mathcal{B}_V(t)$, and one centred at some $V \in (\mathcal{P}_q(n), d_\mathrm{S})$ by $\mathcal{B}^S_V(t)$. Kötter and Kschischang give the

following expression for the size of $\mathcal{B}_V^S(t,k)$ in $\mathcal{G}_q(n,k)$:

Theorem 3.1.1 ([11]). *Let $\mathcal{B}_V(t,k)$ denote the set of all spaces in $\mathcal{G}_q(n,k)$ with subspace distance at most $t \leq 2k$ from $V \in \mathcal{G}_q(n,k)$. The number of spaces in $\mathcal{B}_V^S(t,k)$, denoted $B(t,k)$ is independent of V and equals*

$$|\mathcal{B}_V(t,k)| = \sum_{i=0}^{t} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ i \end{bmatrix}$$

The size of a non-constant-dimension sphere $\mathcal{B}_V^S(t)$ within $\mathcal{P}_q(n)$ is given in [7] as follows:

Theorem 3.1.2 ([7]). *Let V be a space of dimension $k \leq n$ in $\mathcal{P}_q(n)$. For $t \leq n$, the number of spaces in $\mathcal{B}_V^S(t)$ is given by*

$$|\mathcal{B}_V^S(t)| = \sum_{r=0}^{t} \sum_{j=0}^{r} q^{j(r-j)} \begin{bmatrix} n-k \\ r-j \end{bmatrix} \begin{bmatrix} k \\ j \end{bmatrix} \begin{bmatrix} n \\ k \end{bmatrix}$$

3.1.2 Gilbert-Varshamov-type Bounds on $A_q(n,d,k)$ and $A_q^{\mathrm{S}}(n,d)$

In Section 2.5 we presented a general discussion on Gilbert-Varshamov bound for codes in any metric space. As discussed in Section 2.5, the derivation of a Gilbert-Varshamov bound on the size of codes in a homogeneous metric-space is rather simple. This is due to the fact that the size of a sphere in such a space is independent of its center. This condition holds for constant-dimension codes in $\mathcal{G}_q(n,k)$. In particular, by Theorem 3.1.1 the size of a sphere $\mathcal{B}_V(t,k)$ in $\mathcal{G}_q(n,k)$ is independent of V. In this case Equation 2.5 results in the following Gilbert-Varshamov bound for $A_q(n,d,k)$ established by Kötter and Kschischang:

Theorem 3.1.3 ([11]).

$$A_q(n,d,k) \geq \frac{|\mathcal{G}_q(n,k)|}{B(d-1,k)} = \frac{\begin{bmatrix} n \\ k \end{bmatrix}}{q^{(d-1)^2} \begin{bmatrix} k \\ d-1 \end{bmatrix} \begin{bmatrix} n-k \\ d-1 \end{bmatrix}}$$

By Theorem 3.1.2 the size of a sphere $\mathcal{B}_V^S(t)$ of radius t centred at $V \in \mathcal{P}_q(n)$ depends on $\dim V$ as well. Thus, as discussed in Section 2.5, the classical approach may not be suitable for the derivation of a Gilbart-Varshamov bound in $\mathcal{P}_q(n)$. Using the method by Tolhuizen [23] (described in Section 2.5), Etzion and Vardy [7] present the following Gilbert-Varshamov bound on the size of $(n,d)_{d_{\mathrm{S}}}$ codes in $\mathcal{P}_q(n)$:

Theorem 3.1.4 ([7])**.**

$$A_q^{\mathrm{S}}(n,d) \geq \frac{|\mathcal{P}_q(n)|^2}{\sum_{k=0}^{n}\sum_{j=0}^{d-1}\sum_{i=0}^{j}\begin{bmatrix}n-k\\ j-i\end{bmatrix}\begin{bmatrix}k\\ i\end{bmatrix}\begin{bmatrix}n\\ k\end{bmatrix}q^{i(j-i)}}$$

In Section 3.3 we take a similar approach to obtain a Gilbert-Varshamov-type bound on the size of $(n,d)_{d_{\mathrm{I}}}$ codes.

3.2 Spheres in $\mathcal{P}_q(n)$ with Distance Measured According to d_{I}

Definition 3.2.1. *Let V be a k-dimensional subspace in $\mathcal{P}_q(n)$. We define $\mathcal{S}_V(t)$ to be the set of all spaces in $\mathcal{P}_q(n)$ at an injection distance t from V. i.e.*

$$\mathcal{S}_V(t) = \{W \in \mathcal{P}^n | d_I(V,W) = t\}$$

We may view $\mathcal{S}_V(t)$ as a *shell* of radius t centred at V. A sphere $\mathcal{B}_V(t)$ is then a union of shells of radii $r \in \{0,1,2,\cdots,t\}$, i.e. $\mathcal{B}_V(t) = \bigcup_{r=0}^{t} \mathcal{S}_V(t)$

In Theorem 3.2.1 we give the cardinality of $\mathcal{S}_V(t)$, which is independent of the choice of V and depends merely on t and the dimension of V. We use Lemma 3.2.1 to obtain $|\mathcal{S}_V(t)|$.

Lemma 3.2.1. *Let V be a k-dimensional space in $\mathcal{P}_q(n)$. Then $S(k,t,m) = |\mathcal{S}_V(t) \cap \mathcal{G}_q(n,m)|$ is given by,*

$$S(k,t,m) = q^{t(m-k+t)}\begin{bmatrix}k\\ t\end{bmatrix}\begin{bmatrix}n-k\\ m-k+t\end{bmatrix}\mathbf{I}(m \leq k) + q^{t(k-m+t)}\begin{bmatrix}k\\ m-t\end{bmatrix}\begin{bmatrix}n-k\\ t\end{bmatrix}\mathbf{I}(m > k)$$

Proof. See Appendix A. □

Theorem 3.2.1. *Let V be a k-dimensional subspace in $\mathcal{P}_q(n)$, with $k \in \{0,1,\cdots,n\}$. Then,*

$$|S_V(t)| = q^{t^2}\begin{bmatrix}k\\ t\end{bmatrix}\begin{bmatrix}n-k\\ t\end{bmatrix} + \sum_{j=1}^{t} q^{t(t-j)}\left(\begin{bmatrix}k\\ t\end{bmatrix}\begin{bmatrix}n-k\\ t-j\end{bmatrix} + \begin{bmatrix}n-k\\ t\end{bmatrix}\begin{bmatrix}k\\ t-j\end{bmatrix}\right) \tag{3.1}$$

Proof. We have,

$$\begin{aligned}
|\mathcal{S}_V(t)| &= \left|\bigcup_{m=0}^{n} \mathcal{S}_V(t) \cap \mathcal{G}_q(n,m)\right| \\
&= \sum_{m=0}^{n} S(k,t,m) && (3.2)\\
&= \sum_{m=0}^{k} q^{t(m-k+t)} \begin{bmatrix} k \\ t \end{bmatrix} \begin{bmatrix} n-k \\ m-k+t \end{bmatrix} + \sum_{m=k+1}^{n} q^{t(k-m+t)} \begin{bmatrix} k \\ m-t \end{bmatrix} \begin{bmatrix} n-k \\ t \end{bmatrix} && (3.3)\\
&= \begin{bmatrix} k \\ t \end{bmatrix} \sum_{j=0}^{t} q^{t(t-j)} \begin{bmatrix} n-k \\ t-j \end{bmatrix} + \begin{bmatrix} n-k \\ t \end{bmatrix} \sum_{j=1}^{t} q^{t(t-j)} \begin{bmatrix} k \\ t-j \end{bmatrix} && (3.4)\\
&= q^{t^2} \begin{bmatrix} k \\ t \end{bmatrix} \begin{bmatrix} n-k \\ t \end{bmatrix} + \sum_{j=1}^{t} q^{t(t-j)} \left(\begin{bmatrix} k \\ t \end{bmatrix} \begin{bmatrix} n-k \\ t-j \end{bmatrix} + \begin{bmatrix} n-k \\ t \end{bmatrix} \begin{bmatrix} k \\ t-j \end{bmatrix} \right),
\end{aligned}$$

where Equation 3.2 follows from the fact that the Grassmannians of distinct dimensions are disjoint, i.e. for all $m_1 \neq m_2 \in \{0, 1, \cdots n\}$, $\mathcal{G}_q(n, m_1) \cap \mathcal{G}_q(n, m_2) = \emptyset$. Equation 3.3 follows from Lemma 3.2.1 and Equation 3.4 is obtained by a simple change of variables. □

Using Lemma 3.2.1, we derive the size of a non-constant-dimension sphere $\mathcal{B}_V(t)$ within $\mathcal{P}_q(n)$ in the following theorem:

Theorem 3.2.2. *Let V be a k-dimensional subspace in $\mathcal{P}_q(n)$, with $k \geq n$. Then,*

$$|\mathcal{B}_V(t)| = \sum_{i=0}^{t} \left(q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ i \end{bmatrix} + \sum_{j=1}^{i} q^{i(i-j)} \left(\begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ i-j \end{bmatrix} + \begin{bmatrix} n-k \\ i \end{bmatrix} \begin{bmatrix} k \\ i-j \end{bmatrix} \right) \right)$$

Proof. We may view $\mathcal{B}_V(t)$ as a union of shells of radii at most t centred at V: $\mathcal{B}_V(t) = \bigcup_{i=1}^{t} \mathcal{S}_V(i)$. Shells of different radii centred at the same subspace $V \in \mathcal{P}_q(n)$ are disjoint, i.e. for all $i \neq i'$, $\mathcal{S}_V(i) \cap \mathcal{S}_V(i') = \emptyset$. Thus, $|\mathcal{B}_V(t)| = \sum_{i=1}^{t} |\mathcal{S}_V(t)|$ and Theorem 3.2.2 follows directly from Theorem 3.2.1. □

3.3 A Gilbert-Varshamov-type Bound for $(n, d)_{d_I}$ Codes

In this section we derive a Gilbert-Varshamov-type bound on the size of codes in the projective space, with a prescribed minimum injection distance.

As shown in Section 3.2, the size of a sphere $\mathcal{B}_V(t)$ centred at some subspace $V \in \mathcal{P}_q(n)$ depends on $\dim V$. Figure 3.1 shows the geometry of a Gilbert-Varshamov-type bound in $\mathcal{P}_q(n)$, illustrating that spheres of the same radius are not necessarily of the same size in this case. For this reason we take the approach presented by Tolhuizen [23] in our derivation of the Gilbert-Varshamov bound for codes over $\mathcal{P}_q(n)$, which extends the general Gilbert-Varshamov bound to graphs that are not necessarily distance-regular. This method is fully described in Section 2.5 for general metric spaces.

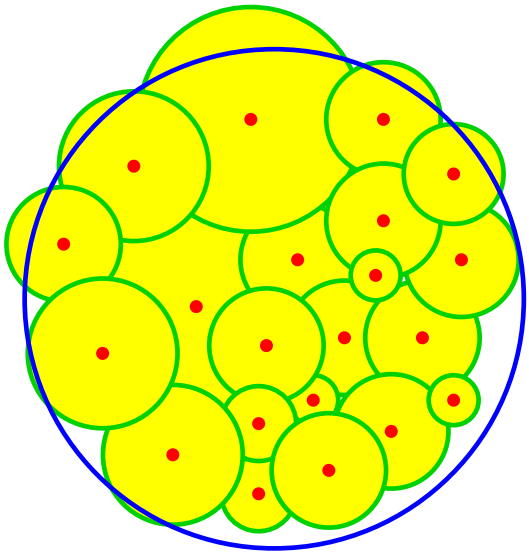

Figure 3.1: Geometry of the Gilbert-Varshamov bound in $\mathcal{P}_q(n)$

The general idea in this approach is to first translate the code design problem to the problem of finding a clique in a simple graph, and apply Turan's Theorem (Theorem 2.5.1) to obtain the bound.

Let

$$\overline{B}(d-1) = \frac{1}{|\mathcal{P}_q(n)|} \sum_{X \in \mathcal{P}_q(n)} |\mathcal{B}_X(d-1)|\,, \tag{3.5}$$

denote the average sphere size in $\mathcal{P}_q(n)$. Let $\mathcal{C}$ be an $(n,d)_{d_{\mathrm{I}}}$ code of maximum size in $\mathcal{P}_q(n)$. Then, by the general method described in Section 2.5, and Theorem 3.2.2 we have,

$$|\mathcal{C}| \;\geq\; \frac{|\mathcal{P}_q(n)|^2}{\displaystyle\sum_{k=0}^{n} \left(\begin{bmatrix} n \\ k \end{bmatrix} \sum_{i=1}^{t} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ i \end{bmatrix} + \sum_{j=1}^{i} q^{i(i-j)} \left(\begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ i-j \end{bmatrix} + \begin{bmatrix} n-k \\ i \end{bmatrix} \begin{bmatrix} k \\ i-j \end{bmatrix} \right) \right)}$$

3.4 Asymptotic Behaviour of Gilbert-Varshamov Bound

In this section we analyze the asymptotic behaviour of the Gilbert-Varshamov bound presented in Section 3.3.

The following upper and lower bound on the Gaussian coefficient is presented in [18]:

$$q^{i(n-i)} \leq \begin{bmatrix} n \\ i \end{bmatrix} \leq h(q)q^{i(n-i)}, \tag{3.6}$$

where $h(q) = \prod_{j=0}^{\infty} \frac{1}{1-q^{-j}}$. Moreover, it has been shown in [18] that $h(q)$ decreases monotonically with q, approaching $q/(q-1)$ for large q. The series for $h(q)$ converges rapidly; the following table lists $h(q)$ for various values of q.

q	2	3	4	5	7	8	9	11	16	32	64	128	256
$h(q)$	3.46	1.78	1.45	1.31	1.19	1.16	1.14	1.11	1.07	1.03	1.01	1.01	1.003

Thus for large values of n we may assume that $\begin{bmatrix} n \\ i \end{bmatrix} \simeq q^{i(n-i)}$.

In Theorem 3.4.1 we show that in the limit as n approaches infinity, the Gilbert-Varshamov bound of Section 3.3 approaches the Gilbert-Varshamov bound on the size of constant-dimension codes contained within $\mathcal{G}_q(n, \lfloor \frac{n}{2} \rfloor)$. We use Lemma 3.4.3 and Lemma 3.4.2 and Lemma 3.4.3 in the proof of Theorem 3.4.1.

Lemma 3.4.1. *Let $k \in \{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil\}$, where n is the ambient space dimension of $\mathcal{P}_q(n)$. We have,*

$$\left(\frac{3-(-1)^n}{2}\right)(1 + \frac{n}{h(q)}q^{-\frac{n^2}{4}}) \leq \frac{|\mathcal{P}_q(n)|}{|\mathcal{G}_q(n,k)|} \leq \left(\frac{3-(-1)^n}{2}\right)(1 + nh(q)q^{-\frac{n^2}{4}}).$$

Proof. See Appendix A. □

Lemma 3.4.2. *Let $\overline{B}(t)$ denote the average size of a sphere of radius t in $\mathcal{P}_q(n)$ as defined by Equation 3.5. We have,*

$$\overline{B}(t) \leq \left(\frac{3-(-1)^n}{2}\right)\left(\sum_{i=0}^{t} q^{i^2} \begin{bmatrix} \ell \\ t \end{bmatrix}^2 + n^2h^2(q)q^{-\frac{n^2}{4}}\right)$$

Proof. See Appendix A. □

Lemma 3.4.3. *Let $\overline{B}(t)$ denote the average size of a sphere of radius t in $\mathcal{P}_q(n)$ as defined by Equation 3.5. We have,*

$$\overline{B}(t) \geq \left(\frac{3-(-1)^n}{2}\right)\left(\sum_{i=0}^{t} q^{i^2}\begin{bmatrix}\ell\\ t\end{bmatrix}^2\right)$$

Proof. See Appendix A. □

Theorem 3.4.1. $\lim_{n\to\infty} A_q(n,d) \geq \lim_{n\to\infty} \dfrac{|\mathcal{P}_q(n)|}{\overline{B}(d-1)} = \dfrac{\begin{bmatrix} n \\ \lfloor \frac{n}{2} \rfloor \end{bmatrix}}{\sum_{i=0}^{d-1} q^{i^2} \begin{bmatrix} \lfloor \frac{n}{2} \rfloor \\ i \end{bmatrix}^2}$

Proof. Let $k = \lfloor \frac{n}{2} \rfloor$. Replacing $|\mathcal{P}_q(n)|$ and $\overline{B}(d-1)$ with their corresponding upper and lower bounds as given by Lemma 3.4.3, Lemma 3.4.3 and Lemma 3.4.2 we have,

$$\frac{(1+nh(q)^{-1}q^{-\frac{n^2}{4}})|\mathcal{G}_q(n,k)|}{\left(\sum_{i=0}^{d-1} q^{i^2}\begin{bmatrix}k\\ i\end{bmatrix}^2 + n^2h^2(q)q^{-\frac{n^2}{4}}\right)} \leq \frac{|\mathcal{P}_q(n)|}{\overline{B}(d-1)} \leq \frac{(1+nh(q)q^{-\frac{n^2}{4}})|\mathcal{G}_q(n,k)|}{\left(\sum_{i=0}^{d-1} q^{i^2}\begin{bmatrix}k\\ i\end{bmatrix}^2\right)}$$

$$\lim_{n\to\infty} \frac{|\mathcal{P}_q(n)|}{\overline{B}(d-1)} = \frac{|\mathcal{G}_q(n,k)|}{\sum_{i=0}^{d-1} q^{i^2}\begin{bmatrix}k\\ i\end{bmatrix}^2}.$$

This limit is the Gilbert-Varshamov bound of Theorem 3.1.4 for constant-dimension codes in $\mathcal{G}_q(n,k)$. □

Chapter 4

Code Construction for the Injection Metric

Due their application in network coding, projective space codes have attracted a great amount of interest [8–12,18,19,27–29]. It has been shown in [12,27,28] that nearly optimal subspace codes in the Grassmannian can be obtained directly from optimal rank-metric codes. With this approach the decoding problem for random network coding can be reformulated purely in terms of rank-metric terms, allowing many tools from the theory of rank-metric codes to be applied to random network coding. In [19] Etzion and Silberstein introduce a multi-level scheme for constructing codes $(n, d, k)_q$ and $(n, d)_{d_{\mathrm{S}}}$ codes in $\mathcal{P}_q(n)$ as unions of lifted rank-metric codes. This construction has the constructions of [8,9] as a special case. Motivated by their approach, in this chapter we provide a multi-level scheme for constructing $(n, d)_{d_{\mathrm{I}}}$ codes in $\mathcal{P}_q(n)$. Our work in this chapter has the construction of [19] as a special case.

4.1 Background and Related Work

Construction of lifted rank-metric codes was first proposed in [29], and then rediscovered in [18] for the special case where the rank-metric code is a Gabidulin code. The construction was later explained in [27, 28] in the context of the subspace/injection distance. In this section we provide a brief review of the lifting construction as presented in [27, 28], and describe the scheme of [19].

4.1.1 Lifted Rank-Metric Codes

For a matrix $x \in \mathbb{F}_q^{k\times m}$, let the subspace $\mathcal{I}(x) \triangleq \left\langle \begin{bmatrix} I_{k\times k} & x \end{bmatrix} \right\rangle$ be called the *lifting* of x. Similarly, for a matrix code $\mathcal{C} \subseteq \mathbb{F}_q^{k\times m}$, let the subspace code $\mathcal{I}(\mathcal{C}) \triangleq \{\mathcal{I}(x),\, x \in \mathcal{C}\}$ be called the *lifting* of $\mathcal{C}$. Since every subspace corresponds to a unique matrix in reduced row echelon form, we have that the mapping $x \to \mathcal{I}(x)$ is injective, and therefore $|\mathcal{I}(\mathcal{C})| = |\mathcal{C}|$. Note that $\mathcal{I}(\mathcal{C})$ is a constant-dimension code, i.e., $\mathcal{I}(\mathcal{C}) \subseteq \mathcal{G}_q(k+m, k)$.

Lemma 4.1.1 (Lifting Lemma [27])**.** *For all $x, x' \in \mathbb{F}_q^{k\times m}$ and all $\mathcal{C} \subseteq \mathbb{F}_q^{k\times m}$,*

$$d_{\mathrm{I}}(\mathcal{I}(x), \mathcal{I}(x')) = d_{\mathrm{R}}(x, x')$$
$$d_{\mathrm{I}}(\mathcal{I}(\mathcal{C})) = d_{\mathrm{R}}(\mathcal{C}).$$

Proof. We have

$$\begin{aligned} d_{\mathrm{I}}(\mathcal{I}(x), \mathcal{I}(x')) &= \dim(\mathcal{I}(x) + \mathcal{I}(x')) - \min\{\dim \mathcal{I}(x),\, \dim \mathcal{I}(x')\} \\ &= \operatorname{rank} \begin{bmatrix} I & x \\ I & x' \end{bmatrix} - k \\ &= \operatorname{rank} \begin{bmatrix} I & x \\ 0 & x' - x \end{bmatrix} - k \\ &= \operatorname{rank}(x' - x). \end{aligned}$$

The second statement is immediate. □

Lemma 4.1.1 shows that a subspace code constructed by lifting inherits the distance properties of its underlying rank-metric code. In particular, let $\mathcal{C} \subseteq \mathbb{F}_q^{k\times(n-k)}$ be an MRD code with $d_{\mathrm{R}}(\mathcal{C}) = d$. Then $\mathcal{I}(\mathcal{C})$ is an (n, d, k) code with cardinality

$$|\mathcal{I}(\mathcal{C})| = q^{\max\{k,n-k\}(\min\{k,n-k\}-d+1)}. \tag{4.1}$$

In [27] Silva et al. introduce a generalized decoding rule for rank-metric codes and show that the minimum subspace distance decoding rule discussed in Section 2.4 may be reformulated to this generalized decoding rule. More specifically they introduce a method for a subspace code obtained by lifting a rank-metric code $\mathcal{C}$ to be decoded using a minimum-rank-distance decoder for $\mathcal{C}$.

4.1.2 Lifted Ferrers Diagram Rank-Metric Codes

In [19] Etzion and Silberstein provide a multi-level construction for codes in $\mathcal{P}_q(n)$. The main idea in this construction is to first partition $\mathcal{P}_q(n)$ into disjoint cells with minimum inter-cell distance d. Then within each cell rank-metric codes are used to preserve a minimum intra-cell distance d. The union of spaces so-obtained makes the code. Below we describe this construction with a slightly different notation.

Definition 4.1.1. *Let V be a subspace in $\mathcal{P}_q(n)$ and let $E(V)$ be its corresponding generator matrix in RREF. Define the profile vector of V denoted $p(V)$, to be a binary vector of length n whose non-zero elements appear only in positions where $E(V)$ has a leading 1.*

Example 4.1.1. *For example, if $E(V)$ is of the form,*

$$E(V) = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

then $p(V) = (1, 0, 1, 1, 0, 0)$.

Theorem 4.1.1 ([19])**.** *Let U and V be two subspaces in $\mathcal{P}_q(n)$, with profile vectors u, and v respectively. Then $d_{\mathrm{S}}(U, V) \geq d_H(x, y)$.*

Proof. First note that the dimension of a subspace is equal to the Hamming weight of its profile vector, i.e. $\dim U = wt(u)$ and $\dim V = wt(v)$. Now let $w = u \wedge v$ and observe that $\dim(U \cap V) \leq wt(w)$. We have

$$\begin{aligned} N(u, v) &= wt(u) - wt(w) \\ &= \dim U - wt(w) \\ &\leq \dim U - \dim(U \cap V) \end{aligned}$$

Similarly $N(v, u) \leq \dim V - \dim(U \cap V)$, thus we have

$$\begin{aligned} d_H(u, v) = N(u, v) + N(v, u) &\leq \dim U + \dim V - 2\dim(U \cap V) \\ &= d_{\mathrm{S}}(U, V) \end{aligned}$$

□

Notice that the profile vector $(1,0,1,1,0,0)$ belongs not only to V considered in example 4.1.1, but also to any 3×6 matrix in RREF, whose rows have their leading coefficients in columns 1, 3 and 4. In fact, all 2^7 generator matrices of the form

$$\begin{bmatrix} 1 & \bullet & 0 & 0 & \bullet & \bullet \\ 0 & 0 & 1 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 1 & \bullet & \bullet \end{bmatrix}$$

regardless of the values of their entries in positions marked by a '$\bullet$' are identified by the same profile vector $(1,0,1,1,0,0)$.

Consider a relation $\sim$ on $\mathcal{P}_q(n)$ where

$$\text{for all } U,\ V \in \mathcal{P}_q(n),\ U \sim V \leftrightarrow p(U) = p(V). \tag{4.2}$$

Clearly $\sim$ is an equivalence relation on $\mathcal{P}_q(n)$, as it is reflexive, symmetric and transitive. Thus, it partitions $\mathcal{P}_q(n)$ into equivalence classes, where U and V belong to the same class provided that they are identified by the same profile vector. Each such class is commonly called a "Schubert cell". Moreover, every binary vector $v \in \{0,1\}^n$ corresponds to a unique class of subspaces in $\mathcal{P}_q(n)$ whose generator matrices in RREF have the same skeleton. We refer to such skeleton for the generator matrix of each class as its profile matrix. More formally, we have the following definition:

Definition 4.1.2. *Let v be a binary vector of length n and weight k. We define the profile matrix $P_M(v)$ to be a $k \times n$ matrix in RREF with the following properties:*

1. *The leading coefficients of the rows of $P_M(v)$ appear in columns indexed by* $\operatorname{supp}(v)$.
2. *$P_M(v)$ has $\bullet$'s in all its entries which are not required to be terminal zeros or leading ones.*

Example 4.1.2. *For example if $v = (0,1,0,1,1,0,0)$ then*

$$P_M(v) = \begin{bmatrix} 0 & 1 & \bullet & 0 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 1 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 0 & 1 & \bullet & \bullet \end{bmatrix}.$$

Figure 4.1.2 shows $\mathcal{P}_q(n)$ partitioned into cells, each represented by a binary vector $v \in \{0,1\}^n$. As can be observed in this figure, $\mathcal{P}_q(n)$ is mostly occupied by $\mathcal{G}(n, \lfloor \frac{n}{2} \rfloor)$.

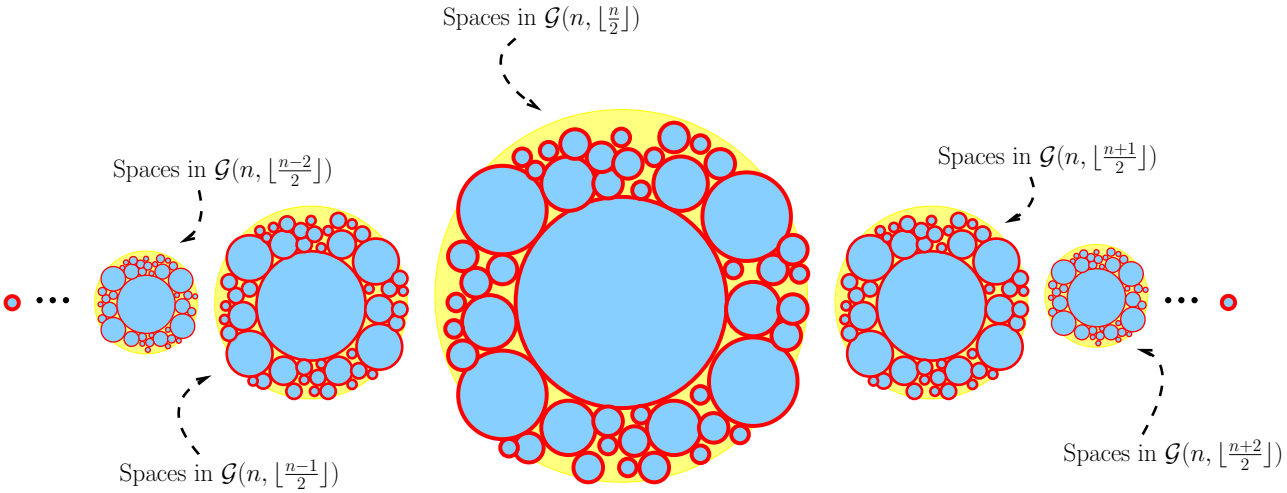

Figure 4.1: $\mathcal{P}_q(n)$ partitioned into cells, each identified by a vector in $\{0,1\}^n$.

Moreover, each Grassmannian $\mathcal{G}(n,\cdot)$ is in turn mostly occupied by the spaces with a profile matrix of the form $\langle [\mathrm{I} \quad X] \rangle$. Such a cell within each Grassmannian is commonly known as the "principal Schubert cell" [30].

Definition 4.1.3. *(Inter-Cell Distance) Let u, v be two distinct vectors in $\{0,1\}^n$. Let $\Omega_v \subset \mathcal{P}_q(n)$ be a set of spaces in $\mathcal{P}_q(n)$ such that for all $W \in \Omega_v$, $p(W) = v$. Similarly, let $\Omega_u \subset \mathcal{P}_q(n)$ be a set of spaces in $\mathcal{P}_q(n)$ such that for all $W \in \Omega_u$, $p(W) = u$. Define the inter-cell subspace distance between Ω_u and Ω_v as,*

$$d_{\mathrm{S}}[\Omega_u; \Omega_v] = \min\{d(U,V) : U \in \Omega_u,\ V \in \Omega_v\}$$

Let Γ denote the super-set of all cells generated according to the equivalence relation defined by Equation 4.2. Define the *minimum inter-cell subspace distance* of a set $\mathcal{S} \subseteq \Gamma$ as,

$$d_{\mathrm{S}}[\mathcal{S}] = \min\{d_{\mathrm{S}}[\Omega_u; \Omega_v] : \Omega_u, \Omega_v \in \mathcal{S}, u \neq v \in \{0,1\}^n\}.$$

Let a code $\mathcal{C} \subseteq \{0,1\}^n$ with $d_{\mathrm{H}}(\mathcal{C}) = d$ be the set of all profile vectors according to which a set $\Omega = \{\Omega_v \in \Gamma : v \in \mathcal{C}\}$ is generated. By Theorem 4.1.2, Ω has a minimum inter-cell subspace distance $d_{\mathrm{S}}[\Omega] = d$.

Definition 4.1.4. *For $v \in \{0,1\}^n$, we define the profile-sub-matrix of v, denoted $S(v)$ to be the sub-matrix of $P_M(v)$ composed of all the rows and columns of $P_M(v)$ which contain at least a single $\bullet$.*

Example 4.1.3. *For example if* $v = (0, 1, 0, 1, 1, 0, 0)$ *then*

$$S(v) = \begin{bmatrix} \bullet & \bullet & \bullet \\ 0 & \bullet & \bullet \\ 0 & \bullet & \bullet \end{bmatrix}.$$

Definition 4.1.5. *For some* $v \in \{0,1\}^n$*, let* $S = S(v)$ *be an* $m \times \eta$ *matrix. A matrix* $M \in \mathbb{F}_q^{m \times \eta}$ *is said to fit* S *if it has zeros in all its entries where* S *has zeros.*

Definition 4.1.6. *Let* $S = S(v)$ *for some* $v \in \{0,1\}^n$*. A code is an* $[S, \kappa, \delta]$ *Ferrers Diagram rank-metric code if it forms a rank-metric code with dimension* κ *and minimum rank-distance* δ*, all of whose codewords fit* S*.*

We refer to Ferrers Diagram rank-metric codes as FD-Codes for brevity. The following theorem by [19] gives an upper bound on the dimension of FD-Codes.

Theorem 4.1.2 ([19])**.** *Let* $C_{\mathcal{F}}$ *be an* $[S, \kappa, \delta]$ *FD-Code. For a given* i *let* ν_i *be the number of* $\bullet$*'s in* S *that are not contained in its first* i *rows, and are not contained in its right-most* $\delta - i - 1$ *columns. Then,*

$$\dim C_{\mathcal{F}} \leq \min_i \nu_i$$

The following corollary, which is also presented in [19], is immediate from Theorem 4.1.2.

Corollary 4.1.1 ([19])**.** *Let* $C_{\mathcal{F}}$ *be an* $[S, \kappa, \delta]$ *FD-Code. An upper bound on* $\dim C_{\mathcal{F}}$ *is the smallest number of* $\bullet$*'s that can be removed from* S *while it remains with at most* $\delta - 1$ *rows of* $\bullet$*'s or at most* $\delta - 1$ *columns of* $\bullet$*'s.*

Definition 4.1.7. *For some* $v \in \{0,1\}^n$*, let* $S = S(v)$ *be an* $m \times \eta$ *matrix, and assume that* $x \in \mathbb{F}_q^{m \times \eta}$ *fits* S*. Then the lifting of* x*, denoted* $\mathcal{I}_v(x)$ *is the row-space of* $P_M(v)$ *with the entries in* S *replaced with those in* x*.*

Example 4.1.4. *For* $v = (0, 1, 0, 1, 1, 0, 0, 0)$*, and* $x = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix}$ *we have,*

$$\mathcal{I}_v(x) = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Notice that the lifting operation defined by Definition 4.1.7 has the original lifting operation of [12] as a special case, i.e. when x is lifted to the profile matrix $P(v)$, where $v = \overbrace{11\cdots1}^{k}\overbrace{00\cdots0}^{n-k}$. In a manner similar to Lemma 4.1.1 we have that a subspace code constructed by lifting inherits the distance properties of its underlying FD-code. More precisely, let $v \in \{0,1\}^n$ be the profile vector of a cell $\Omega_v \in \Gamma$, and let $S = S(v)$ be its corresponding profile sub-matrix. The lifting $\mathcal{I}_v(\mathcal{C})$ of an $[S, \kappa, \delta]$ FD-code $\mathcal{C}$ results in a subspace code $\Omega'_v \subseteq \Omega_v$ with $d_S(\Omega'_v) = 2\delta$.

In the scheme suggested by [19], to construct an $(n, 2\delta)_{d_S}$ a lifted FD-Code $\mathcal{C} \subseteq \mathcal{P}_q(n)$ a set of cells $\Omega \subseteq \Gamma$ is first selected with minimum inter-cell distance $d_S[\Omega] = 2\delta$. As shown previously, this is possible by selecting the profile vectors of the equivalence classes according to a binary code of minimum Hamming distance 2δ. Figure 4.1.2 shows an example of the first step of construction: Ω is composed of the cells marked by red, which are selected according to a set of profile vectors at a minimum Hamming distance 2δ. This choice of profile vectors provides a guarantee for spaces in distinct cells in Ω to have a minimum subspace distance 2δ.

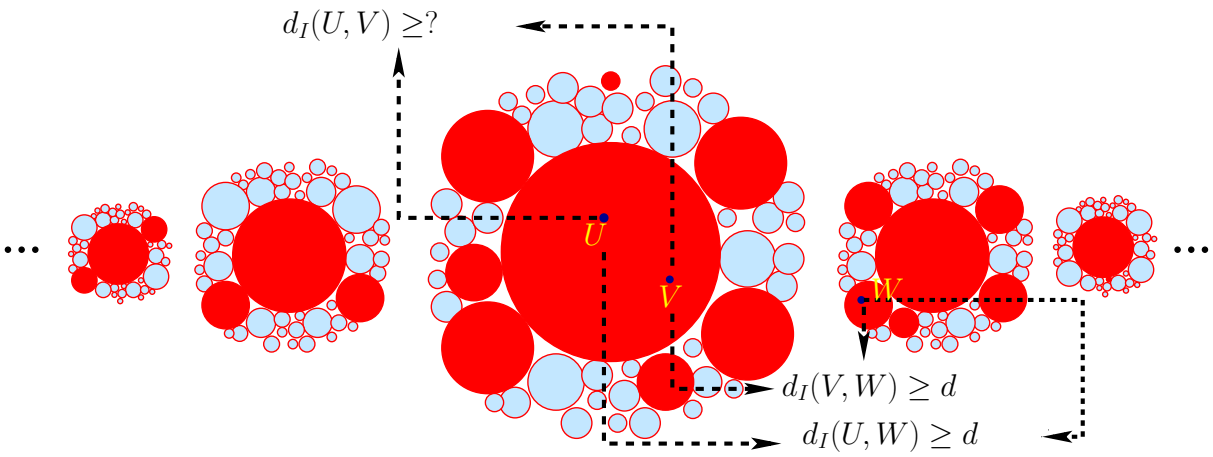

Figure 4.2: Preserving the inter-cell distance: Select a set of cells in $\mathcal{P}_q(n)$ at an inter-cell distance d according to a binary asymmetric code of length n.

While the choice of profile vectors in the previous step preserves a minimum inter-cell distance of 2δ in Ω, there is no guarantee for the intra-cell subspace distance for spaces within each cell to be at least 2δ as well. Thus, in the next step of construction, a lifted FD-Code of minimum rank-distance δ is used within each cell $\Omega_v \in \Omega$ with profile vector

$v \in \mathcal{H}$, to produce a subset $\Omega'_v \subseteq \Omega_v$ such that

$$\text{for all } U,\ V \in \Omega'_v, d_{\mathrm{S}}(U, V) \geq 2\delta.$$

This scheme may be described algorithmically as follows:

1. Take a binary code $\mathcal{H} \subseteq \{0,1\}^n$ with minimum Hamming distance 2δ.
2. For every $v \in \mathcal{C}$, obtain $S = S(v)$ and construct an $[S, \kappa, \delta]$ FD-Code $\mathcal{F}_v$.
3. Finally $\mathcal{C} = \{V \in \mathcal{P}_q(n) | V = \langle \mathcal{I}_v(x) \rangle, x \in \mathcal{F}_v,\ v \in \mathcal{H}\}$.

The scheme of [19] described above is a general construction which depends on two main factors:

1. A method to construct FD-Codes, given any set of parameters.
2. A binary code in the Hamming space to select a subset of the disjoint cells in $\mathcal{P}_q(n)$.

A construction for an $[S, \kappa, \delta]$ FD-Code is presented in [19], using q-cyclic MRD codes. This construction is shown to achieve the bound of Corollary 4.1.1 if S is an $m \times \eta$ matrix with $m \geq \eta$ whose right-most $\delta - 1$ columns have m $\bullet$'s. In Section 4.2 we provide an alternative construction for FD-Codes obtained as subcodes of linear MRD codes, achieving the bound of Corollary 4.1.1 under similar conditions.

In [19] Constant-weight lexicodes are suggested to be used as profile vectors for the construction of (n, d, k) constant-dimension codes in $\mathcal{P}_q(n)$. Based on our results from Section 4.2 we provide a more general profile vector selection algorithm in Section 4.3, which in case of constant-weight vectors, has the constant-weight lexicodes as a special case.

4.2 FD-Codes as Subcodes of Linear MRD Codes

In this section we present a lower bound on the dimension of FD-Codes when viewed as subcodes of linear MRD codes.

For some $v \in \{0,1\}^n$, let $C_{\mathcal{F}}$ be an $[S(v), \kappa, \delta]$, where $S(v)$ is an $m \times \eta$ matrix. We may view $C_{\mathcal{F}}$ as a subcode of a linear rank-metric code C of minimum rank-distance δ, with a further set of linear constraints ensuring that all codewords in $C_{\mathcal{F}}$ fit $S(v)$. In Theorem 4.2.1 we provide a lower bound on the dimension κ of *the largest* $[S(v), \kappa, \delta]$ FD-Code obtained as a subcode of a linear MRD code.

Theorem 4.2.1. *For some $v \in \{0,1\}^n$ with let $S = S(v)$ be an $m \times \eta$ matrix with a total of w $\bullet$'s. Consider the dimension κ of the largest $[S, \kappa, \delta]$ FD-code $C_{\mathcal{F}}$. We have*

$$\kappa \geq w - \max\{m, \eta\}(\delta - 1).$$

Proof. Let $V = \mathbb{F}_q^{m \times \eta}$. Note that $\mathbb{F}_q^{m \times \eta}$ is an $m\eta$-dimensional vector space over $\mathbb{F}_q$.

Let C be a linear MRD code with $d_R(C) \geq \delta$. This code is a k-dimensional subspace of $\mathbb{F}_q^{m \times \eta}$ with

$$k = \max\{m, \eta\}(\min\{m, \eta\} - \delta + 1).$$

There exists a linear transformation $\Phi : V \longrightarrow V/C$ with $\ker \Phi = C$, and by the First Isomorphism Theorem $\dim V/C = m\eta - k$. Let $A = \{(i,j) | S(v)_{ij} = 0\}$ be the set of (i,j) indices where $S(v)$ has zeros, and note that $|A| = m\eta - w$. Let

$$\begin{aligned} f &: V \longrightarrow \mathbb{F}_q^{m\eta - w} \\ f(x) &= (x_{ij}),\ (i,j) \in A \end{aligned}$$

Now any subcode C' of C satisfying $f(c) = 0$ for all $c \in C'$ is an $[S(v), \kappa, \delta]$ an FD-Code. Let $C_{\mathcal{F}}$ be *the largest* such subcode of C. Define a linear transformation

$$\begin{aligned} \Phi' &: V \longrightarrow \mathbb{V}/C \times \mathbb{F}_q^{m\eta - w} \\ x &\mapsto (\Phi(x), f(x)) \end{aligned}$$

Now by construction $\ker \Phi' = C_{\mathcal{F}}$. Noting that $\Phi'(V) \subseteq V/C \times \mathbb{F}_q^{m\eta - w}$ we have

$$\dim \Phi'(V) \leq 2m\eta - k - w,$$

and by the rank-nullity theorem we obtain

$$\begin{aligned} \dim C_{\mathcal{F}} &\geq w + k - m\eta \\ &= w - \max\{m, \eta\}(\delta - 1). \end{aligned}$$

□

As an example, for some profile vector $v \in \{0,1\}^n$, let $S = S(v)$ be an $m \times \eta$ matrix. We may construct an $[S, \kappa, \delta]$ code by taking a Gabidulin code over $F_{q^m}^{\eta}$ of minimum rank-distanceδ, expanding the elements of its parity-check matrix H over the base field $\mathbb{F}_q$, and adding appropriate parity-check equations to H in $\mathbb{F}_q$ to ensure that the resulting code fits S.

Theorem 4.2.2. *Let $\mathcal{C}_{\mathcal{F}}$ be an $[S, \kappa, \delta]$ code obtained as a subcode of a linear MRD code and assume that S is an $m \times \eta$ matrix with w $\bullet$'s satisfying either one of the following two properties:*

1. *$m \geq \eta$ and the right-most $\delta - 1$ columns of S have m $\bullet$'s.*
2. *$m < \eta$ and the first $\delta - 1$ rows of S have η $\bullet$'s.*

Then we have,

$$\kappa = w - \max\{m, \eta\}(\delta - 1)$$

Proof. Let $m \geq \eta$ and assume that right-most $\delta - 1$ columns of S have m $\bullet$'s. Let N_r denote the number of $\bullet$'s that have to be removed from S so that it remains with at most $\delta - 1$ rows of $\bullet$'s; similarly let N_c be the number of $\bullet$'s that have to be removed from S so that it remains with at most $\delta - 1$ columns of $\bullet$'s. Assume that S satisfies the first property, i.e. $m \geq \eta$ and the right-most $\delta - 1$ columns of S have m $\bullet$'s.

$$\begin{aligned} N_r &= w - \sum_{i=1}^{\delta-1} r_i \\ &\geq w - \eta(\delta - 1) \\ &\geq w - m(\delta - 1) \\ &= N_c \end{aligned}$$

By Corollary 4.1.1 $\kappa \leq \min\{N_r, N_c\} = N_c$. On the other hand by Theorem 4.2.1

$$\kappa \geq w - \max\{m, \eta\}(\delta - 1) = w - m(\delta - 1) = N_c$$

Thus κ achieves the bound of Corollary 4.1.1. By a similar argument when S satisfies the second property $\kappa = w - \eta(\delta - 1)$, achieves the bound of Corollary 4.1.1 and the theorem follows. □

4.3 Selecting the Profile Vectors

A naive choice for the binary code as a set of profile vectors would be one with a high information rate. However, a high information rate would only result in a large number of profile vectors, and does not necessarily guarantee a high rate for the resulting projective space code. For example, take the case of constant-weight lexicodes. While they do not have the highest rates among constant-weight binary codes, when used as profile vectors,

they may result in lifted FD-Codes with higher rates than those derived from a higher-rate constant-weight code (assuming the same parameters are used). This was empirically shown in [19] for the case of length-10, weight-4 binary constant-weight binary codes (the authors have not specified the distance). In this section we discuss the criteria for the selection of a single binary vector as profile vector and present a method to construct an appropriate set of profile vectors at a required minimum distance. In the special case of constant-weight profile vectors, this method results in constant-weight lexicodes.

First, notice that the rate of a projective space code obtained through this multilevel approach depends on the rate of its underlying FD-codes. Moreover, as shown in Theorem 4.2.1 the rate of an FD-Code depends on the number of •'s in its profile matrix $P_M(v)$ induced by v. Therefore a low-rate binary code containing vectors which result in a larger number of •'s in their corresponding profile matrices may be preferable over a high-rate binary code that involves vectors resulting in a smaller number of •'s in their profile vectors.

With this observation, given a minimum distance δ we define a scoring function $\text{score}(v, \delta)$ on the set of all binary vectors, which calculates for every $v \in \{0,1\}^n$ the lower bound on the dimension κ of the largest $[S(v), \kappa, \delta]$ FD-Code induced by v.

Definition 4.3.1. *Let $v \in \{0,1\}^n$ be a binary vector. Then*

$$\begin{aligned} \text{score}(v,\delta) &= \sum_{i=1}^{n}\sum_{j=1}^{i} \bar{v}_i v_j - \max\{m(v), \eta(v)\}(\delta - 1) \\ \textit{where } \eta(v) &= n - (wt(v) + \min_{t \in \text{supp}(v)} t) + 1, \textit{ and} \\ m(v) &= wt(v) - (n - \max_{t \in \text{supp}(\bar{v})} t) \end{aligned}$$

In order to select a set $\mathcal{P}$ of profile vectors at a minimum Hamming distance δ, we use a standard greedy algorithm that maintains a list of available profile vectors $\mathcal{P} \subseteq \{0,1\}^n$, (with $\mathcal{P}$ initialized to $\{0,1\}^n$). At each step an available profile vector $v \in \mathcal{P}$ with the highest $\text{score}(v, \delta)$ is added to $\mathcal{P}$, and vectors within asymmetric distance δ of v are made unavailable. The algorithm proceeds until $\mathcal{P} = \emptyset$. This procedure is described in Algorithm 1. We may also select a set of constant-weight profile vectors by simply initializing $\mathcal{P}$ in Algorithm 1 to $\mathcal{P} = \{v \in \{0,1\}^n : wt(v) = k\}$ for some $k \leq n$. In this special case, our selection algorithm in which the initial sorting of the binary vectors is done according to the scoring function of Definition 4.3.1 results in a constant-weight lexicode. In particular, for two binary vectors of the same length and weight, the one with a higher score has a higher lexicographic order as well.

Algorithm 1 Select a Set $\mathcal{P}$ of Profile Vectors with $d_H \geq \delta$

$\Omega \leftarrow \{0,1\}^n$
$\mathcal{P} \leftarrow \emptyset$
for $k = 1$ to 2^n **do**
  $x \leftarrow \underset{v \in (\Omega - \mathcal{P})}{\text{argmax}}\ \text{score}(v, \delta)$
  if ($\mathcal{P} = \emptyset$ OR for all $y \in \mathcal{P}$ $d_H(x, y) \geq \delta$) **then**
    $c \leftarrow x$
  end if
  $\mathcal{P} \leftarrow \mathcal{P} \cup \{c\}$
  $k \leftarrow k + 1$
end for
return $\mathcal{P}$

4.4 Lifted FD-Codes for the Injection Metric

Using our construction for FD-Codes presented in Section 4.2 as well as Algorithm 1 in conjunction with the general scheme of [19] we may obtain an $(n, d)_{d_S}$ code. This scheme is not generally optimal for the construction of $(n, d)_{d_I}$ codes. In particular the partitioning of $\mathcal{P}_q(n)$ in the first step must be done so that a minimum inter-cell ***injection*** distance of at least d is preserved. In this section we provide a relation between the injection distance of two subspaces in $\mathcal{P}_q(n)$ and their corresponding profile vectors. Using this relationship, and a slight modification to Algorithm 1 we provide a multi-level scheme for the construction of construct $(n, d)_{d_I}$ codes.

Theorem 4.4.1. *Let U and V be two subspaces in $\mathcal{P}_q(n)$, with profile vectors u, and v respectively. Then we have*

$$d_I(U, V) \geq \max\{N(u, v), N(v, u)\}$$

Proof. Let $w = u \wedge v$ and observe that $\dim U \cap V \leq wt(w)$. Thus,

$$\dim U - \dim(U \cap V) \geq wt(u) - wt(w).$$

Similarly,
$$\dim V - \dim(U \cap V) \geq wt(v) - wt(w).$$

Taking the $\max\{\cdot, \cdot\}$ of both equations we obtain

$$\begin{aligned} d_I(U, V) &\geq \max\{wt(u), wt(v)\} - wt(w) \\ &= \max\{N(u, v), N(v, u)\} \end{aligned}$$

□

For two binary vectors x and y, the quantity $\max\{N(x,y), N(y,x)\}$ is a metric, known as the asymmetric distance between x and y. The asymmetric distance $d_a(\cdot,\cdot)$ was first introduced by Varshamov in [31] for construction of codes for the Z channel. Constructions exist mainly for single-asymmetric error-correcting codes, and some multi-error correcting codes (see [32] and references therein). Please refer to [33] for a more recent work on general t-asymmetric error-correcting codes.

By Theorem 4.4.1 two spaces are guaranteed to have an injection distance of at least d, provided that the asymmetric distance between their profile vectors is d. Thus to construct an $(n,d)_{d_I}$ code, we may use an asymmetric code to ensure a minimum inter-cell injection distance d. By a slight modification to our profile selection algorithm of Section 4.3 we construct such a code. More specifically, we replace Line 5 of Algorithm 1 with

"**if** $(\mathcal{P} = \emptyset$ OR for all $y \in \mathcal{P}$ $d_a(x,y) \geq \delta)$ **then**"

Construction of our $(n,d)_{d_I}$ code can be described algorithmically as follows:

1. Take an asymmetric code $\mathcal{A} \subseteq \{0,1\}^n$ of minimum asymmetric distance d.
2. For each codeword $c \in \mathcal{A}$, obtain $S(c)$ (composed of the rows and columns of $P_M(c)$ with at least one $\bullet$).
3. Given each profile sub-matrix $S(c)$, use the construction of Section 4.2 to obtain an $[S(c), \kappa, d]$ FD-Code.
4. Lift each matrix $S(c)$ to its corresponding profile matrix $P_M(c)$, to obtain a generator matrix G_c.
5. Finally $\mathcal{C} = \{V \in \mathcal{P}_q(n) | V = \langle G_c \rangle\}$.

4.5 An Alternative Description for Lifted FD-Codes

For a subspace $V \in \mathcal{P}_q(n)$ and a nonsingular matrix $T \in \mathbb{F}_q^{n\times n}$, define $VT \triangleq \{vT,\ v \in V\}$ (which is a subspace isomorphic to V). Given any binary vector b of length n and weight k, define $P(b)$ as the $n \times n$ permutation matrix such that $P(b)_{\mathsf{supp}\,(b)} = \begin{bmatrix} I_{k\times k} & \mathbf{0}_{k\times(n-k)} \end{bmatrix}$ and $P(b)_{\mathsf{supp}\,(\bar{b})} = \begin{bmatrix} \mathbf{0}_{(n-k)\times k} & I_{(n-k)\times(n-k)} \end{bmatrix}$. Multiplication of a matrix $\begin{bmatrix} X & Y \end{bmatrix}$, where X is $k \times k$ and Y is $k \times (n-k)$, by $P(b)^{-1}$ on the right results in a matrix in which the columns are permuted. Specifically, the columns of X appear in columns indexed by

$\mathsf{supp}(b)$, and columns of Y appear in columns indexed by $\mathsf{supp}(\bar{b})$, and the order of the columns within each submatrix is preserved.

Now, let v be a binary vector of length n and weight k. For a matrix $X \in \mathbb{F}_q^{k\times(n-k)}$, define the generalized lifting, $\mathcal{I}_v(X)$, of X with respect to v as

$$\mathcal{I}_v(X) \triangleq \mathcal{I}(X)P(v)^{-1} = \left\langle \begin{bmatrix} I & X \end{bmatrix} P(v)^{-1} \right\rangle.$$

Since $\operatorname{rank}\left(\begin{bmatrix} I & X \end{bmatrix} P(v)^{-1}\right) = k$, we observe that $\mathcal{I}_v(X)$ is a k-dimensional subspace of $\mathbb{F}_q^n$. Similarly, for a matrix code $\mathcal{C} \subseteq \mathbb{F}_q^{k\times(n-k)}$, let

$$\mathcal{I}_v(\mathcal{C}) \triangleq \{\mathcal{I}_v(c),\, c \in \mathcal{C}\}.$$

The generalized lifting of a matrix code does not generally lead to a subspace code confined to a single Schubert cell. However, if the matrix code is suitably constrained in a manner depending on v, then its image will indeed be confined to the Schubert cell corresponding to v. The particular constraints are described as follows.

Let $Q = [Q_{ij}]$ be the $n \times n$ upper triangular matrix with $Q_{ij} = 1$ if $j \geq i$ and $Q_{ij} = 0$ otherwise. Given a binary profile vector v of length n and weight k, regarded as an element of $\mathbb{Z}^{1\times n}$, define the vector $c(v) \in \mathbb{Z}^{1\times n}$ via

$$c(v) \triangleq vQP(v).$$

Then, the generalized lifting $\mathcal{I}_v(X)$ of a matrix $X = [x_{ij}] \in \mathbb{F}_q^{k\times(n-k)}$ is guaranteed to be in the Schubert cell corresponding to v provided that

$$\text{for } \ 1 \leq i \leq k,\ 1 \leq j \leq n-k,\ i > c(v)_{j+k} \text{ implies that } x_{ij} = 0. \tag{4.3}$$

For example, suppose $n = 8$ and $k = 3$, and let $v = (0, 0, 1, 0, 1, 0, 0, 1)$. Then,

$$P(v) = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } c(v) = (1, 2, 3, 0, 0, 1, 2, 2).$$

Let $X \in \mathbb{F}_q^{3\times 5} = [x_{ij}]$. Observe that

$$\begin{bmatrix} I & X \end{bmatrix} P(v)^{-1} = \begin{bmatrix} x_{11} & x_{12} & 1 & x_{13} & 0 & x_{14} & x_{15} & 0 \\ x_{21} & x_{22} & 0 & x_{23} & 1 & x_{24} & x_{25} & 0 \\ x_{31} & x_{32} & 0 & x_{33} & 0 & x_{34} & x_{35} & 1 \end{bmatrix}.$$

Clearly this matrix is in RREF and hence $p(\langle \begin{bmatrix} I & X \end{bmatrix} P(b)^{-1} \rangle) = v$ if

$$x_{11} = x_{21} = x_{31} = x_{12} = x_{22} = x_{32} = x_{23} = x_{33} = x_{34} = x_{35} = 0.$$

These conditions are precisely those implied by (4.3).

Now let v be a binary vector of length n and weight k. Let $\mathcal{C} \subseteq \mathbb{F}_q^{k\times(n-k)}$ be a rank-metric code with $d_{\mathrm{R}}(\mathcal{C}) = d$ in which each codeword satisfies (4.3). Each such code is a Ferrers Diagram rank-metric code, which we call a v-FD code. Clearly, $\mathcal{I}_v(\mathcal{C})$ consists of subspaces with profile vector v, and by Lemma 4.1.1 we have that $d_I(\mathcal{I}_v(\mathcal{C})) = d$.

Now Theorem 4.2.1 may be restated as follows:

Theorem 4.5.1. *For a binary vector $v \in \mathbb{F}_2^n$, let $\mathcal{C}_v$ be a v-FD code of minimum rank-distance δ, obtained as a subcode of a linear MRD code. We have*

$$\dim \mathcal{C}_v \geq w - \max\{\mu, \eta\}(\delta - 1),$$

where $w = \sum_{j=1}^{n-k} c(v)_{k+j}$, $\mu = \max\limits_{j\in\{1,\ldots,n-k\}} c(v)_{k+j}$ and $\eta = wt(c(v)) - k$.

Now let $\mathcal{A} \subseteq \mathbb{F}_2^n$ be a binary code of length n and minimum asymmetric distance δ. For every element $v \in \mathcal{A}$, let $\mathcal{C}_v$ be a v-FD code. Then

$$\Omega = \bigcup_{v\in\mathcal{A}} \mathcal{I}_v(\mathcal{C}_v)$$

is a lifted FD-code of minimum injection distance δ if each v-FD code is designed to have minimum rank-distance δ.

4.6 Experimental Results

4.6.1 Rate Computation

We denote by $\mathcal{C}$, any $(n, d)_{d_{\mathrm{I}}}$ lifted FD-Code obtained via the multi-level procedure described in Section 4.4. As discussed earlier, for each lifted FD-Code $\mathcal{C}$ with $d_{\mathrm{I}}(\mathcal{C}) = \delta$

there is an $(n, d)_{d_S}$ lifted FD-Code $\mathcal{C}^S$ with $d_S(\mathcal{C}^S) = 2\delta$, obtained through a similar procedure, but whose profile vectors are at a minimum ***Hamming*** distance 2δ.

For a given ambient space dimension n, field size q, and minimum ***injection*** distance δ, we compute the rate k of our $(n, d)_{d_I}$ code $\mathcal{C}$ as follows:

1. We use the algorithm presented in Section 4.3 to obtain a set of binary profile vectors $\mathcal{A}$ at a minimum asymmetric distance $d_a \geq \delta$.

2. Given each profile vector $v \in \mathcal{A}$ we compute $\kappa_v = \text{score}(v, \delta)$ (as given by Definition 4.3.1). Note that as discussed in Section 4.3, $\text{score}(v, d)$ gives the lower bound of Theorem 4.2.1 on the dimension of the FD-Code constructed as in Section 4.2.

3. Finally, we have $k = \log_q(\sum_{v \in \mathcal{A}} q^{\kappa_v})$

Similarly, for a given ambient space dimension n, field size q, and minimum ***subspace*** distance 2δ, we compute the rate k^S of of our $(n, d)_{d_S}$ code $\mathcal{C}^S$ as follows:

1. We use the algorithm presented in Section 4.3 to obtain a set of binary profile vectors $\mathcal{H}$ at a minimum ***Hamming*** distance $d_H \geq 2\delta$.

2. Given each profile vector $v \in \mathcal{H}$ we compute $\kappa_v = \text{score}(v, \delta)$.

3. Finally, we have $k^S = \log_q(\sum_{v \in \mathcal{H}} q^{\kappa_v})$

4.6.2 Choice of Parameters

As discussed in Section 3.4, for large values of n and q, the volume of $\mathcal{P}_q(n)$ is mostly occupied by the Grassmannian of order $\frac{n}{2}$ for even n and by the two Grassmannians of orders $\lfloor \frac{n}{2} \rfloor$ and $\lceil \frac{n}{2} \rceil$ for odd n. Thus in this case, the size of a non-constant-dimension code in $\mathcal{P}_q(n)$ cannot be much larger than that of a constant-dimension code in the *largest* Grassmannian contained in $\mathcal{P}_q(n)$. In other words, the benefits of constructing non-constant-dimension codes in $\mathcal{P}_q(n)$ are most significant for small values of n and q. Thus we selected the ambient space dimension n to be an integer ranging between 5 and 19, and for each n we evaluated the rates of our code for the injection distance d ranging between 2 and n. A complete list of the rate values for $\mathcal{C}$ and $\mathcal{C}^S$ with this range of parameters is provided in Appendix D.

4.6.3 Analysis of Numerical Results

First, we compare the rate of our codes designed for the injection distance with their counterparts designed for the subspace distance. As shown in Appendix D, for any given n, δ and q within the range of our parameters, the rate of $\mathcal{C}$ with minimum injection distance δ is higher that of $\mathcal{C}^{\mathrm{S}}$ with minimum subspace distance 2δ. This rate difference ranges between 2.77×10^{-9} and 0.6374 and is most significant for smaller values of n.

This observation is completely aligned with our expectation. In particular, as discussed earlier, non-constant-dimension codes designed for the injection distance are expected to have a higher rate than those designed for the subspace distance. Moreover for larger values of n, the size of $\mathcal{P}_q(n)$ is mostly dominated by that of $\mathcal{G}_q(n,k)$ (with $k \in \{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil\}$ which in turn is mostly occupied by its principal Schubert cell (with profile vector $(\overbrace{11\cdots1}^{k}\overbrace{00\cdots0}^{n-k})$. Thus, for larger values of n both codes are expected to be dominated by their subcode contained within the principal Schubert cell of order $k \in \{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil\}$, and their rates approach that of the lifted rank-metric code within that cell.

4.6.4 Comparison with the work of Etzion and Silberstein

The best codes of [19] are obtained by using constant-weight lexicodes as profile vectors, resulting in constant-dimension codes. Thus we can only compare our constant-dimension codes with theirs. Construction of our constant-dimension codes is done by first selecting a set of constant-weight profile vectors, and then following the procedure described in Section 4.4. In Section 4.4 we showed that constant-dimension codes of [19] may be obtained as a special case of our construction scheme. In particular, by Theorem 4.2.2 we have that the dimension of FD-Codes constructed as in Section 4.2 achieve the same upper bound as those of [19], under the same conditions. Moreover, we showed that in the case of constant-dimension codes, the profile vector selection of [19] is a special case of a more general selection algorithm presented in Section 4.3.

Chapter 5

Conclusions and Future Directions

This thesis concerns the construction of projective space codes for adversarial error-correction in random linear network coding. In this context, the metric used is the so-called injection distance, which perfectly reflects the adversarial nature of the channel. Since the injection distance has been introduced very recently in the literature, almost all existing bounds and constructions on projective space codes for this type of error-correction are based on a different (but related) metric called the subspace distance. Moreover, most of the existing literature concerns the construction of constant-dimension codes. The injection and subspace distance between two subspaces of the same dimension are equal up to a scale. Thus constant-dimension codes designed for the injection metric coincide with those designed for the subspace metric. To our knowledge this thesis is the first to address the construction of non-constant-dimension codes designed for the injection metric.

In this work, we derived a Gilbert-Varshamov-type bound on the size of non-constant-dimension codes designed for the injection metric. We analyzed the asymptotic behaviour of our Gilbert-Varshamov-type bound in the limit as the ambient space dimension approaches infinity. In particular, we showed that for large values of n, the Gilbert-Varshamov bound for non-constant-dimension codes in $\mathcal{P}_q(n)$ approaches that for the constant-dimension codes contained within $\mathcal{G}_q(n, \lfloor \frac{n}{2} \rfloor)$. We also showed that that for larger values of n the size of $\mathcal{P}_q(n)$ is mostly dominated by $|\mathcal{G}_q(n,k)|$ with $k \in \{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil\}$. An important conclusion from this result is that the rate-gain achieved by non-constant-dimension projective space codes cannot be much higher than that achieved by a constant-dimension code contained within the largest Grassmannian within in $\mathcal{P}_q(n)$. Therefore, when there is no restriction on the dimension of the codewords in a subspace code, one

may construct a constant-dimension code in the largest Grassmannian contained in $\mathcal{P}_q(n)$ and achieve a rate that is almost identical to that of a related non-constant-dimension code.

In this context, an interesting research problem would be to investigate the performance of non-constant-dimension codes in the cases where the entire projective space is not available as the code-alphabet (in particular, when the codewords are allowed to have a maximum dimension much smaller than that of the largest Grassmannian in $\mathcal{P}_q(n)$). We conjecture that in this case the rate of a non-constant-dimension code is not much higher than that of the best constant-dimension code contained within the **largest available** Grassmannian.

We presented a multi-level construction for projective space codes designed for this metric. Similar to the construction in [19], our construction involves an appropriate partitioning of the projective space into disjoint cells via binary vectors of length equal to the dimension of the ambient space. We proposed an algorithm to select a set of cells in $\mathcal{P}_q(n)$ at a guaranteed minimum inter-cell injection distance. Moreover, we presented a construction for FD-Codes, using linear rank-metric codes, and provided a lower bound on the dimension of such codes when obtained as subcodes of linear MRD codes. Using this construction along with our selection algorithm we presented a class of non-constant dimension lifted FD-Codes for the injection distance. With appropriate modifications to this construction we obtained a class of non-constant-dimension codes designed for the subspace distance as well as a class of constant-dimension codes. The latter includes the constant-dimension codes of [19] as a special case.

We observed that our non-constant dimension codes designed for the injection distance have rates higher than their counterparts designed for the subspace distance. Moreover, our non-constant-dimension codes (both those designed for the injection distance and those designed for the subspace distance) achieve rates higher than those of the best lifted rank-metric codes, namely those included in the largest principal Schubert cell in $\mathcal{P}_q(n)$. However, the rate improvements gained by the latter are minute from a practical perspective. These results are completely aligned with our conclusions drawn from our analysis of the asymptotic behaviour of the Gilbert-Varshamov bound for $A_q(n, d)$.

Some open problems regarding this construction scheme are as follows:

- Is there an optimal method for the selection of profile vectors? Here the measure of optimality should be quantified so as to reflect the overall rate of the resulting subspace code. The scoring function on the set of profile vectors presented in this

thesis aims to calculate a lower bound on the dimension of the FD-Code induced by each profile vector. However, a greedy profile selection algorithm such as the one described in this thesis may fail to select a set of profile vectors that together result in a lifted FD-Code of highest possible rate. Thus a global search algorithm along with this scoring function may be suitable to obtain an optimal set of profile vectors. Specifications of such an algorithm are yet to be investigated.

- In this thesis an $[S, \kappa, \delta]$ FD-Code $\mathcal{F}$ is constructed as a subcode of a linear MRD code, with a further set of linear constraints. Each linear constraint ensures that a codeword in $\mathcal{F}$ has zeros in one of the positions where S has a zero. Thus there are as many linear constraints as the total number of zeros in S. However it is possible that the structure of S is in such a way that a single linear constraint may simultaneously satisfy several zero-constraints. Thus an interesting problem would be to devise a method that given a profile sub-matrix S constructs an FD-Code of highest possible rate by taking the inter-dependencies of the zero-locations of S into account.

Appendix A

Omitted Proofs

Lemma 3.2.1. *Let V be a k-dimensional space in $\mathcal{P}_q(n)$. Then $S(k,t,m) = |\mathcal{S}_V(t) \cap \mathcal{G}_q(n,m)|$ is given by,*

$$S(k,t,m) = q^{t(m-k+t)} \begin{bmatrix} k \\ t \end{bmatrix} \begin{bmatrix} n-k \\ m-k+t \end{bmatrix} \mathbf{I}(m \leq k) + q^{t(k-m+t)} \begin{bmatrix} k \\ m-t \end{bmatrix} \begin{bmatrix} n-k \\ t \end{bmatrix} \mathbf{I}(m > k)$$

Proof. Let $S_m^-(t)$ denote the set of all m-spaces in $\mathcal{S}_V(t)$ with $m \leq k$, i.e. $S_m^-(t) = \{W \in \mathcal{S}_V(t) : \dim W = m \leq k\}$. For each $W \in S_m^-(t)$ we have $d_{\mathrm{I}}(W,V) = k - \dim(W \cap V) = t$. Thus, $S_m^-(t)$ is the set of all m-spaces in $\mathcal{P}_q(n)$ that intersect V in one of its $(k-t)$-dimensional subspaces. By Lemma 2.2.1 there are a total of $q^{t(m-k+t)} \begin{bmatrix} k \\ k-t \end{bmatrix} \begin{bmatrix} n-k \\ m-k+t \end{bmatrix}$ spaces in $S_m^-(t)$.

Now let $S_m^+(t)$ denote the set of all m-spaces in $\mathcal{S}_V(t)$ with $m > k$, $S_m^+(t) = \{W \in \mathcal{S}_V(t) : \dim W = m > k\}$. For each $W \in S_m^+(t)$ we have $d_{\mathrm{I}}(W,V) = m - \dim(W \cap V) = t$. Thus, $S_m^+(t)$ is the set of all m-spaces in $\mathcal{P}_q(n)$ that intersect V in one of its $(m-t)$-dimensional subspaces. Similar to the previous case, by Lemma 2.2.1 there are a total of $q^{t(k-m+t)} \begin{bmatrix} k \\ m-t \end{bmatrix} \begin{bmatrix} n-k \\ t \end{bmatrix}$ spaces in $S_m^+(t)$. Finally we have,

$$\begin{aligned} S(k,t,m) &= |S_m^-|\mathbf{I}(m \leq k) + |S_m^+|\mathbf{I}(m > k) \\ &= q^{t(m-k+t)} \begin{bmatrix} k \\ t \end{bmatrix} \begin{bmatrix} n-k \\ m-k+t \end{bmatrix} \mathbf{I}(m \leq k) + q^{t(k-m+t)} \begin{bmatrix} k \\ m-t \end{bmatrix} \begin{bmatrix} n-k \\ t \end{bmatrix} \mathbf{I}(m > k) \end{aligned}$$

□

Lemma 3.4.3. *Let $k \in \{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil\}$, where n is the ambient space dimension of $\mathcal{P}_q(n)$. We have,*

$$\left(\frac{3-(-1)^n}{2} \right) (1 + \frac{n}{h(q)} q^{-\frac{n^2}{4}}) \leq \frac{|\mathcal{P}_q(n)|}{|\mathcal{G}_q(n,k)|} \leq \left(\frac{3-(-1)^n}{2} \right) (1 + nh(q) q^{-\frac{n^2}{4}}).$$

Proof. For $n = 2k$ we have,

$$\frac{|\mathcal{P}_q(n)|}{|\mathcal{G}_q(n,k)|} = \frac{\begin{bmatrix} n \\ k \end{bmatrix} + 2\sum_{i=0}^{k-1} \begin{bmatrix} n \\ i \end{bmatrix}}{\begin{bmatrix} n \\ k \end{bmatrix}}$$

Therefore,

$$\begin{aligned} 1 + 2\sum_{i=0}^{k-1} \frac{q^{i(n-i)}}{h(q)q^{k(n-k)}} &\leq \frac{|\mathcal{P}_q(n)|}{|\mathcal{G}_q(n,k)|} \leq 1 + 2\sum_{i=0}^{k-1} \frac{h(q)q^{i(n-i)}}{q^{k(n-k)}} \qquad \text{(A.1)} \\ 1 + 2\sum_{i=0}^{k-1} h(q)^{-1}q^{-(i-k)^2} &\leq \frac{|\mathcal{P}_q(n)|}{|\mathcal{G}_q(n,k)|} \leq 1 + 2\sum_{i=0}^{k-1} h(q)q^{-(i-k)^2} \\ 1 + nh(q)^{-1}q^{-\frac{n^2}{4}} &\leq \frac{|\mathcal{P}_q(n)|}{|\mathcal{G}_q(n,k)|} \leq 1 + nh(q)q^{-\frac{n^2}{4}}, \end{aligned}$$

where Equation A.1 follows from Equation 3.6. Similarly, we have,

For $n = 2k + 1$ we have,

$$\frac{|\mathcal{P}_q(n)|}{|\mathcal{G}_q(n,k)|} = \frac{\begin{bmatrix} n \\ k \end{bmatrix} + \begin{bmatrix} n \\ k+1 \end{bmatrix} + 2\sum_{i=0}^{k-1} \begin{bmatrix} n \\ i \end{bmatrix}}{\begin{bmatrix} n \\ k \end{bmatrix}}$$

$$\begin{aligned} 2(1 + \sum_{i=0}^{k-1} \frac{q^{i(n-i)}}{h(q)q^{k(n-k)}}) &\leq \frac{|\mathcal{P}_q(n)|}{|\mathcal{G}_q(n,k)|} \leq 2(1 + \sum_{i=0}^{k-1} \frac{h(q)q^{i(n-i)}}{q^{k(n-k)}}) \qquad \text{(A.2)} \\ 2(1 + nh(q)^{-1}q^{-\frac{n^2}{4}}) &\leq \frac{|\mathcal{P}_q(n)|}{|\mathcal{G}_q(n,k)|} \leq 2(1 + nh(q)q^{-\frac{n^2}{4}}), \end{aligned}$$

where Equation A.2 follows from Equation 3.6. □

Lemma 3.4.2. *Let $\overline{B}(t)$ denote the average size of a sphere of radius t in $\mathcal{P}_q(n)$ as defined by Equation 3.5. We have,*

$$\overline{B}(t) \leq \left(\frac{3 - (-1)^n}{2}\right)\left(\sum_{i=0}^{t} q^{i^2} \begin{bmatrix} \ell \\ t \end{bmatrix}^2 + n^2h^2(q)q^{-\frac{n^2}{4}}\right)$$

Proof. Let $\ell = \lfloor \frac{n}{2} \rfloor$. We have,

$$\overline{B}(t) = \frac{1}{|\mathcal{P}_q(n)|} \sum_{X \in \mathcal{P}_q(n)} |\mathcal{B}_X(t)| = \sum_{X \in \mathcal{P}_q(n)} \sum_{k=0}^{n} \frac{|\mathcal{B}_X(t) \cap \mathcal{G}_q(n,k)|}{|\mathcal{P}_q(n)|}$$

Thus,

$$\begin{aligned}
\overline{B}(t) &\leq \sum_{X\in\mathcal{P}_q(n)}\sum_{k=\ell}^{n-\ell}\frac{|\mathcal{B}_X(t)\cap\mathcal{G}_q(n,k)|}{|\mathcal{P}_q(n)|}+2\sum_{k=0}^{\ell-1}\frac{|\mathcal{G}_q(n,k)|}{|\mathcal{P}_q(n)|}\\
&\leq \sum_{X\in\mathcal{P}_q(n)}\sum_{k=\ell}^{n-\ell}\frac{|\mathcal{B}_X(t)\cap\mathcal{G}_q(n,k)|}{|\mathcal{P}_q(n)|}+(\frac{3-(-1)^n}{2})\sum_{k=0}^{\ell-1}\frac{\begin{bmatrix}n\\k\end{bmatrix}}{\sum_{j=\ell}^{n-\ell}\begin{bmatrix}n\\j\end{bmatrix}}\\
&\leq \sum_{X\in\mathcal{P}_q(n)}\sum_{k=\ell}^{n-\ell}\frac{|\mathcal{B}_X(t)\cap\mathcal{G}_q(n,k)|}{|\mathcal{P}_q(n)|}+(\frac{3-(-1)^n}{2})\sum_{k=0}^{\ell-1}\frac{h(q)q^{k(n-k)}}{q^{\ell(n-\ell)}} \qquad \text{(A.3)}\\
&\leq \sum_{X\in\mathcal{P}_q(n)}\sum_{k=\ell}^{n-\ell}\frac{|\mathcal{B}_X(t)\cap\mathcal{G}_q(n,k)|}{|\mathcal{P}_q(n)|}+(\frac{3-(-1)^n}{2})nh(q)q^{-\frac{n^2}{4}}\\
&\leq \left(\frac{3-(-1)^n}{2}\right)\left(\sum_{i=0}^{t}q^{i^2}\begin{bmatrix}\ell\\i\end{bmatrix}^2+n^2h^2(q)q^{-\frac{n^2}{4}}\right), \qquad \text{(A.4)}
\end{aligned}$$

where Equation A.3 follows from the bound of Equation 3.6 and Equation A.4 follows from Theorem 3.1.1, and Lemma 3.4.3. □

Lemma 3.4.3. *Let $\overline{B}(t)$ denote the average size of a sphere of radius t in $\mathcal{P}_q(n)$ as defined by Equation 3.5. We have,*

$$\overline{B}(t)\geq\left(\frac{3-(-1)^n}{2}\right)\left(\sum_{i=0}^{t}q^{i^2}\begin{bmatrix}\ell\\t\end{bmatrix}^2\right)$$

Proof. Let $\ell=\lfloor\frac{n}{2}\rfloor$. We have,

$$\overline{B}(t)=\frac{1}{|\mathcal{P}_q(n)|}\sum_{X\in\mathcal{P}_q(n)}|\mathcal{B}_X(t)|=\sum_{X\in\mathcal{P}_q(n)}\sum_{k=0}^{n}\frac{|\mathcal{B}_X(t)\cap\mathcal{G}_q(n,k)|}{|\mathcal{P}_q(n)|}$$

Thus,

$$\begin{aligned}
\overline{B}(t) &\geq \sum_{X\in\mathcal{P}_q(n)}\sum_{k=\ell}^{n-\ell}\frac{|\mathcal{B}_X(t)\cap\mathcal{G}_q(n,k)|}{|\mathcal{P}_q(n)|}\\
&\geq \left(\frac{3-(-1)^n}{2}\right)\sum_{i=0}^{t}q^{i^2}\begin{bmatrix}\ell\\i\end{bmatrix}^2, \qquad \text{(A.5)}
\end{aligned}$$

where Equation A.5 follows from Theorem 3.1.1. □

Appendix B

A Survey of Existing Bounds on the size of (n, d, k) and $(n, d)_{d_S}$ Codes

Since for projective space codes, $A_q(n, d, k) = A_q(n, d, n-k)$, when dealing with $A_q(n, d, k)$, we may safely assume $k \leq n/2$. The following sphere-packing bound for $A_q(n, d, k)$ is given in [11].

Theorem B.0.1 (Sphere-packing bound)**.** *Let* $t = \lfloor (d-1)/2 \rfloor$. *Then*

$$A_q(n, d, k) \leq \frac{\begin{bmatrix} n \\ k \end{bmatrix}}{B(t, k)} < \frac{\begin{bmatrix} n \\ k \end{bmatrix}}{q^{t^2} \begin{bmatrix} k \\ t \end{bmatrix} \begin{bmatrix} n-k \\ t \end{bmatrix}}.$$

In [18] a puncturing operation in $\mathcal{G}_q(n, k)$ is defined that reduces by one the dimension of the ambient space and the dimension of each subspace in $\mathcal{G}_q(n, k)$. According to this puncturing operation, a punctured code obtained by puncturing an $(n, d, k)_q$ code is itself an $(n-1, d', k-1)_q$ code, where $d' \geq d-1$. If an $(n, d, k)_q$ code is punctured $d-1$ times repeatedly, an $(n-d+1, d'', k-d+1)_q$ code (with $d'' \geq 1$) is obtained, which may have size no greater than $|\mathcal{G}_q(n-d+1, k-d+1)|$. Thus the following Singleton-type bound is established [18].

Theorem B.0.2 (Singleton bound)**.**

$$A_q(n, d, k) \leq \begin{bmatrix} n-d+1 \\ k-d+1 \end{bmatrix} = \begin{bmatrix} n-d+1 \\ n-k \end{bmatrix}.$$

It is further observed in [18] that this bound is always stronger than the sphere-packing bound of Theorem B.0.1 for nontrivial codes.

Since $\mathcal{G}_q(n, k)$ is an association scheme, the anticode bound of Delsarte [34] can be applied. Let $\mathcal{C}$ be an $(n, d, k)_q$ code. Then Delsarte's bound implies that

$$|\mathcal{C}| \leq \frac{|\mathcal{G}_q(n, k)|}{|\mathcal{A}|},$$

where $\mathcal{A} \subseteq \mathcal{G}_q(n, k)$ is any set with maximum distance $d-1$ (called an *anticode*).

Note that, for all $U, V \in \mathcal{G}_q(n, k)$, $d(U, V) \leq d-1$ if and only if $\dim(U \cap V) \geq k-d+1$. Thus, we can take $\mathcal{A}$ as a set in which any two elements intersect in a space of dimension at least $k-d+1$. From the results of Frankl and Wilson [35], it follows that, for $k \leq n/2$, the maximum value of $|\mathcal{A}|$ is equal to $\begin{bmatrix} n-k+d-1 \\ d-1 \end{bmatrix}$. Hence, we have the following bound.

Theorem B.0.3 (Anticode bound)**.**

$$A_q(n, d, k) \leq \frac{\begin{bmatrix} n \\ k-d+1 \end{bmatrix}}{\begin{bmatrix} k \\ k-d+1 \end{bmatrix}}.$$

It is easy to observe that Delsarte's bound also implies the sphere-packing bound as a special case, since a sphere $\mathcal{B}_V(\lfloor (d-1)/2 \rfloor, k)$ is (by the triangle inequality) an anticode of maximum distance $d-1$. However, a sphere is not an optimal anticode in $\mathcal{G}_q(n, k)$, and therefore the bound of Theorem B.0.3 is always tighter for nontrivial codes.

The bound in Theorem B.0.3 was first obtained by Wang, Xing and Safavi-Naini in [29] using a different argument. The proof that Theorem B.0.3 follows from Delsarte's bound is due to Etzion and Vardy [7].

As observed in [36], the anticode bound is always stronger than the Singleton bound for non-trivial codes in $\mathcal{G}_q(n, k)$.

An $(n, d, k)_q$ code $\mathcal{C}$ induces a binary constant weight code of length $q^n - 1$, weight $q^k - 1$, and minimum Hamming distance $2q^k(1 - q^{-d})$, having $|\mathcal{C}|$ codewords. This binary code is defined by taking as codewords the rows of the $|\mathcal{C}| \times q^n - 1$ incidence matrix between codewords of $\mathcal{C}$ and the nonzero vectors of $\mathbb{F}_q^n$. The classical Johnson bound on binary constant weight codes immediately implies a Johnson-type bound on $A_q(n, d, k)$ [36]. We also have the following Johnson-type bounds.

Theorem B.0.4 ([7, 36])**.**

$$A_q(n, d, k) \leq \frac{q^n - 1}{q^k - 1} A_q(n-1, d, k-1)$$

Theorem B.0.5 ([7])**.**

$$A_q(n, d, k) \leq \frac{q^n - 1}{q^{n-k} - 1} A_q(n-1, d, k)$$

Theorems B.0.4 and Theorem B.0.5 may be iterated to give an upper bound for $A_q(n, d, k)$. However, as in the classical case of the Johnson space, the order in which the two bounds should be iterated is still an open problem. By iterating Theorem B.0.4 with itself, the following bound is established in [7, 36].

Theorem B.0.6 ([7, 36])**.**

$$A_q(n, d, k) \leq \left\lfloor \frac{q^n - 1}{q^k - 1} \left\lfloor \frac{q^{n-1} - 1}{q^{k-1} - 1} \cdots \left\lfloor \frac{q^{n-k+d} - 1}{q^d - 1} \right\rfloor \cdots \right\rfloor \right\rfloor.$$

It is shown in [36] that Theorem B.0.5 improves on the anticode bound.

Let D be a nonempty subset of $\{1, \ldots, n\}$ and let $\mathcal{C} \subseteq \mathcal{G}_q(n, k)$ be a code. If, for all $U, V \in \mathcal{C}$, with $U \neq V$, we have $d(U, V) \in D$, then we say that $\mathcal{C}$ is a code with distances in D. The following Lemma is given in [37].

Lemma 3.4.3 ([37])**.** *Let $\mathcal{C}_D \subseteq \mathcal{G}_q(n, k)$ be a code with distances from a set D. Then, for a nonempty subset $\mathcal{B} \subseteq \mathcal{G}_q(n, k)$ there exists a code $\mathcal{C}_D^*(\mathcal{B}) \subseteq \mathcal{B}$ with distances from D such that*

$$\frac{|\mathcal{C}_D^*(\mathcal{B})|}{|\mathcal{B}|} \geq \frac{|\mathcal{C}_D|}{\begin{bmatrix} n \\ k \end{bmatrix}},$$

where, if $|\mathcal{C}_D^*| = 1$, then $\mathcal{C}_D^*$ is a code with distances from D by convention.

In particular when $\mathcal{C}_D$ is an $(n, d, k)_q$ code and $\mathcal{B}$ is an anticode of maximum distance $d - 1$, then $|\mathcal{C}_D^*(\mathcal{B})| = 1$ and Delsarte's anticode bound on $\mathcal{G}_q(n, k)$ is obtained. Using Lemma 3.4.3 Ahlswede and Aydianian obtain the following bound:

Theorem B.0.7 ([37])**.** *For integers $0 \leq t \leq d \leq k$, $k - t \leq m \leq n$,*

$$A_q(n, d, k) \leq \frac{\begin{bmatrix} n \\ k \end{bmatrix} A_q(m, d - t, k - t)}{\sum_{i=0}^{t} q^{i(m-i)} \begin{bmatrix} m \\ k - i \end{bmatrix} \begin{bmatrix} n - m \\ i \end{bmatrix}}$$

It is shown in [37] that for $t = 0$ and $m = n - 1$, Theorem B.0.7 gives Theorem B.0.5.

Two linear Programming bounds, one for $A_q^S(n, 3)$ and another for $A_q^S(n, d)$ are derived by Etzion and Vardy Etzion and Vardy [7] Ahlswede and Aydinian [37] respectively.

Appendix C

Graph-Distance Property of the Injection Metric

Definition C.0.1 ([24]). *Let $G(V, E)$ be a graph. Then a function $d : V \times V \mapsto \mathbb{N}$ is a graph distance (i.e. the graph geodesic) if and only if for all vertices u, $v \in V$ with $d(u, v) = d$, there exists some vertex $w \in V$ such that*

$$d(u, w) = 1 \text{ and } d(w, v) = d - 1$$

Definition C.0.2. *Let $\mathcal{P}_q(n)$ be a projective space over the finite field $\mathbb{F}_q$. We define the Generalized Grassmann Graph to be a graph with vertex set*

$$\mathcal{V} = \{V : V \in \mathcal{P}_q(n)\},$$

in which there is an edge between U and W if and only if $d_{\mathrm{I}}(U, W) = 1$.

Figure C.1 shows an example of the $G_{\mathcal{P}_2^3}(1)$ with $\mathcal{P}_2^3 = \{V : V \in \mathbb{F}_2^3\}$.

Theorem C.0.8. *Injection distance $d_I(\cdot, \cdot)$ is the graph geodesic in the Generalized Grassmann Graph.*

Proof. Let $\mathcal{P}_q(n)$ be a projective space of order n and let $G_{\mathcal{P}}$ be the generalized Grassmann graph with vertex set $\mathcal{V} = \mathcal{P}_q(n)$. By Definition C.0.1, in order to show that $d_I(\cdot, \cdot)$ is the graph distance in $G_{\mathcal{P}}$ we must show that for all vertices U and $V \in V$ with $d_I(U, V) = d \geq 1$, there exists some vertex $W \in V$ in such that $d_I(U, W) = 1$ and $d_I(U, W) = d - 1$. Let U and V be two subspaces in $\mathcal{P}_q(n)$ with $d_I(U, V) = d \geq 1$. Assume, with no loss of generality, that $\dim U \geq \dim V$ and let $\dim U = l$.

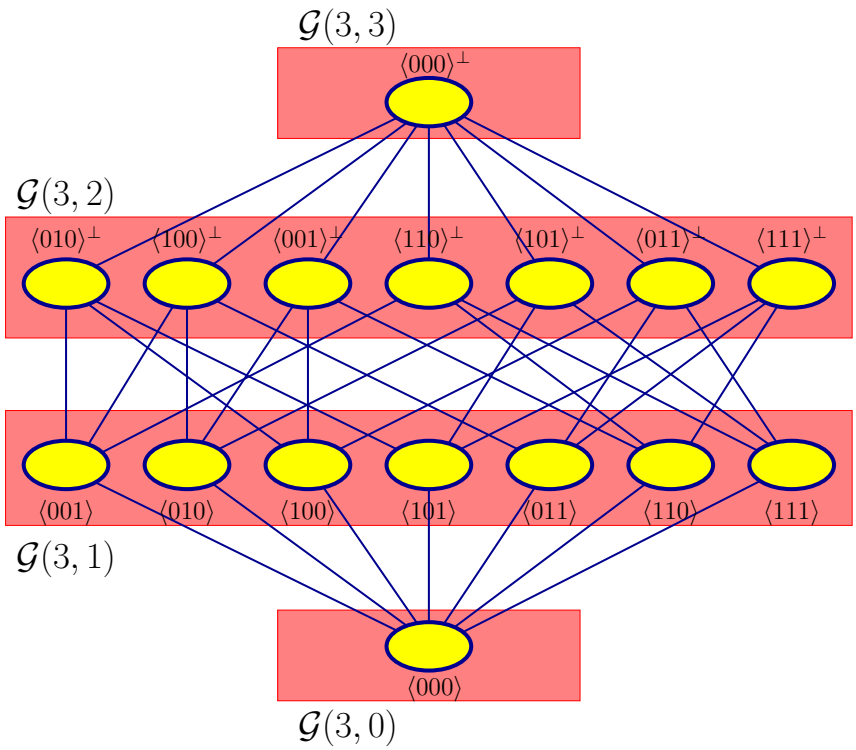

Figure C.1: A Generalized Grassmann Graph $G_{\mathcal{P}_2^3}(1)$ with $\mathcal{P}_2^3 = \{V : V \in \mathbb{F}_2^3\}$.

First consider the case where $\dim U > \dim V$ and let W to be an $(l-1)$-dimensional subspace of U containing the space $(U \cap V)$. We have

$$\begin{aligned} d_I(V,W) &= \dim W - \dim(V \cap W) && \text{(C.1)} \\ &= (\dim U - 1) - \dim(U \cap V) && \text{(C.2)} \\ &= d - 1, && \text{(C.3)} \end{aligned}$$

where Equation C.1 is due to that fact that $\dim V < \dim U \leq \dim U - 1 = \dim W$. Equation C.2 follows from the fact that $(U \cap V) = (W \cap V)$ since $(U \cap V) \subseteq W \subset U$. Finally Equation C.3 follows from the assumption that $\dim U \geq \dim V$ and $d_I(U,V) = d$. On the other hand,

$$d_I(U,W) = \dim U - \dim(U \cap V) = \dim U - \dim W = 1$$

Next consider the situation where $\dim U = \dim V$, in which case

$$d_I(U,V) = \dim U - \dim(U \cap V) = \dim V - \dim(U \cap V).$$

Let W' be the $(l-d+1)$-dimensional subspace of V that contains $(U \cap V)$. Note that we may construct W' by adjoining to $(U \cap V)$ any one of the $(q^l - q^{l-d})$ vectors that are

in V but not in U. Now we may construct W by adjoining to W' a $(d-1)$-dimensional space obtained by taking $(d-1)$ linearly independent vectors from the set of $(q^l - q^{l-d})$ vectors that are in U but not in V. By this construction, W is an l-space that contains W', with the property that $\dim(U \cap W) = l - 1$, and $\dim(V \cap W) = \dim W' = l - d + 1$. Hence we have

$$d_I(U, W) = l - \dim(U \cap W) = 1.$$

Moreover,

$$\begin{aligned} d_I(V, W) &= \dim V - \dim(V \cap W) \\ &= \dim V - \dim W' \\ &= d - 1. \end{aligned}$$

□

Appendix D

Numerical Results

In Table D.1 we list our results for the rate of our non-constant-dimension codes. In this table $\mathcal{C}_1$ denotes the lifted rank-metric codes [18] of maximum rate for the given parameters, $\mathcal{C}_2$ denotes our $(n, d)_{d_\mathrm{S}}$ lifted FD-Codes, and $\mathcal{C}_3$ is our $(n, d)_{d_\mathrm{I}}$ lifted FD-Codes. For a given ambient space dimension n and minimum distance d, we have $\log_q |\mathcal{C}_1| = \lceil \frac{n}{2} \rceil (\lfloor \frac{n}{2} \rfloor - d + 1)$. Rate computation of our codes as well as our choice of parameters have been discussed in Section 4.6. In Tables D.2 to D.12 we list our profile vectors for $\mathcal{C}_3$. Profile vectors of larger lengths are represented via their hexadecimal values.

n	d_{I}	$\log_q \lvert\mathcal{C}_1\rvert$	$\log_q \lvert\mathcal{C}_2\rvert$	$\log_q \lvert\mathcal{C}_3\rvert$	n	d_I	$\log_q \lvert\mathcal{C}_1\rvert$	$\log_q \lvert\mathcal{C}_2\rvert$	$\log_q \lvert\mathcal{C}_3\rvert$
5	2	3	3.16993	3.80735	15	2	48	48.15863	48.62919
6	2	6	6.14975	6.39232	15	3	40	40.00305	40.02578
6	3	3	3.16993	3.45943	15	4	32	32.00002	32.00039
7	2	8	8.17991	8.69000	15	5	24	24.00000	24.00001
7	3	4	4.08746	4.24793	15	6	16	16.00002	16.00007
8	2	12	12.15956	12.36331	15	7	8	8.00562	8.01681
8	3	8	8.00562	8.03892	16	2	56	56.15702	56.33601
8	4	4	4.08746	4.24793	16	3	48	48.00302	48.00443
9	2	15	15.17317	15.64022	16	4	40	40.00002	40.00003
9	3	10	10.00843	10.05257	16	5	32	32.00000	32.00000
9	4	5	5.04439	5.12928	16	6	24	24.00000	24.00000
10	2	20	20.15513	20.33454	16	7	16	16.00002	16.00007
10	3	15	15.00317	15.00895	16	8	8	8.00562	8.01681
10	4	10	10.00141	10.00422	17	2	63	63.15868	63.62857
10	5	5	5.04439	5.12928	17	3	54	54.00301	54.02561
11	2	24	24.15822	24.63210	17	4	45	45.00002	45.00036
11	3	18	18.00367	18.02986	17	5	36	36.00000	36.00000
11	4	12	12.00035	12.00317	17	6	27	27.00000	27.00000
11	5	6	6.02237	6.06609	17	7	18	18.00001	18.00002
12	2	30	30.15610	30.33720	17	8	9	9.00282	9.00843
12	3	24	24.00302	24.00540	18	2	72	72.15707	72.33586
12	4	18	18.00003	18.00024	18	3	63	63.00302	63.00437
12	5	12	12.00035	12.00106	18	4	54	54.00002	54.00002
12	6	6	6.02237	6.06609	18	5	45	45.00000	45.00000
13	2	35	35.15861	35.63034	18	6	36	36.00000	36.00000
13	3	28	28.00320	28.02652	18	7	27	27.00000	27.00000
13	4	21	21.00005	21.00063	18	8	18	18.00001	18.00002
13	5	14	14.00009	14.00035	18	9	9	9.00282	9.00843
13	6	7	7.01123	7.03342	19	2	80	80.15854	80.62836
14	2	42	42.15660	42.33625	19	3	70	70.00302	70.02555
14	3	35	35.00303	35.00464	19	4	60	60.00002	60.00036
14	4	28	28.00002	28.00004	19	5	50	50.00000	50.00000
14	5	21	21.00000	21.00001	19	6	40	40.00000	40.00000
14	6	14	14.00009	14.00026	19	7	30	30.00000	30.00000
14	7	7	7.01123	7.03342	19	8	20	20.00000	20.00000
					19	9	10	10.00141	10.00422

Table D.1: Rates of our non-constant-dimension codes

$n = 5,\ d = 2$
11100, 10010, 11111, 01011, 01000, 00101
$n = 6,\ d = 2$
111000, 110110, 100100, 101101, 010101, 010010, 111111, 100011, 011011, 001110, 001001, 000000
$n = 6,\ d = 3$
111000, 111111, 000111, 000000
$n = 7,\ d = 2$
1111000, 1100100, 1010010, 0110000, 1110110, 1100011, 1010101, 1001000, 0101010, 0011100, 1101101, 1001110, 1011011, 1111111, 0000111, 0000100
$n = 7,\ d = 3$
1111000, 1111111, 1000111, 1000000
$n = 8,\ d = 2$
11110000, 11101100, 11001000, 11100011, 11011010, 11000110, 10101010, 10100100, 10011100, 00111000, 11111001, 11010101, 01101001, 01100010, 01010100, 11110110, 10010010, 11001111, 01010011, 00110110, 00001100, 11111111, 10000001, 01000000, 00111111, 00001111
$n = 8,\ d = 3$
11110000, 11001011, 00101100, 11111111, 10000010, 00110111
$n = 8,\ d = 4$
11110000, 11111111, 00001111, 00000000,
$n = 9,\ d = 2$
111110000, 111001000, 110100100, 111101100, 110010000, 101100000, 111000110, 110101010, 110011100, 101010100, 100111000, 011100010, 111100011, 111011010, 101101001, 111010101, 110111001, 011010001, 011000100, 010101000, 110110110, 110010011, 011100101, 001101100, 001011000, 100110101, 010011010, 000110100, 101000011, 100001100, 011001011, 001111010, 111001111, 010001101, 000110011, 101111110, 100101111, 100000010, 001011101, 111111111, 011111101, 010011111, 010000011, 010000000, 001110111, 001000001
$n = 9,\ d = 3$
111110000, 110001100, 111000111, 001101000, 111111111, 100111110, 100100011, 100010000, 010011011, 001010110
$n = 9,\ d = 4$
111110000, 111111111, 100001111, 100000000

Table D.2: Profile Vectors for Our $(n, d)_{d_{\mathrm{I}}}$ Codes with $n = 5, 6, 7, 8, 9$

$n = 10,\ d = 3$
1111100000, 1110011100, 0011011000, 1101010011, 1100010000, 1110100111, 1000111010, 0110000110, 0001100100, 1011111001, 0101001101, 1111111111, 0101111110, 0010110101, 0010000001
$n = 10,\ d = 4$
1111100000, 1111111111, 1100011110, 1000010001
$n = 10,\ d = 5$
1111100000, 1111111111, 0000011111, 0000000000
$n = 11,\ d = 3$
11111100000, 11100011000, 00111010000, 11110010011, 11010000100, 11011011100, 01101000110, 01010110010, 11000110101, 10110001101, 10011001010, 01100100000, 00101101001, 11101111001, 11100101110, 11011100111, 11111111111, 10100000011, 10001000000, 01001011011, 00111111110, 00010001001, 00000111100
$n = 11,\ d = 4$
11111100000, 00011011000, 11100010111, 11111111111, 11000000100, 10000101011
$n = 11,\ d = 5$
11111100000, 11111111111, 10000011111, 10000000000
$n = 12,\ d = 3$
111111000000, 111100111000, 111000100100, 001110110000, 111010100011, 110100010000, 111011110100, 110010011100, 110001110010, 011001011000, 111101010011, 110101100101, 100101101000, 111110001101, 101100010110, 101010001000, 010110101001, 010011100000, 111001001110, 110111101010, 101011011001, 001101000100, 011100000011, 001111101100, 100110000101, 111000111111, 010111010110, 000000111000, 001011000111, 101111100111, 000110000010, 111111111111, 100001000011, 100000101111, 100000000100, 011111111001, 010000001110, 000110111111, 000101011101, 000010011011
$n = 12,\ d = 4$
111111000000, 111100001111, 001100111000, 110010110011, 000011100100, 111111111111, 110000010000, 101011111100, 100001001011
$n = 12,\ d = 5$
111111000000, 111111111111, 110000111110, 100000100001
$n = 12,\ d = 6$
111111000000, 111111111111, 000000111111, 000000000000

Table D.3: Profile Vectors for Our $(n, d)_{d_{\mathrm{I}}}$ Codes with $n = 10, 11, 12$

$n = 13,\ d = 3$
$1FC0, 1E30, 1D08, 7A0, 1F2C, 19A4, 1F13, 1CA9, 1A80, E8C, B68, 18D8, D92, 1EF8, 1C46, 1971, 13B8, 1350, 1A95, 1705,$ $E41, 1AE3, 16A6, 165C, 15F4, 156A, 1E8F, 1494, 1460, 5C9, B8B, 6F1, 1FE5, 19CD, B06, 1C4, 1BD6, 191E, DA7, 930, 8E2, 618,$ $122C, 53C, E76, C5B, 7DA, 333, 1D3F, F6B, 1813, 124B, C04, 2D6, A8, 1FFF, 13FB, 123F, 1102, BBD, 82F, 4FF, 483, 240, 79$
$n = 13,\ d = 4$
$1FC0, 1C38, 3B0, 1E27, E04, 70B, 1FFF, 1D9E, 1B79, 1883, 129D, 1176, 1148, 6FA, 4E5, 80$
$n = 13,\ d = 5$
$1FC0, 1FFF, 1C3E, 1821, 31D$
$n = 13,\ d = 6$
$1FC0, 1FFF, 103F, 10009$
$n = 14,\ d = 3$
$3F80, 3E70, 3C48, 3A20, 3964, F60, 3DE8, 3D43, 3530, 38B8, 3358, 1AD0, 3D1C, 3B29, 3ACC, 362C, 34E2, 3EA3, 3BD1, 31C0, 2E14,$ $1CA4, 1E45, 1D00, 3FB4, 3699, 2DB1, 2D2A, 2BE2, 1B0C, E88, 3A13, 27D4, 17E1, 328A, 26C1, 1F26, 19C9, D92, 2702, 23A4, 3F5A,$ $3CD6, 370F, 3196, 2F65, 1A6A, F19, 2C8D, 2951, 1B9A, 1546, 4F0, 390, 3405, 28C6, 14DC, 7CA, 3FC7, 3C3F, 3267, 1AB5, 1923, ED3,$ $5A9, 2272, B87, 938, 644, 32FA, 3018, 2880, 2479, 1B7C, 349, 3EF9, 35F3, 29CF, 157A, 142A, 2A3E, 1816, 1239, C76, C43, 162, AC, 33ED,$ $2EEE, 14AF, 627, 23B7, 185F, 375, 3FFF, 39FE, 277F, 210F, 20A3, 1DDD, 1203, 1040, FBB, 86D, 6FD, 421, DB$
$n = 14,\ d = 4$
$3F80, 3C78, 3E47, E64, 3D0, 3842, 3333, 321C, 1955, 1528, 29CB, 12E9, C9A, 3BF4, 3FFF, 35AF, 2601, 24B5, 17DA, 1084, F3D$
$n = 14,\ d = 5$
$3F80, 3C4F, 370, 3FFF, 300C, 23BE, 8AB$
$n = 14,\ d = 6$
$3F80, 3FFF, 307E, 2041$
$n = 14,\ d = 7$
$3F80, 3FFF, 7F, 0$

Table D.4: Profile Vectors for Our $(n, d)_{d_{\mathrm{I}}}$ Codes with $n = 13, 14$

$n = 15,\ d = 3$
$7F80, 7C60, 7A10, 7E58, 7348, 7500, 1F40, 7B64, 7951, 7498, 72F0, 69C0, 6730, 7E23, 7DF0, 6E0C, 3AC4, 36A0, 7645, 71A4, 5AA8, 4ED0,$ $3B22, 7CAC, 78CA, 7529, 5E34, 5C84, 6CB1, 5D4C, 35C2, 67E8, 5762, 7F15, 7EC6, 7BC9, 7987, 6D26, 6642, 65D4, 5992, 2F61, 7316, 7283,$ $6BD2, 2DA8, 5B05, 4E20, 3C0A, 5BB1, 52C0, 4788, 793A, 74D3, 6B0B, 3A99, 3880, 3170, 1791, BB0, 7FAA, 4B78, 37B4, 2C50, 2B08, 1EC3,$ $19E1, 4FC5, 3F0E, 76B9, 6856, 579A, 4D11, 1CF8, 172C, 5E0, 6829, 60B0, 5C1B, 5432, 363A, 2E96, 26C9, 7567, 6C4F, 61E3, 5449, 39DC,$ $3189, 2D5A, 1924, 1618, 77DC, 6BBC, 62AD, 611C, 5A57, 4AE6, 4364, 3C75, 2705, 1A5A, EA5, 7E6D, 7C9F, 7B73, 678F, 6676, 6204, 44EC,$ $34A7, 3235, 239A, 1386, 4DAB, 671, 350, 5B2F, 5803, 519D, 33AB, 304C, 294D, 28A6, 1FEC, D02, C3C, 635D, 5AFA, 4A33, 3CEB, 2FB3, C89,$ $680, 5028, 316E, 1A6D, 1855, 2AC, 51F6, 4F5B, 4587, 365F, 1937, 1779, F1D, A46, 756, 68F7, 4840, 2493, 773F, 5067, 4295, 188F,$ $15CF, 323, CA, 6FF9, 42DB, 2A7B, 2421, 34, 5FE7, 4181, 55FB, 440E, 2F7E, 25FD, 2100, 1BDF, 6BF, 53B, 3F5, 96A, 7FFF, 79FE, 3D14,$
$n = 15,\ d = 4$
$7F80, 7870, F60, 7C47, 364C, 6C08, 7639, 1C94, 3310, 7B6C, 656A, 62C2, 1AA9, 6355, 79B3, 64A5, 590E, 4CD9, 2E13, 55F4, 15C3, 678F, F0,$ $3ADA, 4AB6, 7FFF, 6EF5, 5F5B, 5045, 4200, 4139, 107F, 903, 22E$
$n = 15,\ d = 5$
$7F80, E70, 7C1F, 706C, 7FFF, 6803, 63FA, 1B67, 1508, 129B$
$n = 15,\ d = 6$
$7F80, 7FFF, 707E, 6041$
$n = 15,\ d = 7$
$7F80, 7FFF, 407F, 4000$

Table D.5: Profile Vectors for Our $(n, d)_{d_I}$ Codes with $n = 15$

$n = 16,\ d = 3$
$FF00, FCE0, F890, F440, F2C8, FBD0, EA60, F170, E6B0, 3EC0, FA83, FA38, F598, EC58, E9C4, D5A0, FE8C, F654, F3A4, E380, 7C28,$ $F949, F768, F486, E7C1, CE88, B9A8, FFA1, FD34, DA00, 9DD0, F825, F523, F10C, DC32, D942, CF70, 6E10, 5BE0, DE4A, DD85, DA51,$ $B662, B618, AD30, 9EA4, 6D82, 3B20, EE26, D392, 6FA8, 6748, FC53, E9B1, CD04, AF94, 7A06, 6D61, FF46, EF19, E605, E32A, D629,$ $B341, AC80, 7511, 5B18, EDCA, BC03, AB52, 72A1, 5670, E80A, BEB2, 9B4C, 6B34, 6940, 3F64, 3E31, 3588, EB63, DE65, C746, BD0E,$ $B0E4, 6ED2, 5CCC, 5C81, 5702, 4F91, 3954, F30F, EEF8, DBAA, CCC3, B110, AE69, 9F13, 3B85, DE0, F9EC, C4D4, B8DC, B2F1, 98C8,$ $87E8, 71C3, 6E0B, 68A4, 27A4, F5F2, F01B, DCB9, D0BC, CAEC, AA99, 9FC9, 7996, 7080, 51D0, 3604, FF9A, FC2F, F6CB, F06E, E4AD,$ $C929, B44D, A1D8, 9A2A, 92B0, 8E42, 7C1D, 7AE9, 7793, 68C9, 3C9A, 1D49, 1D00, E031, C51A, C258, B9C7, 735A, 46C0, FED5, CA1E,$ $C428, A4AA, 65F4, 629C, 5B47, 556A, 3716, 31B2, 1C34, B90, F0B7, ED97, D026, C535, C38D, A8B6, A593, 973C, 8B86, 76E6,$ $6466, 5F5C, 4AB2, 3DF8, 3252, 2C4C, 1DA3, FD79, F375, E157, C69B, A27C, A240, A162, C7A7, B7DC, A6CE, 95E6, 8721, 75CD, 6EB5,$ $6222, 578E, 3B2B, 3819, 2C95, 2AE3, 22E8, 1A65, 1348, 754, EA5F, DAF3, A57A, 9A76, 46E5, DB9D, CCF6, BB7A, ABAD, A416, 98EB,$ $53B9, 49DA, 3E4F, 2470, 18A2, 1693, D1DB, C092, 9195, 8C6E, 8951, 58F5, 5637, 5121, 14C6, E09, D73B, C100, AEE7, 9327, 636D,$ $524B, 5215, 487C, 432C, 32AE, 292E, 1C57, 3C3, DDE7, 96D7, 8D5D, 8864, 687B, 515D, 2339, F3A, 1C4, FF37, E4FF, C93F, 9079,$ $7CDE, 5FB6, 4830, 44B9, 2D37, FBCF, EBF6, A63F, A08D, 79BB, 6107, 4373, 1A9F, 620, BABF, 910B, 4863, 141A, 70F, 526, 2128,$ $16FA, 2A5, DFFC, B76F, 900C, 4FCF, 3F3D, 245B, 28A, D9, 8BDE, 63BE, 5E7F, 48AF, 317F, 2806, 27EB, 89E, FFFF, AFFB, 8411,$ $8257, 404E, 2010, 1043, 881, 1ED$
$n = 16,\ d = 4$
$FF00, FCE0, F890, F440, F2C8, FBD0, EA60, F170, E6B0, 3EC0, FA83, FA38, F598, EC58, E9C4, FF00, F8F0, E4C8, FC87, 3CA0, 33D0,$ $F24B, D2A4, F010, E7E1, C960, 7846, 6A38, D599, FE6C, E436, CEAA, B1AA, 9678, 4ED1, EB9C, AD53, 69A5, 1D49, F14, FB33, 9BC5,$ $B81D, AA83, 5727, 560A, 3A8, 3FCA, 1A40, F0FF, 2665, C96F, 2E3F, 2542, FFFF, DFD6, 9107, 8484, 480D, 43CE, 4100, 40B3, 3DF5$
$n = 16,\ d = 5$
$FF00, F88F, 38F0, 7C0, E473, C2EC, FFFF, E020, DDF8, A11E, 5419, 3F67, 13DB, A27$
$n = 16,\ d = 6$
$FF00, FFFF, F0FC, C0C3, 3030, FF3$
$n = 16,\ d = 7$
$FF00, FFFF, C0FE, 8081$
$n = 16,\ d = 8$
$FF00, FFFF, FF, 0$

Table D.6: Profile Vectors for Our $(n, d)_{d_I}$ Codes with $n = 16$

$n = 17,\ d = 3$
$1FF00, 1F8C0, 1F420, 1FCB0, 1E690, 1EA00, 1F6C8, 1F270, 1E930, 1E5E0, 1D3A0, 1CE60, 1CD80, BDA0, 1DDC4,$
$1DA94, 1BA22, ED48, 1FD58, 1D961, 1AEC1, 1AB84, 17642, 1FA25, 1F383, 1ED89, 1FBE0, 1EAA8, 1DC18, 7E80, 1F20C,$
$1F198, 1B550, F340, 1FC43, 1F485, 1EC54, 1BC68, 1B908, 15B10, DC40, 1EB4C, 1E751, 1D629, 17A49, 12F40, F6A2,$
$1FF91, 1E503, 1D762, 1D4D2, 1CB0A, 19E04, 179A4, 16BD0, FC06, FA11, 1FE86, 1FA1A, 1F52C, 1F146, 1A728, 19BC8,$
$17C8A, 17180, 1B794, 1B281, 1AD92, 1AA58, 17168, 15D22, D6C4, 7C70, 1EF34, 1C78C, 1A4C0, 19FA1, 17531, 16CA1,$
$157C1, DA28, BE98, 1C2C8, 1B9D1, 19D34, 198B0, 16FA2, 15F98, 13F70, 13C94, E510, DD91, D712, 7724, 1E052,$
$1D803, 1CE13, 1C354, 1AC11, 16C0C, 13C00, F92A, F0B4, E898D98C, 1FF2A, 1EE69, 1E43A, 1D010, 1CCA6, 1C160,$
$1BF45, 1A864, 1968A, 15AE2, 15608, 15544, EEE4, EB43, DE4A, BFC2, BB64, 9F41, 9B80, 69E0, 1F933, 1D0EC, 1AE0E,$
$17D16, 162E4, ED25, E60A, B2E8, 7992, 1B125, 1A3B1, 19502, 194E1, 16322, 1374C, F459, E389, CF38, C6A0, AE34,$
$3A60, 1FCEC, 1E897, 1CFD2, 1CAF1, 1B81D, 1B633, 1B369, 19D0B, 18CCC, 16A16, 16945, 10FB0, 7DE8, 3718, 1F61D,$
$1F4AB, 1E0CB, 1D6F4, 1B98E, 19E5C, 18C28, 18B21, 189E2, 178DC, 15824, 14F46, 13EAC, 13589, 116D0, FE72, F7B8,$
$DF07, D509, CAD2, B492, 7ED1, 784A, 55B0, 1DB8D, 1B4E6, 14CF8, 13B13, F063, B814, B44C, AB12, 97F0, 7B1C, 75D4,$
$6640, 1DC8, 1FB56, 1FACB, 1F5F2, 1E5C7, 1D876, 19319, 177A5, 17019, 1595A, 15615, 15261, 148D0, E186, DBB2, CC32,$
$B120, 7A87, 4F04, 3E29, 3D05, 1D1B5, 1C82D, 1C405, 1BAB9, 19AC7, 16B39, 15286, 133AA, 13234, 125A4, 11B2C, B8F2,$
$A746, 9978, 770B, 7212, 4E58, 3CC3, 3562, 1F667, 1A2D6, 1A0AA, 19196, 18765, 16DF1, 15F6C, 15B55, 145CA, 12D59,$
$ECDA, E225, E080, D0D1, C908, 53D8, 34A8, 2D82, 1ADEA, 1A967, 1A17C, 1908C, 1875A, 18600, 172B6, 16F0F, 16873, 16627,$
$1523A, 14A99, F24F, C9F4, C571, BD39, A941, A59C, 5A00, 4F83, 1EFF8, 1EBA7, 1E37A, 1D7E9, 173D9, 1667C, 16028, 13EE3,$
$12671, 11340, E336, 9AA5, 8D54, 78B9, 5E65, 4EAC, 2AD4, 1E11, 1FD8F, 1EC3F, 1C0B3, 1BA6E, 1A4F9, 195BA, 18882, 18643,$
$1669B, 159AB, 1453C, 1342E, 130DA, E5B3, DDE3, DCAD, BDF4, ABF8, 91E4, 8E89, 8748, 64C9, 38A6, D60, 790, 1DD75, 19D97,$
$182BC, 1656B, 14ECD, 12298, D29B, B517, ACAB, 5484, 33C5, 1D15F, 1C32F, 18A6B, 17BBC, 12606, 11CB3, F96D, EBD5, C6B5,$
$C3EA, 7045, 6C1B, 6831, 5935, 5889, 4CC6, 4B69, 3E56, 30D0, 2BCA, 2721, 1B46, 1B77C, 18B9B, 18476, 18232, 18191, 15E5B,$
$153CE, 130F5, 118C5, D37C, D05E, B5CD, 8A50, 615C, B38, 1FFE3, 1FAF5, 1E79E, 1AF73, 19FE6, 17CD7, 1544F, 14281, 141A9,$
$12FDC, 12A0B, 10D1A, CA5D, C303, C21C, 50E2, 2F95, 1C3C, 1A9A, 1F75B, 1C8EF, DFDC, DA3F, BF1E, A078, 972E, 7373, 6C6E, 6806,$
$55A7, 32B3, 320C, 1622, 193F3, 1814E, 13023, 121C3, 10DAD, 10A4C, 8DC7, 7D9B, 394F, 2910, CF1, AA4, 1611F, 11376, B08F,$
$A409, 743F, 2B27, 27E9, 1508, 6C5, 1E1FF, 15EAF, 145F6, 14116, 128BE, 110A0, F0F7, CFAE, AECF, A857, 6AEB, 512E, 4474, 7AA,$
$1BB3F, 14100, 13C7D, 10F37, 1070D, 105D5, FFB6, BFAD, 96EB, 8926, 7F79, 4953, 4395, 145A, C80, 2C8, 1849F, 12A5F, C97B, 943B,$
$4D9E, 1903, 1171, E4F, 1BEDE, 194FF, 137CF, 12105, 106EE, F3EE, 9044, 6EB7, 28ED, 1AFC, 1F6BF, 1CF6F, 18B7D, 131BF, 12042, 10C27,$
$A6BE, 9217, 76DE, 2424, 226E, 1E9F, 156D, 1C6, 70, 1404B, C777, 4493, 10451, B9DF, 467B, 21F6, 1FD7E, 14BDF, FCFB, 8821, 15DB,$
$BF3, 98F, B9, 1FFFF, 19FFD, 157FE, 1017B, 1001C, EFDF, E6FD, 881B, 8416, 813D, 800A, 6DFE, 61FD, 3001, 1FFA, 213, 204$

Table D.7: Profile Vectors for Our $(n, d)_{d_{\mathrm{I}}}$ Codes with $n = 17$

$n = 17,\ d = 4$
$1FF00, 1F0E0, 1CC90, 3EC0, 1F887, 1FCD8, F808, 1AA58, 1E6B1, E68C, 7530, 1D839, 1C340, D954, 1CDE4, 1A924, 19628, 169D1, CE62,$ $1F563, 1E456, 1D3C9, 1ACAA, 15A8A, 1B19C, 17A74, 15651, B54A, 9DA1, 1DBB2, 1A383, 16E4B, 6B29, 1D61F, 1F7AC, 13C0D, B665, F20,$ $137D2, 1C32E, 19843, 13180, 1EF55, 7317, 1BB4E, 11F27, A2B0, 9F78, 9E96, 15406, 1F87F, 107B4, 61C6, 9D8, C59B, 79EA, 9450, 52A5,$ $12D9F, 12461, E1B, E4, 1FFFF, 1CFEB, 18AFD, 18800, 1808D, 1407C, 110F7, E17D, C023, BFF6, 7F3B, 66FE, 4218, 2816, FCD$
$n = 17,\ d = 5$
$1FF00, 1E0F0, 3CC8, 1F81F, F30, 1C6C7, D284, 33A3, 199E9, CC2E, 5955, 1FFFF, 1E7BC, 1A803, 15F73, 14440, 1261D, B67A$
$n = 17,\ d = 6$
$1FF00, EE0, 1F09F, 1FFFF, 1C018, 18167, 4F7E$
$n = 17,\ d = 7$
$1FF00, 1FFFF, 1C0FE, 18081$
$n = 17,\ d = 8$
$1FF00, 1FFFF, 100FF, 10000$

Table D.8: Profile Vectors for Our $(n, d)_{d_I}$ Codes with $n = 17$ (cont'd)

$n = 18,\ d = 3$
$3FE00, 3F9C0, 3F120, 3E880, 3E590, 3F7A0, 3D4C0, 3E2E0, 3CD60, 3F470, 3EB30, 3D8B0, 3D388, 3AB40, 3FD18, 3ECA8, 3E748, 3C700, 33D80, 3F503, 3EED0, 3E90C,$ $3B544, 3B290, 37850, FD40, 3FA68, 3CF84, 3B400, 2F350, 1F240, 3FF44, 3F086, 3B912, 3AC30, 39F50, 37D24, 2BBA0, 1DB10, 3FC85, 3F049, 3EA83, 3CA28, 3B6C1, 3ACC2,$ $35EE0, 35C20, 3E40A, 3DC4C, 3BB09, 39AC4, 37A98, 35730, 2F864, 2DD82, 27B00, 26FC0, 17AA0, 3F225, 3D692, 3A722, 374A1, 36684, 35B42, 33660, 1F414, 1B708, 3D805,$ $3C654, 3AE64, 39908, 2EC58, 2DF28, 2CE90, 19E80, 3FE8A, 3FE31, 3EC16, 3DE43, 3DB91, 3BD61, 3782A, 1D741, 1CD88, 17CC8, FF90, EE20, 39C89, 32F18, 2FB06, 2F68C,$ $2BC94, 1FA54, 1F238, 1E9A1, 1E382, 3D012, 3CE19, 36D51, 361C8, 35280, 2E641, 2D840, 2D624, 2B8C8, 1CE42, 3DDF0, 3B1B8, 39C26, 3964A, 37646, 36230, 33FC8, 33A34,$ $2D518, 1EC45, 1E689, 1D5A4, 1BA61, 16F01, FA0C, F4A8, 3F3D8, 3BCB2, 38C44, 37203, 3700C, 34E8A, 34D14, 32E02, 2E911, 29F01, 27D09, 27490, 25E48, 1F362, 1A5E0,$ $16E70, FAC2, F180, 3F9AC, 3F0E3, 3EBE1, 3E715, 3D5C9, 3A385, 391E2, 38A10, 389D8, 389A4, 37B23, 33794, 32FA1, 2DCD1, 1B824, 17994, 17502, 16C40, 159C0, 3E947,$ $3E0DC, 3DAA6, 3A114, 3A068, 39306, 386B8, 365E2, 3646C, 36100, 34AC1, 33E13, 2EF89, 2EF62, 2EC23, 2E208, 2DA1A, 27C06, 23D70, 1EA26, 1DD31, 1C920, 1BD8C, 1BC03,$ $19C68, 17F0A, D3E0, 3F42E, 3F21B, 3D374, 3D15A, 3CDA3, 3A8F1, 3A3D2, 39221, 36329, 3549C, 2F839, 2F5D4, 2E6B1, 2E142, 2BD4A, 29A70, 295A0, 27A85, 27761, 15E91,$ $F832, AF84, 3FDC3, 3F387, 3CBCA, 3C853, 3B65C, 39151, 381C0, 378F4, 36316, 359A9, 34E25, 2B629, 2B452, 1EDE4, 1E89A, 1DAC9, 1D14C, 1C4B0, EB68, 3E50, 3C53C,$ $3C4E5, 34364, 330C2, 307D0, 2E1AA, 2E0B4, 2BF34, 1E174, 1E0D1, 1DEB8, 1D409, 1C7F0, 1BF83, 1BBF0, D610, 3FBB2, 3AFB8, 3AF0E, 39DC6, 36A4D, 3570D, 351C5,$ $336AA, 32C49, 31618, 2D99C, 2D963, 2CB45, 2C8E2, 2C5CC, 272B2, 24D80, 1F80F, 1C858, 1A2A0, 19E1C, 16962, 137C2, 11F44, F613, E4C4, BA00, 6DB0, 3D20, 3FFE8,$ $3E6EC, 3DD0F, 38683, 36E3C, 35F16, 3395C, 32921, 2D2F8, 26528, 24F22, 236D8, 22EA8, 1E3AC, 1D2A3, 1BC59, 19592, 17C63, 12B90, 11FA8, FEE1, D8D4, B330, 7868,$ $3FCDC, 3F457, 3E179, 3D76A, 3BB53, 3A41D, 39333, 3907C, 38529, 3828C, 37CE9, 374DA, 33987, 31894, 2E24E, 2CA06, 2C7C3, 2B5A5, 2ABCC, 29EA3, 27DB1, 25544, 233C4,$ $1C9C6, 1C71A, 1AA09, 173D1, 15328, 13938, A740, 7398, 3EC7A, 3E1B6, 3CB2D, 3C68F, 3C26B, 34472, 341A2, 30DB2, 2C420, 2B183, 2AE9A, 27BD2, 246E0, 1D004, 15C1A,$ $14CE4, 13A4A, 13888, FCA6, D8A1, B6E4, AD18, 3F73C, 3EF59, 3DFA5, 3C127, 38EE9, 36F93, 33772, 32B6A, 32244, 31C55, 2F8CE, 2F34D, 2AA25, 27E59, 2713C, 24BB8,$ $1EE2B, 1D4EA, 1AE95, 1AD72, 1A8EC, 15DD2, 15A6C, 14E0C, F50E, EF25, E814, D462, B9D1, 7B31, 7585, 35C8, 3FA67, 3EA9D, 3AEC7, 35039, 3480A, 3258E, 31B65, 31130,$ $2F6F2, 2D447, 2A822, 28F16, 28B8A, 2738B, 258AC, 1FD96, 1E023, 1CD4B, 1A272, 19CF4, 18734, 152D2, 13725, B606, AF43, 9B42, 6B54, 6680, 3AA37, 3A99B, 3A047, 396B5,$ $3643B, 34AD6, 34411, 33C4F, 33279, 31800, 315F1, 2EC75, 2D727, 2CF5C, 2C1F1, 2A489, 29799, 27021, 268E9, 2556A, 24970, 21E04, 1B636, 1B0B5, 1A359, 17FE2, 17065,$ $169F8, 15D07, 15959, 11A60, F778, E305, DE72, D28A, CEAC, C678, A8F0, 7BE4, 6C8A, 5D11, 3CE1, 3B5AB, 3881E, 3719D, 35837, 32893, 2BAD5, 25FC5, 23CEC, 23A19,$ $1E5D3, 1CB17, 1B12B, 19B9A, 1976C, 18C08, 18AB1, 16787, 138F2, 13599, 13301, FBAA, E4F2, C992, 3DA5E, 3B7F1, 368AF, 31F39, 31C7A, 31863, 2B02E, 2A090, 29935,$ $27F9C, 26CC7, 26845, 24789, 17AC7, 1688D, 14350, 134A6, 126C1, F1E9, E539, D90B, A6CA, 7459, 7326, 5A34, 1CC0, 3FF17, 3D8BB, 3C7D6, 390D7, 353BA, 343B5,$ $306E6, 304A8, 28358, 26A73, 25251, 24DF4, 22948, 21BC9, 21AA2, 1B2CE, 1A10A, 19185, 13431, 12584, D395, AC66, 96D1, 7050, 3986, EB0, 39BCD, 36FF4, 36DCE, 3596E,$ $33DD5, 322CB, 30B0D, 3054A, 2FF2B, 2F976, 2DE97, 2B92F, 2B3E6, 28632, 24394, 22A81, 22731, 219D2, 1F96B, 1C83D, 1BAAD, 1A040, 176B3, 16092, 14622, 14561, 11B83,$ $8DC1, 5908, 27A2, 3ECB7, 36767, 312AD, 30DCD, 2C49B, 2B4F9, 29415, 29102, 28324, 2672E, 23212, 2299C, 20F6C, 1C0AE, 1B51F, 19473, 18BE3, 184DC, 1705E, 16119, 14F66,$ $FE1E, E756, C880, C50C, B09C, 9C8E, 6E96, 54A4, 4AC8, 1E29, 3D79B, 3B87D, 3B74F, 3875B, 32173, 2E11F, 2DE6D, 2C21D, 2C085, 2A375, 29A6E, 290E5, 28D79, 23169,$ $23074, 229E6, 1FDB9, 1EB7C, 1E2FA, 167E9, 14A01, CC03, C5A3, A3A9, 95F8, 92C4, 62AC, 3E8B, F00, 38F75, 3563F, 31AF3, 31049, 3033A, 2D0AF, 2A88F, 29576, 21F8E,$ $20EF1, 20CD8, 1FBD5, 1DCE7, 1CD9D, 18886, 18605, 18452, 17F2D, 17575, 15BDC, 143EA, 12830, 113F4, C555, 9D4D, 9838, 6A13, 6164, 13A0, 3B2BE, 3793F, 325FC, 2FAF9,$ $29C1F, 25597, 2494E, 21696, 1CAF5, 1921B, 1565B, 140E0, 12556, C261, 6EEA, 575C, 56E9, 4BA5, 363C, 1954, 170A, 3F6AF, 35F73, 339FA, 3140F, 304B5, 2C5FA, 2A5CF,$ $29FDA, 28363, 24C3E, 238DB, 225D5, 21753, 1EF8F, 1BE6E, 1A4AF, 188CB, FDCD, F077, 7C9D, 6B0F, 662B, 5A47, 47C6, 3E1DF, 35ECF, 31EFC, 2CFAE, 250CB, 24240,$ $2287A, 1C1BB, 18166, 16B5B, 110F8, DD57, B043, 9AB6, 8A6C, 75BA, 65CB, 6436, 3F55, 340C, 2C95, 3F5F6, 3DC7F, 3ADED, 373EB, 2E27F, 2ADF3, 23FA7, 23267, 22442,$ $1D75D, 1D3F3, 1ACDE, 18FB6, F7B5, D63D, AA3B, A31E, 515A, 4CD3, DAC, 9E2, 668, 28ABD, 24303, 22D37, 2118C, 20C61, 1CEDB, 14617, 12A57, 11E2F, D7CE, A85D,$ $324D, F07, 598, 3FEF3, 2BD9F, 280D6, 246DD, 2369F, 1C47F, 1A36F, 18111, 155AF, 14400, 11483, 5976, 39AD, F59, 38AFF, 33EBB, 24EBB, 22EF6, 22BF9, 1F67B, 19B3F,$ $1424B, 12B3D, 109D5, ED3F, 62F5, 3100, 2BDA, 2A0E, 2619, 2314, 3FBCF, 349F7, 2804C, 2757B, 21DEB, 170FF, 1403C, 1153E, 9401, 8ECF, 6028, 59CF, 58BB, 5099, 21D1,$ $1C37, A52, 1C4, 208A4, 146BE, 766F, 30AB, 1432, 3BBBD, 2EFE7, 2D9EF, 277D7, 202FC, 1BD77, 17F5E, 1134F, 1066D, C01A, B3DB, 30D7, 2903, 3C7FF, 30016, 22F5F, 20593,$ $117D7, 10290, A9BE, 535, 70, 3AFDE, 315FF, 2810F, 243EF, 19FEB, 191FD, 102B6, A02D, 872F, 6BB7, 41CD, 15E7, 10C9F, EFFA, 8289, 4445, 27F3, 4CE, 37AFE, 2DFDD, 121DF,$ $5FF9, 93B, 3FFFF, 37F7D, 36DFB, 2FFBE, 28000, 22005, 2081D, 2039F, 20231, 2008A, 1EEFD, 15FBF, 127BF, 1203F, 10122, FB7F, B5FE, 8206, 80FF, 80B3, 5CFE, 3B7E, 1227, 849

Table D.9: Profile Vectors for Our $(n, d)_{d_{\mathrm{I}}}$ Codes with $n = 18$

$n = 18,\ d = 4$
$3FE00, 3F1E0, 3C990, 3A540, 3F907, F948, 3ED58, 1F080, E7A0, 3E493, 3E02C, 3CFA1, 3A2D8, 3958C, 35860, 3D319, 38B64, 33938,$ $3EC0, 3FAD1, 36B8C, 35552, 33382, 2CCE8, 16DC1, 3BCB4, 39C63, 2D2C4, 29FD0, 3F78A, 19AA8, 34688, 2EB32, 2E745, 1F055, 3FF64,$ $2B230, 26B00, F8A3, EC14, 37669, 1EA4B, 1B41A, 5F11, 356A6, 29C08, 1DECC, 34C35, 33A56, 2D81E, 1A8C6, 136B1, 3E23F, 38A03,$ $2BA2D, 2AD0B, 1C272, 14F2A, 274DC, 27403, 21768, 1C387, 1B753, 9D26, DB0, 3ACCF, 13905, C640, 6A65, 2A476, 259CB, 1A73C, 6A9A,$ $31E9B, 31110, 1D9BA, 16EF2, 37DB3, 25F3C, 243F1, 12624, 107D4, 752D, 3F87, 3D55F, B6EA, 3162, 393E7, 2C059, 12858, FDE9, 519C,$ $F3B5, 787F, 1A20, A30E, 3C9, 3216F, 284A5, CD9D, 3DEAF, 91D3, D4, 3FFFF, 3EBFA, 349FD, 33FDD, 300BB, 2C3DE, 2BE7B, 2A002,$ $267EF, 24036, 2261D, 18029, 1444F, 14000, 135FE, CF77, 4883, 1ADD,$
$n = 18,\ d = 5$
$3FE00, 3E1F0, 3F10F, 79C0, 195A8, 31DC3, 3C104, 1E30, 1CAA7, E83C, C752, 28BCC, 3DCEC, 35059, 3FAD3, 38F39, 32492, 1A261,$ $13395, 7467, 3FFFF, 367BE, 25B76, 23008, 2092B, 12E5E, BF6F, 468D, E6$
$n = 18,\ d = 6$
$3FE00, 3F03F, 39E0, 3FFFF, 38FF8, 381C7, 38038, 7FC7, 651E, 6201$
$n = 18,\ d = 7$
$3FE00, 3FFFF, 3C1FC, 30183$
$n = 18,\ d = 8$
$3FE00, 3FFFF, 301FE, 20101$
$n = 18,\ d = 9$
$3FE00, 3FFFF, 1FF, 0$

Table D.10: Profile Vectors for Our $(n, d)_{d_I}$ Codes with $n = 18$ (cont'd)

$n = 19,\ d = 3$
$7FE00, 7F180, 7E840, 7F960, 7CD20, 7D400, 7ED90, 7E4E0, 7D260, 7CBC0, 7A740, 79CC0, 79B00, 7F7C0, 7D550, 7B830, 7E418, 7E330, 76AA0, 7D8A8, 778D0, 77210, 6E680, 67D40, 1FD00, 7E90C, 7BB88,$ $7B528, 7FAB0, 7F883, 7F049, 77424, 757A0, 6DA90, 3EC84, 7F505, 7D806, 7B2C4, 73C08, 6EB02, 6D708, 3F442, 3B6A0, 7FC58, 7EF28, 7DB14, 7BCA4, 7B491, 77342, 74E50, 6F911, 6DD84, 576C0, 4FCA0,$ $3E300, 37B08, 7F432, 7EA51, 7E28A, 7E205, 7DD0A, 7D698, 7AA68, 73D82, 6B880, 6AFA0, 5ED41, 35E80, 2FA20, 7F22C, 7CEA1, 7AC54, 79F41, 79614, 76F44, 76502, 6F2A1, 6B510, 5E784, 5D948, 5CE88,$ $5BB50, 5AE20, 3E2D0, 7C0B0, 7AEC2, 78F18, 76C89, 75C61, 74980, 73F30, 73A41, 5F028, 5BA82, 3B944, 7FF11, 7DE64, 7C703, 7C64C, 7AC03, 73160, 6F054, 67EE0, 5DB21, 4F760, 4DE40, 3DC11, 3C5C0,$ $6D6C2, 6BA0C, 67B24, 5C710, 5B240, 57D18, 55F04, 3A9A0, 37800, 2F8C8, 2F790, 7FE8C, 7FDA2, 7A020, 77391, 75A85, 75492, 750C8, 73658, 729C8, 71E22, 6FC29, 6EC4A, 6E168, 6CA00, 66C20, 5E9A2,$ $5D881, 5B484, 56C90, 3AC10, 2BE50, 1FFA0, 1EB60, 7F60B, 7EB85, 7C872, 7BF06, 79392, 78994, 783A8, 77686, 74628, 725B0, 724C0, 6F358, 5F654, 5DC34, 5BC62, 5B324, 4EED0, 47B80, 3F825, 3F661,$ $3E421, 3DA58, 3BB22, 359E0, 1FA14, 7E1A9, 7D1CC, 7C109, 7A626, 79C0D, 791E1, 77A1A, 75138, 72A04, 6FA46, 6EE34, 6D142, 6CC14, 3E82A, 3D28C, 3D124, 375C8, 7EC63, 7DAC9, 76151, 74344, 70F81,$ $6E8C5, 6DBA2, 6B48A, 6B461, 68D40, 67F03, 67108, 63784, 5E629, 5D589, 5788C, 56C68, 55A20, 4FDC8, 4F612, 4BF01, 3F213, 3DCF0, 39648, 36F21, 2F341, 2CEE0, 1FAC1, 1F090, 7FB4A, 7F9D4, 7CF52,$ $7B0F8, 78DE8, 78464, 782C2, 7458C, 71850, 6F89C, 66B98, 667C1, 5F40E, 5F2E2, 5E1D8, 5B985, 5A908, 59D12, 56600, 53EA8, 4FA38, 3D943, 3CE92, 3AB11, 36714, 1E644, 7F19A, 7E574, 7DC95, 760C6,$ $718A4, 71280, 6BD52, 69E31, 674B8, 5EE07, 5C8E4, 55FD0, 4E930, 3FD89, 3EAE4, 3C912, 3B0C1, 39598, 2F40C, 2EE09, 2ED70, 27640, 275A0, 1D782, 7F0E5, 7BEE1, 78218, 74D15, 74B2A, 71B4C, 6E516,$ $6E012, 6DA0B, 6C591, 6A8E2, 6A270, 69868, 67805, 66662, 5F1B4, 5D445, 5C160, 596F0, 57E49, 57903, 3D62A, 3BE4C, 3BC1A, 3B206, 35C4C, 33701, 2AF04, 1E5A8, 1D870, 1CCA0, 1B388, 7D569, 7C927,$ $7905A, 779AC, 7771C, 755C3, 74CA6, 74A03, 735D4, 6C88A, 6C7F0, 6A1C4, 699D8, 67615, 65470, 5E74A, 5C284, 5B783, 591D0, 56E32, 4E5C2, 38A60, 37D51, 33E94, 31D20, 2E3A4, 2BDC1, 25F30, 1ADD0,$ $19E00, 17A42, EAC0, 7FA27, 7B371, 7AE99, 7A94B, 785C6, 76BE2, 73C47, 73116, 730A9, 6F5B1, 6E693, 6B6C9, 68B64, 61DA8, 5FCC6, 5D219, 5BDF0, 5AAB4, 57CB1, 4E504, 4D3C4, 3CF8C, 3C80C, 3C34A,$ $3A789, 39764, 39140, 32E64, 2FE8A, 2F132, 29780, 27E06, 1BC89, 19F28, 7FED2, 7E81F, 7E2DC, 7D347, 79EAA, 79939, 79023, 742F8, 72925, 71549, 70C00, 6BED4, 68E86, 66321, 63CCC, 633F0, 62E38,$ $5F153, 5CE78, 57271, 56392, 55562, 5370A, 52D44, 51BB0, 4F000, 3C9B1, 3B31C, 3A158, 374A3, 36834, 35F68, 2D901, 27994, 26B50, 1F531, 1E2A2, 13CE0, 7D7B4, 7C09D, 7A7B2, 7936A, 77933, 75236, 7382E,$ $72A93, 7229C, 6E363, 6C5AA, 6C2C9, 6B1A6, 69F2C, 69983, 69224, 68CA1, 68722, 652A2, 5D726, 5C44A, 5ABE1, 58580, 561A4, 55CCA, 53430, 4E989, 4D4D8, 4ACC8, 3C080, 3B5E2, 38C78, 36ED8, 36B86,$ $33892, 32E8A, 2E891, 2DE45, 2D0E0, 1B824, 14F40, BB10, 7C88, 7EFE4, 7C457, 7BD6C, 7A356, 79FD8, 798D6, 78A47, 78106, 774EA, 7687C, 6E93A, 6C565, 61E01, 5E063, 5A451, 57F8A, 5730D, 4D818, 4D521,$ $4B2E8, 45D00, 3E166, 3DF23, 37D26, 37AA9, 360A8, 356D1, 34C62, 33454, 33184, 2F50B, 2D4B4, 2B90A, 19AC4, 17638, 173A1, FF0C, F258, 7960, 7FBA9, 7F778, 7A48F, 792A7, 78795, 766F1, 7651B, 75E39,$ $74042, 727AC, 72563, 70B71, 6F94D, 6ECEC, 6CD5C, 6C839, 6BBC3, 6ACF1, 6A559, 6A409, 6756C, 64DD2, 63404, 62390, 5DA8E, 5BA33, 57006, 4B54C, 4A798, 479E1, 46748, 3A50E, 339B8, 2D3E8, 2C630, 29D62,$ $F886, F422, D9A8, 7E11, 7FD47, 7E6C7, 76FC9, 741A3, 72E2B, 7168B, 66DA5, 64E25, 62C52, 61B52, 61698, 5DF0D, 5CB99, 5A816, 5A303, 58AD1, 56289, 53C15, 52A58, 51DE4, 51C82, 4FF32, 4FBE4, 4D6AC,$ $4CB0C, 3A0EC, 38A89, 37EC3, 35829, 35191, 34510, 32F52, 2D603, 2B208, 1E859, 1E048, 1D9D4, 1CE43, 1CB85, 16570, F685, D550, B742, 7CDF1, 7C23B, 7A74D, 796D3, 7817C, 77763, 754AD, 71CD9, 6D875,$ $65094, 64C49, 6324A, 61D06, 5D0B3, 5CC1B, 5C355, 59D9C, 57B78, 5541C, 546B4, 52EC5, 507E0, 4CF46, 49F8A, 48E90, 47264, 3F3A6, 3E9F8, 3E4BC, 3E30F, 3D596, 3C635, 3C48B, 3C2E3, 3C051, 3BE72, 3A778,$ $37374, 36A4B, 3520A, 33272, 32942, 2C398, 26D2C, 23768, 1EB1A, 1E803, 1DC87, 1D89A, 1CD1C, 1A681, 19F91, 169C1, FE23, BC38, 7D98F, 7B12F, 78BF4, 6D06E, 6CADA, 6938D, 66081, 63319, 62F0D, 5D86B,$ $5BE3C, 5A23A, 56956, 4BC96, 4BA65, 4B291, 4AD2A, 47872, 3B917, 3AD65, 386C5, 37FF0, 32622, 2EBC9, 2DF19, 2BA99, 2A900, 27AB2, 26A8C, 22E80, 17449, 15B51, 154C0, D320, BC41, 7F43D, 7925D, 75FC6,$ $743E5, 74025, 73A8F, 71FA5, 71ABC, 7120D, 704EA, 6FCCB, 6FB3C, 6EAAB, 6E78E, 6C21E, 6B61E, 68CBC, 67D96, 65C1E, 63B69, 62848, 613C1, 5F297, 5ECBA, 5CCCD, 5C136, 5A8CE, 58C05, 57D65, 56FB4,$ $530F4, 4DE53, 4AC02, 46E83, 3F54E, 3E1D5, 3DD3C, 3998E, 3701D, 313D4, 2FEA5, 2EDC6, 2CA46, 2B8F4, 21DD0, 1B6CA, 15368, CD64, 6F22, 760B7, 7082A, 6B03D, 680D0, 65533, 649EC, 64606, 6291C, 5AD36,$ $59014, 564D3, 53BC6, 53101, 52774, 51652, 4F6F8, 4F4A7, 4E09C, 4CA6A, 38A36, 35E0F, 35507, 32250, 2BFE8, 2A4A4, 29AAA, 264D8, 25C12, 1FBD2, 1E115, 1DA66, 1D0E9, 1B969, 1AE71, 18B82, 15914, ED13,$ $7FC2, 7D8FA, 7C7EA, 7B597, 77C76, 72DD3, 6F756, 6D5E6, 67E2E, 65DF8, 651D5, 6473C, 62645, 61931, 5EF5C, 5BD1B, 5B46D, 5870D, 586A3, 5524E, 54F63, 528A1, 50D38, 50B10, 4EB96, 4E47C, 4C671, 4C4C1,$ $49E5C, 49A32, 494A8, 473AA, 46B45, 45E99, 39473, 38D2B, 381F2, 378CE, 36479, 328F1, 3232C, 2C50A, 2C444, 29830, 28DCC, 2796A, 266B1, 1FC1D, 19631, 1950C, 1711A, 6C50, 6B08, 79E4F, 78E37, 753AB, 74D4F,$ $7499E, 715BA, 70495, 7019A, 6D51F, 6B667, 6A02E, 6718F, 6626D, 64EC7, 64120, 60AD4, 60708, 5F5D9, 5EA76, 4CCE3, 45C2A, 3EF9A, 3AABA, 345F4, 3362D, 30E1C, 2CCD9, 2A61A, 29F16, 25CC3, 1F07A, 1D7C5,$ $1B547, 1B436, 1B24D, 1B193, 16C0E, 163CC, 12F49, 12B94, 11ED8, D842, CCD2, C990, A728, 7284, 3700, 1BC0, 7FA5D, 79BB3, 6EE79, 6867A, 68315, 65F55, 63476, 61AE6, 60EE9, 60C8C, 590AE, 565E6, 5585D,$ $51386, 4EB2D, 4D9C7, 4B84B, 4A4B2, 472DC, 3F6B3, 3CC6E, 323C3, 303C8, 2F85B, 2C955, 2AC35, 2A583, 2993C, 297A3, 24B24, 1C772, 19919, 195A5, 15DB2, 15626, 14AB8, 13A09, E1A1, C688, 3AA2, 2DB0,$ $7EB73, 7DF2E, 7CB6D, 73DB9, 6BF2B, 6640F, 6566B, 630D3, 58269, 58200, 51739, 4FF87, 4D179, 49945, 49666, 48660, 47051, 46D8E, 459A6, 44F1A, 35A73, 34296, 3374B, 31489, 294C6, 2728B, 270E5, 2565A, 25428,$ $22D61, 1C212, 1BCD3, 1A404, 17B9C, 16261, 16182, FB71, B1B4, 8FC1, 75D1, 5D85, 5AE1, 3E4C, 1E70, 7ED9D, 7B2F6, 7ABAE, 77EB5, 76CAF, 7469F, 7395E, 6B8B7, 68D9B, 63227, 5E1CF, 597EC, 54809, 539AB,$ $50F96, 4C826, 4B735, 4A28A, 48B21, 46238, 45312, 45248, 449D8, 4399A, 43589, 3C7D9, 3A0DB, 39DC7, 38BD3, 36F17, 307A6, 2E04B, 2DA97, 2A6DC, 29329, 292F1, 29252, 1EEE9, 1A132, 188D8, 186AC, 16A2D,$ $14DC6, 12C28, 11D4A, CFB8, 7E74, 6692, 7D7CD, 772DB, 70E5E, 6ED37, 62BD5, 62202, 61747, 6127C, 5F66E, 5DE9B, 5C53D, 5ADAD, 583CB, 52098, 51A7A, 519D3, 4EDD5, 4E837, 4E25B, 4B97C, 4A1F1, 47135,$ $45D2D, 448E0, 431C2, 42DF8, 42BAC, 41744, 3B8EB, 38403, 353DA, 3516D, 3284D, 31B1B, 3143A, 308C4, 2D67C, 2CAAD, 2B26B, 2B015, 2AF33, 2AB4E, 29400, 25366, 25210, 1FA4F, 1C27C, 1C18E, 19363, 176EC,$ $F22E, E074, 56D4, 38D4, 7FE6B, 7ACDE, 7947E, 7088F, 6A2EE, 664DD, 658BB, 6501B, 627DA, 60534, 5B8DD, 5745F, 5369D, 52587, 51060, 4D19E, 4A2D6, 48BF2, 3D1F3, 373CD, 2B3E5, 2A89E, 2773A, 24F8B,$ $24B69, 23866, 230C0, 22D99, 1E3B3, 1DEDC, 1A0C6, 19BF8, 190A2, 18354, 16C67, 158B5, 1575C, 15108, 14799, F356, E339, DD5A, D245, ABA3, 64A0, 5709, 7FCFC, 7FB97, 7F1EE, 7633F, 74EFC, 739E7, 71177,$ $6DFE3, 6D2BD, 66B5B, 64FB3, 64B76, 63BBA, 611CE, 54433, 5206C, 51E75, 50A66, 4E2F5, 4DDAB, 445A2, 436E3, 42984, 37F2D, 35EB6, 323B5, 2F976, 2E4EB, 26C97, 2515C, 24CBA, 23C2B, 1E8AF, 1BF55,$ $1A697, 14A04, 14765, CC01, A2B0, 3B25, 1CA4, 7CC7F, 7B6AF, 73FEA, 72F75, 6800C, 5DAF5, 5A11F, 585F3, 5245E, 52235, 4A4AD, 48E0B, 46727, 460EA, 41CF1, 3DD5B, 2FE1F, 2F4D7, 26145, 24878, 23122,$ $21E8D, 1A0B9, 14DE9, 14C55, 13AA7, 131EA, 12CBC, F1CD, E6E6, 8B78, 7B9DB, 7A57B, 6F79B, 58093, 57B57, 556E7, 52D5D, 510C5, 4B34F, 4A205, 4989D, 4910A, 477D3, 467B9, 45B17, 3DCED, 3C5AF, 39B9D,$ $33CFC, 332D7, 31807, 30331, 2B59D, 28753, 281A8, 20BE2, 15143, 11890, D90F, CA35, 43F0, 2EA9, 2A60, 25C8, 1C48, 7FFF1, 73F1F, 6E0FF, 69A7B, 67FDC, 67AED, 6287B, 62063, 5F93F, 521ED, 4C031, 49CFA,$ $497D6, 48FA7, 42716, 386F6, 34B5D, 32008, 30FB9, 3096E, 2DBCE, 2945D, 25DCD, 1FDB5, 1E767, 19EAD, 19857, 188E3, 17637, 137F1, BF66, ACC7, AA53, A86A, A511, 54B1, 37B2, 6CBD7, 60903, 602A9, 5C0FE,$ $559F6, 5333E, 4F9F3, 4E63F, 4192C, 3EABD, 3D27F, 2793D, 261F3, 2601C, 24840, 225D6, 21FF4, 21A59, 218CA, 1D7BA, 1A3AE, 18309, 16D7A, 112B4, D43B, C8CD, A889, 9A0E, 74CE, 6ADA, 345A, F06, D80, 7A1,$ $6D0, 79DF6, 7043F, 6F3F5, 6EDFA, 6A7FC, 680B7, 5D577, 5B3EB, 58B5F, 4AECF, 4845C, 44963, 42E6E, 42170, 416A5, 3BFBC, 32FCE, 329F6, 3213B, 320A7, 314DE, 2C087, 24539, 21D79, 1F33D, 1971F, 16257,$ $16011, 12525, 119CD, 10F13, D3B5, A2E5, 1592, 542AF, 49417, 4895E, 3DF75, 3B6DD, 3044E, 26F7C, 1880A, B4F9, 95CB, 9184, 87F4, 702D, 6387, 466C, 3804, 3607, 7E75F, 791FD, 689EF, 6597F, 60159, 5FFBA,$ $5D3DE, 57ECF, 57ABE, 5050B, 50426, 44418, 43ADB, 42440, 41B2B, 40B4A, 3EBCF, 388FD, 2CB3F, 29C3F, 28927, 28241, 2607E, EE5E, 459C, 161C, 7FFCE, 755BF, 637CF, 4BC7F, 42C27, 40A88, 3F8F7, 3801F,$ $2F3FA, 2EEF6, 2AD5F, 21451, 1B4BF, 1B1DE, 18B3D, 105D1, F99F, C0BA, 9166, 894C, 656B, 3E1F, 3813, 352E, 1921, 72AFF, 6FDAF, 6767F, 603BB, 5E7B7, 4FF6D, 4455D, 442D3, 41481, 34AEF, 287CF, 22825,$ $21305, 14402, 11246, 9ACF, 969E, 8E6D, 683B, 6200, 4A83, 3DB5, 3179, 3038, 16EA, 12A0, B99, 564, 625BF, 5AFF9, 50FFA, 4F5BE, 4818D, 3267F, 30069, 30034, 2230B, 185DD, C1E7, 640B, 4FD5, 4342, 2C1D,$ $1C9B, 7D6F7, 61EBF, 60080, 44EBE, 4357B, 365DF, 22BAF, 20996, 206C3, 1EDEE, 1CCF7, 18227, 1421D, D56F, C028, A052, 8C33, 6EF3, 29CE, 7E9FF, 79B7F, 586FF, 43DEE, 41110, 293BE, 23A7E, 20DE7,$ $20A1A, 20676, 10872, 7F6B, 70BF, 9E5, 62A, 75FDB, 569FD, 523F7, 50157, 44FED, 40E57, 33B7B, 27BB7, 2315F, 208A2, 1AF3F, 154FB, 112BB, 101FC, 99BB, 5036, 2B76, A55, 5BFE7, 51DDF, 4C3FB, 4813B,$ $4408E, 41223, 11B6F, 30C, 70, 6BEDF, 573FF, 2422F, 1146F, 134F, 11AB, CA, 4577E, 44045, 405BE, 3B5FF, 2C7FF, 242DF, 21FDB, 210BD, DFF9, 81C3, 637F, 39EFB, 40D9, 7FFFF, 66FF7, 4DFFF, 4BBFE,$ $413FD, 4087D, 40816, 404CF, 400F6, 3FF3F, 35BFE, 317F7, 29F7E, 2100B, 20191, 1FFDD, 17DFB, 11001, 1011E, 1008D, ABFD, 8800, 842D, 8015, 75FD, 22BE, 2107, 18FE, 27B,$

Table D.11: Profile Vectors for Our $(n, d)_{d_{\mathrm{I}}}$ Codes with $n = 19$

$n = 19,\ d = 4$
$7FE00, 7E1C0, 79920, 7F9B0, FD80, 7F107, 7C410, 7D568, 77038, 79591, 73280, 3D894, 357A0, 1F260, 7C8A9, 71CC8, 6ACB0, 36B10, 7CB51,$ $7B2E1, 3B50C, 7ECC3, 7A334, 79252, 74A64, 72D61, 6E80C, 6B958, 7E49C, 3AC42, 7F7C4, 7AB8A, 6D38C, 5CD0A, 6A701, 678E2, 5C6F0, 6D445,$ $67D89, 57554, 52F84, 2E658, 76293, 5B883, 2EFE0, 2DA00, 19F41, 79F23, 64E82, 37349, 1EC25, 7AE78, 57AD8, 75C35, 64F38, 56840, 4B7C2,$ $47B21, 2F532, 7771A, 6E62B, 69ED4, 5560C, 4EAC5, 3C746, 2BA2A, 1B818, 7DE99, 7DA4E, 43E50, 36489, 18EA0, 65148, 5BC66, 7E83F, 6366C,$ $5EF0D, 3BC1B, 3A100, 682E8, 55192, 4B420, 1DF92, 139F0, 59A1D, 2E0A2, 2B9A5, 7FB69, 61D16, 58344, 37EAC, 26564, 1E28E, 7168F, 2B0D1,$ $29634, 27E47, 17C0, 6D0DB, 4F771, 3692E, 1D873, C970, 51B6A, 33FD1, 31C05, 24DD1, 1C339, 185D8, 7603, 7855F, 64BA7, 589D6, F4E9,$ $5AC9, 7BD8F, 4F2B6, 458A4, 3A0FA, 72027, 60990, 28E8D, 7114, 7E7B3, 761ED, 5264B, 30E33, 3070A, 13727, 2CCC, 2B28, 5599F, 4FFAA,$ $3285D, 31070, 71C7, 6C3A, 6BB57, 527B9, D12E, 66D76, 3D4F6, 2A797, 15400, E99B, 3882, 792FF, 5808A, 57AE7, 2D33F, 611AB, 242D4,$ $1C5AF, 12531, C509, E14, 77CFA, 63ABB, 4A173, 114E6, CA17, BF3C, 4349D, 1F65F, 17D6B, A252, E8, 6CBFC, 64021, 5ADF5, 441FC, 313FC,$ $7FFFF, 7EF5E, 75FF5, 604F7, 60446, 5427F, 4F9FF, 48EEF, 48800, 4803D, 4231E, 40A63, 34FCF, 2B5FB, 14226, 1405B, 109AD, 9045, 5CDE,$ $12BA, 303$
$n = 19,\ d = 5$
$7FE00, 7C1E0, F990, 7B187, 73108, 7CC1F, 3E60, 779D8, 3A85C, 3C410, 334B2, 1A789, 76273, 69939, 1D24A, 15D45, 70A91, 68D06, 7D7B1,$ $664CD, 26B2A, 7A76C, 4DCE3, 496D4, 38FD2, 4E225, 3D0, 67F47, 1DBAC, 6F0FF, 7FFFF, 60820, 5BF9E, 5162F, 50076, 49083, 42FB5, 2557E,$ $600E, 3ADB, 9AD$
$n = 19,\ d = 6$
$7FE00, F1E0, 7E11F, 709D8, 1F10, 7FFFF, 79DE6, 78026, 67AF9, 494BD, 46009, 44B67, 137D3$
$n = 19,\ d = 7$
$7FE00, 7FFFF, 7C1FC, 70183, E070, 3FF3$
$n = 19,\ d = 8$
$7FE00, 7FFFF, 701FE, 60101$
$n = 19,\ d = 9$
$7FE00, 7FFFF, 401FF, 40000,$

Table D.12: Profile Vectors for Our $(n, d)_{d_{\mathrm{I}}}$ Codes with $n = 19$

Bibliography

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, pp. 1204–1216, July 2000.

[2] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, pp. 371–381, Feb. 2003.

[3] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, pp. 782–795, Oct. 2003.

[4] T. Ho, R. Kötter, M. Médard, D. R. Karger, M. Effros, J. Shi, and B. Leong, "The benefits of coding over routing in a randomized setting," in *Proc. IEEE Int. Symp. Information Theory*, (Yokohama, Japan), p. 442, June 29–July 4, 2003.

[5] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, pp. 4413–4430, Oct. 2006.

[6] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," in *Proc. Allerton Conf. on Comm., Control, and Computing*, (Monticello, IL), pp. 40–49, Oct. 2003.

[7] T. Etzion and A. Vardy, "Error-correcting codes in projective space," in *Proc. IEEE Int. Symp. Information Theory*, (Toronto, Canada), pp. 871–875, July 6–11, 2008.

[8] E. Gabidulin and M. Bossert, "Codes for network coding," in *Proc. IEEE Int. Symp. Information Theory*, (Toronto, Canada), July 6–11, 2008.

[9] F. Manganiello, E. Gorla, and J. Rosenthal, "Spread codes and spread decoding in network coding," in *Proc. IEEE Int. Symp. Information Theory*, (Toronto, Canada), July 6–11, 2008.

[10] A. Kohnert and S. Kurz, "Construction of large constant dimension codes with a prescribed minimum distance," *Mathematical Methods in Computer Science: Essays in Memory of Thomas Beth*, pp. 31–42, 2008.

[11] R. Kötter and F. R. Kschischang, "Coding for errors and erasures in random network coding," in *Proc. IEEE Int. Symp. Information Theory*, (Nice, France), pp. 791–795, June 24–29, 2007.

[12] D. Silva, F. R. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," in *Proc. IEEE Information Theory Workshop on Information Theory for Wireless Networks*, (Bergen, Norway), July 1–6, 2007.

[13] N. Cai and R. Yeung, "Network coding and error correction," in *Proc. IEEE Inform. Theory Workshop*, (Bangalore, India), pp. 119–122, Oct.20–25 2002.

[14] R. W. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds," *Commun. Inform. Syst.*, vol. 6, no. 1, pp. 19–36, 2006.

[15] R. W. Yeung and N. Cai, "Network error correction, part II: lower bounds," *Commun. Inform. Syst.*, vol. 6, no. 1, pp. 37–54, 2006.

[16] Z. Zhang, "Network error correction coding in packetized networks," in *Proc. IEEE Inform. Theory Workshop*, (Chengdu, China), pp. 433–437, Oct.22–26 2006.

[17] Z. Zhang, "Linear network error correction codes in packet networks," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 209–218, 2008.

[18] R. Kötter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, p. 35793591, Aug. 2008.

[19] T. Etzion and N. Silberstein, "Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams," *IEEE Trans. Inf. Theory*, vol. 55, pp. 2909–2919, July 2009.

[20] D. Silva and F. R. Kschischang, "On metrics for error correction in network coding," *IEEE Trans. Inf. Theory*, 2008. to be published.

[21] A. Khaleghi and F. R. Kschischang, "Projective space codes for the injection metric," in *Proc. 11th Canadian Workshop Inform. Theory*, (Ottawa, Canada), pp. 9–12, May 13–15, 2009.

[22] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*. Cambridge, UK: Cambridge University Press, second ed., 2001.

[23] L. M. G. M. Tolhuizen, "The generalized Gilbert-Varshamov bound is implied by Túran's theorem," *IEEE Trans. Inf. Theory*, vol. 43, pp. 1605–1606, Sept. 1997.

[24] D. B. West, *Introduction to Graph Theory*. Prentice -Hall, Inc. Upper Saddle River, NJ07458: Springer Verlag, 2001.

[25] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inform. Transm.*, vol. 21, no. 1, pp. 1–12, 1985.

[26] D. Silva and F. R. Kschischang, "Fast encoding and decoding of Gabidulin codes," in *Proc. IEEE Int. Symp. Information Theory*, (Seoul, Korea), pp. 2858–2862, June 28–July 3, 2009.

[27] D. Silva, F. R. Kschischang, and R. Kötter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3951–3967, 2008.

[28] D. Silva, *Error Control for Network Coding*. PhD thesis, University of Toronto, Toronto, Canada, 2009.

[29] H. Wang, C. Xing, and R. Safavi-Naini, "Linear authentication codes: bounds and constructions," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 866–872, 2003.

[30] A. Borel, *Linear algebraic groups, Grad. Texts Math. 126*. Springer, second ed., 1991.

[31] R. Varshamov, "A class of codes for asymmetric channels and a problem from the additive theory of numbers.," *IEEE Trans. Inf. Theory*, vol. 19, pp. 92–95, Jan. 1973.

[32] T. Klove, "Error correction codes for the asymmetric channel," 1981.

[33] V. Shilo, "New lower bounds of the size error-correcting codes for the Z-channel," *Cybernetics and Sys. Anal*, vol. 38, pp. 13–16, 2002.

[34] P. Delsarte, "An algebraic approach to association schemes of coding theory," *Philips J. Res.*, pp. 1–97, 1973.

[35] P. Frankl and R. Wilson, "The Erdös-Ko-Rado Theorem for Vector Spaces," *Journal of Combinatorial Theory*, vol. 43, pp. 228–236, 1986.

[36] S.-T. Xia and F.-W. Fu, "Johnson type bounds on constant dimension codes," *Designs, Codes and Cryptography*, vol. 50, pp. 163–172, Feb. 2009.

[37] R. Ahlswede and H. Aydinian, "On error control for random network coding," in *IEEE Workshop on Network Coding, Theory and Applications*, 2009.