Matrix Algebras and Semidefinite Programming Techniques for Codes

Dion Gijswijt

Matrix Algebras and Semidefinite Programming Techniques for Codes

Academisch Proefschrift

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus prof. mr. P.F. van der Heijden
ten overstaan van een door het college voor promoties ingestelde
commissie, in het openbaar te verdedigen in de Aula der Universiteit

op donderdag 22 september 2005, te 12.00 uur

door

Dion Camilo Gijswijt

geboren te Bunschoten.

Promotiecommissie

Promotor:	Prof. dr. A. Schrijver
Overige leden:	Prof. dr. A.E. Brouwer
	Prof. dr. G. van der Geer
	Prof. dr. T.H. Koornwinder
	Prof. dr.ir. H.C.A. van Tilborg

Faculteit der Natuurwetenschappen, Wiskunde en Informatica

This research was supported by the Netherlands Organisation for Scientific Research (NWO) under project number 613.000.101.

NWO
Netherlands Organisation for Scientific Research

THOMAS STIELTJES INSTITUTE
FOR MATHEMATICS

voor Violeta

Contents

Chapter 1

Introduction

In this thesis, we consider codes of length n over an alphabet of q symbols. We give new upper bounds on the maximum size $A_q(n, d)$ of codes with minimum distance d, and new lower bounds on the minimum size $K_q(n, r)$ of codes of covering radius r. The bounds are based on semidefinite programming and on an explicit block diagonalisation of the (non-commutative) Terwilliger algebra of the Hamming scheme. Our methods can be seen as a refinement of Delsarte's linear programming approach and are related to the theory of matrix cuts. They build upon the recent work of Schrijver [38] for binary codes.

1.1 Codes

A *code* is a collection of *words* of some fixed length, for example the collection of all six letter words in a dictionary. However, the words need not have any meaning. They are merely concatenations of symbols chosen from a fixed set called the *alphabet*. Other examples of codes are: all possible strings of eight binary digits, a set of bets in a football pool, or a collection of DNA sequences. Here the alphabets are $\{0, 1\}$, $\{\text{Win}, \text{Lose}, \text{Tie}\}$ and $\{\text{A}, \text{C}, \text{T}, \text{G}\}$ respectively.

It is often important to know how similar two words are. This can be measured by their *Hamming distance*. By definition, this is the number of positions in which the two words differ. Suppose for example that we want to transmit information over a noisy communication channel. The letters in a transmitted word each have some small chance of being changed into a different letter. At the receiving end, we would like to be able to recover the original message (if not too many letters are erroneous). This can be achieved by using a code in which any two words have distance at least $d = 2e + 1$ for some integer e. If we only transmit words belonging to this code, it is always possible to recover the sent code word if at most e errors are introduced during transmission. The received word is interpreted as the code word that is the closest match. If we aim for a highest possible information rate, we should maximize the number of words in the code, under the condition that any two code words have distance at least d. Geometrically, this means that we want to pack a maximum number of spheres ('balls' would be more accurate) of radius r inside the *Hamming space* consisting of all q^n words of length n. Here the chosen code words correspond to the centers of the spheres. This leads to the following central question in coding theory.

What is the maximum cardinality of a code of word length n, in which any two words have distance at least d?

When the alphabet consists of q symbols, this maximum is denoted by $A_q(n, d)$. The number $A_q(n, d)$ can also be seen as the *stability number* of a graph. Let G be the graph with the set of all q^n words as vertices, and two words are joined by an edge if their distance is less than d. Then the maximum size of a set of vertices, no two of which are joined by an edge, equals $A_q(n, d)$.

The problem of determining $A_q(n, d)$ is hard in general and we will have to be satisfied with lower and upper bounds. One major field of research is to find explicit examples of (families of) good codes. In this thesis we will address the converse problem and give upper bounds on the numbers $A_q(n, d)$. In the case $d = 2e + 1$ the geometric idea of packing spheres already gives an upper bound. Since the spheres are disjoint, their 'volumes' should add up to a number that is at most q^n. This gives an upper bound on $A_q(n, d)$ called the *sphere packing bound*.

1.2 The Delsarte bound

Currently, many of the best bounds known, are based on Delsarte's linear programming approach [15]. When viewed from the right perspective, the work in this thesis can be seen as a refinement of this method. Let us give a very rough sketch of Delsarte's method.

As is often the case in mathematics, we first seem to make the problem harder. Instead of optimizing the cardinality of a code directly, we associate to each code C a symmetric matrix of which the rows and columns correspond to all q^n possible code words. The matrix is constructed by putting a 1 in those positions where both the row and the column of the matrix belong to C, and a 0 in all other positions. The size of the code can be recovered from the matrix by dividing the total number of ones by the number of ones on the diagonal. Although we have no good grasp of the set of matrices that arise this way, they share some important and elegant abstract properties:

- the matrix has zeros in positions indexed by a row and column that are at distance $1, 2, \ldots, d - 1$,
- the matrix is *positive semidefinite*: it has no negative *eigenvalues*.

We enlarge our set of matrices from those associated to codes, to include *all* symmetric matrices sharing the two given properties. The resulting *relaxation* is much 'smoother' and has a very clear description which allows more efficient optimization. Of course the magical part is, that optimizing over this larger set gives a good approximation of the original problem! This bound was given in the more general setting of bounding the stability number of a graph by Lovász [31]. It can be calculated using semidefinite programming in time bounded by a polynomial in the number of vertices of the graph.

In the coding setting, this will not suffice since the size of the matrices is prohibitively large. Even for codes of length $n = 20$, we have to deal with matrices of more then a million rows and columns. However, the problem admits a very large symmetry group. It turns out that we can use these symmetries to our advantage to —dramatically—

reduce the complexity of the problem. We may restrict ourselves to only those matrices, that are invariant under the full group of symmetries. These matrices live in a low-dimensional commutative subalgebra called the *Bose-Mesner algebra* of the *Hamming scheme*. Diagonalising this algebra reduces the huge optimization problem to a simple *linear* program of only n variables! The resulting linear programming bound (adding the constraint that the matrix is nonnegative) is due to Delsarte.

1.3 Overview of the thesis

In this thesis, we give tighter bounds for codes by essentially isolating more properties satisfied by the zero-one matrices associated to a code. More accurately, we associate to each code C *two* matrices. Both matrices are obtained by summing zero-one matrices corresponding to certain permutations of the code C. This allows to include constraints that come from *triples* of code words, instead of pairs. This method was initiated recently by Schrijver [38] to obtain bounds for binary error correcting codes, resulting in a large number of improved upper bounds.

The main result in this thesis is to generalize the methods to include non-binary codes. The primary issue that we need to deal with, is how to exploit the remaining symmetries to obtain a semidefinite program of a size that is polynomially bounded by the word length n. This is the most technical part of the thesis and requires an explicit *block diagonalisation* of the *Terwilliger algebra* of the nonbinary Hamming scheme. Such a block diagonalisation is described in Chapter 3. It uses the block diagonalisation of the Terwilliger algebra of the binary Hamming scheme found by Schrijver, which we will describe as well.

In Chapter 4 we apply our methods to obtain a semidefinite programming bound for nonbinary codes. Computationally, we have found a large number of improved upper bounds for $q = 3, 4, 5$, which we have tabulated in the final section.

In Chapter 5 we discuss covering codes. The problem here is to cover the Hamming space with as few spheres as possible. When the spheres have radius r, this minimum number of required spheres is denoted by $K_q(n, r)$. We give new linear and semidefinite programming bounds on $K_q(n, r)$. For $q = 4, 5$ we obtain several improved lower bounds on $K_q(n, r)$.

In Chapter 6 we relate our coding bounds to the general theory of matrix cuts for obtaining improved relaxations of 0–1 polytopes. It is shown that the bound for error correcting codes is stronger than the bound obtained from a single iteration of the N_+ operator applied to the modified theta body of the graph on all words in which two words are joined by an edge if they are at distance smaller then d.

Chapter 2

Preliminaries

This thesis is largely self-contained and most results are derived from explicit constructions. However, some theory is desirable for putting them into the right perspective and relating them to the body of mathematics to which they connect. In this chapter we give some definitions and basic facts. After giving some general notation in the first section, we introduce matrix $*$-algebras in the second section, which are an important tool throughout the thesis. The main (classical) theorem says (roughly) that any matrix $*$-algebra is isomorphic to a direct sum of full matrix $*$-algebras. In the third section we describe semidefinite programming. The bounds we derive for codes, are defined as the optimum of certain semidefinite programs and can be computed efficiently. Finally, we recall the basics of association schemes. In particular we describe the Delsarte bound on the maximum size of cliques in association schemes.

2.1 Notation

For positive integers n, m and a set R (usually $R = \mathbb{C}, \mathbb{R}$), we denote by $R^{n\times m}$ the set of n by m matrices with entries in R and by R^n the set of (column) vectors of length n. When R is a ring, we define matrix addition and multiplication of matrices (with compatible dimensions) as usual. Frequently, the rows and columns correspond to the elements of some given finite sets X and Y. When we want to explicitly index the rows and columns of the matrix using these sets, we will write $R^{X\times Y}$ for the set of matrices with rows indexed by X and columns indexed by Y. The i-th row of a matrix A is denoted by A_i and the entry in row i and column j by $A_{i,j}$. The *transpose* of an $X \times Y$ matrix is the $Y \times X$ matrix A^T, where $A^\mathsf{T}_{i,j} = A_{j,i}$ for $i \in Y$, $j \in X$. When $|Y| = 1$, we often identify the matrices in $R^{X\times Y}$ and the vectors in R^X.

For finite sets X, Y, the all-one vector in R^X is denoted by $\mathbf{1}$. The $X \times Y$ all-one matrix is denoted by J, the all-zero matrix by 0 and the $X \times X$ identity matrix by I. The sets X and Y will be clear from the context.

Given a matrix $A \in R^{X\times X}$, we define $\mathrm{diag}(A)$ to be the vector $a \in R^X$ of diagonal elements of A, that is $a_i := A_{i,i}$ for $i \in X$. The *trace* of A is the sum of the diagonal elements of A and is denoted $\mathrm{tr}A$. So $\mathrm{tr}A = \mathbf{1}^\mathsf{T}\mathrm{diag}(A)$. We mention the useful fact that

for matrices $A \in R^{k\times l}$ and $B \in R^{l\times k}$ the following identity holds:

$$\operatorname{tr}(AB) = \operatorname{tr}(BA). \tag{2.1}$$

Given a vector $a \in R^X$, we denote by $\operatorname{Diag}(a)$ the diagonal matrix $A \in R^{X\times X}$ with $\operatorname{diag}(A) = a$.

For a subset $S \subseteq X$ we denote by χ^S the vector in R^X definied by

$$(\chi^S)_i := \begin{cases} 1 & \text{if } i \in S \\ 0 & \text{otherwise.} \end{cases} \tag{2.2}$$

For a vector x and a set S, we define

$$x(S) := \sum_{i\in S} x_i. \tag{2.3}$$

For a matrix $A \in \mathbb{C}^{X\times Y}$, the *conjugate transpose* of A is denoted by A^*. That is $A^*_{i,j} = \overline{A_{j,i}}$ for $i \in X$ and $j \in Y$, where $\overline{z}$ is the complex conjugate of a complex number z. A square matrix A is called *normal* if $A^*A = AA^*$, *hermitian* if $A^* = A$ and *unitary* if $A^*A = AA^* = I$.

For $A, B \in \mathbb{C}^{X\times Y}$, we define

$$\langle A, B\rangle := \operatorname{tr}(AB^*) = \sum_{i\in X, j\in Y} A_{i,j}\overline{B_{i,j}}. \tag{2.4}$$

This is the standard complex *inner product* on $\mathbb{C}^{X\times Y}$. Observe that

$$\langle A, J\rangle = \mathbf{1}^\mathsf{T} A \mathbf{1}. \tag{2.5}$$

For matrices $A \in \mathbb{C}^{X_1\times Y_1}$ and $B \in \mathbb{C}^{X_2\times Y_2}$, we denote by $A \otimes B$ the *tensor product* of A and B defined as the $(X_1 \times X_2) \times (Y_1 \times Y_2)$ matrix given by

$$(A \otimes B)_{(i,i'),(j,j')} := A_{i,j}B_{i',j'}. \tag{2.6}$$

2.2 Matrix $*$-algebras

In this section we consider algebras of matrices. For general background on linear algebra we refer the reader to [22, 27].

A *matrix $*$-algebra* is a nonempty set of matrices $\mathcal{A} \subseteq \mathbb{C}^{n\times n}$ that is closed under addition, scalar multiplication, matrix multiplication and under taking the conjugate transpose. A matrix $*$-algebra is a special case of a finite dimensional C^*-algebra. Trivial examples are the full matrix algebra $\mathbb{C}^{n\times n}$ and the *zero algebra* $\{0\}$.

Most of the matrix $*$-algebras that we will encounter in this thesis are of a special type. They are the set of matrices that commute with a given set of *permutation matrices*. More precisely, we have the following.

Let $G \subseteq S_n$ be a subgroup of the symmetric group on n elements. To every element $\sigma \in G$ we associate the permutation matrix $M_\sigma \in \mathbb{C}^{n\times n}$ given by

$$(M_\sigma)_{i,j} := \begin{cases} 1 & \text{if } \sigma(j) = i, \\ 0 & \text{otherwise.} \end{cases} \tag{2.7}$$

Observe that

$$M_\sigma^* = M_\sigma^{\mathsf{T}} = M_{\sigma^{-1}}. \tag{2.8}$$

The map $\sigma \mapsto M_\sigma$ defines a *representation* of G. This means that for all $\sigma, \tau \in G$ we have

$$M_{\tau\sigma} = M_\tau M_\sigma \quad \text{and} \quad M_{\sigma^{-1}} = M_\sigma^{-1}. \tag{2.9}$$

Here $\tau\sigma$ denotes the permutation $(\tau\sigma)(i) := \tau(\sigma(i))$. We define the *centralizer algebra* (see [2]) of G to be the set $\mathcal{A}$ of matrices that are invariant under permuting the rows and columns by elements of G. That is,

$$\mathcal{A} := \{A \in \mathbb{C}^{n\times n} \mid M_\sigma^{-1} A M_\sigma = A \quad \text{for all } \sigma \in G\}. \tag{2.10}$$

If we denote by $\mathcal{B}$ the matrix $*$-algebra spanned by the set of permutation matrices $\{M_\sigma,\ \sigma \in G\}$, then $\mathcal{A}$ is also called the *commutant algebra* of $\mathcal{B}$: the algebra of matrices that commute with all the elements of $\mathcal{B}$. To see that the set $\mathcal{A}$ is indeed a matrix $*$-algebra, we first observe that it is closed under addition and scalar multiplication. That $\mathcal{A}$ is closed under matrix multiplication and taking the conjugate transpose follows from

$$\begin{aligned} M_\sigma^{-1} AB M_\sigma &= M_\sigma^{-1} A M_\sigma M_\sigma^{-1} B M_\sigma = AB, \\ M_\sigma^{-1} A^* M_\sigma &= (M_\sigma^{-1} A M_\sigma)^* = A^* \end{aligned} \tag{2.11}$$

for any $A, B \in \mathcal{A}$.

One of the special features of $\mathcal{A}$ is that it contains the identity and is spanned by a set of zero-one matrices whose supports partition $\{1,\ldots,n\} \times \{1,\ldots,n\}$ (that is, it is the algebra belonging to a *coherent configuration*, see [12]). These matrices have a combinatorial interpretation. Indeed, from (2.10) it follows that

$$A \in \mathcal{A} \text{ if and only if } A_{i,j} = A_{\sigma(i),\sigma(j)} \text{ for all } i, j \in X. \tag{2.12}$$

Hence $\mathcal{A}$ is spanned by zero-one matrices $A_1, \ldots, A_t$, where the supports of the A_i are the orbits of $\{1,\ldots,n\} \times \{1,\ldots,n\}$ under the action of G, called the *orbitals* of G.

The following structure theorem is one of the main motivations for this thesis. It allows to give a matrix $*$-algebra a simple appearance by performing a unitary transformation (a block diagonalisation). We will not use this theorem, but rather give explicit block diagonalisations for the matrix $*$-algebras under consideration.

Theorem 1. *Let $\mathcal{A} \subseteq \mathbb{C}^{n\times n}$ be a matrix $*$-algebra containing the identity matrix I. Then there exists a unitary $n \times n$ matrix U and positive integers $p_1, \ldots, p_m$ and $q_1, \ldots, q_m$ such that $U^*\mathcal{A}U$ consists of* all *block diagonal matrices*

$$\begin{pmatrix} C_1 & 0 & \cdots & 0 \\ 0 & C_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & C_m \end{pmatrix} \tag{2.13}$$

where each C_k is a block diagonal matrix

$$\begin{pmatrix} B_k & 0 & \cdots & 0 \\ 0 & B_k & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & B_k \end{pmatrix} \tag{2.14}$$

with q_k identical blocks $B_k \in \mathbb{C}^{p_k \times p_k}$ on the diagonal.

Observe that the numbers $p_1, \ldots, p_m$ and $q_1, \ldots, q_m$ satisfy

$$\begin{aligned} q_1 p_1 + q_2 p_2 + \cdots + q_m p_m &= n, \\ p_1^2 + p_2^2 + \cdots + p_m^2 &= \dim \mathcal{A}. \end{aligned} \tag{2.15}$$

We call the algebra $U^* \mathcal{A} U$ a *block diagonalisation* of $\mathcal{A}$. This theorem was proved in [3] by using (a special case of) the Wedderburn-Artin theorem (see also [43], [35]). However, we will present a self-contained proof here.

A well-known instance is when $\mathcal{A} \subseteq \mathbb{C}^{n \times n}$ is commutative. This occurs for example when $\mathcal{A}$ is the Bose–Mesner algebra of an association scheme. In the commutative case we must have $p_1 = \ldots = p_m = 1$, since for any $p \geq 2$ the algebra $\mathbb{C}^{p \times p}$ is non-commutative. The theorem then says that the matrices in $\mathcal{A}$ can be simultaneously diagonalised:

$$U^* \mathcal{A} U = \{x_1 I_1 + x_2 I_2 + \cdots + x_m I_m \mid x \in \mathbb{C}^m\}, \tag{2.16}$$

where for each k the matrix $I_k \in \mathbb{C}^n$ is a zero-one diagonal matrix with q_k ones, and $I_1 + \cdots + I_m = I$. The rest of this section is devoted to proving Theorem 1.

We first introduce some more notation. For two square matrices $A \in \mathbb{C}^{n \times n}$ and $B \in \mathbb{C}^{m \times m}$, we define their *direct sum* $A \oplus B \in \mathbb{C}^{(n+m) \times (n+m)}$ by

$$A \oplus B := \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}. \tag{2.17}$$

For two matrix $*$-algebras $\mathcal{A}$ and $\mathcal{B}$, we define their direct sum by

$$\mathcal{A} \oplus \mathcal{B} := \{A \oplus B \mid A \in \mathcal{A}, B \in \mathcal{B}\}. \tag{2.18}$$

This is again a matrix $*$-algebra. For a positive integer t, we define

$$t \odot \mathcal{A} := \{t \odot A \mid A \in \mathcal{A}\}, \tag{2.19}$$

where $t \odot A$ denotes the iterated direct sum $\oplus_{i=1}^{t} A$.

We call two square matrices $A, B \in \mathbb{C}^{n \times n}$ *equivalent* if there exists a unitary matrix U such that $B = U^* A U$. We extend this to matrix $*$-algebras and call two matrix $*$-algebras $\mathcal{A}$ and $\mathcal{B}$ equivalent if $\mathcal{B} = U^* \mathcal{A} U$ for some unitary matrix U.

Theorem 1 can thus be expressed by saying that every matrix $*$-algebra $\mathcal{A}$ containing the identity matrix is equivalent to a matrix $*$-algebra of the form

$$\bigoplus_{i=1}^{m} (q_i \odot \mathbb{C}^{p_i \times p_i}). \tag{2.20}$$

We start by considering the commutative case. We first introduce some more notions. Let $\mathcal{A} \subseteq \mathbb{C}^{n\times n}$ and let $V \subseteq \mathbb{C}^n$ be a linear subspace. We say that V is $\mathcal{A}$-*invariant* when $Av \in V$ for every $A \in \mathcal{A}$ and every $v \in V$. Observe that if $\mathcal{A}$ is closed under taking the conjugate transpose, also the orthoplement

$$V^\perp := \{v \in \mathbb{C}^n \mid \langle v, u\rangle = 0 \text{ for all } u \in V\} \tag{2.21}$$

is $\mathcal{A}$-invariant. Indeed, for every $u \in V$, $v \in V^\perp$ and $A \in \mathcal{A}$ we have

$$\langle Av, u\rangle = \langle v, A^*u\rangle = 0, \tag{2.22}$$

since $A^*u \in V$.

A nonzero vector $v \in \mathbb{C}^n$ is called a *common eigenvector* for $\mathcal{A}$ when $\mathbb{C}v$ is $\mathcal{A}$-invariant. We recall the following basic fact from linear algebra.

Fact. *Let V be a complex linear space of finite, nonzero dimension, and let $A : V \longrightarrow V$ be a linear map. Then there exist $\lambda \in \mathbb{C}$ and $v \in V \setminus \{0\}$ such that $Av = \lambda v$.*

In particular, this implies that when $A \in \mathbb{C}^{n\times n}$ and $V \subseteq \mathbb{C}^n$ is $\{A\}$-invariant, there exists an eigenvector of A that belongs to V. We are now ready to prove the following theorem.

Theorem 2. *Let $\mathcal{A} \subseteq \mathbb{C}^{n\times n}$ be a* commutative *matrix $*$-algebra and let $V \subseteq \mathbb{C}^n$ be an $\mathcal{A}$-invariant subspace. Then V has an orthonormal basis of common eigenvectors for $\mathcal{A}$.*

Proof. The proof is by induction on $\dim V$. If all vectors in V are common eigenvectors for $\mathcal{A}$, then we are done since we can take any orthonormal basis of V. Therefore we may assume that there exists an $A \in \mathcal{A}$ such that not every $v \in V$ is an eigenvector for A. Since V is $\{A\}$-invariant, A has some eigenvector $v \in V$ of eigenvalue $\lambda \in \mathbb{C}$. Denote by

$$E_\lambda := \{x \in \mathbb{C}^n \mid Ax = \lambda x\} \tag{2.23}$$

the eigenspace of A for eigenvalue λ. As $\mathcal{A}$ is commutative, the space E_λ is $\mathcal{A}$-invariant. This follows since for any $B \in \mathcal{A}$ and any $v \in E_\lambda$ we have

$$A(Bv) = B(Av) = \lambda Bv, \tag{2.24}$$

and hence $Bv \in E_\lambda$. It follows that also $V' := V \cap E_\lambda$ and $V'' := V \cap E_\lambda^\perp$ are $\mathcal{A}$-invariant. By assumption on A, V'' has positive dimension, yielding a nontrivial orthogonal decomposition $V = V' \oplus V''$. By induction both V' and V'' have an orthonormal basis of common eigenvectors of $\mathcal{A}$. The union of these two bases gives an orthonormal basis of V consisting of common eigenvectors of $\mathcal{A}$. □

Let us consider the special case $V := \mathbb{C}^n$. Let $\{U_1, \ldots, U_n\}$ be an orthonormal basis of common eigenvectors for $\mathcal{A}$ and denote by U the square matrix with these vectors as columns (in some order). Then U is a unitary matrix that diagonalises $\mathcal{A}$. That is, all matrices in $U^*\mathcal{A}U$ are diagonal matrices.

Proposition 1. *Let $\mathcal{A} \subseteq \mathbb{C}^{n\times n}$ be an algebra consisting of diagonal matrices. Then there exist zero-one diagonal matrices $I_1, \ldots I_m$ with disjoint support such that*

$$\mathcal{A} = \mathbb{C}I_1 + \cdots + \mathbb{C}I_m. \tag{2.25}$$

Proof. Let $S := \{i \in \{1, \ldots, n\} \mid A_{i,i} \neq 0 \text{ for some } A \in \mathcal{A}\}$ be the union of the supports on the diagonal, of the matrices in $\mathcal{A}$. Define an equivalence relation on S by calling i and j equivalent when $A_{i,i} = A_{j,j}$ for every $A \in \mathcal{A}$, and let $S_1, \ldots, S_m$ be the equivalence classes. Denote for $k = 1, \ldots, m$ by $I_k := \mathrm{Diag}(\chi^{S_k})$ the zero-one diagonal matrix with support S_k. The inclusion

$$\mathcal{A} \subseteq \mathbb{C}I_1 + \cdots + \mathbb{C}I_m \tag{2.26}$$

is clear.

To finish the proof, we show that $I_1, \ldots, I_m \in \mathcal{A}$. It is not hard to see that there is a matrix $A \in \mathcal{A}$ with

$$A = c_1 I_1 + c_2 I_2 + \cdots + c_m I_m, \tag{2.27}$$

for pairwise different nonzero numbers $c_1, \ldots, c_m$. It then follows that for $k = 1, \ldots, m$ we have

$$I_k = \frac{A \prod_{i\neq k}(A - c_i I)}{c_k \prod_{i\neq k}(c_k - c_i)}. \tag{2.28}$$

Since the right-hand side is a polynomial in A with constant term equal to zero, we obtain $I_k \in \mathcal{A}$. □

When $\mathcal{A}$ is a commutative matrix $*$-algebra containing the identity, and U is a unitary matrix diagonalising the algebra, say $U^*\mathcal{A}U = \mathbb{C}I_1 + \cdots + \mathbb{C}I_m$, then the matrices

$$E_k := U I_k U^* \in \mathcal{A} \tag{2.29}$$

form a basis of *orthogonal idempotents* of $\mathcal{A}$. They satisfy

$$\begin{aligned} E_1 + \cdots + E_m &= I, \\ E_i E_j &= \delta_{i,j}, \\ E_i &= E_i^*, \end{aligned} \tag{2.30}$$

for $i, j \in \{1, \ldots, m\}$. Geometrically, we have an orthogonal decomposition

$$\mathbb{C}^n = V_1 \oplus \cdots \oplus V_m \tag{2.31}$$

and E_k is the orthogonal projection of $\mathbb{C}^n$ onto V_k.

We will now consider the case that the matrix $*$-algebra $\mathcal{A}$ is not necessarily commutative. We first introduce some terminology. Let $\mathcal{A} \subseteq \mathbb{C}^{n\times n}$ be a matrix $*$-algebra. An element $E \in \mathcal{A}$ is called a *unit* of $\mathcal{A}$ when $EA = AE = A$ for every $A \in \mathcal{A}$. Every matrix $*$-algebra has a unit, see Proposition 3 below. A *sub $*$-algebra* of $\mathcal{A}$ is a subset of $\mathcal{A}$ that is a matrix $*$-algebra. An important example is

$$C_{\mathcal{A}} := \{A \in \mathcal{A} \mid AB = BA \text{ for all } B \in \mathcal{A}\}. \tag{2.32}$$

An *ideal* of $\mathcal{A}$ is a sub $*$-algebra that is closed under both left and right multiplication by elements of $\mathcal{A}$. We observe that if $\mathcal{I}$ is an ideal of $\mathcal{A}$ and E is the unit of $\mathcal{I}$, then $E \in C_{\mathcal{A}}$. This follows since for any $A \in \mathcal{A}$ both EA and AE belong to $\mathcal{I}$ and hence $EA = EAE = AE$.

We say that a commutative sub $*$-algebra of $\mathcal{A}$ is *maximal* if it is not strictly contained in a commutative sub $*$-algebra of $\mathcal{A}$. We have the following useful property.

Proposition 2. *Let $\mathcal{B}$ be a maximal commutative sub $*$-algebra of the matrix $*$-algebra $\mathcal{A}$ and let*

$$\mathcal{B}' := \{A \in \mathcal{A} \mid AB = BA \text{ for all } B \in \mathcal{B}\}. \tag{2.33}$$

Then $\mathcal{B}' = \mathcal{B}$.

Proof. Clearly $\mathcal{B} \subseteq \mathcal{B}'$. We show the converse inclusion. First observe that for any $A \in \mathcal{B}'$ also $A^* \in \mathcal{B}'$. This follows since for any $B \in \mathcal{B}$ we have

$$A^*B = (B^*A)^* = (AB^*)^* = BA^*. \tag{2.34}$$

Next, we show that $\mathcal{B}$ contains every $A \in \mathcal{B}'$ that is normal (that is $AA^* = AA^*$). This follows since for any normal $A \in \mathcal{B}' \setminus \mathcal{B}$ the commutative matrix $*$-algebra generated by A, A^* and $\mathcal{B}$, strictly contains $\mathcal{B}$.

Finally, let $A \in \mathcal{B}'$ be arbitrary. The matrix $A + A^*$ is normal, and hence belongs to $\mathcal{B}$. It follows that $A(A + A^*) = (A + A^*)A$, or $AA^* = A^*A$, and hence A itself is normal and therefore belongs to $\mathcal{B}$. □

When a matrix $*$-algebra does not contain the identity, the following proposition is useful.

Proposition 3. *Every nonzero matrix $*$-algebra $\mathcal{A}$ is equivalent to a direct sum of a matrix $*$-algebra containing the identity and (possibly) a zero algebra. In particular, $\mathcal{A}$ has a unit.*

Proof. Let $\mathcal{B}$ be a maximal commutative sub $*$-algebra of $\mathcal{A}$. By diagonalising $\mathcal{B}$ we may assume that

$$\mathcal{B} = \mathbb{C}I_1 + \cdots + \mathbb{C}I_m \tag{2.35}$$

for diagonal zero-one matrices $I_0, I_1, \ldots, I_m$ with $I = I_0 + I_1 + \cdots + I_m$. If $I_0 = 0$, we are done. So we may assume that $I_0 \neq 0$. To prove the proposition, it suffices to show that

$$I_0\mathcal{A} = \mathcal{A}I_0 = \{0\}, \tag{2.36}$$

since this implies that $\mathcal{A}$ is the direct sum of the algebra obtained by restricting $\mathcal{A}$ to the support of $I_1 + \cdots + I_m$ and the zero algebra on the support of I_0.

First observe that

$$I_0A = A - (I_1 + \cdots + I_m)A \in \mathcal{A} \text{ for every } A \in \mathcal{A}. \tag{2.37}$$

Let $A \in \mathcal{A}$ be arbitrary and let

$$A' := (I_0A)(I_0A)^* \in \mathcal{A}. \tag{2.38}$$

Then for $k = 1, \ldots, m$ we have

$$I_k A' = I_k I_0 A A^* I_0 = 0 = I_0 A A^* I_0 I_k = A' I_k. \tag{2.39}$$

It follows that A' commutes with $I_1, \ldots, I_m$ and hence is a linear combination of $I_1, \ldots, I_m$ by the maximality of $\mathcal{B}$. On the other hand $A' I_k = 0$ for $k = 1, \ldots, m$, and hence $A' = 0$. It follows that also $I_0 A = 0$.

Similarly, by considering A^* we obtain $I_0 A^* = 0$ and hence $A I_0 = 0$. □

We call a nonzero matrix $*$-algebra $\mathcal{A}$ *simple* if $C_{\mathcal{A}} = \mathbb{C}E$, where E is the unit of $\mathcal{A}$. Since the unit of any ideal of $\mathcal{A}$ belongs to $C_{\mathcal{A}}$, it follows that if $\mathcal{A}$ is simple, it has only the two trivial ideals $\{0\}$ and $\mathcal{A}$. The reverse implication also holds (see Proposition 4).

Proposition 4. *Every matrix $*$-algebra $\mathcal{A}$ containing the identity is equivalent to a direct sum of simple matrix $*$-algebras.*

Proof. Since $C_{\mathcal{A}}$ is commutative, we may assume it is diagonalised by replacing $\mathcal{A}$ by $U^* \mathcal{A} U$ for a unitary matrix U diagonalising $C_{\mathcal{A}}$. Then

$$C_{\mathcal{A}} = \mathbb{C}I_1 + \cdots + \mathbb{C}I_m \tag{2.40}$$

where $I_1, \ldots, I_m$ are zero-one diagonal matrices with $I_1 + \cdots + I_m = I$. For every $i, j \in \{1, \ldots, m\}$ with $i \neq j$ we have

$$I_i \mathcal{A} I_j = I_i I_j \mathcal{A} = \{0\}. \tag{2.41}$$

It follows that $\mathcal{A}$ is the direct sum

$$\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_m, \tag{2.42}$$

where for $i = 1, \ldots, m$ the matrix $*$-algebra $\mathcal{A}_i$ is obtained from $I_i \mathcal{A} I_i$ by restricting to the rows and columns in which I_i has a 1. □

Finally, we show that every simple matrix $*$-algebra can be brought into block diagonal form.

Proposition 5. *Every simple matrix $*$-algebra $\mathcal{A}$ containing the identity is equivalent to a matrix $*$-algebra of the form $t \odot \mathbb{C}^{m \times m}$ for some t, m.*

Proof. Let $\mathcal{A} \subseteq \mathbb{C}^{n \times n}$ be a simple matrix $*$-algebra containing the identity, and let $\mathcal{B}$ be a maximal commutative sub $*$-algebra of $\mathcal{A}$. We may assume that $\mathcal{B}$ consists of diagonal matrices, say

$$\mathcal{B} = \mathbb{C}I_1 + \cdots + \mathbb{C}I_m \tag{2.43}$$

where $I_i = \chi^{S_i}$ for $i = 1, \ldots, m$ and $S_1 \cup \cdots \cup S_m$ is a partition of $\{1, \ldots, n\}$. For every i and every $A \in \mathcal{A}$ the matrix $I_i A I_i$ commutes with $I_1, \ldots, I_m$ and hence, by the maximality of $\mathcal{B}$, the matrix $I_i A I_i$ is a linear combination of $I_1, \ldots, I_m$. It follows that

$$I_i \mathcal{A} I_i = \mathbb{C}I_i \text{ for } i = 1, \ldots, m. \tag{2.44}$$

For any i, the set $\mathcal{I} := \mathcal{A}I_i\mathcal{A}$ is a nonzero ideal of $\mathcal{A}$. Hence the unit of $\mathcal{I}$ belongs to $C_\mathcal{A} = \mathbb{C}I$. It follows that $I \in \mathcal{I}$ and hence

$$I_i\mathcal{A}I_j \neq \{0\} \text{ for every } i,j = 1,\ldots,m. \tag{2.45}$$

For any $A \in \mathbb{C}^{n\times n}$, and $i,j \in \{1,\ldots,m\}$, we denote by $A_{i,j} \in \mathbb{C}^{|S_i|\times|S_j|}$ the matrix obtained from A by restricting the rows to S_i and the columns to S_j (and renumbering the rows and columns). By (2.45) we can fix an $A \in \mathcal{A}$ with $A_{i,j} \neq 0$ for every $i,j \in \{1,\ldots,m\}$. In fact we can arrange that

$$\mathrm{tr}((A_{i,j})^*A_{i,j}) = |S_i|. \tag{2.46}$$

Let i be arbitrary and let $A' := I_1AI_i$. Then

$$\begin{aligned} &A'(A')^* \text{ is a nonzero matrix in } \mathbb{C}I_1, \\ &(A')^*A' \text{ is a nonzero matrix in } \mathbb{C}I_i. \end{aligned} \tag{2.47}$$

This shows that I_1 and I_i have the same rank t, namely the rank of A'. In other words: $|S_1| = |S_i| = t$. Moreover by (2.46), the matrices $A_{1,i}$ are unitary since

$$(A_{1,i})^*A_{1,i} = A_{1,i}(A_{1,i})^* = I. \tag{2.48}$$

Let $U := A_{1,1}^* \oplus \cdots \oplus A_{1,m}^* \in \mathbb{C}^{n\times n}$ be the unitary matrix with blocks $A_{1,i}^*$ on the diagonal. By replacing $\mathcal{A}$ by $U^*\mathcal{A}U$ we may assume that $A_{1,i} = I$ for $i = 1,\ldots,m$.

This implies that for any $i,j \in \{1,\ldots,m\}$

$$B_{i,1} = A_{1,i}B_{i,1} = (I_1AI_iBI_1)_{1,1} \in \mathbb{C}I \text{ for any } B \in \mathcal{A}, \tag{2.49}$$

and hence

$$B_{i,j} = B_{i,j}(A^*)_{j,1} = (I_iBI_jA^*I_1)_{i,1} \in \mathbb{C}I \text{ for any } B \in \mathcal{A}. \tag{2.50}$$

Summarizing, we have

$$\mathcal{A} = \{A \in \mathbb{C}^{n\times n} \mid A_{i,j} \in \mathbb{C}I \text{ for all } i,j \in \{1,\ldots,m\}\}. \tag{2.51}$$

By reordering the rows and columns, we obtain the proposition. □

Proposition 4 and 5 together imply Theorem 1.

2.3 Semidefinite programming

In this section we introduce semidefinite programming. For an overview of semidefinite programming and further references, we refer the reader to [41].

Recall that a complex matrix A is called hermitian if $A^* = A$. It follows that all eigenvalues of A are real. An hermitian matrix $A \in \mathbb{C}^{n\times n}$ is called *positive semidefinite*, in notation $A \succeq 0$, when it has only nonnegative eigenvalues.

Proposition 6. *For an hermitian matrix $A \in \mathbb{C}^{n\times n}$ the following are equivalent:*

$$\begin{aligned} &\text{(i)} && A \succeq 0, \\ &\text{(ii)} && x^*Ax \geq 0 \quad \textit{for all } x \in \mathbb{C}^n, \\ &\text{(iii)} && A = B^*B \quad \textit{for some } B \in \mathbb{C}^{n\times n}. \end{aligned} \tag{2.52}$$

In the case that A is real, we may restrict to real vectors x in (ii) and take B real in (iii).

It follows that for positive semidefinite matrices $A, B \in \mathbb{C}^{n\times n}$ the inner product is nonnegative:

$$\langle A, B\rangle = \operatorname{tr}(C^*CDD^*) = \operatorname{tr}(CDD^*C^*) = \langle CD, CD\rangle \geq 0, \tag{2.53}$$

when $A = C^*C$ and $B = D^*D$. Another useful observation is that when A is positive semidefinite, every principal submatrix is positive semidefinite as well. In particular, the diagonal of A consists of nonnegative real numbers. Also

$$\text{if } U \text{ is nonsingular, then } A \succeq 0 \text{ if and only if } U^*AU \succeq 0. \tag{2.54}$$

In the remainder of this section, all matrices will be real. A *semidefinite program* is a an optimization problem of the following form, where $A_1, \ldots, A_n, B$ are given symmetric matrices in $\mathbb{R}^{n\times n}$ and $c \in \mathbb{R}^n$ is a given vector:

$$\begin{aligned} \text{minimize} \quad & c^{\mathsf{T}}x \\ \text{subject to} \quad & x_1A_1 + \cdots + x_nA_n - B \succeq 0. \end{aligned} \tag{2.55}$$

When $A_1, \ldots, A_n, B$ are diagonal matrices, the program reduces to a linear program. In particular, linear constraints $Ax \leq b$ can be incorporated into the program (2.55) by setting

$$\widetilde{A}_i := \begin{pmatrix} A_i & 0 \\ 0 & -\operatorname{Diag}(a_i) \end{pmatrix} \tag{2.56}$$

and

$$\widetilde{B} := \begin{pmatrix} B & 0 \\ 0 & -\operatorname{Diag}(b) \end{pmatrix}, \tag{2.57}$$

where a_i is the i-th column of A. Semidefinite programs can be approximated in polynomial time within any specified accuracy by the ellipsoid algorithm ([17]) or by practically efficient interior point methods ([34]).

For any symmetric matrix $A \in \mathbb{R}^{n\times n}$, the matrix $R(A)$ is defined by:

$$R(A) := \begin{pmatrix} 1 & a^{\mathsf{T}} \\ a & A \end{pmatrix}, \tag{2.58}$$

where $a := \operatorname{diag}(A)$ is the vector of diagonal elements of A. We will index the extra row and column of $R(A)$ by 0.

The following propositions are helpful when dealing with semidefinite programs that involve matrices of the form $R(A)$.

Proposition 7. *Let $A \in \mathbb{R}^{n\times n}$ be a symmetric matrix such that* $\mathrm{diag}(A) = c \cdot A\mathbf{1}$ *for some $c \in \mathbb{R}$. Then the following are equivalent:*

$$\begin{array}{ll} \text{(i)} & R(A) \text{ is positive semidefinite,} \\ \text{(ii)} & A \text{ is positive semidefinite and } \mathbf{1}^\mathsf{T} A\mathbf{1} \geq (\mathrm{tr}A)^2. \end{array} \tag{2.59}$$

Proof. First assume that (i) holds. Let $R(A) = U^\mathsf{T}U$, where $U \in \mathbb{R}^{(n+1)\times(n+1)}$. Using $U_0^\mathsf{T}U_0 = 1$, we obtain

$$\begin{aligned} \mathbf{1}^\mathsf{T}A\mathbf{1} = \sum_{i,j=1}^{n} U_i^\mathsf{T}U_j &= (\sum_{i=1}^{n} U_i)^\mathsf{T}(\sum_{i=1}^{n} U_i)\cdot U_0^\mathsf{T}U_0 \\ &\geq ((\sum_{i=1}^{n} U_i)^\mathsf{T}U_0)^2 = (\mathrm{tr}A)^2. \end{aligned} \tag{2.60}$$

Here the inequality follows using Cauchy-Schwarz, and in the last equality we use $U_i^\mathsf{T}U_0 = A_{i,i}$. Next assume that (ii) holds. We may assume that $\mathrm{tr}A > 0$, since otherwise $A = 0$ and hence $R(A)$ is positive semidefinite. Let $A = U^\mathsf{T}U$ where $U \in \mathbb{R}^{n\times n}$. Let $a := \mathrm{diag}(A)$. For any $x \in \mathbb{R}^n$ the following holds:

$$\begin{aligned} x^\mathsf{T}Ax &\geq (\mathbf{1}^\mathsf{T}A\mathbf{1})^{-1}(x^\mathsf{T}A\mathbf{1})^2 \\ &\geq \left(\frac{\mathrm{tr}A}{\mathbf{1}^\mathsf{T}A\mathbf{1}}x^\mathsf{T}A\mathbf{1}\right)^2 \\ &= c\frac{\mathbf{1}^\mathsf{T}a}{\mathbf{1}^\mathsf{T}a}c^{-1}x^\mathsf{T}a \\ &= (x^\mathsf{T}a)^2. \end{aligned} \tag{2.61}$$

Here the first inequality follows by applying Cauchy-Schwartz on the inner product of Ux and $U\mathbf{1}$, and the second inequality follows from the assumption $\mathbf{1}^\mathsf{T}A\mathbf{1} \geq (\mathrm{tr}A)^2$. It follows that for any vector $\binom{\alpha}{x}$ with $x \in \mathbb{R}^n$ and $\alpha \in \mathbb{R}$, we have

$$\begin{aligned} (\alpha, x^\mathsf{T})R(A)\begin{pmatrix}\alpha\\ x\end{pmatrix} &= \alpha^2 + 2\alpha a^\mathsf{T}x + x^\mathsf{T}Ax \\ &\geq \alpha^2 + 2\alpha a^\mathsf{T}x + (a^\mathsf{T}x)^2 \\ &= (\alpha + a^\mathsf{T}x)^2 \geq 0. \end{aligned}$$

□

This implies the folowing useful equivalence of semidefinite programs.

Proposition 8. *Let $C \subseteq \mathbb{R}^{n\times n}$ be a cone, and assume that the following two maxima exist:*

$$\begin{aligned} O_1 &:= \max\{\mathbf{1}^\mathsf{T}A\mathbf{1} \mid \mathrm{tr}A = 1, A \succeq 0, A \in C\}, \\ O_2 &:= \max\{\mathrm{tr}A \mid R(A) \succeq 0, A \in C\}. \end{aligned} \tag{2.62}$$

Further assume that the maximum in the first program is attained by a matrix A with $\mathrm{diag}(A) = c \cdot A\mathbf{1}$ *for some $c \in \mathbb{R}$. Then $O_1 = O_2$.*

Proof. Let A be an optimal solution to the first program with $\mathrm{diag}(A) = c \cdot A\mathbf{1}$ for some $c \in \mathbb{R}$, and define $A' := (\mathbf{1}^\mathsf{T} A\mathbf{1})A$. Then

$$\mathbf{1}^\mathsf{T} A'\mathbf{1} = (\mathbf{1}^\mathsf{T} A\mathbf{1})^2 = (\mathrm{tr}A')^2. \tag{2.63}$$

Hence A' is feasible for the second program by Proposition 7. Since $\mathrm{tr}A' = \mathbf{1}^\mathsf{T} A\mathbf{1}$ we obtain $O_2 \geq O_1$.

Let A be an optimal solution to the second program. If $\mathrm{tr}A = 0$ we have $O_1 \geq O_2$ and we are done. Hence we may assume that $\mathrm{tr}A > 0$. Observe that $(\mathrm{tr}A)^2 = \mathbf{1}^\mathsf{T} A\mathbf{1}$, since otherwise we would have $\mathbf{1}^\mathsf{T} A\mathbf{1} = \lambda(\mathrm{tr}A)^2$ for some $\lambda > 1$ by Proposition 7. This would imply that λA is also feasible, contradicting the optimality of A. Define $A' := \frac{1}{\mathrm{tr}A} A$. Then A' is feasible for the first program and

$$\mathbf{1}^\mathsf{T} A'\mathbf{1} = \frac{1}{\mathrm{tr}A} \mathbf{1}^\mathsf{T} A\mathbf{1} = \mathrm{tr}A \tag{2.64}$$

This implies that $O_1 \geq O_2$. □

An important special case is when all feasible matrices have constant diagonal and constant row sum. this occurs for example in semidefinite programs where the feasible matrices belong to the Bose-Mesner algebra of an association scheme. Another case is when the cone C is closed under scaling rows and columns by nonnegative numbers.

Proposition 9. *Let $C \subseteq \mathbb{R}^{n\times n}$ be a cone of symmetric matrices, such that for any nonnegative $x \in \mathbb{R}^n$ and any $A \in C$ also $\mathrm{Diag}(x)A\mathrm{Diag}(x)$ belongs to C. Then any optimal solution A to the program*

$$\max\{\mathbf{1}^\mathsf{T} A\mathbf{1} \mid \mathrm{tr}A = 1, A \succeq 0, A \in C\} \tag{2.65}$$

satisfies $\mathrm{diag}(A) = c \cdot A\mathbf{1}$ for some $c \in \mathbb{R}$.

Proof. Let A be an optimal solution. If $A_{i,i}$=0 for some i, we have $A_i = 0$ and the claim follows by induction on n. Therefore we may assume that $a_i := \sqrt{A_{i,i}} > 0$ for $i = 1, \ldots, n$. The matrix $A' := (\mathrm{Diag}(a))^{-1} A (\mathrm{Diag}(a))^{-1}$ is scaled to have only ones on the diagonal. Now for every nonnegative $x \in \mathbb{R}^n$ with $\|x\| = 1$, the matrix $A(x) := \mathrm{Diag}(x)A'\mathrm{Diag}(x)$ is a feasible solution to (2.65) and has value $x^\mathsf{T} A'x$. By the optimality of A, the vector a maximizes $x^\mathsf{T} A'x$ over all nonnegative vectors x with $\|x\| = 1$. In fact, since $a > 0$, it maximizes $x^\mathsf{T} A'x$ over all x with $\|x\| = 1$. As $\mathbb{R}^n$ has an orthonormal basis of eigenvectors for A', it follows that a is an eigenvector of A' belonging to the maximal eigenvalue λ. This implies that

$$\begin{aligned} A\mathbf{1} = \mathrm{Diag}(a)A'\mathrm{Diag}(a)\mathbf{1} &= \mathrm{Diag}(a)A'a \\ &= \lambda \mathrm{Diag}(a)a \\ &= \lambda(a_1^2, \ldots, a_n^2)^\mathsf{T}. \end{aligned} \tag{2.66}$$

This finishes the proof since

$$\mathrm{diag}(A) = (a_1^2, \ldots, a_n^2)^\mathsf{T}. \tag{2.67}$$

□

2.4 Association schemes

In this section, we give some basic facts and notions related to association schemes, including Delsarte's linear programming approach for bounding the size of cliques in an association scheme. This is by no means a complete introduction to the theory of association schemes. For further reading, we recommend [8, 1, 15] on association schemes and [10] on the related topic of distance regular graphs.

Roughly speaking, an association scheme is a very regular colouring of the edges of a complete graph. The colouring is such, that the number of walks from a vertex a to a vertex b traversing colours in a prescribed order, does not depend on the two vertices a and b, but merely on the colour of the edge ab. The following formal definition is due to Bose and Shimamoto [8]. A *t-class association scheme* $S = (X, \{R_0, R_1, \ldots, R_t\})$ is a finite set X together with $t+1$ relations $R_0, \ldots, R_t$ on X that satisfy the following axioms

(i) $\{R_0, R_1, \ldots, R_t\}$ is a partition of $X \times X$,

(ii) $R_0 = \{(x, x) \mid x \in X\}$,

(iii) $(x, y) \in R_i$ if and only if $(y, x) \in R_i$ for all $x, y \in X, i \in \{0, \ldots, t\}$,

(iv) for any $i, j, k \in \{0, \ldots, t\}$ there is an integer $p^k_{i,j}$ such that $|\{z \in X \mid (x, z) \in R_i, (z, y) \in R_j\}| = p^k_{i,j}$ whenever $(x, y) \in R_k$.

The set X is called the set of *points* of the association scheme and two points $x, y \in X$ are said to be i-related when $(x, y) \in R_i$. An association scheme defined as above, is sometimes called a *symmetric* association scheme since all relations are symmetric by (iii). Some authors prefer to allow for 'non-symmetric association schemes' by replacing condition (iii) by

$$\begin{aligned} &(\text{iii}') && \text{for each } i \in \{0, \ldots, t\} \text{ there is an } i^* \in \{0, \ldots, t\} \text{ such that} \\ &&& (x, y) \in R_i \text{ implies } (y, x) \in R_{i^*} \text{ for all } x, y \in X, \\ &(\text{iii}'') && p^k_{i,j} = p^k_{j,i} \quad \text{for all } i, j, k \in \{0, \ldots, t\}. \end{aligned} \tag{2.68}$$

In this thesis we will only use symmetric association schemes.

The numbers $p^k_{i,j}$ are called the *intersection numbers* of the association scheme. The intersection numbers are not free of relations. We mention some obvious relations:

$$\begin{aligned} p^k_{i,j} &= p^k_{j,i}, \\ p^0_{i,j} &= 0 \text{ when } i \neq j. \end{aligned} \tag{2.69}$$

The numbers $n_i := p^0_{i,i}$ are called the *degrees* of the scheme and give the number of points that are i-related to a given point (each relation R_i induces an n_i-regular graph on X).

To each relation R_i, we associate the $X \times X$ matrix A_i in the obvious way:

$$(A_i)_{x,y} := \begin{cases} 1 & \text{if } (x, y) \in R_i \\ 0 & \text{otherwise.} \end{cases} \tag{2.70}$$

The matrices $A_0, \ldots, A_t$ are called the *adjacency matrices* of the association scheme and allow to study the association scheme using algebraic (spectral) tools. In terms of the adjacency matrices, the axioms in (2.68) become

$$\begin{aligned} &\text{(i)} && A_0 + A_1 + \cdots + A_t = J, \\ &\text{(ii)} && A_0 = I, \\ &\text{(iii)} && A_i = A_i^{\mathsf{T}} \quad \text{for all } i \in \{0, \ldots, t\}, \\ &\text{(iv)} && A_i A_j = \sum_{k=0}^{t} p_{i,j}^k A_k \quad \text{for any } i, j \in \{0, \ldots, t\}. \end{aligned}$$

Let

$$\mathcal{A} := \{ x_0 A_0 + x_1 A_1 + \cdots + x_t A_t \mid x_0, \ldots, x_t \in \mathbb{C} \} \tag{2.71}$$

be the linear space spanned by the adjacency matrices. Axiom (iv) says that $\mathcal{A}$ is closed under matrix multiplication. Since all matrices in $\mathcal{A}$ are symmetric, it follows that $\mathcal{A}$ is a commutative matrix $*$-algebra, which is called the *Bose–Mesner algebra* of the association scheme. Since the adjacency matrices are nonzero and have disjoint support, they are linearly independent. This implies that the dimension of $\mathcal{A}$ equals $t + 1$.

Since the algebra $\mathcal{A}$ is commutative, it has a basis $E_0, E_1, \ldots, E_t$ of matrices satisfying

$$\begin{aligned} &\text{(i)} && E_i E_j = \delta_{i,j} E_i, \\ &\text{(ii)} && E_0 + \ldots + E_t = I, \\ &\text{(iii)} && E_i^* = E_i, \end{aligned} \tag{2.72}$$

for every $i, j \in \{0, \ldots, t\}$. The matrices E_i are called the *minimal idempotents* of the algebra and are uniquely determined by $\mathcal{A}$. Geometrically, this means that there is an orthogonal decomposition

$$\mathbb{C}^X = V_0 \oplus V_1 \oplus \cdots \oplus V_t, \tag{2.73}$$

where E_i is the orthogonal projection onto V_i for $i = 0, \ldots, t$. For each i the dimension

$$m_i := \dim V_i \tag{2.74}$$

equals the rank of E_i. The numbers $m_0, \ldots, m_t$ are called the *multiplicities* of the association scheme.

In general, there is no natural way to order the E_i. However, there is one exception. The matrix $|X|^{-1}J$ is always a minimal idempotent, hence it is customary to take $E_0 := |X|^{-1}J$ (and $V_0 = \mathbb{C}\mathbf{1}$, $m_0 = 1$). Since all matrices in $\mathcal{A}$ are symmetric, the idempotents E_i are real by (2.72)(iii).

Since both $\{E_0, \ldots, E_k\}$ and $\{A_0, \ldots, A_k\}$ are bases for $\mathcal{A}$, we can express every matrix in one base as a linear combination of matrices in the other base. The $(t+1) \times (t+1)$ real matrices P, Q are defined as follows:

$$\begin{aligned} A_j &= \sum_{i=0}^{t} P_{i,j} E_i, \\ |X| \cdot E_j &= \sum_{i=0}^{t} Q_{i,j} A_i, \end{aligned} \tag{2.75}$$

for $j = 0, \ldots, t$. The matrices P and Q are called the *first* and *second eigenmatrix* of the scheme respectively. Indeed, since

$$\sum_{i=0}^{t} c_i E_i \tag{2.76}$$

has eigenvalue c_i with multiplicity m_i (if the c_i are different), the i-th column of P gives the eigenvalues of A_i. Clearly

$$PQ = QP = |X| \cdot I, \tag{2.77}$$

but additionally, the matrices P and Q satisfy the following relation

$$m_j P_{j,i} = n_i Q_{i,j}, \quad \text{for all } i, j \in \{0, \ldots, t\}. \tag{2.78}$$

In matrix form:

$$P^{\mathsf{T}} \mathrm{Diag}(m_0, \ldots, m_t) = \mathrm{Diag}(n_0, \ldots, n_t) Q. \tag{2.79}$$

This is a consequence of the fact that both bases $\{A_0, \ldots, A_t\}$ and $\{E_0, \ldots, E_t\}$ are orthogonal. Indeed, this implies by (2.75) that both the left-hand side and the right-hand side in equation (2.78) are equal to $\langle A_i, E_j \rangle$.

Given a subset $Y \subseteq X$ of the point set, the *distribution vector* of Y is the $(t+1)$-tuple $(a_0, a_1, \ldots, a_t)$ of nonnegative numbers defined by

$$a_i := |Y|^{-1} \cdot |(Y \times Y) \cap R_i|, \quad i = 0, \ldots, t. \tag{2.80}$$

The numbers a_i give the average number of elements in Y that are i-related to a given element in Y. In particular $a_0 = 1$ and $a_0 + \cdots + a_t = |Y|$. Delsarte [15] showed that the distribution vector satisfies the following system of inequalities:

$$\sum_{i=0}^{t} Q_{i,j} a_i \geq 0 \quad \text{for } j = 0, \ldots, t. \tag{2.81}$$

Let $K \subseteq \{1, \ldots, t\}$. A subset $S \subseteq X$ of the point set is called a *K-clique* if any two different elements $x, y \in K$ are i-related for some $i \in K$. The inequalities (2.81) yield an upper bound on the maximum size of a K-clique called the *Delsarte bound*.

Theorem 3. *Let $(X, \{R_0, \ldots, R_t\})$ be an association scheme and let $K \subseteq \{1, \ldots, t\}$. Then the maximum size of a K-clique is upper bounded by*

$$\begin{aligned} \max \{ a_1 + \cdots + a_t \mid \quad & a_0 = 1,\ a_i = 0 \text{ for } i \in \{1, 2, \ldots, t\} \setminus K \\ & a_i \geq 0 \text{ for all } i \in \{1, 2, \ldots, t\} \\ & a_0, \ldots, a_t \text{ satisfy the inequalities (2.81)} \}. \end{aligned} \tag{2.82}$$

The Delsarte bound can be efficiently calculated using linear programming and often gives a remarkably good upper bound.

One source of association schemes are (permutation) groups. Let G be a group acting on a finite set X. Then G has a natural action on $X \times X$ given by $g(x, y) := (gx, gy)$. The orbits

$$\{(gx, gy) \mid g \in G\} \tag{2.83}$$

of $X \times X$ are called *orbitals*. The group G is said to act *generously transitive* when for every pair $(x, y) \in X \times X$ there is a group element $g \in G$ that exchanges x and y, that is $gx = gy$ and $gy = gx$. When G acts generously transitive, the orbitals form the relations of an association scheme.

Indeed, the orbitals partition $X \times X$, for any $x \in X$ the orbital $\{(gx, gx) \mid g \in G\}$ is the identity relation (as G acts transitively on X) and the orbitals are symmetric (since G acts generously transitive). Finally, let R_i, R_j, R_k be orbitals and let for $(x, y) \in R_k$

$$Z_{x,y} := \{z \in X \mid (x, z) \in R_i, (z, y) \in R_j\}. \tag{2.84}$$

We have to show that the cardinality $p_{i,j}^k$ of $Z_{x,y}$ only depends on the relations i, j, k and not on the particular choice of x and y. This follows since

$$Z_{gx,gy} \supseteq \{gz \mid z \in Z_{x,y}\} \tag{2.85}$$

for any $g \in G$. In this case, the Bose–Mesner algebra is the centralizer algebra of G.

Given an association scheme $S = (X, \mathcal{R})$ with adjacency matrices $A_0, A_1, \ldots, A_t \in \mathbb{C}^{X \times X}$, and a point $x \in X$, the *Terwilliger algebra of S with respect to x* is the complex algebra generated by $A_0, \ldots, A_t$ and the diagonal matrices $E'_0, \ldots, E'_t$ defined by

$$(E'_i)_{y,y} := \begin{cases} 1 & \text{if } (x, y) \in R_i \\ 0 & \text{otherwise.} \end{cases} \tag{2.86}$$

Observe that $E'_0 + \cdots + E'_t = I$. These algebras were introduced by Terwilliger in [39] under the name *subconstituent algebra* as a tool for studying association schemes. In this thesis we will use the Terwilliger algebra of the Hamming scheme to obtain bounds for codes, improving the Delsarte bound.

Chapter 3

The Terwilliger algebra of the Hamming scheme

A particular association scheme that plays an important role in the theory of error correcting codes is the Hamming scheme. In this chapter we will consider this scheme together with matrix algebras associated to it. In particular we construct a block diagonalisation of the Terwilliger algebra of the binary and the nonbinary Hamming scheme.

3.1 The Hamming scheme and its Terwilliger algebra

Fix integers $n \geq 1$ and $q \geq 2$, and fix an alphabet $\mathbf{q} = \{0, 1, \ldots, q-1\}$. We will consider the *Hamming space* $\mathbb{E} = \mathbf{q}^n$ consisting of words of length n equipped with the *Hamming distance* given by

$$d(\mathbf{u}, \mathbf{v}) := |\{i \mid \mathbf{u}_i \neq \mathbf{v}_i\}|. \tag{3.1}$$

For a word $\mathbf{u} \in \mathbb{E}$, we denote the *support* of $\mathbf{u}$ by $S(\mathbf{u}) := \{i \mid \mathbf{u}_i \neq 0\}$. Note that $|S(\mathbf{u})| = d(\mathbf{u}, \mathbf{0})$, where $\mathbf{0}$ is the all-zero word. This number is called the *weight* of $\mathbf{u}$.

Denote by $\mathrm{Aut}(q, n)$ the set of permutations of $\mathbb{E}$ that preserve the Hamming distance. It is not hard to see that $\mathrm{Aut}(q, n)$ consists of the permutations of $\mathbb{E}$ obtained by permuting the n coordinates followed by independently permuting the alphabet $\mathbf{q}$ at each of the n coordinates. If we consider the action of $\mathrm{Aut}(q, n)$ on the set $\mathbb{E} \times \mathbb{E}$, the orbits form an association scheme known as the *Hamming scheme* $H(n, q)$, with adjacency matrices $A_0, A_1, \ldots, A_n$ defined by

$$(A_i)_{\mathbf{u},\mathbf{v}} := \begin{cases} 1 & \text{if } d(\mathbf{u}, \mathbf{v}) = i, \\ 0 & \text{otherwise,} \end{cases} \tag{3.2}$$

for $i = 0, 1, \ldots, n$. The adjacency matrices span a commutative algebra over the complex numbers called the Bose–Mesner algebra of the scheme.

We will now consider the action of $\mathrm{Aut}(q, n)$ on ordered triples of words, leading to a noncommutative algebra $\mathcal{A}_{q,n}$ containing the Bose–Mesner algebra. To each ordered

triple $(\mathbf{u},\mathbf{v},\mathbf{w}) \in \mathbb{E}\times\mathbb{E}\times\mathbb{E}$ we associate the four-tuple

$$\begin{aligned} d(\mathbf{u},\mathbf{v},\mathbf{w}) \;:=\; & (i,j,t,p), \text{ where} \\ & i := d(\mathbf{u},\mathbf{v}), \\ & j := d(\mathbf{u},\mathbf{w}), \\ & t := |\{i \mid \mathbf{u}_i \neq \mathbf{v}_i \text{ and } \mathbf{u}_i \neq \mathbf{w}_i\}|, \\ & p := |\{i \mid \mathbf{u}_i \neq \mathbf{v}_i = \mathbf{w}_i\}|. \end{aligned} \tag{3.3}$$

We remark that the case $q = 2$ is special since in that case we always have $p = t$. Note that $d(\mathbf{v},\mathbf{w}) = i + j - t - p$ and $|\{i \mid \mathbf{u}_i \neq \mathbf{v}_i \neq \mathbf{w}_i \neq \mathbf{u}_i\}| = t - p$. The set of four-tuples (i,j,t,p) that occur as $d(\mathbf{u},\mathbf{v},\mathbf{w})$ for some $\mathbf{u},\mathbf{v},\mathbf{w} \in \mathbb{E}$ is given by

$$\mathcal{I}(2,n) := \{(i,j,t,p) \mid 0 \leq p = t \leq i,j \text{ and } i+j \leq n+t\}, \tag{3.4}$$

and

$$\mathcal{I}(q,n) := \{(i,j,t,p) \mid 0 \leq p \leq t \leq i,j \text{ and } i+j \leq n+t\}, \tag{3.5}$$

for $q \geq 3$. The sets $\mathcal{I}(q,n)$ will be used to index various objects defined below.

Proposition 10. *Let $n \geq 1$. We have*

$$|\mathcal{I}(q,n)| \begin{cases} \binom{n+3}{3} & \text{for } q = 2, \\ \\ \binom{n+4}{4} & \text{for } q \geq 3. \end{cases} \tag{3.6}$$

Proof. Substitute $p' := p$, $t' := t - p$, $i' := i - t$ and $j' := j - t$. Then the integer solutions of

$$0 \leq p \leq t \leq i,j, \quad i + j \leq n + t \tag{3.7}$$

are in bijection with the integer solutions of

$$0 \leq p', t', i', j', \quad p' + t' + i' + j' \leq n. \tag{3.8}$$

The proposition now follows since

$$|\{(n_1,n_2,\ldots,n_k) \in \mathbb{Z}_{\geq 0} \mid n_1 + \cdots + n_k = n\}| = \binom{n+k}{k}. \tag{3.9}$$

□

The integers i,j,t,p parametrize the ordered triples of words up to symmetry. We define

$$X_{i,j,t,p} := \{(\mathbf{u},\mathbf{v},\mathbf{w}) \in \mathbb{E}\times\mathbb{E}\times\mathbb{E} \mid d(\mathbf{u},\mathbf{v},\mathbf{w}) = (i,j,t,p)\}, \tag{3.10}$$

for $(i,j,t,p) \in \mathcal{I}(q,n)$. The meaning of the sets $X_{i,j,t,p}$ is given by the following proposition.

Proposition 11. *The sets $X_{i,j,t,p}$, $(i,j,t,p) \in \mathcal{I}(q,n)$ are the orbits of $\mathbb{E}\times\mathbb{E}\times\mathbb{E}$ under the action of $\mathrm{Aut}(q,n)$.*

Proof. Let $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{E}$ and let $(i, j, t, p) = d(\mathbf{u}, \mathbf{v}, \mathbf{w})$. Since the Hamming distances $i, j, i + j - t - p$ and the number $t - p = |\{i \mid \mathbf{u}_i \neq \mathbf{v}_i \neq \mathbf{w}_i \neq \mathbf{u}_i\}|$ are unchanged when permuting the coordinates or permuting the elements of $\mathbf{q}$ at any coordinate, we have $d(\mathbf{u}, \mathbf{v}, \mathbf{w}) = d(\pi\mathbf{u}, \pi\mathbf{v}, \pi\mathbf{w})$ for any $\pi \in \mathrm{Aut}(q, n)$.

Hence it suffices to show that there is an automorphism π such that $(\pi\mathbf{u}, \pi\mathbf{v}, \pi\mathbf{w})$ only depends upon i, j, t and p. By permuting $\mathbf{q}$ at the coordinates in the support of $\mathbf{u}$, we may assume that $\mathbf{u} = \mathbf{0}$. Let $A := \{i \mid \mathbf{v}_i \neq 0, \mathbf{w}_i = 0\}$, $B := \{i \mid \mathbf{v}_i = 0, \mathbf{w}_i \neq 0\}$, $C := \{i \mid \mathbf{v}_i \neq 0, \mathbf{w}_i \neq 0, \mathbf{v}_i \neq \mathbf{w}_i\}$ and $D := \{i \mid \mathbf{v}_i = \mathbf{w}_i \neq 0\}$. Note that $|A| = i - t$, $|B| = j - t$, $|C| = t - p$ and $|D| = p$. By permuting coordinates, we may assume that $A = \{1, 2, \ldots, i-t\}$, $B = \{i-t+1, \ldots, i+j-2t\}$, $C = \{i+j-2t+1, \ldots, i+j-t-p\}$ and $D = \{i+j-t-p+1, \ldots, i+j-t\}$. Now by permuting $\mathbf{q}$ at each of the points in $A \cup B \cup C \cup D$, we can accomplish that $\mathbf{v}_i = 1$ for $i \in A \cup C \cup D$ and $\mathbf{w}_i = 2$ for $i \in B \cup C$ and $\mathbf{w}_i = 1$ for $i \in D$. □

Denote the stabilizer of $\mathbf{0}$ in $\mathrm{Aut}(q, n)$ by $\mathrm{Aut}_{\mathbf{0}}(q, n)$. For $(i, j, t, p) \in \mathcal{I}(q, n)$, let $M_{i,j}^{t,p}$ be the $\mathbb{E} \times \mathbb{E}$ matrix defined by:

$$(M_{i,j}^{t,p})_{\mathbf{u},\mathbf{v}} := \begin{cases} 1 & \text{if } |S(\mathbf{u})| = i,\ |S(\mathbf{v})| = j,\ |S(\mathbf{u}) \cap S(\mathbf{v})| = t, \\ & |\{i \mid \mathbf{v}_i = \mathbf{u}_i \neq 0\}| = p, \\ 0 & \text{otherwise.} \end{cases} \tag{3.11}$$

Let $\mathcal{A}_{q,n}$ be the set of matrices

$$\sum_{(i,j,t,p) \in \mathcal{I}(q,n)} x_{i,j}^{t,p} M_{i,j}^{t,p}, \tag{3.12}$$

where $x_{i,j}^{t,p} \in \mathbb{C}$. In the binary case, we will usually drop the superfluous p from the notation and write $x_{i,j}^{t}$ and $M_{i,j}^{t}$.

From Proposition 11 it follows that $\mathcal{A}_{q,n}$ is the set of matrices that are stable under permutations $\pi \in \mathrm{Aut}_{\mathbf{0}}(q, n)$ of the rows and columns. Hence $\mathcal{A}_{q,n}$ is the centralizer algebra of $\mathrm{Aut}_{\mathbf{0}}(q, n)$. The $M_{i,j}^{t,p}$ constitute a basis for $\mathcal{A}_{q,n}$ and hence

$$\dim \mathcal{A}_{q,n} = \begin{cases} \binom{n+3}{3} & \text{if } q = 2, \\ \\ \binom{n+4}{4} & \text{if } q \geq 3, \end{cases} \tag{3.13}$$

by Proposition 10. Note that the algebra $\mathcal{A}_{q,n}$ contains the Bose–Mesner algebra since

$$A_k = \sum_{\substack{(i,j,t,p) \in \mathcal{I}(q,n) \\ i+j-t-p=k}} M_{i,j}^{t,p}. \tag{3.14}$$

We would like to point out here, that $\mathcal{A}_{q,n}$ coincides with the Terwilliger algebra (see [39]) of the Hamming scheme $H(n, q)$ (with respect to $\mathbf{0}$). Recall that the Terwilliger algebra $\mathcal{T}_{q,n}$ is the complex matrix algebra generated by the adjacency matrices $A_0, A_1, \ldots, A_n$ of the Hamming scheme and the diagonal matrices $E_0', E_1', \ldots, E_n'$ defined by

$$(E_i')_{\mathbf{u},\mathbf{u}} := \begin{cases} 1 & \text{if } |S(\mathbf{u})| = i, \\ 0 & \text{otherwise,} \end{cases} \tag{3.15}$$

for $i = 0, 1, \ldots, n$.

Proposition 12. *The algebras $\mathcal{A}_{q,n}$ and $\mathcal{T}_{q,n}$ coincide.*

Proof. Since $\mathcal{A}_{q,n}$ contains the matrices A_k and the matrices $E'_k = M^{k,k}_{k,k}$ for $k = 0, 1, \ldots, n$, it follows that $\mathcal{T}_{q,n}$ is a subalgebra of $\mathcal{A}_{q,n}$. We show the converse inclusion. In the case $q = 2$ this follows since

$$M^{t,t}_{i,j} = E'_i A_{i+j-2t} E'_j, \tag{3.16}$$

as is readily verified. We concentrate on the case $q \geq 3$. Define the zero-one matrices $B_i, C_i, D_i \in \mathcal{T}_{q,n}$ by

$$\begin{aligned} B_i &:= E'_i A_1 E'_i, \\ C_i &:= E'_i A_1 E'_{i+1}, \\ D_i &:= E'_i A_1 E'_{i-1}. \end{aligned} \tag{3.17}$$

Observe that:

$$\begin{aligned} (B_i)_{\mathbf{u},\mathbf{v}} &= 1 \quad \text{if and only if} \\ &\qquad |S(\mathbf{u})| = i, d(\mathbf{u},\mathbf{v}) = 1, |S(\mathbf{v})| = i, S(\mathbf{u}) = S(\mathbf{v}), \\ (C_i)_{\mathbf{u},\mathbf{v}} &= 1 \quad \text{if and only if} \\ &\qquad |S(\mathbf{u})| = i, d(\mathbf{u},\mathbf{v}) = 1, |S(\mathbf{v})| = i+1, |S(\mathbf{u})\Delta S(\mathbf{v})| = 1, \\ (D_i)_{\mathbf{u},\mathbf{v}} &= 1 \quad \text{if and only if} \\ &\qquad |S(\mathbf{u})| = i, d(\mathbf{u},\mathbf{v}) = 1, |S(\mathbf{v})| = i-1, |S(\mathbf{u})\Delta S(\mathbf{v})| = 1. \end{aligned} \tag{3.18}$$

For given $(i, j, t, p) \in \mathcal{I}(q, n)$, let $A^{t,p}_{i,j} \in \mathcal{T}_{q,n}$ be given by

$$A^{t,p}_{i,j} := (D_i D_{i-1} \cdots D_{t+1})(C_t C_{t+1} \cdots C_{j-1})(B_j)^{t-p}. \tag{3.19}$$

Then for words $\mathbf{u}, \mathbf{v} \in \mathbb{E}$, the entry $(A^{t,p}_{i,j})_{\mathbf{u},\mathbf{v}}$ counts the number of $(i+j-t-p+3)$-tuples

$$\mathbf{u} = \mathbf{d}_i, \mathbf{d}_{i-1}, \ldots, \mathbf{d}_t = \mathbf{c}_t, \mathbf{c}_{t+1}, \ldots, \mathbf{c}_j = \mathbf{b}_0, \ldots, \mathbf{b}_{t-p} = \mathbf{v} \tag{3.20}$$

where any two consecutive words have Hamming distance 1, the $\mathbf{b}_k$ have equal support of cardinality j, and $|S(\mathbf{d}_k)| = k$, $|S(\mathbf{c}_k)| = k$ for all k. Hence for $\mathbf{u}, \mathbf{v} \in \mathbb{E}$ the following holds.

$$\begin{aligned} (A^{t,p}_{i,j})_{\mathbf{u},\mathbf{v}} &= 0 \quad \text{if } d(\mathbf{u},\mathbf{v}) > i+j-t-p \quad \text{or} \\ &\qquad |S(\mathbf{u})\Delta S(\mathbf{v})| > i+j-2t \end{aligned} \tag{3.21}$$

and

$$\begin{aligned} (A^{t,p}_{i,j})_{\mathbf{u},\mathbf{v}} &> 0 \quad \text{if } |S(\mathbf{u})| = i,\ |S(\mathbf{v})| = j, \\ &\qquad d(\mathbf{u},\mathbf{v}) = i+j-t-p \quad \text{and} \\ &\qquad |S(\mathbf{u})\Delta S(\mathbf{v})| = i+j-2t. \end{aligned} \tag{3.22}$$

Equation (3.21) follows from the triangle inequality for d and $d'(\mathbf{x},\mathbf{y}) := |S(\mathbf{x}) \cap S(\mathbf{y})|$. To see (3.22) one may take for $\mathbf{d}_k$ the zero-one word with support $\{i+1-k,\ldots,i\}$, for $\mathbf{c}_k$ the zero-one word with support $\{i+1-t,\ldots,i+k-t\}$ and for $\mathbf{b}_k$ the word with support $\{i+1-t,\ldots,i+j-t\}$ where the first k nonzero entries are 2 and the other nonzero entries are 1.

Now suppose that $\mathcal{A}_{q,n}$ is not contained in $\mathcal{T}_{q,n}$, and let $M_{i,j}^{t,p}$ be a matrix not in $\mathcal{T}_{q,n}$ with t maximal and (secondly) p maximal. If we write

$$A_{i,j}^{t,p} = \sum_{t',p'} x_{i,j}^{t',p'} M_{i,j}^{t',p'}, \tag{3.23}$$

then by (3.21) $x_{i,j}^{t',p'} = 0$ if $t'+p' < t+p$ or $t' < t$ implying that $A_{i,j}^{t,p} - x_{i,j}^{t,p} M_{i,j}^{t,p} \in \mathcal{T}_{q,n}$ by the maximality assumption. Therefore since $x_{i,j}^{t,p} > 0$ by (3.22), also $M_{i,j}^{t,p}$ belongs to $\mathcal{T}_{q,n}$, a contradiction. □

3.2 Block diagonalisation of $\mathcal{A}_n$

A block diagonalisation of $\mathcal{A}_n := \mathcal{A}_{2,n}$ was first given by Schrijver in [38]. In this section we will describe this block diagonalisation. In the next section we will use it to describe a block diagonalisation of $\mathcal{A}_{q,n}$ for general q.

Let n be a fixed positive integer and let $\mathcal{P} = \mathcal{P}_n$ denote the collection of subsets of $\{1,\ldots,n\}$. It will be convenient to identify binary words with their supports (as elements of $\mathcal{P}$). We will use capital letters to denote sets. For convenience, we use the notation

$$C_i := M_{i-1,i}^{i-1}, \tag{3.24}$$

that is

$$(C_i)_{X,Y} = \begin{cases} 1 & \text{if } |X| = i-1, |Y| = i, X \subseteq Y, \\ 0 & \text{otherwise} \end{cases}, \tag{3.25}$$

for $i = 0,\ldots n$. In particular observe that C_0 is the zero matrix. The matrices $C_1,\ldots,C_n$ and their transposes $C_1^{\mathsf{T}},\ldots,C_n^{\mathsf{T}}$ play a prominent role in the block diagonalisation of $\mathcal{A}_n$. They generate the algebra $\mathcal{A}_n$ as can be easily seen from the identities

$$C_{i+1}C_{i+1}^{\mathsf{T}} - C_i^{\mathsf{T}}C_i = (n-2i)E_i' \tag{3.26}$$

and

$$\sum_{i=0}^{n}(C_i + C_i^{\mathsf{T}}) = M_1. \tag{3.27}$$

Indeed, the adjacency matrix M_1 of the Hamming cube generates the Bose–Mesner algebra of the Hamming scheme. Since $I = \sum_{i=1}^{n} E_i'$ is in the Bose–Mesner algebra it follows by (3.26) that also the diagonal matrices $E_1',\ldots,E_n'$ are in the algebra generated by $C_1,\ldots,C_n,C_1^{\mathsf{T}},\ldots,C_n^{\mathsf{T}}$.

For $k = 0,\ldots,\left\lfloor \frac{n}{2} \right\rfloor$, define the linear space L_k to be the intersection of the space of vectors with support contained in the collection of sets of cardinality k, and the kernel of C_k:

$$L_k := \{b \in \mathbb{R}^{\mathcal{P}} \mid C_k b = 0, b_X = 0 \text{ if } |X| \neq k\}. \tag{3.28}$$

Proposition 13. *For each $k \leq \lfloor \frac{n}{2} \rfloor$ the dimension of L_k is given by*

$$\dim L_k = \binom{n}{k} - \binom{n}{k-1}. \tag{3.29}$$

Proof. It suffices to prove that C_k has rank $\binom{n}{k-1}$. This follows since for any nonzero $x \in \mathbb{R}^{\mathcal{P}}$ with $x_I = 0$ when $|I| \neq k-1$, we have $C_k x \neq 0$. Indeed

$$x^{\mathsf{T}} C_k C_k^{\mathsf{T}} x = x^{\mathsf{T}} C_{k-1}^{\mathsf{T}} C_{k-1} x + (n-2k+2) x^{\mathsf{T}} x > 0 \tag{3.30}$$

by (3.26). □

Before giving an explicit block diagonalisation, we will first sketch the basic idea. Let $b \in L_k$ be nonzero and consider the vectors $b_k, b_{k+1}, b_{k+2}, \ldots$, where $b_k := b$ and

$$b_{i+1} := C_{i+1}^{\mathsf{T}} \cdots C_{k+2}^{\mathsf{T}} C_{k+1}^{\mathsf{T}} b \tag{3.31}$$

for $i \geq k$. It can be shown (see Proposition 15 below) that

$$\|b_i\| = \|b\| \cdot \binom{n-2k}{i-k}^{\frac{1}{2}} (i-k)!. \tag{3.32}$$

It follows that b_i is zero for $i > n-k$ and nonzero for $i = k, \ldots, n-k$. Since the b_i have disjoint support, $b_k, \ldots, b_{n-k}$ are an orthogonal basis for the linear space V_b they span. From (3.26) it follows that

$$C_{i+1} b_{i+1} = C_{i+1} C_{i+1}^{\mathsf{T}} b_i = (n-2i) b_i + C_i^{\mathsf{T}} (C_i b_i) \tag{3.33}$$

and hence, since $C_k b_k = 0$, that

$$C_{i+i} b_{i+1} = b_i \cdot \sum_{s=k}^{i} (n-2s). \tag{3.34}$$

The space V_b is thus mapped to itself by each of the C_i and C_i^{T} and hence by every $M \in \mathcal{A}_n$. The action of $\mathcal{A}_n$ restricted to V_b is determined by

$$\begin{aligned} C_{i+1}(\sum_{j=k}^{n-k} x_j b_j) &= x_{i+1}(\sum_{s=k}^{i} (n-2s)) b_i \\ C_{i+1}^{\mathsf{T}}(\sum_{j=k}^{n-k} x_j b_j) &= x_i b_{i+1} \end{aligned} \tag{3.35}$$

and does not depend on the particular choice of $b \in L_k$, but only on k. If we take for each k an orthonormal basis of L_k and let b range over the union of these bases, we will obtain a decomposition of $\mathbb{R}^{\mathcal{P}}$ as a direct sum of orthogonal subspaces V_b. This yields a block diagonalisation of $\mathcal{A}_n$, where for each k there is a block of multiplicity $\dim L_k$. In order to obtain a formula for the image of $M_{i,j}^t$ in each of the blocks, we need to express $M_{i,j}^t$ (as a polynomial) in the matrices C_l and C_l^{T}.

We will now give a detailed proof, see also [38]. We begin by giving a convenient way to express the matrices $M^t_{i,j}$ in terms of $C_1, \ldots, C_n, C_1^\mathsf{T}, \ldots, C_n^\mathsf{T}$. A first observation is that

$$(k-i)M^i_{i,k} = M^i_{i,k-1}C_k \quad \text{for all } i < k. \tag{3.36}$$

An important consequence is that

$$M^i_{i,k}b = 0 \quad \text{for all } i < k \text{ and } b \in L_k. \tag{3.37}$$

Secondly, we have the following identity.

Proposition 14. *For all $l, k, p \in \{0, \ldots, n\}$:*

$$M^p_{l,k} = \sum_{s=0}^{n} (-1)^{s-p} \binom{s}{p} M^s_{l,s} M^s_{s,k}. \tag{3.38}$$

Proof. The entry of

$$\sum_{s=0}^{n} (-1)^{s-p} \binom{s}{p} M^s_{l,s} M^s_{s,k} \tag{3.39}$$

in position (X, Y), with $|X| = k$, $|Y| = l$ and $|X \cap Y| = t$, equals

$$\begin{aligned} \sum_{s=0}^{n} (-1)^{s-p} \binom{s}{p} \binom{t}{s} &= \sum_{s=p}^{t} (-1)^{s-p} \binom{t}{p} \binom{t-p}{s-p} \\ &= \binom{t}{p} \sum_{s'=0}^{t-p} (-1)^{s'} \binom{t-p}{s'}. \end{aligned} \tag{3.40}$$

This last sum equals zero if $t \neq p$ and equals 1 if $t = p$. □

The following proposition gives the inner products between vectors of the form $M^k_{j,k}b$, where $b \in L_k$. These will be used to construct an orthonormal basis with respect to which the algebra is in block diagonal form.

Proposition 15. *For $i, j, k, l \in \{0, \ldots, n\}$ with $k, l \leq \lfloor \frac{n}{2} \rfloor$, and for $c \in L_l, b \in L_k$:*

$$c^\mathsf{T} M^l_{l,i} M^k_{j,k} b = \begin{cases} \binom{n-2k}{i-k} c^\mathsf{T} b & \text{if } l = k, i = j \\ 0 & \text{otherwise.} \end{cases} \tag{3.41}$$

Proof. Clearly $M^l_{l,i} M^k_{j,k} = 0$ if $i \neq j$, hence we may assume $i = j$ in the remainder of the proof. By (3.38) we have for $0 \leq p \leq k, l$:

$$c^\mathsf{T} M^p_{l,k} b = \begin{cases} (-1)^{k-p} \binom{k}{p} c^\mathsf{T} b & \text{if } k = l \\ 0 & \text{otherwise,} \end{cases} \tag{3.42}$$

since $c^{\mathsf{T}} M^s_{l,s} = 0$ for $s \neq l$ and $M^s_{s,k} b = 0$ for $s \neq k$. Hence we obtain

$$\begin{aligned} c^{\mathsf{T}} M^l_{l,i} M^k_{i,k} b &= \sum_{p=0}^{n} \binom{n+p-l-k}{n-i} c^{\mathsf{T}} M^p_{l,k} b \\ &= \delta_{k,l} \cdot \sum_{p=0}^{k} \binom{n+p-2k}{n-i} (-1)^{k-p} \binom{k}{p} c^{\mathsf{T}} b \\ &= \delta_{k,l} \cdot \binom{n-2k}{i-k} c^{\mathsf{T}} b. \end{aligned} \tag{3.43}$$

□

Define for $i, j, k, t \in \{0, \ldots, n\}$ the number

$$\beta^t_{i,j,k} := \binom{n-2k}{i-k} \sum_{p=0}^{n} (-1)^{k-p} \binom{k}{p} \binom{i-p}{t-p} \binom{n+p-i-k}{n+t-i-j}. \tag{3.44}$$

These numbers will be used to describe the block diagonalisation.

Proposition 16. *For $i, j, k, t \in \{0, \ldots, n\}$ with $k \leq \lfloor \frac{n}{2} \rfloor$, and for $b \in L_k$:*

$$\binom{n-2k}{i-k} M^t_{i,j} M^k_{j,k} b = \beta^t_{i,j,k} M^k_{i,k} b. \tag{3.45}$$

Proof. By (3.38), it follows that for $0 \leq p \leq n$:

$$M^p_{i,k} b = (-1)^{k-p} \binom{k}{p} M^k_{i,k} b. \tag{3.46}$$

This implies that

$$\begin{aligned} M^t_{i,j} M^k_{j,k} b &= \sum_{p=0}^{n} \binom{i-p}{t-p} \binom{n+p-i-k}{n+t-i-j} M^p_{i,k} b \\ &= \sum_{p=0}^{n} \binom{i-p}{t-p} \binom{n+p-i-k}{n+t-i-j} (-1)^{k-p} \binom{k}{p} M^k_{i,k} b. \end{aligned} \tag{3.47}$$

This proves the proposition. □

We will now describe the block diagonalisation. For each $k = 0, \ldots, \lfloor \frac{n}{2} \rfloor$, choose an orthonormal basis B_k of the linear space L_k. By Proposition 13 we know that $|B_k| = \binom{n}{k} - \binom{n}{k-1}$. Let

$$\mathcal{V} := \{(k, b, i) \mid k \in \{0, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\}, b \in B_k, i \in \{k, k+1, \ldots, n-k\}\}. \tag{3.48}$$

Then

$$\begin{aligned} |\mathcal{V}| &= \sum_{i=0}^{n} \sum_{k=0}^{\min\{i,n-i\}} \left(\binom{n}{k} - \binom{n}{k-1} \right) \\ &= \sum_{i=0}^{n} \binom{n}{\min\{i, n-i\}} = \sum_{i=0}^{n} \binom{n}{i} = 2^n. \end{aligned} \tag{3.49}$$

Define for each $(k, b, i) \in \mathcal{V}$ the vector $u_{k,b,i} \in \mathbb{R}^{\mathcal{P}}$ by

$$u_{k,b,i} := \binom{n-2k}{i-k}^{-\frac{1}{2}} M_{i,k}^{k} b. \tag{3.50}$$

If follows from Proposition 15 and $|\mathcal{V}| = 2^n$ that the vectors $u_{k,b,i}$ form an orthonormal base of $\mathbb{R}^{\mathcal{P}}$. Let U be the $\mathcal{P} \times \mathcal{V}$ matrix with $u_{k,b,i}$ as the (k, b, i)-th column. We will show that for each triple i, j, t the matrix

$$\widetilde{M}_{i,j}^{t} := U^{\mathsf{T}} M_{i,j}^{t} U \tag{3.51}$$

is in block diagonal form. Indeed we have

Proposition 17. *For $(l, c, i'), (k, b, j') \in \mathcal{V}$ and $i, j, t \in \{0, \ldots, n\}$:*

$$(\widetilde{M}_{i,j}^{t})_{(l,c,i'),(k,b,j')} = \begin{cases} \binom{n-2k}{i-k}^{-\frac{1}{2}} \binom{n-2k}{j-k}^{-\frac{1}{2}} \beta_{i,j,k}^{t} & \text{if } l = k, i = i', j = j', b = c, \\ 0 & \text{otherwise.} \end{cases} \tag{3.52}$$

Proof. We have

$$\begin{aligned} M_{i,j}^{t} u_{k,b,j'} &= \binom{n-2k}{j'-k}^{-\frac{1}{2}} M_{i,j}^{t} M_{j',k}^{k} b \\ &= \delta_{j,j'} \binom{n-2k}{j-k}^{-\frac{1}{2}} \binom{n-2k}{i-k}^{-1} \beta_{i,j,k}^{t} M_{i,k}^{k} b \\ &= \delta_{j,j'} \binom{n-2k}{j-k}^{-\frac{1}{2}} \binom{n-2k}{i-k}^{-\frac{1}{2}} \beta_{i,j,k}^{t} u_{k,b,i}. \end{aligned} \tag{3.53}$$

Since

$$(\widetilde{M}_{i,j}^{t})_{(l,c,i'),(k,b,j')} = u_{l,c,i'}^{\mathsf{T}} M_{i,j}^{t} u_{k,b,j'} \tag{3.54}$$

the proposition follows. □

Proposition 18. *The matrix U gives a block diagonalisation of $\mathcal{A}_n$.*

Proof. Proposition 17 implies that each matrix $\widetilde{M}_{i,j}^{t}$ has a block diagonal form, where for each $k = 0, \ldots \lfloor \frac{n}{2} \rfloor$ there are $\binom{n}{k} - \binom{n}{k-1}$ copies of an $(n+1-2k) \times (n+1-2k)$ block on the diagonal. For each k the copies are indexed by the elements of B_k, and in each copy the rows and columns are indexed by the integers $i \in \{k, k+1, \ldots, n-k\}$. Hence we

need to show that all matrices of this block diagonal form belong to $U^{\mathsf{T}}\mathcal{A}_n U$. It suffices to show that the dimension $\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor}(n+1-2k)^2$ of the algebra consisting of the matrices in the given block diagonal form equals the dimension of $\mathcal{A}_n$, which is $\binom{n+3}{3}$. This follows by induction on n from

$$\binom{n+3}{3} - \binom{(n-2)+3}{3} = \binom{n+1}{1} + 2\binom{n+1}{2} = (n+1)^2. \tag{3.55}$$

□

Remark 1. *Since*

$$\begin{aligned} (\widetilde{M}^t_{i,j})^{\mathsf{T}} &= U^{\mathsf{T}}(M^t_{i,j})^{\mathsf{T}}U \\ &= U^{\mathsf{T}}M^t_{j,i}U \\ &= \widetilde{M}^t_{j,i}, \end{aligned} \tag{3.56}$$

if follows from Proposition 17 that $\beta^t_{i,j,k} = \beta^t_{j,i,k}$, which is not obvious from the definition of $\beta^t_{i,j,k}$. In [38], Proposition 17 is derived in a slightly different manner, resulting in a different expression for $\beta^t_{i,j,k}$ which displays the symmetry between i and j:

$$\beta^t_{i,j,k} = \sum_{u=0}^{n}(-1)^{u-t}\binom{u}{t}\binom{n-2k}{u-k}\binom{n-k-u}{i-u}\binom{n-k-u}{j-u}. \tag{3.57}$$

3.3 Block-diagonalisation of $\mathcal{A}_{q,n}$

In this section we give an explicit block diagonalisation of the algebra $\mathcal{A}_{q,n}$. The block diagonalisation can be seen as an extension of the block diagonalisation in the binary case as given in the previous section. There the binary Hamming space was taken to be the collection of subsets $\mathcal{P}$ of $\{1,\ldots,n\}$. Now it will be convenient to replace this by the collection of subsets of a given finite set V. Let V be a finite set of cardinality $|V| = m$. By $\mathcal{P}(V)$ we denote the collection of subsets of V. For integers i, j, define the $\mathcal{P}(V) \times \mathcal{P}(V)$ matrix $C^V_{i,j}$ by

$$(C^V_{i,j})_{I,J} := \begin{cases} 1 & \text{if } |I| = i,\ |J| = j,\ I \subseteq J \text{ or } J \subseteq I, \\ 0 & \text{otherwise.} \end{cases} \tag{3.58}$$

The matrices $C^V_{i,k}$ correspond to the matrices $M^k_{i,k}$ from the binary Terwilliger algebra. We have renamed them in order to avoid confusion with the matrices $M^{t,p}_{i,j} \in \mathcal{A}_{q,n}$. For $k = 0,\ldots,\lfloor \frac{m}{2} \rfloor$ define the linear space L^V_k by

$$L^V_k := \{x \in \mathbb{C}^{\mathcal{P}(\mathcal{V})} \mid C^V_{k-1,k}x = 0,\ x_I = 0 \text{ if } |I| \neq k\}, \tag{3.59}$$

and let B^V_k be an orthonormal base of L^V_k. For $i,j,k,t \in \{0,\ldots,m\}$, define the number

$$\beta^{m,t}_{i,j,k} := \binom{m-2k}{i-k}\sum_{p=0}^{m}(-1)^{k-p}\binom{k}{p}\binom{i-p}{t-p}\binom{m+p-i-k}{m+t-i-j}. \tag{3.60}$$

We recall the following facts.

Proposition 19. *Let V be a finite set of cardinality m. Then*

(i) For $k \in \{0, \dots, \lfloor \frac{m}{2} \rfloor\}$ we have

$$\dim L_k^V = \binom{m}{k} - \binom{m}{k-1}. \tag{3.61}$$

(ii) For $i, k, l \in \{0, \dots, n\}$ with $k, l \leq \lfloor \frac{m}{2} \rfloor$, and for $b \in L_k^V, c \in L_l^V$

$$(C_{i,l}^V c)^{\mathsf{T}} C_{i,k}^V b = \begin{cases} \binom{m-2k}{i-k} c^{\mathsf{T}} b & \text{if } k = l, \\ 0 & \text{otherwise.} \end{cases} \tag{3.62}$$

(iii) For $i, j, k, t \in \{0, \dots, n\}$ with $k \leq \lfloor \frac{m}{2} \rfloor$, $b \in L_k^V$ and $Y \subseteq V$ with $|Y| = j$

$$\sum_{\substack{U \subseteq V \\ |U|=i \\ |U \cap Y|=t}} (C_{i,k}^V b)_U = \beta_{i,j,k}^{m,t} \binom{m-2k}{j-k}^{-1} (C_{j,k}^V b)_Y. \tag{3.63}$$

Proof. Items (i),(ii) and (iii) follow directly from Propositions 13, 15 and 16. □

We will now describe a block diagonalisation of $\mathcal{A}_{q,n}$. Let $\phi \in \mathbb{C}$ be a primitive $(q-1)$-th root of unity. Let

$$\begin{aligned} \mathcal{V} \;:=\; \{&(a, k, i, \mathbf{a}, b) \mid \\ &a, k, i \text{ are integers satisfying } 0 \leq a \leq k \leq i \leq n + a - k, \\ &\mathbf{a} \in \mathbf{q}^n \text{ satisfies } |S(\mathbf{a})| = a, \mathbf{a}_h \neq q-1 \text{ for } h = 1, \dots, n, \\ &b \in B_{k-a}^{\overline{S(\mathbf{a})}}\}, \end{aligned} \tag{3.64}$$

where $\overline{U} := \{1, 2, \dots, n\} \setminus U$ for any set $U \subseteq \{1, 2, \dots, n\}$. For each tuple $(a, k, i, \mathbf{a}, b)$ in $\mathcal{V}$, define the vector $\Psi_{\mathbf{a},b}^{a,k,i} \in \mathbb{C}^{\mathbf{q}^n}$ by

$$(\Psi_{\mathbf{a},b}^{a,k,i})_{\mathbf{x}} := \begin{cases} (q-1)^{-\frac{1}{2}i} \binom{n+a-2k}{i-k}^{-\frac{1}{2}} \phi^{\langle \mathbf{a}, \mathbf{x} \rangle} (C_{i-a,k-a}^{\overline{S(\mathbf{a})}} b)_{S(\mathbf{x}) \setminus S(\mathbf{a})} & \text{if } S(\mathbf{a}) \subseteq S(\mathbf{x}), \\ 0 & \text{otherwise,} \end{cases} \tag{3.65}$$

for any $\mathbf{x} \in \mathbf{q}^n$. Here the nonnegative integer $\langle \mathbf{x}, \mathbf{y} \rangle$ is given by

$$\langle \mathbf{x}, \mathbf{y} \rangle := \sum_{h=0}^{n} \mathbf{x}_h \mathbf{y}_h \tag{3.66}$$

for any $\mathbf{x}, \mathbf{y} \in \mathbf{q}^n$. We stress that $\langle \mathbf{x}, \mathbf{y} \rangle$ is *not* taken modulo q. Observe that $(\Psi_{\mathbf{a},b}^{a,k,i})_{\mathbf{x}} = 0$ if $|S(\mathbf{x})| \neq i$. We have:

Proposition 20. *The vectors $\Psi_{\mathbf{a},b}^{a,k,i}$, $(a, k, i, \mathbf{a}, b) \in \mathcal{V}$ form an orthonormal base of $\mathbb{C}^{\mathbf{q}^n}$.*

Proof. First, the number $|\mathcal{V}|$ of vectors $\Psi_{\mathbf{a},b}^{a,k,i}$ equals q^n since:

$$\begin{aligned}
&\sum_{\substack{a,k,i\\ 0\le a\le k\le i\le n+a-k}} \binom{n}{a}(q-2)^a\left[\binom{n-a}{k-a}-\binom{n-a}{k-a-1}\right]\\
&\quad=\sum_{i=0}^{n}\sum_{a=0}^{i}\binom{n}{a}(q-2)^a\sum_{k=a}^{\min(i,n+a-i)}\left[\binom{n-a}{k-a}-\binom{n-a}{k-a-1}\right]\\
&\quad=\sum_{i=0}^{n}\sum_{a=0}^{i}\binom{n}{a}(q-2)^a\binom{n-a}{\min\{i-a,n-i\}}\\
&\quad=\sum_{i=0}^{n}\binom{n}{i}\sum_{a=0}^{i}(q-2)^a\binom{i}{a}\\
&\quad=\sum_{i=0}^{n}\binom{n}{i}(q-1)^i=q^n.
\end{aligned}\tag{3.67}$$

Secondly, we calculate the inner product of $\Psi_{\mathbf{a},b}^{a,k,i}$ and $\Psi_{\mathbf{a}',b'}^{a',k',i'}$. If $i\neq i'$ then the inner product is zero since the two vectors have disjoint support. So we may assume that $i'=i$. We obtain:

$$\begin{aligned}
\left\langle \Psi_{\mathbf{a},b}^{a,k,i},\ \Psi_{\mathbf{a}',b'}^{a',k',i}\right\rangle &= (q-1)^{-i}\binom{n+a-2k}{i-k}^{-\frac{1}{2}}\binom{n+a'-2k'}{i-k'}^{-\frac{1}{2}}\\
&\cdot\sum_{\mathbf{x}}\phi^{\langle\mathbf{a},\mathbf{x}\rangle-\langle\mathbf{a}',\mathbf{x}\rangle}(C_{i-a,k-a}^{\overline{S(\mathbf{a})}}b)_{S(\mathbf{x})\setminus S(\mathbf{a})}\cdot(C_{i-a',k'-a'}^{\overline{S(\mathbf{a}')}}b')_{S(\mathbf{x})\setminus S(\mathbf{a}')},
\end{aligned}\tag{3.68}$$

where the sum ranges over all $\mathbf{x}\in\mathbf{q}^n$ with $|S(\mathbf{x})|=i$ and $S(\mathbf{x})\supseteq S(\mathbf{a})\cup S(\mathbf{a}')$. If $\mathbf{a}_j\neq\mathbf{a}'_j$ for some j, then the inner product equals zero, since we can factor out $\sum_{\mathbf{x}_j=1}^{q-1}\phi^{\mathbf{x}_j(\mathbf{a}_j-\mathbf{a}'_j)}=0$. So we may assume that $\mathbf{a}=\mathbf{a}'$ (and hence $a=a'$), which simplifies the right-hand side of (3.68) to

$$\binom{n+a-2k}{i-k}^{-\frac{1}{2}}\binom{n+a-2k'}{i-k'}^{-\frac{1}{2}}(C_{i-a,k-a}^{\overline{S(\mathbf{a})}}b)^{\mathsf{T}}C_{i-a,k'-a}^{\overline{S(\mathbf{a})}}b'.\tag{3.69}$$

Indeed, since $\mathbf{a}'=\mathbf{a}$, we observe that

$$\phi^{\langle\mathbf{a},\mathbf{x}\rangle-\langle\mathbf{a},\mathbf{x}\rangle}=1,\tag{3.70}$$

and hence the summand only depends on the support of $\mathbf{x}$. We obtain

$$\begin{aligned}
&\sum_{\substack{\mathbf{x}\\ |S(\mathbf{x})|=i,S(x)\supseteq S(\mathbf{a})}}(C_{i-a,k-a}^{\overline{S(\mathbf{a})}}b)_{S(\mathbf{x})\setminus S(\mathbf{a})}\cdot(C_{i-a,k'-a}^{\overline{S(\mathbf{a})}}b')_{S(\mathbf{x})\setminus S(\mathbf{a})}\\
&\quad=\sum_{\substack{X\\ |X|=i,X\supseteq S(\mathbf{a})}}(q-1)^i(C_{i-a,k-a}^{\overline{S(\mathbf{a})}}b)_{X\setminus S(\mathbf{a})}\cdot(C_{i-a,k'-a}^{\overline{S(\mathbf{a})}}b')_{X\setminus S(\mathbf{a})}\\
&\quad=(q-1)^i\sum_{\substack{Y\subseteq\overline{S(\mathbf{a})}\\ |Y|=i-a}}(C_{i-a,k-a}^{\overline{S(\mathbf{a})}}b)_Y\cdot(C_{i-a,k'-a}^{\overline{S(\mathbf{a})}}b')_Y\\
&\quad=(q-1)^i(C_{i-a,k-a}^{\overline{S(\mathbf{a})}}b)^{\mathsf{T}}C_{i-a,k'-a}^{\overline{S(\mathbf{a})}}b'.
\end{aligned}\tag{3.71}$$

From equation (3.69) and Proposition 19 we conclude that $\left\langle \Psi^{a,k,i}_{\mathbf{a},b}, \Psi^{a,k',i}_{\mathbf{a},b'} \right\rangle$ is nonzero only if $k = k'$ and $b = b'$, in which case the inner product equals 1. □

The block diagonalisation will follow by writing the matrices $M^{t,p}_{i,j}$ with respect to the new orthonormal basis of $\mathbb{C}^{\mathbf{q}^n}$ formed by the vectors $\Psi^{a,k,i}_{\mathbf{a},b}$. To this end we define for $i,j,t,p,a,k \in \{0,\ldots,n\}$ with $a \le k \le i,j$ the number

$$\begin{aligned}\alpha(i,j,t,p,a,k) :=& \beta^{n-a,t-a}_{i-a,j-a,k-a}(q-1)^{\frac{1}{2}(i+j)-t} \\ & \cdot \sum_{g=0}^{p}(-1)^{a-g}\binom{a}{g}\binom{t-a}{p-g}(q-2)^{t-a-p+g}.\end{aligned} \tag{3.72}$$

We obtain the following.

Proposition 21. *For $(i,j,t,p) \in \mathcal{I}(q,n)$ and $(a,k,i',\mathbf{a},b) \in \mathcal{V}$ we have:*

$$\begin{aligned}&M^{t,p}_{j,i}\Psi^{a,k,i'}_{\mathbf{a},b} = \\ &\quad \delta_{i,i'}\binom{n+a-2k}{i-k}^{-\frac{1}{2}}\binom{n+a-2k}{j-k}^{-\frac{1}{2}}\alpha(i,j,t,p,a,k)\Psi^{a,k,j}_{\mathbf{a},b}.\end{aligned} \tag{3.73}$$

Proof. Clearly, both sides of (3.73) are zero if $i \neq i'$, hence we may assume that $i = i'$. We calculate $(M^{t,p}_{j,i}\Psi^{a,k,i}_{\mathbf{a},b})_{\mathbf{y}}$. We may assume that $|S(\mathbf{y})| = j$, since otherwise both sides of (3.73) have a zero in position $\mathbf{y}$. We have:

$$\begin{aligned}(M^{t,p}_{j,i}\Psi^{a,k,i}_{\mathbf{a},b})_{\mathbf{y}} &= \sum_{\mathbf{x}\in\mathbf{q}^n}(M^{t,p}_{j,i})_{\mathbf{y},\mathbf{x}}(\Psi^{a,k,i}_{\mathbf{a},b})_{\mathbf{x}} \\ &= (q-1)^{-\frac{1}{2}i}\binom{n+a-2k}{i-k}^{-\frac{1}{2}}\sum_{\mathbf{x}}\phi^{\langle\mathbf{x},\mathbf{a}\rangle}(C^{\overline{S(\mathbf{a})}}_{i-a,k-a}b)_{S(\mathbf{x})\setminus S(\mathbf{a})},\end{aligned} \tag{3.74}$$

where the last sum ranges over all $\mathbf{x} \in \mathbf{q}^n$ with $|S(\mathbf{x})| = i$, $S(\mathbf{x}) \supseteq S(\mathbf{a})$, $|S(\mathbf{x}) \cap S(\mathbf{y})| = t$ and $|\{h \mid \mathbf{x}_h = \mathbf{y}_h \neq 0\}| = p$.

We will work out the sum:

$$\sum_{\substack{\mathbf{x}\\ |S(\mathbf{x})|=i, S(\mathbf{x})\supseteq S(\mathbf{a})\\ |S(\mathbf{x})\cap S(\mathbf{y})|=t\\ |\{h|\mathbf{x}_h=\mathbf{y}_h\neq 0\}|}} \phi^{\langle\mathbf{x},\mathbf{a}\rangle}(C^{\overline{S(\mathbf{a})}}_{i-a,k-a}b)_{S(\mathbf{x})\setminus S(\mathbf{a})}. \tag{3.75}$$

If there exists an $h \in S(\mathbf{a}) \setminus S(\mathbf{y})$, we can factor out $\sum_{l=1}^{q-1}\phi^{l\cdot\mathbf{a}_h} = 0$, implying that both sides of (3.73) have a zero at position $\mathbf{y}$. Hence we may assume that $S(\mathbf{y}) \supseteq S(\mathbf{a})$. Now the support of each word $\mathbf{x}$ in this sum can be split into five parts U, U', V, V', W, where

$$\begin{aligned}U &= \{h \in S(\mathbf{a}) \mid \mathbf{x}_h = \mathbf{y}_h\} \\ U' &= S(\mathbf{a}) \setminus U, \\ V &= \{h \in S(\mathbf{y}) \setminus S(\mathbf{a}) \mid \mathbf{x}_h = \mathbf{y}_h\}, \\ V' &= ((S(\mathbf{y}) \setminus S(\mathbf{a})) \cap S(\mathbf{x})) \setminus V, \\ W &= S(\mathbf{x}) \setminus S(\mathbf{y}).\end{aligned} \tag{3.76}$$

Setting $g := |U|$, gives $|U'| = a - g$, $|V| = p - g$, $|V'| = t - a - p + g$ and $|W| = i - t$. Hence splitting the sum over g, we obtain:

$$\sum_{g=0}^{p} \sum_{U,U',V,V',W} (C_{i-a,k-a}^{\overline{S(\mathbf{a})}} b)_{V \cup V' \cup W} \prod_{h \in U} \phi^{\mathbf{a}_h \mathbf{y}_h} \prod_{h \in U'} (-\phi^{\mathbf{a}_h \mathbf{y}_h}) \prod_{h \in V} 1 \prod_{h \in V'} (q-2) \prod_{h \in W} (q-1), \quad (3.77)$$

where U, U', V, V', W are as indicated. Substituting $T = V \cup V' \cup W$, we can rewrite this as

$$\sum_{g=0}^{p} \binom{a}{g} \binom{t-a}{p-g} (-1)^{a-g} (q-2)^{t-a-p+g} \cdot (q-1)^{i-t} \phi^{\langle \mathbf{a}, \mathbf{y} \rangle} \sum_{T} (C_{i-a,k-a}^{\overline{S(\mathbf{a})}} b)_T, \quad (3.78)$$

where the sum ranges over all $T \subseteq \overline{S(\mathbf{a})}$ with $|T| = i - a$ and $|T \cap S(\mathbf{y})| = t - a$. Now by Proposition 19(iii), this is equal to

$$(q-1)^{i-t} \sum_{g=0}^{p} \binom{a}{g} \binom{t-a}{p-g} (-1)^{a-g} (q-2)^{t-a-p+g} \cdot \phi^{\langle \mathbf{a}, \mathbf{y} \rangle} \binom{n+a-2k}{j-k}^{-1} \beta_{i-a,j-a,k-a}^{n-a,t-a} (C_{j-a,k-a}^{\overline{S(\mathbf{a})}} b)_{S(\mathbf{y}) \setminus S(\mathbf{a})}, \quad (3.79)$$

which equals

$$(\Psi_{\mathbf{a},b}^{a,k,j})_{\mathbf{y}} \cdot \beta_{i-a,j-a,k-a}^{n-a,t-a} \binom{n+a-2k}{j-k}^{-\frac{1}{2}} (q-1)^{i-t+\frac{1}{2}j} \cdot \sum_{g=0}^{p} (-1)^{a-g} \binom{a}{g} \binom{t-a}{p-g} (q-2)^{t-a-p+g}. \quad (3.80)$$

This completes the proof. □

If we define U to be the $\mathbf{q}^n \times \mathcal{V}$ matrix with $\Psi_{\mathbf{a},b}^{a,k,i}$ as the $(a, k, i, \mathbf{a}, b)$-th column, then Proposition 21 shows that for each $(i, j, t, p) \in \mathcal{I}(q, n)$ the matrix $\widetilde{M}_{i,j}^{t,p} := U^* M_{i,j}^{t,p} U$ has entries

$$(\widetilde{M}_{i,j}^{t,p})_{(a,k,l,\mathbf{a},b),(a',k',l',\mathbf{a}',b')} = \begin{cases} \binom{n+a-2k}{i-k}^{-\frac{1}{2}} \binom{n+a-2k}{j-k}^{-\frac{1}{2}} \alpha(i,j,t,p,a,k) & \text{if } a = a',\ k = k',\ \mathbf{a} = \mathbf{a}',\ b = b' \text{ and} \\ & l = i,\ l' = j, \\ 0 & \text{otherwise.} \end{cases} \quad (3.81)$$

This implies

Proposition 22. *The matrix U gives a block diagonalisation of $\mathcal{A}_{q,n}$.*

Proof. Equation (3.81) implies that each matrix $\widetilde{M}_{i,j}^{t,p}$ has a block diagonal form, where for each pair (a,k) there are $\binom{n}{a}(q-2)^a\left[\binom{n-a}{k-a}-\binom{n-a}{n-a-1}\right]$ copies of an $(n+a+1-2k)\times(n+a+1-2k)$ block on the diagonal. For fixed a,k the copies are indexed by the pairs $(\mathbf{a},b)$ such that $\mathbf{a}\in\mathbf{q}^n$ satisfies $|S(\mathbf{a})|=a$, $\mathbf{a}_h\neq q-1$ for $h=1,\ldots,n$, and $b\in B_{k-a}^{\overline{S(\mathbf{a})}}$. In each copy the rows and columns in the block are indexed by the integers i with $k\leq i\leq n+a-k$. Hence we need to show that all matrices of this block diagonal form belong to $U^*\mathcal{A}_{q,n}U$. It suffices to show that the dimension $\sum_{0\leq a\leq k\leq n+a-k}(n+a+1-2k)^2$ of the algebra consisting of the matrices in the given block diagonal form equals the dimension of $\mathcal{A}_{q,n}$, which is $\binom{n+4}{4}$. This follows from

$$\begin{aligned}
&\sum_{0\leq a\leq k\leq n+a-k}(n+a+1-2k)^2\\
&\qquad=\sum_{a=0}^{n}\sum_{k=0}^{\lfloor\frac{n-a}{2}\rfloor}(n-a+1-2k)^2\\
&\qquad=\sum_{a=0}^{n}\binom{n-a+3}{3}\\
&\qquad=\binom{n+4}{4}.
\end{aligned}\tag{3.82}$$

□

This implies the following result.

Theorem 4. *The matrix*

$$M=\sum_{(i,j,t,p)}x_{i,j}^{t,p}M_{i,j}^{t,p}\tag{3.83}$$

is positive semidefinite if and only if for all a,k with $0\leq a\leq k\leq n+a-k$ the matrices

$$\left(\sum_{t,p}\alpha(i,j,t,p,a,k)x_{i,j}^{t,p}\right)_{i,j=k}^{n+a-k}\tag{3.84}$$

are positive semidefinite.

Proof. The matrix M is positive semidefinite if and only if U^*MU is positive semidefinite. Since U^*MU is in block diagonal form, where the blocks are exactly the matrices in (3.84), each with multiplicity at least one, the theorem follows. □

Theorem 5. *The matrix*

$$R\left(\sum_{(i,j,t,p)}x_{i,j}^{t,p}M_{i,j}^{t,p}\right)\tag{3.85}$$

is positive semidefinite if and only if for all a, k with $0 \leq a \leq k \leq n + a - k$ and $k \neq 0$ the matrix

$$\left(\sum_{t,p} \alpha(i, j, t, p, a, k) x_{i,j}^{t,p} \right)_{i,j=k}^{n+a-k} \tag{3.86}$$

is positive semidefinite, and also the matrix

$$\begin{pmatrix} 1 & x^{\mathsf{T}} \\ x & L \end{pmatrix} \tag{3.87}$$

is positive semidefinite, where

$$L := \left(\sum_{t,p} \alpha(i, j, t, p, 0, 0) x_{i,j}^{t,p} \right)_{i,j=0}^{n} \tag{3.88}$$

and

$$x_i = \binom{n}{i} (q-1)^i \cdot x_{i,i}^{i,i} \quad \textit{for } i = 0, \ldots, n. \tag{3.89}$$

Proof. Let

$$M := \sum_{(i,j,t,p)} x_{i,j}^{t,p} M_{i,j}^{t,p}. \tag{3.90}$$

Observe that

$$\begin{pmatrix} 1 & 0 \\ 0 & U \end{pmatrix}^* R(M) \begin{pmatrix} 1 & 0 \\ 0 & U \end{pmatrix} = \begin{pmatrix} 1 & (\mathrm{diag}(M))^{\mathsf{T}} U \\ U^* \mathrm{diag}(M) & U^* M U \end{pmatrix}. \tag{3.91}$$

Since

$$\chi^{S_i(\mathbf{0})} = \binom{n}{i} (q-1)^i \Psi_{\mathbf{0},1}^{0,0,i} = \binom{n}{i} (q-1)^i U_{(0,0,i,\mathbf{0},1)} \tag{3.92}$$

and $U^* U = I$, we see that

$$\begin{aligned} U^* \mathrm{diag}(M) &= U^* \sum_{i=0}^{n} x_{i,i}^{i,i} \chi^{S_i(\mathbf{0})} \\ &= \sum_{i=0}^{n} x_{i,i}^{i,i} \binom{n}{i} (q-1)^i U^* U_{(0,0,i,\mathbf{0},1)} \\ &= \sum_{i=0}^{n} x_{i,i}^{i,i} \binom{n}{i} (q-1)^i \chi^{(0,0,i,\mathbf{0},1)} \end{aligned} \tag{3.93}$$

has nonzero entries only in the block corresponding to $a = k = 0$. The theorem follows. □

3.4 The Terwilliger algebra of the Johnson scheme

The Hamming scheme is a natural and powerful tool in studying subsets of the binary Hamming space with prescribed distance relations. In particular, the Delsarte bound gives good upper bounds on the size of a code. In the case of constant weight codes, one considers subsets of the Johnson space, consisting of the subsets of some fixed size w. Now the appropiate tool to use is the *Johnson scheme*.

Let $w \leq n$ be positive integers and let $\mathcal{P}_n^w$ be the collection of subsets of $\{1, \ldots, n\}$ of cardinality w. So $\mathcal{P}_n$ is the disjoint union of $\mathcal{P}_n^0, \mathcal{P}_n^1, \ldots, \mathcal{P}_n^n$. We will assume that $w \leq \left\lfloor \frac{n}{2} \right\rfloor$. This is not a severe restriction since $\mathcal{P}_n^w$ and P_n^{n-w}, with the Hamming distance, are isomorphic. This is because the Hamming distance is preserved under taking complements: $d(U, V) = d(\overline{U}, \overline{V})$ for sets $U, V \in \{1, \ldots, n\}$. It is convenient to define the *Johnson distance* d_J by

$$d_J(U, V) := w - |U \cap V| = \frac{1}{2} d(U, V). \tag{3.94}$$

We denote by $\mathrm{Aut}(n, w)$ the set of automorphisms of the Johnson space. It is easy to see that the automorphisms are just the permutations of $\mathcal{P}_n^w$ induced by permuting the ground set $\{1, \ldots, n\}$. The distance relations $R_0, \ldots, R_w$ given by

$$R_d := \{(U, V) \in \mathcal{P}_n^w \times \mathcal{P}_n^w \mid d_J(U, V) = d\} \tag{3.95}$$

are precisely the orbits under the action of $\mathrm{Aut}(n, w)$ on $\mathcal{P}_n^w \times \mathcal{P}_n^w$:

$$R_d = \{(\sigma U, \sigma V) \mid \sigma \in \mathrm{Aut}(n, w)\}, \quad \text{when } d_J(U, V) = d. \tag{3.96}$$

Hence $R_0, \ldots, R_w$ form an association scheme called the *Johnson scheme* $J(n, w)$. The Bose–Mesner algebra of the Johnson scheme is spanned by the matrices $A_d \in \mathbb{C}^{\mathcal{P}_n^w \times \mathcal{P}_n^w}$, $d = 0, \ldots, w$ given by

$$(A_d)_{U,V} := \begin{cases} 1 & \text{if } d_J(U, V) = d \\ 0 & \text{otherwise} \end{cases}. \tag{3.97}$$

Like in the case of the Hamming scheme, it useful to consider the refinement of the Johnson scheme obtained by replacing the full symmetry group $\mathrm{Aut}(n, w)$ by the stabilizer subgroup $\mathrm{Aut}_W(n, w)$ of some arbitrary element $W \in \mathcal{P}_n^w$. Therefore we fix some $W \in \mathcal{P}_n^w$. Consider the complex algebra $\mathcal{T}$ spanned by the 0–1 matrices $M_{i,j}^{s,t}$ where $0 \leq s \leq i, j \leq w$ and $t \leq w - i, w - j$, given by

$$(M_{i,j}^{s,t})_{U,V} := \begin{cases} 1 & \text{if } |U \cap W| = i, |V \cap W| = j, \\ & |U \cap V \cap W| = s, |U \cap V \setminus W| = t\,. \\ 0 & \text{otherwise} \end{cases} \tag{3.98}$$

It is not hard to verify that supports of the matrices $M_{i,j}^{s,t}$ correspond to the orbits of $\mathcal{P}_n^w \times \mathcal{P}_n^w$ under the action of $\mathrm{Aut}_W(n, w)$. The algebra $\mathcal{T}$ is in fact the Terwilliger algebra of the Johnson scheme $J(n, w)$ with respect to W.

We will give a block diagonalisation of the Terwilliger algebra of the Johnson scheme. This was implicit in the work of Schrijver ([38]).

Let $\mathcal{A}_{w,n-w} := \mathcal{A}_w \otimes \mathcal{A}_{n-w}$ be the tensor product of the algebras $\mathcal{A}_w$ and $\mathcal{A}_{n-w}$. The algebra $\mathcal{A}_{w,n-w}$ consists of the matrices

$$\sum_{i,j,t,i',j',t'} x^{t,t'}_{i,j,i',j'} M^t_{w;i,j} \otimes M^{t'}_{n-w;i',j'}, \tag{3.99}$$

where $x^{t,t'}_{i,j,i',j'} \in \mathbb{C}$. From Section 3.2 we obtain matrices U_w and U_{n-w} such that $U_w^\mathsf{T} \mathcal{A}_w U_w$ and $U_{n-w}^\mathsf{T} \mathcal{A}_{n-w} U_{n-w}$ are in block diagonal form. It follows that $U := U_w \otimes U_{n-w}$ block diagonalises $\mathcal{A}_{w,n-w}$ since

$$U^\mathsf{T} \mathcal{A}_{w,n-w} U = U_w^\mathsf{T} \mathcal{A}_w U_w \otimes U_{n-w}^\mathsf{T} \mathcal{A}_{n-w} U_{n-w}. \tag{3.100}$$

It follows from Proposition 17 that the blocks are indexed by the pairs

$$(k,k') \in \{0,1,\ldots,\left\lfloor \frac{w}{2} \right\rfloor\} \times \{0,1,\ldots,\left\lfloor \frac{n-w}{2} \right\rfloor\}. \tag{3.101}$$

For each such pair (k,k') we have a block $B_{k,k'}$, consisting of all $(V_k \times V'_{k'}) \times (V_k \times V'_{k'})$ matrices, where $V_k := \{k,\ldots,w-k\}$ and $V'_{k'} := \{k',\ldots,n-w-k'\}$. The image of (3.99) in block (k,k') is given by

$$\left(\sum_{t,t'} x^{t,t'}_{i,j,i',j'} \beta^{w,t}_{i,j,k} \cdot \beta^{n-w,t'}_{i',j',k'} \left[\tbinom{w-2k}{i-k} \tbinom{w-2k}{j-k} \tbinom{n-w-2k'}{i'-k'} \tbinom{n-w-2k'}{j'-k'} \right]^{-\frac{1}{2}} \right)_{\substack{i,j \in V_k \\ i',j' \in V'_{k'}}} \tag{3.102}$$

By extending each matrix in $\mathcal{T}$ by zeros to a $\mathcal{P}_n \times \mathcal{P}_n$ matrix, and identifying $\mathcal{P}_n$ with $\mathcal{P}_w \times \mathcal{P}_{n-w}$ (by identifying U and $(U \cap W, U \setminus W)$ for any $U \in \mathcal{P}_n$), the Terwilliger algebra $\mathcal{T}$ can be seen as a subalgebra of $\mathcal{A}_{w,n-w}$, where $M^{s,t}_{i,j}$ is identified with $M^s_{i,j} \otimes M^t_{w-i,w-j}$. It follows that in the block diagonalisation given above, $\mathcal{T}$ is mapped in block (k,k') to those matrices that have nonzeros only in positions with rows and columns indexed by $\{(i,w-i) \mid i \in V_k, w-i \in V'_{k'}\}$. Hence restricting each block to those indices, we obtain a block diagonalisation of $\mathcal{T}$ with blocks of size

$$|\{k,\ldots,n-k\} \cap \{2w-n+k',\ldots,w-k'\}| \tag{3.103}$$

for each pair (k,k') with $k+k' \leq w$. This was used in [38] to obtain bounds on constant weight codes.

In the nonbinary case, let $\mathbb{E}$ be the set of q-ary word of length n and weight w, equipped with the Hamming distance. The q-ary Johnson scheme $J_q(n,w)$ has adjacency matrices $M_{t,p}$ for $0 \leq p \leq t \leq w$ given by the orbits of $\mathbb{E} \times \mathbb{E}$ under the action of the automorphism group of $\mathbb{E}$:

$$(M_{t,p})_{\mathbf{x},\mathbf{y}} := \begin{cases} 1 & \text{if } |S(\mathbf{x}) \cap S(\mathbf{y})| = t, |\{i \mid \mathbf{x}_i = \mathbf{y}_i \neq 0\}| = p, \\ 0 & \text{otherwise.} \end{cases} \tag{3.104}$$

Replacing the full automorphism group by the stabilizer of some word $\mathbf{w} \in \mathbb{E}$ we obtain an algebra containing the Bose–Mesner algebra of the nonbinary Johnson scheme which may serve to improve bounds for constant weight codes in the nonbinary case. We do not know if this is the Terwilliger algebra (with respect to $\mathbf{w}$) of the nonbinary Johnson scheme $J_q(n,w)$. The algebra is a subalgebra of a tensor product of $\mathcal{A}_{q,n-w}$ and an algebra of dimension $\binom{w+9}{9}$ (or $\binom{w+8}{8}$ if $q=3$). It would be interesting to find a block diagonalisation of this algebra.

Chapter 4

Error correcting codes

Given a code $C \subseteq \mathbb{E} := q^n$, the *minimum distance* of C is defined to be the minimum of $\{d(\mathbf{u},\mathbf{v}) \mid \mathbf{u} \neq \mathbf{v}, \mathbf{u}, \mathbf{v} \in C\}$. The maximum cardinality of a code with minimum distance at least d is denoted by $A_q(n,d)$. In this chapter we give new upper bounds on $A_q(n,d)$ based on a semidefinite programming approach, strengthening Delsarte's linear programming bound. For more information on coding theory, the reader is referred to [30, 33].

4.1 Delsarte's linear programming bound

Given a code $C \subseteq \mathbb{E}$, the $(n+1)$-tuple $(x_0, x_1, \ldots, x_n)$ defined by

$$x_i := |C|^{-1} \cdot |\{(\mathbf{u},\mathbf{v}) \in C \times C \mid d(\mathbf{u},\mathbf{v}) = i\}| \tag{4.1}$$

is called the *distance distribution* of the code C. For each i the number x_i equals the average number of code words at distance i from a given code word. Observe that $x_0 = 1$ and $x_0 + x_1 + \cdots + x_n = |C|$. The key observation that leads to the linear programming bound is that the following inequalities hold:

$$\sum_{i=0}^{n} x_i K_j(i) \geq 0 \quad \text{for all } j = 0, \ldots, n, \tag{4.2}$$

where

$$K_j(x) := \sum_{k=0}^{j} (-1)^k \binom{x}{k} \binom{n-x}{j-k} (q-1)^{j-k}, \quad j = 0, \ldots, n \tag{4.3}$$

are the *Krawtchouk polynomials*. These inequalities give rise to the following linear programming bound on the size of a code with minimum distance at least d:

$$\begin{aligned} A_q(n,d) \leq \max\{\sum_{i=0}^{n} x_i \mid \quad & x_0 = 1, x_1, \ldots, x_n \geq 0, \\ & x_1 = \cdots = x_{d-1} = 0, \\ & \text{the } x_i \text{ satisfy (4.2)}\}. \end{aligned} \tag{4.4}$$

This approach turned out to be very powerful. Many of the best known upper bounds on $A_q(n,d)$ are obtained using this method.

A proof of the validity of (4.2) can be found for example in [15, 30]. To illustrate the semidefinite programming approach in this chapter, we sketch a proof here. For any code $C \subseteq \mathbb{E}$, we denote by M_C the 0–1 matrix defined by

$$(M_C)_{\mathbf{u},\mathbf{v}} := \begin{cases} 1 & \text{if } \mathbf{u},\mathbf{v} \in C \\ 0 & \text{otherwise} \end{cases}. \tag{4.5}$$

We prove (4.2).

Proof. Consider the matrix

$$M := \frac{1}{|\mathrm{Aut}(q,n)| \cdot |C|} \sum_{\sigma \in \mathrm{Aut}(q,n)} M_{\sigma C}. \tag{4.6}$$

The matrix M is an element of the Bose–Mesner algebra of the Hamming scheme and the coefficients with respect to the adjacency matrices A_i of the Hamming scheme reflect the distance distribution:

$$M = \sum_{i=0}^{n} x_i \gamma_i^{-1} A_i, \tag{4.7}$$

where

$$\gamma_i := q^n (q-1)^i \binom{n}{i} \tag{4.8}$$

is the number of nonzero entries of A_i. Indeed, we have $\langle A_i, M_{\sigma C}\rangle = |C| x_i$, and hence $\langle A_i, M\rangle = x_i$ for every $i = 0,\dots,n$ and every $\sigma \in \mathrm{Aut}(q,n)$.

The matrix M is a nonnegative combination of the positive semidefinite matrices $M_{\sigma C}$ and is therefore positive semidefinite itself. The inequalities (4.2) will follow from this semidefiniteness by diagonalising the Bose–Mesner algebra. Let the unitary matrix $U \in \mathbb{C}^{\mathbb{E}\times\mathbb{E}}$ be given by

$$(U)_{\mathbf{u},\mathbf{v}} := q^{-n/2} \phi^{\langle \mathbf{u},\mathbf{v}\rangle} \tag{4.9}$$

for $\mathbf{u},\mathbf{v} \in \mathbb{E}$, where ϕ is a primitive q-th root of unity. It is a straightforward calculation to show that for each $i = 0,\dots,n$ the matrix $\widetilde{A}_i := U^* A_i U$ is a diagonal matrix with

$$(\widetilde{A}_i)_{\mathbf{u},\mathbf{u}} = K_i(j) = \gamma_i \gamma_j^{-1} K_j(i) \quad \text{when } d(\mathbf{0},\mathbf{u}) = j. \tag{4.10}$$

Since M is positive semidefinite, also the diagonal matrix U^*MU is positive semidefinite, which means that all diagonal elements $\sum_{i=0}^{n} x_i K_j(i) \gamma_j^{-1}$, $j = 0,\dots n$ are nonnegative. This implies (4.2). □

In fact, the equivalence of $U^*MU \succeq 0$ and $M \succeq 0$ shows the following, which we mention for future reference.

Proposition 23. *For $x_0, x_1, \dots, x_n \in \mathbb{R}$, we have*

$$\begin{aligned} x_0 A_0 + x c_1 A_1 + \cdots + x_n A_n \succeq 0 \quad &\textit{if and only if} \\ x_0 K_j(0) + x_1 K_j(1) + \cdots + x_n K_j(n) \geq 0 \quad &\textit{for } j = 0,\dots,n. \end{aligned} \tag{4.11}$$

4.2 Semidefinite programming bound

In this section we describe a way to obtain upper bounds on $A_q(n,d)$ by semidefinite programming. The method strengthens Delsarte's linear programming bound and was introduced by Schrijver in [38] in the case of binary codes. There it was used to find a large number of improved bounds for binary codes. While this thesis was being written, the same method was used by de Klerk and Pasechnik in [26] to bound the stability number of *orthogonality graphs*, (or equivalently) the maximum size of a binary code of length n in which no two words have Hamming distance $\frac{1}{2}n$, where n is divisible by four.

In this section we will describe this method, but restrict ourselves to the nonbinary case. In Section 4.3 we give a list of improved upper bounds that we found with this method for $q = 3, 4, 5$.

Let C be any code. We define the matrices M' and M'' by:

$$\begin{aligned} M' &:= |\mathrm{Aut}(q,n)|^{-1} \sum_{\substack{\sigma \in \mathrm{Aut}(q,n) \\ \mathbf{0} \in \sigma C}} M_{\sigma C} \\ M'' &:= |\mathrm{Aut}(q,n)|^{-1} \sum_{\substack{\sigma \in \mathrm{Aut}(q,n) \\ \mathbf{0} \notin \sigma C}} M_{\sigma C}. \end{aligned} \tag{4.12}$$

By construction, the matrices M' and M'' are invariant under permutations $\sigma \in \mathrm{Aut}_{\mathbf{0}}(q,n)$ of the rows and columns. Hence M' and M'' are elements of the algebra $\mathcal{A}_{q,n}$. We write

$$M' = \sum_{(i,j,t,p)} x_{i,j}^{t,p} M_{i,j}^{t,p}. \tag{4.13}$$

Here the matrices $M_{i,j}^{t,p}$ are the standard basis matrices of the algebra $\mathcal{A}_{q,n}$.

The matrix M'' can be expressed in terms of the coefficients $x_{i,j}^{t,p}$ as follows.

Proposition 24. *The matrix M'' satisfies*

$$M'' = \sum_{(i,j,t,p)} (x_{i+j-t-p,0}^{0,0} - x_{i,j}^{t,p}) M_{i,j}^{t,p}. \tag{4.14}$$

Proof. The matrix

$$M := M' + M'' = |\mathrm{Aut}(q,n)|^{-1} \sum_{\sigma \in \mathrm{Aut}(q,n)} M_{\sigma C} \tag{4.15}$$

is invariant under permutation of the rows and columns by any permutation $\sigma \in \mathrm{Aut}(q,n)$, and hence is an element of the Bose–Mesner algebra, say

$$M = \sum_k y_k A_k. \tag{4.16}$$

Observe that for any $\mathbf{u} \in \mathbb{E}$ with $d(\mathbf{u}, \mathbf{0}) = k$, we have

$$y_k = (M)_{\mathbf{u},\mathbf{0}} = (M')_{\mathbf{u},\mathbf{0}} = x_{k,0}^{0,0}, \tag{4.17}$$

since $(M'')_{\mathbf{u},\mathbf{0}} = 0$. Hence we have

$$\begin{aligned} M'' &= M - M' \\ &= \sum_k x_{k,0}^{0,0} A_k - \sum_{(i,j,t,p)} x_{i,j}^{t,p} M_{i,j}^{t,p} \\ &= \sum_k \sum_{i+j-t-p=k} x_{k,0}^{0,0} M_{i,j}^{t,p} - \sum_{(i,j,t,p)} x_{i,j}^{t,p} M_{i,j}^{t,p} \\ &= \sum_{(i,j,t,p)} (x_{i+j-t-p,0}^{0,0} - x_{i,j}^{t,p}) M_{i,j}^{t,p}, \end{aligned} \tag{4.18}$$

which proves the proposition. □

The coefficients $x_{i,j}^{t,p}$ carry important information about the code C, comparable to the distance distribution in Delsarte's linear programming approach. Where the distance distribution records for each distance d the number of pairs in C at distance d, the coefficients $x_{i,j}^{t,p}$ count the number of *triples* $(\mathbf{u}, \mathbf{v}, \mathbf{w}) \in C^3$ for each equivalence class of $\mathbb{E}^3$ under the action of $\mathrm{Aut}(q, n)$. We express this formally as follows. Recall that

$$X_{i,j,t,p} := \{(\mathbf{u}, \mathbf{v}, \mathbf{w}) \in \mathbb{E} \times \mathbb{E} \times \mathbb{E} \mid d(\mathbf{u}, \mathbf{v}, \mathbf{w}) = (i, j, t, p)\}, \tag{4.19}$$

for $(i, j, t, p) \in \mathcal{I}(q, n)$. Now denote for each $(i, j, t, p) \in \mathcal{I}(q, n)$ the numbers

$$\lambda_{i,j}^{t,p} := |(C \times C \times C) \cap X_{i,j,t,p}|, \tag{4.20}$$

and let

$$\gamma_{i,j}^{t,p} := |(\{\mathbf{0}\} \times \mathbb{E} \times \mathbb{E}) \cap X_{i,j,t,p}| \tag{4.21}$$

be the number of nonzero entries of $M_{i,j}^{t,p}$. A simple calculation yields:

$$\gamma_{i,j}^{t,p} = (q-1)^{i+j-t}(q-2)^{t-p} \binom{n}{p, t-p, i-t, j-t}. \tag{4.22}$$

The numbers $x_{i,j}^{t,p}$ are related to the numbers $\lambda_{i,j}^{t,p}$ by

Proposition 25. $x_{i,j}^{t,p} = q^{-n}(\gamma_{i,j}^{t,p})^{-1} \lambda_{i,j}^{t,p}$.

Proof. Observe that the matrices $M_{i,j}^{t,p}$ are pairwise orthogonal and that $\langle M_{i,j}^{t,p}, M_{i,j}^{t,p} \rangle = \gamma_{i,j}^{t,p}$ for $(i, j, t, p) \in \mathcal{I}(q, n)$. Hence

$$\begin{aligned} \langle M', M_{i,j}^{t,p} \rangle &= |\mathrm{Aut}(q,n)|^{-1} \sum_{u \in C} \sum_{\substack{\sigma \in \mathrm{Aut}(q,n) \\ \sigma \mathbf{u} = \mathbf{0}}} \langle M_{\sigma C}, M_{i,j}^{t,p} \rangle \\ &= |\mathrm{Aut}(q,n)|^{-1} \cdot |\mathrm{Aut}_{\mathbf{0}}(q,n)| \sum_{\mathbf{u} \in C} \cdot |(\{\mathbf{u}\} \times C \times C) \cap X_{i,j,t,p}| \\ &= q^{-n} |(C \times C \times C) \cap X_{i,j,t,p}| = q^{-n} \lambda_{i,j}^{t,p} \end{aligned} \tag{4.23}$$

implies that

$$M' = q^{-n} \sum_{(i,j,t,p) \in \mathcal{I}(q,n)} \lambda_{i,j}^{t,p} (\gamma_{i,j}^{t,p})^{-1} M_{i,j}^{t,p}. \tag{4.24}$$

Comparing the coefficients of the $M_{i,j}^{t,p}$ with those in (4.13) proves the proposition. □

Proposition 26. *The $x_{i,j}^{t,p}$ satisfy the following linear constraints, where (iii) holds if C has minimum distance at least d:*

$$\begin{aligned} &(i) && 0 \le x_{i,j}^{t,p} \le x_{i,0}^{0,0} \\ &(ii) && x_{i,j}^{t,p} = x_{i',j'}^{t',p'} \text{ if } t-p = t'-p' \text{ and} \\ & && (i,j,i+j-t-p) \text{ is a permutation of } (i',j',i'+j'-t'-p') \\ &(iii) && x_{i,j}^{t,p} = 0 \text{ if } \{i,j,i+j-t-p\} \cap \{1,2,\ldots,d-1\} \neq \emptyset. \end{aligned} \tag{4.25}$$

Proof. Conditions (ii) and (iii) follow directly from Proposition 25. Condition (i) follows from the fact that if $M = M_{\sigma C}$ for some $\sigma \in \mathrm{Aut}(q,n)$ with $\mathbf{0} \in \sigma C$, then $0 \le M_{\mathbf{u},\mathbf{v}} \le M_{\mathbf{0},\mathbf{u}}$ for any $\mathbf{u},\mathbf{v} \in \mathbb{E}$. □

An important feature of the matrices M' and M'' is, that they are positive semidefinite. This follows since M' and M'' are nonnegative combinations of the matrices $M_{\sigma C} = \chi^{\sigma C}(\chi^{\sigma C})^{\mathsf{T}}$ which are clearly positive semidefinite. Using the block diagonalisation of $\mathcal{A}_{q,n}$, the positive semidefiniteness of M' and M'' is equivalent to:

$$\begin{gathered} \text{for all } a,k \text{ with } 0 \le a \le k \le n+a-k, \text{ the matrices} \\ \left(\sum_{t,p} \alpha(i,j,t,p,a,k) x_{i,j}^{t,p} \right)_{i,j=k}^{n+a-k} \\ \text{and} \\ \left(\sum_{t,p} \alpha(i,j,t,p,a,k) (x_{i+j-t-p,0}^{0,0} - x_{i,j}^{t,p}) \right)_{i,j=k}^{n+a-k} \\ \text{are positive semidefinite.} \end{gathered} \tag{4.26}$$

If we view the $x_{i,j}^{t,p}$ as variables, we obtain an upper bound on the size of a code of minimum distance d as follows.

Theorem 6. *The semidefinite programming problem*

$$\begin{gathered} \text{maximize } \sum_{i=0}^{n} \binom{n}{i} (q-1)^i x_{i,0}^{0,0} \quad \text{subject to} \\ x_{0,0}^{0,0} = 1, \text{ and conditions (4.25) and (4.26)} \end{gathered} \tag{4.27}$$

is an upper bound on $A_q(n,d)$.

Proof. We first remark that conditions (4.25) and (4.26) are invariant under scaling the numbers $x_{i,j}^{t,p}$ with a common positive factor. The constraint $x_{0,0}^{0,0} = 1$ serves as a normalisation. If $C \subseteq \mathbb{E}$ is a code of minimum distance d. Setting

$$x_{i,j}^{t,p} := q^n \cdot \lambda_{i,j}^{t,p} \gamma_{i,j}^{t,p} \tag{4.28}$$

gives a feasible solution with objective value $|C|$. □

This is a semidefinite programming problem with $O(n^4)$ variables, and can be solved in time polynomial in n. This semidefinite programming bound is at least as strong as the Delsarte bound. Indeed, the Delsarte bound is equal to the maximum of $\sum_{i=0}^{n} x_{i,0}^{0,0}\binom{n}{i}(q-1)^i$ subject to the conditions $x_{0,0}^{0,0} = 1$, $x_{1,0}^{0,0} = \cdots = x_{d-1,0}^{0,0} = 0$, $x_{i,0}^{0,0} \geq 0$ for all $i = d, \ldots, n$ and

$$\sum_{i=0}^{n} x_{i,0}^{0,0} A_i \quad \text{is positive semidefinite,} \tag{4.29}$$

as was shown in the previous section. This last constraint is equivalent to

$$\sum_{i,j,t,p} x_{i+j-t-p,0}^{0,0} M_{i,j}^{t,p} \quad \text{is positive semidefinite,} \tag{4.30}$$

since $A_k = \sum_{i+j-t-p=k} M_{i,j}^{t,p}$. It follows that (4.29) is implied by the condition that M' and M'' be positive semidefinite, that is condition (4.26).

4.2.1 Variations

There are a number of obvious variations to the semidefinite program (4.27), altering the objective function and the constraint $x_{0,0}^{0,0} = 1$. For convenience we will optimize over matrices

$$M := \sum_{i,j,t,p} x_{i,j}^{t,p} M_{i,j}^{t,p} \tag{4.31}$$

in the Terwilliger algebra. Observe that the numbers $x_{i,j}^{t,p}$ are uniquely determined by M and vice versa. The semidefinite program (4.27) can be rewritten as

$$\text{maximize } \mathrm{tr}M \quad \text{subject to (4.25), (4.26) and } x_{0,0}^{0,0} = 1. \tag{4.32}$$

Consider the following two variations

$$\begin{aligned} &\text{maximize} && x_{0,0}^{0,0} \\ &\text{subject to} && \text{(4.25), (4.26) and } \begin{pmatrix} 1 & x_{0,0}^{0,0} \\ x_{0,0}^{0,0} & \mathrm{tr}M \end{pmatrix} \succeq 0, \end{aligned} \tag{4.33}$$

and

$$\begin{aligned} &\text{maximize} && \mathbf{1}^{\mathsf{T}} M \mathbf{1} \\ &\text{subject to} && \text{(4.25), (4.26) and } \mathrm{tr}M = 1. \end{aligned} \tag{4.34}$$

The idea behind variation (4.33) is that for a code C, setting

$$x_{i,j}^{t,p} := \lambda_{i,j}^{t,p} \cdot q^n (\gamma_{i,j}^{t,p})^{-1}, \tag{4.35}$$

we obtain a feasible solution with $x_{0,0}^{0,0} = |C|$ and $\mathrm{tr}M = |C|^2$. If $M' = \sum_{i,j,t,p} y_{i,j}^{t,p} M_{i,j}^{t,p}$ is a feasible solution to (4.33), then $M := (y_{0,0}^{0,0})^{-1} M'$ is a feasible solution to (4.32) with $\mathrm{tr}M = \mathrm{tr}M' \cdot (y_{0,0}^{0,0})^{-1} \geq y_{0,0}^{0,0}$. Conversely, if $M' = \sum_{i,j,t,p} y_{i,j}^{t,p} M_{i,j}^{t,p}$ is a feasible solution to

(4.32), then setting $x^{t,p}_{i,j} := y^{t,p}_{i,j} \cdot \mathrm{tr}M'$ gives a feasible solution to (4.33) with $x^{0,0}_{0,0} = 1 \cdot \mathrm{tr}M'$. Hence both semidefinite programs yield the same value.

The validity of variation (4.34) can be seen by setting $x^{t,p}_{i,j} := \lambda^{t,p}_{i,j} \cdot q^n(\gamma^{t,p}_{i,j})^{-1}|C|^{-2}$ for a given code C. Then $\mathrm{tr}M = 1$ and $\mathbf{1}^\mathsf{T} M \mathbf{1} = |C|$. For any feasible solution M' to (4.32), we have $\mathbf{1}^\mathsf{T} M' \mathbf{1} \geq (\mathrm{tr}M')^2$, hence $M := (\mathrm{tr}M')^{-1}M'$ is a feasible solution to (4.34) with $\mathbf{1}^\mathsf{T} M \mathbf{1} \geq \mathrm{tr}M'$. It follows that the optimum value in (4.34) is at least the optimum value in (4.32). We do not know if the reverse inequality holds.

4.2.2 A strengthening

It was observed by Laurent (see [28]) that not only is the matrix M'' defined in (4.14) positive semidefinite, also the following stronger property holds:

$$\begin{pmatrix} 1 - x^{0,0}_{0,0} & (\mathrm{diag}(M''))^\mathsf{T} \\ \mathrm{diag}(M'') & M'' \end{pmatrix} \quad \text{is positive semidefinite.} \tag{4.36}$$

This follows from the fact that for a code C and $\sigma \in \mathrm{Aut}(q,n)$ the matrix

$$\begin{pmatrix} 1 & (\chi^{\sigma C})^\mathsf{T} \\ \chi^{\sigma C} & \chi^{\sigma C}(\chi^{\sigma C})^\mathsf{T} \end{pmatrix} = \begin{pmatrix} 1 \\ \chi^{\sigma C} \end{pmatrix} \begin{pmatrix} 1 \\ \chi^{\sigma C} \end{pmatrix}^\mathsf{T} \quad \text{is positive semidefinite} \tag{4.37}$$

and the fact that semidefiniteness is preserved under taking nonnegative linear combinations. This yields the stronger semidefinite programming bound

$$\text{maximize } q^n \cdot x^{0,0}_{0,0} \quad \text{subject to (4.25), (4.26) and (4.36),} \tag{4.38}$$

where

$$M'' := \sum_{i,j,t,p} (x^{0,0}_{i+j-t-p,0} - x^{t,p}_{i,j}) M^{t,p}_{i,j}. \tag{4.39}$$

Observe that condition (4.36) can be checked in time polynomial in n by Theorem 5. The bound obtained is as least as good as the one obtained from (4.32). Indeed, given a feasible solution to (4.38), the matrix $M := M' + M''$ satisfies: $R(M)$ is positive semidefinite. Hence

$$q^n \mathrm{tr}M' = \mathbf{1}^\mathsf{T} M \mathbf{1} \geq \mathrm{tr}M^2 = (q^n \cdot x^{0,0}_{0,0})^2. \tag{4.40}$$

This implies that $N' := \frac{1}{x^{0,0}_{0,0}} M'$ is a feasible solution to (4.32) with $\mathrm{tr}N' \geq q^n \cdot x^{0,0}_{0,0}$. Hence the optimum in(4.38) is at most the optimum in (4.32). In the binary case, this yields an improved bound when $n = 25$ and $d = 6$. We did not find new improvements using this strengthening in the range $q = 3, n \leq 16$, $q = 4, n \leq 12$ or $q = 5, n \leq 11$.

4.3 Computational results

The semidefinite programming method was successfully applied to binary codes in [38] where a large number of upper bounds were improved. In this section we describe the computational results obtained in the nonbinary case. Apart from the binary case, tables of bounds on $A_q(n,d)$ are maintained for $q = 3, 4, 5$. We have limited the computations to

these three cases and computed the semidefinite programming bound for the range $n \leq 16$, $n \leq 12$ and $n \leq 11$, respectively. The instances in which we found an improvement over the best upper bound that was known, are summarized in Tables 4.1, 4.2 and 4.3 below. As a reference we have used the tables given by Brouwer, Hämäläinen, Östergård and Sloane [11] and by Bogdanova, Brouwer, Kapralov and Östergård [5] for the cases $q = 3$ and $q = 4$, along with subsequent improvements recorded on the website of Brouwer [9] and the table by Bogdanova and Östergård [6] for the case $q = 5$.

Table 4.1: New upper bounds on $A_3(n, d)$

n	d	best lower bound known	new upper bound	best upper bound previously known	Delsarte bound
12	4	4374	6839	7029	7029
13	4	8019	19270	19682	19683
14	4	24057	54774	59046	59049
15	4	72171	149585	153527	153527
16	4	216513	424001	434815	434815
12	5	729	1557	1562	1562
13	5	2187	4078	4163	4163
14	5	6561	10624	10736	10736
15	5	6561	29213	29524	29524
13	6	729	1449	1562	1562
14	6	2187	3660	3885	4163
15	6	2187	9904	10736	10736
16	6	6561	27356	29524	29524
14	7	243	805	836	836
15	7	729	2204	2268	2268
16	7	729	6235	6643	6643
13	8	42	95	103	103
15	8	243	685	711	712
16	8	297	1923	2079	2079
14	9	31	62	66	81
15	9	81	165	166	166
16	10	54	114	117	127

Table 4.2: New upper bounds on $A_4(n, d)$

n	d	best lower bound known	new upper bound	best upper bound previously known	Delsarte bound
7	4	128	169	179	179
8	4	320	611	614	614
9	4	1024	2314	2340	2340
10	4	4096	8951	9360	9362
10	5	1024	2045	2048	2145
10	6	256	496	512	512
11	6	1024	1780	2048	2048
12	6	4096	5864	6241	6241
12	7	256	1167	1280	1280

Table 4.3: New upper bounds on $A_5(n, d)$

n	d	best lower bound known	new upper bound	best upper bound previously known	Delsarte bound
7	4	250	545	554	625
7	5	53	108	125	125
8	5	160	485	554	625
9	5	625	2152	2291	2291
10	5	3125	9559	9672	9672
11	5	15625	44379	44642	44642
10	6	625	1855	1875	1875
11	6	3125	8840	9375	9375

Chapter 5

Covering codes

Consider the following combinatorial problem. Given integers q, n and r, what is the smallest number of Hamming spheres of radius r that cover the Hamming space consisting of all q-ary words of length n? This covering problem is the dual of the packing problem from the previous chapter. Apart from being an aesthetically appealing combinatorial problem, it has several technical applications, for example to write-once memories and data compression. Another, down to earth, application is to betting systems. In many countries a popular game is played that involves forecasting the outcomes of a set of n (football)matches. Each match can end in three ways: a loss, a tie or a win for the hosting club. The goal is to find an efficient set of bets that is guaranteed to have a forecast with at most one wrong outcome. For this reason the covering problem in the case $q = 3$ and $r = 1$ is widely known as the *football pool problem*, see [20].

In this chapter we show how the method of matrix cuts from Chapter 6 can be applied to obtain new lower bounds on the minimum size of covering codes. For a survey of results on covering codes as well as many applications, the reader is referred to [14].

5.1 Definitions and notation

Let $q \geq 2$ and $n \geq 1$ be integers. Let $\mathbb{E} := \mathbf{q}^n$ be the Hamming space consisting of all words of length n over the alphabet $\mathbf{q} := \{0, 1, \ldots, q-1\}$. Recall that the Hamming distance $d(\mathbf{u}, \mathbf{v})$ of two words $\mathbf{u}, \mathbf{v} \in \mathbb{E}$ is defined as the number of positions in which $\mathbf{u}$ and $\mathbf{v}$ differ. We define $\overline{d}(\mathbf{u}, \mathbf{v}) := (i, j, t)$ where $i = d(\mathbf{u}, \mathbf{0})$, $j = d(\mathbf{v}, \mathbf{0})$ and $2t = i + j - d(\mathbf{u}, \mathbf{v})$. For a word $\mathbf{u} \in \mathbb{E}$, we denote the *support* of $\mathbf{u}$ by $S(\mathbf{u}) := \{i \mid \mathbf{u}_i \neq 0\}$. Note that $|S(\mathbf{u})| = d(\mathbf{u}, \mathbf{0})$, where $\mathbf{0}$ is the all-zero word. Denote by

$$\begin{aligned} B_r(\mathbf{u}) &:= \{\mathbf{v} \in \mathbb{E} \mid d(\mathbf{u}, \mathbf{v}) \leq r\} \quad \text{and} \\ S_r(\mathbf{u}) &:= \{v \in \mathbb{E} \mid d(\mathbf{u}, \mathbf{v}) = r\} \end{aligned} \tag{5.1}$$

the ball and the sphere respectively, with center $\mathbf{u} \in \mathbb{E}$ and radius r. They are generally referred to as the *Hamming sphere* and the *Hamming ring* with center $\mathbf{u}$ and radius r in the literature. The *covering radius* of a code $C \subseteq E$ is the smallest integer r for which

$$\bigcup_{\mathbf{u} \in C} B_r(\mathbf{u}) = \mathbb{E}. \tag{5.2}$$

A code $C \subseteq \mathbb{E}$ is called an $(n, K, q)r$ code if $|C| = K$ and the covering radius of C is r. We denote

$$K_q(n, r) := \min\{K \mid \text{there exists an } (n, K, q)r \text{ code}\}. \tag{5.3}$$

In this chapter we will be interested in lower bounds on $K_q(n, r)$.

5.2 Method of linear inequalities

An important tool used in deriving lower bounds on $K_q(n, r)$ is the method of linear inequalities. Let $C \subseteq \mathbb{E}$ be a code and denote

$$A_i(\mathbf{u}) := |C \cap S_i(\mathbf{u})| \tag{5.4}$$

for $\mathbf{u} \in \mathbb{E}$ and $i = 0, \ldots, n$. We consider linear inequalities of a code. That is, valid inequalities of the form

$$\sum_{i=0}^{n} \lambda_i A_i(\mathbf{u}) \geq \beta \quad \text{for all } \mathbf{u} \in \mathbb{E}, \tag{5.5}$$

where $\lambda_0, \ldots, \lambda_n \geq 0$ and $\beta > 0$. Such a set of inequalities is denoted by $(\lambda_0, \ldots, \lambda_n)\beta$ and leads to a lower bound on $K_q(n, r)$ by the following proposition.

Proposition 27. *If any $(n, K, q)r$ code satisfies $(\lambda_0, \ldots, \lambda_n)\beta$ then*

$$K \geq \frac{\beta q^n}{\sum_{i=0}^{n} \lambda_i \binom{n}{i} (q-1)^i}. \tag{5.6}$$

Proof. Summing 5.5 over all $\mathbf{u} \in \mathbb{E}$ we obtain

$$\begin{aligned} \beta q^n \leq \sum_{\mathbf{u} \in \mathbb{E}} \sum_{i=0}^{n} \lambda_i A_i(\mathbf{u}) &= \sum_{i=0}^{n} \lambda_i \sum_{\mathbf{u} \in \mathbb{E}} A_i(\mathbf{u}) \\ &= \sum_{i=0}^{n} \lambda_i \sum_{\mathbf{v} \in C} |S_i(\mathbf{v})| \\ &= |C| \sum_{i=0}^{n} \lambda_i \binom{n}{i} (q-1)^i. \end{aligned} \tag{5.7}$$

□

The basic *sphere covering inequalities*

$$\sum_{i=0}^{r} A_i(\mathbf{u}) \geq 1 \quad \text{for all } \mathbf{u} \in \mathbb{E} \tag{5.8}$$

give the *sphere covering bound*

$$K_q(n, r) \geq \frac{q^n}{\sum_{i=0}^{r} \binom{n}{i} (q-1)^i}. \tag{5.9}$$

Many other valid inequalities have been obtained, in particular in the binary case ($q = 2$), by studying the way the elements in $B_s(\mathbf{u})$ can be covered for $s = 1, 2, 3$. In the case $s = 1$ this gives the van Wee inequalities [44]:

$$\sum_{i=0}^{r-1} \left\lceil \frac{n+1}{r+1} \right\rceil A_i(\mathbf{u}) + A_r(\mathbf{u}) + A_{r+1}(\mathbf{u}) \geq \left\lceil \frac{n+1}{r+1} \right\rceil \tag{5.10}$$

which improve upon the sphere covering bound whenever $r + 1$ does not divide $n + 1$.

The case $s = 2$ leads to the *pair covering inequalities* found by Johnson [23] and Zhang [46]:

$$\sum_{i=0}^{r-2} m_0 A_i(\mathbf{u}) + m_1(A_{r-1}(\mathbf{u}) + A_r(\mathbf{u})) + A_{r+1}(\mathbf{u}) + A_{r+2}(\mathbf{u}) \geq m_0, \tag{5.11}$$

where

$$\begin{aligned} m_1 &= \max_{i \geq 2} \tfrac{F(n-r+1,r+2)-F(n-iR+1,R+2)}{i-1}, \\ m_0 &= m_1 + F(n-r+1, r+2), \end{aligned} \tag{5.12}$$

and $F(m, k)$ is the minimum number of k-sets needed to cover all pairs of an m-set. Other inequalities can be found in [47].

Starting from a set of inequalities for a code, new inequalities can be obtained by taking nonnegative linear combinations. Also by summing the inequality $(\lambda_0, \ldots, \lambda_n)\beta$ over $S_i(\mathbf{u})$, we obtain the *induced* inequality $(\lambda'_0, \ldots, \lambda'_n)\beta'$, where

$$\begin{aligned} \lambda'_k &:= \sum_{j=0}^{n} \lambda_j \alpha_{i,j}^k \\ \beta' &:= \binom{n}{i} (q-1)^i \beta, \end{aligned} \tag{5.13}$$

and

$$\alpha_{i,j}^k := |\{\mathbf{v} \mid d(\mathbf{0}, \mathbf{v}) = i, d(\mathbf{v}, \mathbf{u}) = j\}| \tag{5.14}$$

when $d(\mathbf{0}, \mathbf{u}) = k$. The numbers $\alpha_{i,j}^k$ can be expressed as

$$\alpha_{i,j}^k = \begin{cases} \sum_{\substack{p,t \\ t+p=k+i-j}} \binom{k}{t-p,p} \binom{n-k}{i-t} (q-1)^{i-t}(q-2)^{t-p} & \text{if } q \geq 3 \\ \sum_{\substack{t \\ 2t=k+i-j}} \binom{k}{t} \binom{n-k}{i-t} & \text{if } q = 2. \end{cases} \tag{5.15}$$

Note that the bound obtained from an induced inequality is equal to the bound obtained from the original one. Using the fact that the $A_i(\mathbf{u})$ are integers, the inequality $(\lambda_0, \ldots, \lambda_n)\beta$ implies the inequality $(\lceil \lambda_0 \rceil, \ldots, \lceil \lambda_n \rceil) \lceil \beta \rceil$. This way the van Wee inequalities, for example, can be derived from the sphere covering inequalities as follows. Starting from the sphere covering inequalities, we obtain

$$\sum_{i=0}^{r-1} (n+1) A_i(\mathbf{u}) + (r+1)(A_r(\mathbf{u}) + A_{r+1}(\mathbf{u})) \geq n+1 \quad \text{for every } \mathbf{u} \in \mathbb{E} \tag{5.16}$$

by summing the sphere covering inequalities over $B_1(\mathbf{u})$. Then dividing by $r+1$ and rounding up the coefficients, the van Wee inequalities are obtained.

Using this method, Habsieger and Plagne obtained many new lower bounds in the binary and ternary case, by computer search see [19].

5.3 Semidefinite programming bounds

The bound from Proposition 27 may be viewed as a linear programming bound as follows. Given $\lambda \in \mathbb{R}^{n+1}$ and $\beta \in \mathbb{R}$, define the polyhedron

$$P_{\lambda,\beta} := \{x \in \mathbb{R}^{\mathbb{E}} \mid \sum_{i=0}^{n} \lambda_i x(S_i(\mathbf{u})) \geq \beta \quad \text{for all } \mathbf{u} \in \mathbb{E}\ \}. \tag{5.17}$$

We have the following proposition.

Proposition 28.

$$\min\{\mathbf{1}^{\mathsf{T}} x \mid x \in P_{\lambda,\beta}\} = \frac{\beta q^n}{\sum_{i=0}^{n} \lambda_i \binom{n}{i} (q-1)^i}. \tag{5.18}$$

Proof. Observe that for any $x \in P_{\lambda,\beta}$ also

$$\overline{x} := \frac{1}{|\mathrm{Aut}(q,n)|} \sum_{\sigma \in \mathrm{Aut}(q,n)} \sigma(x) \in P_{\lambda,\beta} \tag{5.19}$$

and $\overline{x} = c\mathbf{1}$ where $\mathbf{1}^{\mathsf{T}} c\mathbf{1} = \mathbf{1}^{\mathsf{T}} x$. Hence

$$\begin{aligned} \min\{\mathbf{1}^{\mathsf{T}} x \mid x \in P_{\lambda,\beta}\} &= \min\{\mathbf{1}^{\mathsf{T}} c\mathbf{1} \mid c\mathbf{1} \in P_{\lambda,\beta}\} \\ &= \min\{q^n c \mid \sum_{i=0}^{n} \lambda_i c |S_i(\mathbf{0})| \geq \beta\} \\ &= \min\{q^n c \mid c \geq \frac{\beta}{\sum_{i=0}^{n} \lambda_i \binom{n}{i} (q-1)^i}\} \\ &= \frac{\beta q^n}{\sum_{i=0}^{n} \lambda_i \binom{n}{i} (q-1)^i}. \end{aligned} \tag{5.20}$$

□

Clearly, replacing $P_{\lambda,\beta}$ by $P_{\lambda,\beta} \cap \{0,1\}^{\mathbb{E}}$ and considering the 0–1 optimization problem, can be expected to give a better lower bound. In fact, when $(\lambda_0, \ldots, \lambda_n)\beta$ corresponds to the sphere covering inequalities, this 0–1 program gives the exact value $K_q(n,r)$[1]. This motivates to replace the linear relaxation $P_{\lambda,\beta}$ by a tighter (semidefinite) relaxation using the method of matrix cuts from Chapter 6. We will pursue this idea in the following.

[1] In general there may be solutions that do not have covering radius $\leq r$, for example when $n = 3, r = 1$, the code $\{100, 010, 001\}$ has covering radius 2 but satisfies the van Wee inequalities.

5.3.1 The first SDP bound

In this section we derive a semidefinite programming lower bound on $K_q(n,r)$ with $O(n)$ variables and $O(n)$ constraints. This bound is equal to the value obtained by minimizing $\mathbf{1}^\mathsf{T} x$ over $N_+(P_{\lambda,\beta})$, see Chapter 6.

To any code $C \subseteq \mathbb{E}$, we associate the symmetric 0–1 matrix M_C defined by:

$$(M_C)_{\mathbf{u},\mathbf{v}} := \begin{cases} 1 & \text{if } \mathbf{u},\mathbf{v} \in C, \\ 0 & \text{otherwise.} \end{cases} \tag{5.21}$$

Let $C \subseteq E$ be a code. Define the matrix

$$M := |\mathrm{Aut}(q,n)|^{-1} \sum_{\sigma \in \mathrm{Aut}(q,n)} M_{\sigma C}. \tag{5.22}$$

By construction, the matrix M is invariant under permutations of the rows and columns by any $\sigma \in \mathrm{Aut}(q,n)$. Hence M is an element of the Bose–Mesner algebra of the Hamming scheme and we write

$$M = \sum_{i=0}^{n} x_i A_i, \tag{5.23}$$

where A_i is the i-th basis matrix of the Bose–Mesner algebra and $x_0, \ldots, x_n \in \mathbb{R}$.

Proposition 29. *The matrix M satisfies the following.*

$$\begin{aligned} &\text{(i)} && \mathrm{tr}M = |C|, \\ &\text{(ii)} && M \geq 0 \text{ and } R(M) \succeq 0, \\ &\text{(iii)} && \text{If } C \text{ satisfies } (\lambda_0, \ldots, \lambda_n)\beta, \text{ then} \\ & && M_{\mathbf{u}} \in M_{\mathbf{u},\mathbf{u}} P_{\lambda,\beta} \quad \text{and} \quad \mathrm{diag}(M) - M_{\mathbf{u}} \in (1 - M_{\mathbf{u},\mathbf{u}}) P_{\lambda,\beta} \\ & && \text{for every } \mathbf{u} \in \mathbb{E}. \end{aligned} \tag{5.24}$$

Proof. Since M is a convex combination of the $M_{\sigma C}$, $\sigma \in \mathrm{Aut}(q,n)$, it suffices to observe that the contraints hold for each $M_{\sigma C}$. Clearly, $\mathrm{tr}M_{\sigma C} = |C|$ and $M_{\sigma C} \geq 0$. As $R(M_{\sigma C}) = \binom{1}{\chi^{\sigma C}}\binom{1}{\chi^{\sigma C}}^\mathsf{T}$, $R(M_{\sigma C})$ is positive semidefinite. Finally, for any $\mathbf{u} \in \mathbb{E}$

$$(M_{\sigma C})_{\mathbf{u}} = (M_{\sigma C})_{\mathbf{u},\mathbf{u}} \chi^{\sigma C} \tag{5.25}$$

and

$$\mathrm{diag}(M_{\sigma C}) - (M_{\sigma C})_{\mathbf{u}} = (1 - (M_{\sigma C})_{\mathbf{u},\mathbf{u}}) \chi^{\sigma C} \tag{5.26}$$

and hence (iii) follows from the fact that σC satisfies $(\lambda_0, \ldots, \lambda_n)\beta$ for every $\sigma \in \mathrm{Aut}(q,n)$. □

Below, we will make these constraints more explicit by expressing them in terms of the variables x_i.

Proposition 30. *$R(M) \succeq 0$ is equivalent to*

$$\sum_{i=0}^{n} x_i P_j(i) \geq 0 \quad \textit{for every } j = 0, \ldots, n \tag{5.27}$$

and

$$\begin{pmatrix} q^n & q^n x_0 \\ q^n x_0 & \sum_{i=0}^{n} x_i \binom{n}{i} (q-1)^i \end{pmatrix} \succeq 0.$$

Proof. Since $\mathrm{tr} M = q^n x_0$ and $\mathbf{1}^{\mathsf{T}} M \mathbf{1} = q^n \sum_{i=0}^{n} x_i \binom{n}{i} (q-1)^i$, it follows from Proposition 7 that $R(M) \succeq 0$ if and only if $M \succeq 0$ and

$$\begin{pmatrix} q^n & q^n x_0 \\ q^n x_0 & \sum_{i=0}^{n} x_i \binom{n}{i} (q-1)^i \end{pmatrix}$$

is positive semidefinite. By Proposition 23 it follows that $M = \sum_{i=0}^{n} x_i A_i$ is positive semidefinite if and only if $\sum_{i=0}^{n} x_i P_j(i) \geq 0$ for every $j = 0, \ldots, n$. □

Proposition 31. *Let $x = \sum_{i=0}^{n} x_i \chi^{S_i(\mathbf{0})} \in \mathbb{R}^{\mathbb{E}}$. Then the following are equivalent:*

$$\text{(i)} \quad \sum_{i=0}^{n} \lambda_i x(S_i(\mathbf{u})) \geq \beta \quad \textit{for every } \mathbf{u} \in \mathbb{E}, \tag{5.28}$$

$$\text{(ii)} \quad \sum_{j=0}^{n} x_j \cdot \sum_{i=0}^{n} \lambda_i \alpha_{i,j}^k \geq \beta \quad \textit{for every } k = 0, \ldots, n.$$

Proof. If $d(\mathbf{u}, \mathbf{0}) = k$ then

$$\begin{aligned} \sum_{i=0}^{n} \lambda_i x(S_i(\mathbf{u})) &= \sum_{i=0}^{n} \lambda_i \sum_{j=0}^{n} \sum_{\substack{\mathbf{v} \in \mathbb{E} \\ d(\mathbf{0},\mathbf{v})=j \\ d(\mathbf{u},\mathbf{v})=i}} x_j \\ &= \sum_{i=0}^{n} \lambda_i \sum_{j=0}^{n} \alpha_{i,j}^k x_j \\ &= \sum_{j=0}^{n} x_j \sum_{i=0}^{n} \lambda_i \alpha_{i,j}^k. \end{aligned} \tag{5.29}$$

□

Proposition 32. *The following are equivalent*

$$\begin{aligned} &\text{(i)} \quad M_{\mathbf{u}} \in M_{\mathbf{u},\mathbf{u}} P_{\lambda,\beta} \quad \textit{and} \\ &\qquad \mathrm{diag}(M) - M_{\mathbf{u}} \in (1 - M_{\mathbf{u},\mathbf{u}}) P_{\lambda,\beta} \\ &\qquad \textit{for every } \mathbf{u} \in \mathbb{E}, \end{aligned} \tag{5.30}$$

$$\begin{aligned} &\text{(ii)} \quad \sum_{j=0}^{n} x_j \cdot \sum_{i=0}^{n} \lambda_i \alpha_{i,j}^k \geq x_0 \beta \\ &\qquad \sum_{j=0}^{n} (x_0 - x_j) \cdot \sum_{i=0}^{n} \lambda_i \alpha_{i,j}^k \geq (1 - x_0) \beta \\ &\qquad \textit{for every } k = 0, \ldots, n. \end{aligned} \tag{5.31}$$

Proof. Directly from Proposition 31 □

Collecting all the propositions, we obtain the following theorem.

Theorem 7. *If every code $C \subseteq \mathbb{E}$ with covering radius r satisfies $(\lambda_0, \ldots, \lambda_n)\beta$, we have*

$$K_q(n, r) \geq \min_x q^n x_0, \tag{5.32}$$

where the minimum ranges over all $x = (x_0, x_1, \ldots, x_n)^{\mathsf{T}} \in \mathbb{R}^{n+1}$ satisfying

$$\begin{aligned}
&\text{(i)} && x_k \geq 0, \\
&\text{(ii)} && \sum_{i=0}^{n} x_i P_k(i) \geq 0, \\
&\text{(iii)} && \sum_{i=0}^{n} x_i \cdot \sum_{j=0}^{n} \lambda_j \alpha_{i,j}^k \geq \beta x_0, \\
&\text{(iv)} && \sum_{i=0}^{n} (x_0 - x_i) \cdot \sum_{j=0}^{n} \lambda_j \alpha_{i,j}^k \geq \beta(1 - x_0), \\
&\text{(v)} && \begin{pmatrix} q^n & q^n x_0 \\ q^n x_0 & \sum_{i=0}^{n} x_i \binom{n}{i} (q-1)^i \end{pmatrix} \succeq 0
\end{aligned} \tag{5.33}$$

for all $k = 0, \ldots, n$.

Proof. □

Observe that if we relax the semidefinite program by only requiring M to be positive semidefinite instead of $R(M)$ (that is: delete condition (v)), we obtain for a linear program in $O(n)$ variables and inequalities that is a lower bound on $K_q(n, r)$.

5.3.2 The second SDP bound

In this section we describe a stronger semidefinite programming relaxation that uses more of the symmetry of the Hamming space, but requires $O(n^3)$ variables in the binary case and $O(n^4)$ variables in the nonbinary case. In this section we will focus on the binary case. The nonbinary case is very similar, although more complicated and it will be adressed in the next section.

Restricting ourselves to the binary case, we have $\mathbb{E} = \{0, 1\}^n$, the n-dimensional Hamming cube. Let $C \subseteq \mathbb{E}$ be any code and define the matrices M' and M'' by:

$$\begin{aligned}
M' &:= |\mathrm{Aut}(2, n)|^{-1} \sum_{\substack{\sigma \in \mathrm{Aut}(2,n) \\ \mathbf{0} \in \sigma C}} M_{\sigma C} \\
M'' &:= |\mathrm{Aut}(2, n)|^{-1} \sum_{\substack{\sigma \in \mathrm{Aut}(2,n) \\ \mathbf{0} \notin \sigma C}} M_{\sigma C}.
\end{aligned} \tag{5.34}$$

By construction, the matrices M' and M'' are invariant under permutations $\sigma \in \mathrm{Aut}_{\mathbf{0}}(2,n)$ of the rows and columns, that fix the element $\mathbf{0}$. Hence M' and M'' are elements of the algebra $\mathcal{A}_{2,n}$. Write

$$M' = \sum_{(i,j,t)} x_{i,j}^t M_{i,j}^t, \tag{5.35}$$

where the matrices $M_{i,j}^t$ are the zero–one basis matrices of $\mathcal{A}_{2,n}$. The matrix M'' can be expressed in terms of the coefficients $x_{i,j}^t$ as follows.

Proposition 33. *The matrix M'' satisfies*

$$M'' = \sum_{(i,j,t)} (x_{i+j-2t,0}^{0,0} - x_{i,j}^t) M_{i,j}^t. \tag{5.36}$$

Proof. The matrix

$$M := M' + M'' = |\mathrm{Aut}(2,n)|^{-1} \sum_{\sigma \in \mathrm{Aut}(2,n)} M_{\sigma C} \tag{5.37}$$

is invariant under permutation of the rows and columns by any permutation $\sigma \in \mathrm{Aut}(2,n)$, and hence is an element of the Bose–Mesner algebra, say

$$M = \sum_k y_k A_k. \tag{5.38}$$

Observe that for any $\mathbf{u} \in \mathbb{E}$ with $d(\mathbf{u},\mathbf{0}) = k$, we have

$$y_k = (M)_{\mathbf{u},\mathbf{0}} = (M')_{\mathbf{u},\mathbf{0}} = x_{k,0}^0, \tag{5.39}$$

since $(M'')_{\mathbf{u},\mathbf{0}} = 0$. Hence we have

$$\begin{aligned} M'' &= M - M' \\ &= \sum_k x_{k,0}^0 A_k - \sum_{(i,j,t)} x_{i,j}^t M_{i,j}^t \\ &= \sum_k \sum_{i+j-2t=k} x_{k,0}^0 M_{i,j}^t - \sum_{(i,j,t)} x_{i,j}^t M_{i,j}^t \\ &= \sum_{(i,j,t)} (x_{i+j-2t,0}^0 - x_{i,j}^t) M_{i,j}^t, \end{aligned} \tag{5.40}$$

which proves the proposition. □

Proposition 34. *The matrices*

$$M' \quad \textit{and} \quad \begin{pmatrix} 1 - x_{0,0}^0 & (\mathrm{diag}(M''))^{\mathsf{T}} \\ \mathrm{diag}(M'') & M'' \end{pmatrix} \tag{5.41}$$

are positive semidefinite.

Proof. Clearly, $R(M_{\sigma C}) = \binom{1}{\chi^{\sigma C}}\binom{1}{\chi^{\sigma C}}^{\mathsf{T}}$ is positive semidefinite for each $\sigma \in \mathrm{Aut}(2,n)$. Hence $R((x^0_{0,0})^{-1}M')$ and $R((1-x^0_{0,0})^{-1}M'')$ are positive semidefinite as they are convex combinations of the $R(M_{\sigma C})$. This implies the statement in the proposition. □

Using the block diagonalisation of $\mathcal{A}_{2,n}$, Proposition 34 is equivalent to the following matrices being positive semidefinite

$$\left(\sum_{t=0}^{n}\beta^t_{i,j,k}x^t_{i,j}\right)^{n-k}_{i,j=k}, \quad \left(\sum_{t=0}^{n}\beta^t_{i,j,k}(x^0_{i+j-2t,0}-x^t_{i,j})\right)^{n-k}_{i,j=k}$$

for each $k = 1,\dots,\lfloor\frac{n}{2}\rfloor$,

$$\left(\sum_{t=0}^{n}\beta^t_{i,j,0}x^t_{i,j}\right)^{n}_{i,j=0}, \quad \begin{pmatrix}1-x^0_{0,0} & x^{\mathsf{T}}\\ x & L\end{pmatrix} \succeq 0$$

where

$$L := \left(\sum_{t=0}^{n}\beta^t_{i,j,0}(x^0_{i+j-2t,0}-x^t_{i,j})\right)^{n}_{i,j=0},$$
$$x_i := (x^0_{0,0}-x^0_{i,0})\binom{n}{i}, \text{ for } i = 0,\dots,n.$$

Proposition 35. *The coefficients $x^t_{i,j}$ satisfy the following:*

$$2^n x^0_{0,0} = |C|, \tag{5.42}$$

and for any i,j,t

$$\begin{aligned}
&\text{(i)} && 0 \le x^t_{i,j} \le x^i_{i,i}, \\
&\text{(ii)} && x^0_{i,0}+x^0_{i+j-2t,0}-x^0_{0,0} \le x^t_{i,j} \le x^0_{i+j-2t,0}, \\
&\text{(iii)} && x^t_{i,j} = x^{t'}_{i',j'} \quad \textit{if } (i,j,i+j-2t) \textit{ is a permutation} \\
& && \textit{of } (i',j',i'+j'-2t').
\end{aligned} \tag{5.43}$$

Proof. Since for any $\mathbf{u} \in \mathbb{E}$

$$|\{\sigma \in \mathrm{Aut}(2,n) \mid \sigma\mathbf{u} = \mathbf{0}\}| = |\mathrm{Aut}_{\mathbf{0}}(2,n)|, \tag{5.44}$$

we obtain

$$x^0_{0,0} = \frac{|\{\sigma \in \mathrm{Aut}(2,n) \mid \mathbf{0} \in \sigma C\}|}{|\mathrm{Aut}(2,n)|} = |C|\frac{|\mathrm{Aut}_{\mathbf{0}}(2,n)|}{|\mathrm{Aut}(2,n)|} = 2^{-n}|C|. \tag{5.45}$$

Inequalities (i) and (ii) follow from the fact that $(M')_{\mathbf{u},\mathbf{u}} \ge (M')_{\mathbf{u},\mathbf{v}}$ and $(M'')_{\mathbf{u},\mathbf{u}} \ge (M'')_{\mathbf{u},\mathbf{v}}$ for any $\mathbf{u},\mathbf{v} \in \mathbb{E}$ respectively. The truth of (iii) can be seen as follows. Let $\mathbf{u},\mathbf{v} \in \mathbb{E}$ be such that $\overline{d}(\mathbf{u},\mathbf{v}) = (i,j,t)$ and let (i',j',t') be such that $(i,j,i+j-2t)$ is a permutation of $(i',j',i'+j'-2t')$. It can be seen that in that case there is a $\sigma \in \mathrm{Aut}(2,n)$ such that $\sigma\{\mathbf{0},\mathbf{u},\mathbf{v}\} = \{\mathbf{0},\mathbf{u}',\mathbf{v}'\}$ with $\overline{d}(\mathbf{u}',\mathbf{v}') = (i',j',t')$. Hence

$$x^t_{i,j} = (M')_{\mathbf{u},\mathbf{v}} = (M')_{\mathbf{u}',\mathbf{v}'} = x^{t'}_{i',j'}. \tag{5.46}$$

□

Given two words $\mathbf{u}, \mathbf{v} \in \mathbb{E}$ with $\overline{d}(\mathbf{u}, \mathbf{v}) = (i, j, t)$, we denote by $\alpha^{(i,j,t)}_{(i,j',t'),d}$ the number of words $\mathbf{w} \in \mathbb{E}$ with $\overline{d}(\mathbf{u}, \mathbf{w}) = (i, j', t')$ and $d(\mathbf{v}, \mathbf{w}) = d$. This number is well-defined, and indeed we have the following proposition.

Proposition 36. *The numbers $\alpha^{(i,j,t)}_{(i,j',t'),d}$ are given by*

$$\alpha^{(i,j,t)}_{(i,j',t'),d} = \sum_{a_{00},a_{01},a_{10},a_{11}} \binom{i-t}{a_{10}} \binom{j-t}{a_{01}} \binom{t}{a_{11}} \binom{n+t-i-j}{a_{00}}, \tag{5.47}$$

where the indices a_{00}, a_{01}, a_{10} and a_{11} range over the nonnegative integers that satisfy

$$\begin{aligned} j' &= a_{00} + a_{01} + a_{10} + a_{11} \\ t' &= a_{10} + a_{11} \\ d - j &= a_{00} + a_{10} - a_{01} - a_{11}. \end{aligned} \tag{5.48}$$

Proof. Partition the support of the words $\mathbf{w}$ into four sets A_{00}, A_{01}, A_{10} and A_{11} as follows:

$$\begin{aligned} A_{00} &:= \{k \in S(\mathbf{w}) \mid \mathbf{u}_k = 0, \mathbf{v}_k = 0\} \\ A_{01} &:= \{k \in S(\mathbf{w}) \mid \mathbf{u}_k = 0, \mathbf{v}_k \neq 0\} \\ A_{10} &:= \{k \in S(\mathbf{w}) \mid \mathbf{u}_k \neq 0, \mathbf{v}_k = 0\} \\ A_{11} &:= \{k \in S(\mathbf{w}) \mid \mathbf{u}_k \neq 0, \mathbf{v}_k \neq 0\}. \end{aligned} \tag{5.49}$$

If we denote the sizes of these four sets by a_{00}, a_{01}, a_{10} and a_{11} respectively, we obtain the claimed result by summing over all possible sets A_{00}, A_{01}, A_{10} and A_{11}. □

Proposition 37. *Let $\mathbf{u} \in \mathbb{E}$ be a word with $d(\mathbf{u}, \mathbf{0}) = i$ and let $x \in \mathbb{R}^{\mathbb{E}}$ be such that $x_{\mathbf{v}}$ only depends on $\overline{d}(\mathbf{u}, \mathbf{v})$, say $x_{\mathbf{v}} = x^t_{i,j}$, when $\overline{d}(\mathbf{u}, \mathbf{v}) = (i, j, t)$. Then*

$$\sum_{d=0}^{n} \lambda_d x(S_d(\mathbf{v})) \geq \beta \quad \textit{for all } \mathbf{v} \in \mathbb{E} \tag{5.50}$$

is equivalent to

$$\sum_{j',t'} x^{t'}_{i,j'} \cdot \sum_{d=0}^{n} \lambda_d \alpha^{(i,j,t)}_{(i,j',t'),d} \geq \beta \quad \textit{for all } j, t. \tag{5.51}$$

Proof. Let $\mathbf{v} \in \mathbb{E}$ and let $\overline{d}(\mathbf{u}, \mathbf{v}) = (i, j, t)$. Then we have the following equalities.

$$\begin{aligned} \sum_{d=0}^{n} \lambda_d x(S_d(\mathbf{v})) &= \sum_{d=0}^{n} \lambda_d \sum_{\substack{\mathbf{w} \in \mathbb{E} \\ d(\mathbf{v},\mathbf{w}) = d}} x_{\mathbf{w}} \\ &= \sum_{d=0}^{n} \lambda_d \sum_{j',t'} \sum_{\substack{\mathbf{w} \in \mathbb{E} \\ d(\mathbf{v},\mathbf{w}) = d) \\ \overline{d}(\mathbf{u},\mathbf{w}) = (i,j',t')}} x_{\mathbf{w}} \\ &= \sum_{d=0}^{n} \lambda_d \sum_{j',t'} \alpha^{(i,j,t)}_{(i,j',t'),d} x^{t'}_{i,j'} \\ &= \sum_{j',t'} x^{t'}_{i,j'} \cdot \sum_{d=0}^{n} \lambda_d \alpha^{(i,j,t)}_{(i,j',t'),d}. \end{aligned} \tag{5.52}$$

□

Proposition 38. *If the code C satisfies the set of inequalities $(\lambda_0, \ldots, \lambda_n)\beta$, then the variables $x^t_{i,j}$ satisfy the following set of inequalities. For every tuple (i, j, t)*

$$\begin{aligned}
\sum_{j',t'} x^{t'}_{i,j'} \cdot \lambda^{i,j,t}_{j',t'} &\geq x^0_{i,0}\beta \qquad (5.53)\\
\sum_{j',t'} (x^0_{j',0} - x^{t'}_{i,j'}) \cdot \lambda^{i,j,t}_{j',t'} &\geq (x^0_{0,0} - x^0_{i,0})\beta\\
\sum_{j',t'} (x^0_{i+j-2t,0} - x^t_{i,j}) \cdot \lambda^{i,j,t}_{j',t'} &\geq (x^0_{0,0} - x^0_{i,0})\beta\\
\sum_{j',t'} (x^0_{0,0} - x^0_{j',0} - x^0_{i+j'-2t',0} + x^{t'}_{i,j'}) \cdot \lambda^{i,j,t}_{j',t'} &\geq (1 - 2x^0_{0,0} + x^0_{i,0})\beta,
\end{aligned}$$

where we use the shorthand notation

$$\lambda^{i,j,t}_{j',t'} := \sum_{d=0}^{n} \lambda_d \alpha^{(i,j,t)}_{(i,j',t'),d}. \qquad (5.54)$$

Proof. For any $\sigma \in \mathrm{Aut}(2, n)$, the matrix $M := M_{\sigma C}$ satisfies

$$\begin{aligned}
M_{\mathbf{u}} &\in M_{\mathbf{u},\mathbf{u}} P_{\lambda,\beta}, \qquad (5.55)\\
\mathrm{diag}(M) - M_{\mathbf{u}} &\in (1 - M_{\mathbf{u},\mathbf{u}}) P_{\lambda,\beta}\\
\text{for every } \mathbf{u} &\in \mathbb{E}.
\end{aligned}$$

This implies that also the matrices $\frac{1}{x^0_{0,0}} M'$ and $\frac{1}{1-x^0_{0,0}} M''$ satisfy (5.55) as they are convex combinations of the matrices $M_{\sigma C}$. Now using Proposition 37 gives a proof of the claim. □

This leads to the following semidefinite programming bound on $K_2(n, r)$.

Theorem 8. *If any code $C \subseteq \mathbb{E}$ with covering radius r satisfies $(\lambda_0, \ldots, \lambda_n)\beta$, we have*

$$K_2(n, r) \geq \min_x 2^n x^0_{0,0}, \qquad (5.56)$$

where the minimum ranges over all $x = (x^t_{i,j})$ satisfying (5.42), (5.43) and (5.53).

Proof. □

5.4 Nonbinary case

In this section we consider the nonbinary case, that is $q \geq 3$. The nonbinary case is very similar to the binary case described in the previous section and we will skip some of the details in the proofs.

Again define the matrices M' and M'' by

$$\begin{aligned} M' &:= |\mathrm{Aut}(2,n)|^{-1} \sum_{\substack{\sigma \in \mathrm{Aut}(2,n) \\ \mathbf{0} \in \sigma C}} M_{\sigma C} \\ M'' &:= |\mathrm{Aut}(2,n)|^{-1} \sum_{\substack{\sigma \in \mathrm{Aut}(2,n) \\ \mathbf{0} \notin \sigma C}} M_{\sigma C}. \end{aligned} \tag{5.57}$$

The matrices M' and M'' are invariant under permutations of the rows and columns by permutations $\sigma \in \mathrm{Aut}_{\mathbf{0}}(q,n)$. Hence M' and M'' are elements of the algebra $\mathcal{A}_{q,n}$. We write

$$M' = \sum_{(i,j,t,p)} x_{i,j}^{t,p} M_{i,j}^{t,p} \tag{5.58}$$

where the $M_{i,j}^{t,p}$ are the 0–1 basis matrices of the algebra $\mathcal{A}_{q,n}$. The matrix M'' can be expressed in terms of the coefficients $x_{i,j}^{t,p}$ as follows.

Proposition 39. *The matrix M'' is given by*

$$M'' = \sum_{(i,j,t,p)} (x_{i+j-t-p,0}^{0,0} - x_{i,j}^{t,p}) M_{i,j}^{t,p}. \tag{5.59}$$

Proof. The matrix

$$M := M' + M'' = |\mathrm{Aut}(q,n)|^{-1} \sum_{\sigma \in \mathrm{Aut}(q,n)} M_{\sigma C} \tag{5.60}$$

is invariant under permutation of the rows and columns by permutations $\sigma \in \mathrm{Aut}(q,n)$, and hence is an element of the Bose–Mesner algebra, say

$$M = \sum_k y_k A_k. \tag{5.61}$$

Note that for any $\mathbf{u} \in \mathbb{E}$ with $|S(\mathbf{u})| = k$, we have

$$y_k = (M)_{\mathbf{u},\mathbf{0}} = (M')_{\mathbf{u},\mathbf{0}} = x_{k,0}^{0,0}, \tag{5.62}$$

since $(M'')_{\mathbf{u},\mathbf{0}} = 0$. Hence we have

$$\begin{aligned} M'' &= M - M' \\ &= \sum_k x_{k,0}^{0,0} A_k - \sum_{(i,j,t,p)} x_{i,j}^{t,p} M_{i,j}^{t,p} \\ &= \sum_k \sum_{i+j-t-p=k} (x_{k,0}^{0,0} - x_{i,j}^{t,p}) M_{i,j}^{t,p} \\ &= \sum_{(i,j,t,p)} (x_{i+j-t-p,0}^{0,0} - x_{i,j}^{t,p}) M_{i,j}^{t,p}, \end{aligned} \tag{5.63}$$

which proves the proposition. □

Proposition 40. *The matrices*

$$M' \quad \text{and} \quad \begin{pmatrix} 1-x_{0,0}^{0,0} & (\mathrm{diag}(M''))^{\mathsf{T}} \\ \mathrm{diag}(M'') & M'' \end{pmatrix} \tag{5.64}$$

are positive semidefinite.

Using the block diagonalisation of $\mathcal{A}_{q,n}$, the positive semidefiniteness of R and R' is equivalent to:

$$\text{for all } a,k \text{ with } 0 \le a \le k \le n+a-k,\ k \neq 0 \text{ the matrices} \tag{5.65}$$

$$\left(\sum_{t,p} \alpha(i,j,t,p,a,k) x_{i,j}^{t,p}\right)_{i,j=k}^{n+a-k}$$

and

$$\left(\sum_{t,p} \alpha(i,j,t,p,a,k)(x_{i+j-t-p,0}^{0,0} - x_{i,j}^{t,p})\right)_{i,j=k}^{n+a-k}$$

are positive semidefinite, and

$$\left(\sum_{t,p} \alpha(i,j,t,p,0,0) x_{i,j}^{t,p}\right)_{i,j=0}^{n}$$

and

$$\begin{pmatrix} 1-x_{0,0}^{0,0} & x^{\mathsf{T}} \\ x & L \end{pmatrix}$$

are positive semidefinite, where

$$L := \left(\sum_{t,p} \alpha(i,j,t,p,0,0)(x_{i+j-t-p,0}^{0,0} - x_{i,j}^{t,p})\right)_{i,j=0}^{n},$$

$$x_i := (x_{0,0}^{0,0} - x_{i,i}^{i,i})\binom{n}{i}(q-1)^i \text{ for } i = 0,\dots,n. \tag{5.66}$$

Proposition 41. *The coefficients $x_{i,j}^{t,p}$ satisfy the following.*

$$q^n x_{0,0}^0 = |C|, \tag{5.67}$$

and for any i,j,t,p

$$\begin{aligned} &(i) && 0 \le x_{i,j}^{t,p} \le x_{i,i}^{i,i}, \\ &(ii) && x_{i,0}^{0,0} + x_{i+j-t-p,0}^{0,0} - x_{0,0}^{0,0} \le x_{i,j}^{t,p} \le x_{i+j-t-p,0}^{0,0}, \\ &(iii) && x_{i,j}^{t,p} = x_{i',j'}^{t',p'} \quad \textit{if } (i,j,i+j-t-p) \textit{ is a permutation of} \\ & && (i',j',i'+j'-t'-p') \textit{ and } t-p{=}t'-p'. \end{aligned} \tag{5.68}$$

Proposition 42. *Let $\mathbf{u}, \mathbf{v} \in \mathbb{E}$ be words with $d(\mathbf{u}, \mathbf{v}) = (i, j, t, p)$ and let (i, j', t', p') and d be given. Then the number $\alpha^{(i,j,t,p)}_{(i,j',t',p'),d}$ of words $\mathbf{w} \in \mathbb{E}$ with $d(\mathbf{u}, \mathbf{w}) = (i, j', t,' p')$ and $d(\mathbf{v}, \mathbf{w}) = d$ is given by*

$$\alpha^{(i,j,t,p)}_{(i,j',t',p'),d} = \sum_{\substack{a_1,a_2 \\ b_1,b_2 \\ c_1,c_2 \\ d_1,d_2,d_3 \\ e}} \binom{i-t}{a_1, a_2} \binom{j-t}{b_1, b_2} \binom{p}{c_1, c_2} \binom{t-p}{d_1, d_2, d_3} \cdot \binom{n+t-i-j}{e} (q-1)^e (q-2)^{a_2+b_2+c_2} (q-3)^{d_3}, \quad (5.69)$$

where the indices $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2, d_3$ and e range over the nonnegative integers that satisfy

$$\begin{aligned} j' &= a_1 + a_2 + b_1 + b_2 + c_1 + c_2 + d_1 + d_2 + d_3 + e \quad (5.70) \\ t' &= a_1 + a_2 + c_1 + c_2 + d_1 + d_2 + d_3 \\ p' &= a_1 + c_1 + d_1 \\ d &= a_1 + a_2 + e + j - b_1 - c_1 - d_2. \end{aligned}$$

Note that in the case $q = 3$ we adopt the convention that $0^0 = 1$.

Proof. Partition the support of the word w into sets A_1, A_2, B_1, B_2, C_1, C_2, D_1, D_2, D_3 and E as follows

$$\begin{aligned} A_1 &:= \{k \in S(\mathbf{w}) \mid \mathbf{u}_k \neq 0, \mathbf{v}_k = 0, \mathbf{w}_k = \mathbf{u}_k\} \quad (5.71) \\ A_2 &:= \{k \in S(\mathbf{w}) \mid \mathbf{u}_k \neq 0, \mathbf{v}_k = 0, \mathbf{w}_k \neq \mathbf{u}_k\} \\ B_1 &:= \{k \in S(\mathbf{w}) \mid \mathbf{u}_k = 0, \mathbf{v}_k \neq 0, \mathbf{w}_k = \mathbf{v}_k\} \\ B_2 &:= \{k \in S(\mathbf{w}) \mid \mathbf{u}_k = 0, \mathbf{v}_k \neq 0, w_k \neq \mathbf{v}_k\} \\ C_1 &:= \{k \in S(\mathbf{w}) \mid \mathbf{u}_k \neq 0, \mathbf{v}_k = \mathbf{u}_k, w_k = \mathbf{u}_k\} \\ C_2 &:= \{k \in S(\mathbf{w}) \mid \mathbf{u}_k \neq 0, \mathbf{v}_k = \mathbf{u}_k, w_k \neq \mathbf{u}_k\} \\ D_1 &:= \{k \in S(\mathbf{w}) \mid \mathbf{u}_k \neq 0, \mathbf{v}_k \neq 0, \mathbf{u}_k, w_k = \mathbf{u}_k\} \\ D_2 &:= \{k \in S(\mathbf{w}) \mid \mathbf{u}_k \neq 0, \mathbf{v}_k \neq 0, \mathbf{u}_k, w_k = \mathbf{v}_k\} \\ D_3 &:= \{k \in S(\mathbf{w}) \mid \mathbf{u}_k \neq 0, \mathbf{v}_k \neq 0, \mathbf{u}_k, w_k \neq \mathbf{u}_k, \mathbf{v}_k\} \\ E &:= \{k \in S(\mathbf{w}) \mid \mathbf{u}_k = 0, \mathbf{v}_k = 0\}. \end{aligned}$$

If we denote the sizes by $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2, d_3$ and e respectively, we obtain the proposition by summing over all possible sets A_1, A_2, B_1, B_2, C_1, C_2, D_1, D_2, D_3 and E. □

Proposition 43. *Let $\mathbf{u} \in \mathbb{E}$ be a word with $|S(\mathbf{u})| = i$ and let $x \in \mathbb{R}^{\mathbb{E}}$ be such that $x_{\mathbf{v}}$ only depends on $d(\mathbf{u}, \mathbf{v})$, say $x_{\mathbf{v}} = x^{t,p}_{i,j}$, when $d(\mathbf{u}, \mathbf{v}) = (i, j, t, p)$. Then*

$$\sum_{d=0}^{n} \lambda_d x(S_d(\mathbf{v})) \geq \beta \quad \textit{for all } \mathbf{v} \in \mathbb{E} \quad (5.72)$$

is equivalent to

$$\sum_{j',t',p'} x_{i,j'}^{t',p'} \cdot \sum_{d=0}^{n} \lambda_d \alpha_{(i,j',t',p'),d}^{(i,j,t,p)} \geq \beta \quad \textit{for every } j,t,p. \tag{5.73}$$

Proof. Let $\mathbf{v} \in \mathbb{E}$ and let $d(\mathbf{u},\mathbf{v}) = (i,j,t,p)$. Then we have the following equality.

$$\begin{aligned} \sum_{d=0}^{n} \lambda_d x(S_d(\mathbf{v})) &= \sum_{d=0}^{n} \sum_{\substack{\mathbf{w}\in\mathbb{E} \\ d(\mathbf{v},\mathbf{w})=d}} x_{\mathbf{w}} && (5.74)\\ &= \sum_{d=0}^{n} \lambda_d \sum_{j',t',p'} x_{i,j'}^{t',p'} \alpha_{(i,j',t',p'),d}^{(i,j,t,p)} && (5.75)\\ &= \sum_{j',t',p'} x_{i,j'}^{t',p'} \cdot \sum_{d=0}^{n} \lambda_d \alpha_{(i,j',t',p'),d}^{(i,j,t,p)}. && (5.76) \end{aligned}$$

□

Proposition 44. *If the code C satisfies the set of inequalities (λ,β), then the variables $x_{i,j}^{t,p}$ satisfy the following set of inequalities. For every tuple (i,j,t,p)*

$$\begin{aligned} \sum_{j',t',p'} x_{i,j'}^{t',p'} \cdot \lambda_{(i,j',t',p')}^{(i,j,t,p)} &\geq x_{i,0}^{0,0}\beta && (5.77)\\ \sum_{j',t',p'} (x_{j',0}^{0,0} - x_{i,j'}^{t',p'}) \cdot \lambda_{(i,j',t',p')}^{(i,j,t,p)} &\geq (x_{0,0}^{0,0} - x_{i,0}^{0,0})\beta \\ \sum_{j',t',p'} (x_{i+j-t-p,0}^{0,0} - x_{i,j}^{t,p}) \cdot \lambda_{(i,j',t',p')}^{(i,j,t,p)} &\geq (x_{0,0}^{0,0} - x_{i,0}^{0,0})\beta \\ \sum_{j',t',p'} (x_{0,0}^{0,0} - x_{j',0}^{0,0} - x_{i+j'-t'-p',0}^{0,0} + x_{i,j'}^{t',p'}) \cdot \lambda_{(i,j',t',p')}^{(i,j,t,p)} &\geq (1 - 2x_{0,0}^{0,0} + x_{i,0}^{0,0})\beta, \end{aligned}$$

where we have used the shorthand notation

$$\lambda_{(i,j',t',p')}^{(i,j,t,p)} := \sum_{d=0}^{n} \lambda_d \alpha_{(i,j',t',p'),d}^{(i,j,t,p)}. \tag{5.78}$$

Proof. For any $\sigma \in \mathrm{Aut}(q,n)$, the matrix $M := M_{\sigma C}$ satisfies

$$M_{\mathbf{u}} \in M_{\mathbf{u},\mathbf{u}} P_{\lambda,\beta} \quad \text{and} \quad \mathrm{diag}(M) - M_{\mathbf{u}} \in (1 - M_{\mathbf{u},\mathbf{u}}) P_{\lambda,\beta} \quad \text{for every } \mathbf{u} \in \mathbb{E}. \tag{5.79}$$

This implies that also the matrices $\frac{1}{x_{0,0}^{0,0} M'}$ and $\frac{1}{1-x_{0,0}^{0,0}}$ satisfy (5.79) as they are convex combinations of the matrices $M_{\sigma C}$. Now using Proposition 43 gives a proof of the claim. □

Theorem 9. *If any code $C \subseteq \mathbb{E}$ with covering radius r satisfies $(\lambda_0,\ldots,\lambda_n)\beta$, we have*

$$K_q(n,r) \geq \min_x q^n x_{0,0}^{0,0}, \tag{5.80}$$

where the minimum ranges over all $x = (x_{i,j}^{t,p})$ satisfying (5.65), (5.68) and (5.77).

Proof. □

5.5 Computational results

Using the sphere covering inequalities, we obtained a number of explicit new upper bounds in the case $q = 4$ and $q = 5$. The results[2] are shown in table 5.1 and 5.2 below. The upper bounds and previous lower bounds are taken from the website of G. Kéri ([24]), who maintains an updated table of upper and lower bounds on covering codes. In the binary and ternary case, no new lower bounds were found.

Table 5.1: New lower bounds on $K_4(n, R)$

n	R	best upper bound known	new lower bound	best lower bound previously known	Sphere covering bound
7	1	1008	762	752	745
11	1	131072	123846	123362	123362
9	2	1024	748	747	745
10	2	4096	2412	2408	2405
11	2	16128	7942	7929	7929
11	3	2048	843	842	842
9	4	64	22	21	21
11	4	512	134	133	133
11	5	128	31	30	30
11	6	32	10	9	9

[2]In the instance $R = 1$, $n = 11$ we were unable to solve the second SDP. The given number is the bound obtained from the first SDP.

Table 5.2: New lower bounds on $K_5(n, R)$

n	R	best upper bound known	new lower bound	best lower bound previously known	Sphere covering bound
7	1	3125	2722	2702	2694
8	1	15625	11945	11887	11838
9	1	78125	53138	52800	52788
10	1	390625	238993	238200	238186
11	2	115000	52842	52788	52788
11	3	21875	4253	4252	4252
11	4	3125	510	509	509
11	5	625	87	86	86
11	6	125	21	20	20

Chapter 6

Matrix cuts

In Chapter 4 we discussed the problem of finding good upper bounds on the maximum size of a code with certain distance constraints. This is a special case of the general problem to find bounds for the stability number of a graph. There exist general methods for bounding the stability number. In this chapter we explore the relationship between these general methods, when applied to codes, and the method from Chapter 4.

Recall that for any symmetric matrix $A \in \mathbb{R}^{n\times n}$, the matrix $R(A)$ is defined by:

$$R(A) := \begin{pmatrix} 1 & a^{\mathsf{T}} \\ a & A \end{pmatrix}, \tag{6.1}$$

where $a := \operatorname{diag}(A)$ is the vector of diagonal elements of A. We will index the extra row and column of $R(A)$ by 0. Denote the convex set of symmetric matrices

$$\mathcal{R}_n := \{A \in \mathbb{R}^{n\times n} \mid R(A) \succeq 0\}. \tag{6.2}$$

Observe that for $A \in \mathcal{R}_n$, the entries of A belong to $[-1, 1]$. Indeed, let $i, j \in \{0, \ldots, n\}$. The principal submatrix

$$\begin{pmatrix} 1 & A_{i,i} \\ A_{i,i} & A_{i,i} \end{pmatrix} \tag{6.3}$$

of $R(A)$ indexed by 0 and i is positive semidefinite. This is equivalent to $A_{i,i}^2 \leq 1 \cdot A_{i,i}$, which implies that $A_{i,i} \in [0, 1]$. For $i \leq j$ the semidefiniteness of the principal submatrix of $R(A)$ indexed by i and j

$$\begin{pmatrix} A_{i,i} & A_{i,j} \\ A_{i,j} & A_{j,j} \end{pmatrix} \tag{6.4}$$

implies that $A_{i,j}^2 \leq A_{i,i}A_{j,j} \leq 1$ and hence $A_{i,j} \in [-1, 1]$. We define the projection $p(\mathcal{M})$ of a set $\mathcal{M} \subseteq \mathcal{R}_n$ and the lift $l(K)$ of a set $K \subseteq [0, 1]^n$ by

$$\begin{aligned} p(\mathcal{M}) &:= \{\operatorname{diag}(A) \mid A \in \mathcal{M}\} \\ l(K) &:= \{A \in \mathcal{R}_n \mid \operatorname{diag}(A) \in K\}. \end{aligned} \tag{6.5}$$

By the previous remarks we see that $p(\mathcal{M}) \subseteq [0, 1]^n$ for $\mathcal{M} \subseteq \mathcal{R}_n$. Observe that for any $K \subseteq [0, 1]^n$ we have $p(l(K)) = K$. Indeed, if $x \in [0, 1]^n$, the matrix

$$\begin{pmatrix} 1 \\ x \end{pmatrix} \begin{pmatrix} 1 \\ x \end{pmatrix}^{\mathsf{T}} + \operatorname{Diag}(0, x_1 - x_1^2, \ldots, x_n - x_n^2) \tag{6.6}$$

is a positive semidefinite matrix of the form $R(A)$ with diagonal x. Conversely, we only have $l(p(\mathcal{M})) \supseteq \mathcal{M}$ for $\mathcal{M} \subseteq \mathcal{R}_n$.

In the following, the idea will be for a given convex set K, to find approximations of the convex hull of the 0–1 points in K. The method will be to describe these approximations as the projection of set in the larger space $\mathcal{R}_n$. The most prominent example is the so-called theta body of a graph, and the associated *Lovász theta number*.

6.1 The theta body $\mathrm{TH}(G)$

Let $G = (V, E)$ be a graph. We will assume that the vertex set is given by $V = \{1, \ldots, n\}$. Define the set $\mathcal{M}(G)$ by

$$\mathcal{M}(G) := \{A \in \mathcal{R}_n \mid A_{i,j} = 0 \text{ if } \{i, j\} \in E\}. \tag{6.7}$$

The projection

$$\mathrm{TH}(G) := p(\mathcal{M}(G)) = \{\mathrm{diag}(A) \mid A \in \mathcal{M}(G)\} \tag{6.8}$$

was defined in [17] and is referred to as the *theta body* of G. The number

$$\vartheta(G) := \max\{\mathbf{1}^{\mathsf{T}} x \mid x \in \mathrm{TH}(G)\} \tag{6.9}$$

was introduced by Lovász in [31] as an upper bound on the Shannon capacity of the graph G. Although we will not be concerned with Shannon capacities, the following two properties of $\vartheta(G)$ are relevant to our discussion: the number $\vartheta(G)$ can be approximated in polynomial time, and gives an (often close) upper bound on the stability number $\alpha(G)$. This last fact follows since for every stable set $S \subseteq V$ in the graph G, the matrix $\chi^S(\chi^S)^{\mathsf{T}}$ belongs to $\mathcal{M}(G)$. The theta body gives a good approximation of the stable set polytope. In particular, for perfect graphs G, equality holds, implying that the stability number can be calculated in polynomial time for perfect graphs.

The following strengthening of the theta body was given by Schrijver in [36]. Define

$$\mathcal{M}'(G) := \{A \in \mathcal{R}_n \mid A \geq 0, A_{i,j} = 0 \text{ if } \{i, j\} \in E\}, \tag{6.10}$$

and

$$\mathrm{TH}'(G) := p(\mathcal{M}'(G)). \tag{6.11}$$

Again the number

$$\vartheta'(G) := \max\{\mathbf{1}^{\mathsf{T}} x \mid x \in \mathrm{TH}'(G)\} \tag{6.12}$$

gives an upper bound on $\alpha(G)$ and clearly $\vartheta'(G) \leq \vartheta(G)$. We note that $\vartheta'(G)$ can be alternatively defined by

$$\begin{aligned} \vartheta'(G) = \max\{ \quad & \mathbf{1}^{\mathsf{T}} A \mathbf{1} \mid A \in \mathbb{R}^{n \times n}_{\geq 0}, \mathrm{tr} A = 1, \\ & A_{i,j} = 0 \text{ when } \{i, j\} \in E\}, \end{aligned} \tag{6.13}$$

and similarly for $\vartheta(G)$. The equivalence of the two definitions follows from Propositions 9 and 8 in Chapter 2 (see also [37]).

It was shown in [36] that for association schemes, the number $\vartheta'(G)$ corresponds to the Delsarte bound. Given a scheme (X, R) with adjacency matrices $I = A_0, A_1, \ldots, A_n$ and $M \subseteq \{1, \ldots, n\}$ we are interested in the maximum size of an M-clique, that is a subset $S \subseteq X$ with the property that $(A_i)_{x,y} = 0$ for all $x, y \in X$ and $i \notin M$. Consider the graph $G = (X, E)$, where $E = \{\{x, y\} \mid (A_i)_{x,y} = 1 \text{ for some } i \notin M\}$. Then the stable sets of G are precisely the M-cliques of the scheme (X, R). By (6.13), the upper bound $\vartheta'(G)$ on the maximum size of a stable set in G is given by

$$\max\{\mathbf{1}^\mathsf{T} A \mathbf{1} \mid A \in \mathbb{R}^{X\times X}_{\geq 0}, \mathrm{tr}A = 1, A_{i,j} = 0 \text{ when } \{i, j\} \in E\}. \tag{6.14}$$

We will sketch a proof that this maximum equals the Delsarte bound. The proof consists of two ideas.

Proof. First, we may restrict the range of A in the program to the matrices in the Bose–Mesner algebra, without decreasing the maximum. Indeed, let π denote the orthogonal projection onto the Bose–Mesner algebra (as a subspace of $\mathbb{R}^{X\times X}$) given by

$$\pi(A) := \sum_{i=0}^{n} \frac{\langle A, E_i\rangle}{\langle E_i, E_i\rangle} \cdot E_i, \tag{6.15}$$

where the matrices $E_0, \ldots, E_n$ are the orthogonal idempotents of the scheme. Since the E_i have eigenvalues 0 and 1, they are positive semidefinite. Hence for positive semidefinite A the projection $\pi(A)$ is a nonnegative combination of positive semidefinite matrices, and hence again positive semidefinite. Furthermore, π preserves the inner product with matrices in the Bose-Mesner algebra. In particular

$$\begin{aligned} \mathrm{tr}\pi(A) = \langle I, \pi(A)\rangle &= \langle I, A\rangle = \mathrm{tr}A \\ \mathbf{1}^\mathsf{T}\pi(A)\mathbf{1} = \langle J, \pi(A)\rangle &= \langle J, A\rangle = \mathbf{1}^\mathsf{T} A \mathbf{1} \\ \langle A_i, \pi(A)\rangle &= \langle A_i, A\rangle = 0 \quad \text{for } i \notin M \\ \langle A_i, \pi(A)\rangle &= \langle A_i, A\rangle \geq 0 \quad \text{for } i = 0, \ldots, n. \end{aligned} \tag{6.16}$$

It follows that $\pi(A)$ is a feasible point with the same objective value as A.

Secondly, writing

$$A = \sum_{i=0}^{n} x_i \widetilde{A}_i, \tag{6.17}$$

where $\widetilde{A}_i := \langle A_i, A_i\rangle^{-1} A_i$, the program becomes

$$\max\{\sum_{i\in M} x_i \mid x_0 = 1, x_i \geq 0 \text{ for } i \in M, \sum_{i\in M} x_i \widetilde{A}_i \succeq 0\}. \tag{6.18}$$

Since $\widetilde{A}_i = \sum_{j=0}^{n} Q_{j,i} \langle E_j, E_j\rangle^{-1} E_j$, where Q is the second eigenmatrix of the scheme, the positive semidefinite constraint reduces to linear constraints

$$\sum_{i\in M} x_i Q_{j,i} \geq 0 \quad \text{for } j = 0, \ldots, n. \tag{6.19}$$

□

We remark that when the Bose–Mesner algebra is the centralizer algebra of its automorphism group, for example in the case of the Hamming schemes and the Johnson schemes, the orthogonal projection π satisfies

$$\pi(A) = |\Gamma|^{-1} \sum_{\sigma \in \Gamma} \sigma A, \tag{6.20}$$

where Γ denotes the automorphism group of the scheme.

6.2 Matrix cuts

In [32], Lovász and Schrijver introduced a general *lift and project method* for strengthening approximations of 0–1 polytopes. Given a convex body K contained in the unit cube $[0,1]^n$, a convex body $N_+(K)$ is constructed such that

$$K \supseteq N_+(K) \supseteq N_+(N_+(K)) \supseteq \cdots \supseteq N_+^{(n)}(K) = K \cap \{0,1\}^n. \tag{6.21}$$

An important property of the operator N_+ is that for a family $\mathcal{K}$ of convex bodies, if one can optimize in polynomial time over K for each $K \in \mathcal{K}$, then also the optimization problem over $N_+(K)$ is polynomial time solvable for $K \in \mathcal{K}$. An important instance is when $G = (V, E)$ is a perfect graph and $K = \mathrm{FRAC}(G)$ is the fractional stable set polytope of G. In that case one iteration of the N_+ operator suffices to obtain the stable set polytope $\mathrm{STAB}(G) := \mathrm{FRAC}(G) \cap \{0,1\}^V$.

We start by describing the lift-and-project-method of Lovász and Schrijver and prove some of the basic properties of the operator N_+. The idea is to lift a convex set $K \subseteq [0,1]^n$ to a convex set in the space of symmetric positive semidefinite $n \times n$ matrices and then to project it back into $[0,1]^n$.

For $\mathcal{M} \subseteq \mathcal{R}_n$, define the set $N(\mathcal{M})$ by

$$\begin{aligned} N(\mathcal{M}) \ := \{A \in \mathcal{R}_m \mid \ & \text{for } i = 1, \ldots, n \text{ there are } U, V \in \mathcal{M} \\ & \text{such that } A_i = A_{i,i} \cdot \mathrm{diag}(U), \\ & \mathrm{diag}(A) - A_i = (1 - A_{i,i})\mathrm{diag}(V)\}. \end{aligned} \tag{6.22}$$

The operator N_+ is now defined as

$$N_+(K) := p(N(l(K))). \tag{6.23}$$

Clearly

$$N_+(K) \subseteq [0,1]^n, \tag{6.24}$$

since if $R(A)$ is positive semidefinite $\mathrm{diag}(A) \in [0,1]^n$ as we have seen before. Furthermore, we have:

$$N_+(K) \subseteq K. \tag{6.25}$$

Indeed, if $A \in N(l(K))$, then for any $i = 1, \ldots, n$ we have:

$$\mathrm{diag}(A) = A_i + (\mathrm{diag}(A) - A_i) \in A_{i,i} \cdot K + (1 - A_{i,i}) \cdot K \tag{6.26}$$

and hence $\mathrm{diag}(A) \in K$, since $A_{i,i} \in [0,1]$. Note that this argument shows that in fact

$$N_+(K) \subseteq \text{conv.hull}\{x \in K \mid x_i \in \{0,1\}\} \tag{6.27}$$

for $i = 1, \ldots n$ since for each i we have

$$A_i \in A_{i,i} \cdot \{x \in K \mid x_i = 1\}, \quad \mathrm{diag}(A) - A_i \in (1 - A_{i,i}) \cdot \{x \in K \mid x_i = 0\}. \tag{6.28}$$

By induction it then follows that

$$N_+^n(K) \subseteq \{0,1\}^n \cap K. \tag{6.29}$$

On the other hand, N_+ does not cut off any integer points:

$$\{0,1\}^n \cap K \subseteq N_+(K), \tag{6.30}$$

since for any $x \in \{0,1\}^n \cap K$ the matrix xx^T belongs to $N(l(K))$. The operator N_+ was introduced in [32], see also [37].

Let $G = (V, E)$ be a graph and let $\mathrm{FRAC}(G)$ denote the fractional stable set polytope of G, that is:

$$\mathrm{FRAC}(G) := \{x \in \mathbb{R}^V \mid x \geq 0, x_i + x_j \leq 1 \text{ for any edge } \{i,j\} \in E\}. \tag{6.31}$$

We observe that $N_+(\mathrm{FRAC}(G))$ is contained in the modified theta body $\mathrm{TH}'(G)$. Indeed, if $A \in N(l(\mathrm{FRAC}(G)))$, then $A_{i,j} = 0$ for any edge $\{i,j\}$ since $A_i \in A_{i,i} \cdot \mathrm{FRAC}(G)$ implies that

$$A_{i,i} + A_{i,j} \leq A_{i,i} \cdot 1. \tag{6.32}$$

We will also consider the operator $\widetilde{N}$ given by

$$\begin{aligned} \widetilde{N}(\mathcal{M}) \;:= \{A \in \mathcal{R}_n \mid\; & \text{for } i = 1, \ldots, n \text{ there are} \\ & U \in A_{i,i}\mathcal{M}, V \in (1 - A_{i,i})\mathcal{M} \\ & \text{such that } U_{i,i} = A_{i,i} \text{ and } A = U + V\}. \end{aligned} \tag{6.33}$$

Clearly $\widetilde{N}(\mathcal{M}) \subseteq N(\mathcal{M})$ for any $\mathcal{M} \subseteq \mathcal{R}_n$. We show that any $x \in p(\mathcal{M}) \cap \{0,1\}^n$ belongs to $p(N(\mathcal{M}))$. Let $A \in \mathcal{M}$ have diagonal $x \in \{0,1\}^n$. Then for $i = 1, \ldots, n$ we have $A = A_{i,i}U + (1 - A_{i,i})V$, where we take $U = A, V = 0$ if $A_{i,i} = 1$ and $U = 0, V = A$ if $A_{i,i} = 0$. The set $\widetilde{N}(\mathcal{M})$ can alternatively be described by:

$$\widetilde{N}(\mathcal{M}) = \{A \mid A \in \text{conv.hull}\{M \in \mathcal{M} \mid M_{i,i} \in \{0,1\}\} \text{ for each } i = 1, \ldots, n\}. \tag{6.34}$$

Proof. Let $A \in \widetilde{N}(\mathcal{M})$. Let $i \in \{1, \ldots, n\}$ and let U, V be as in the definition. Observe that $R(A)$ is positive semidefinite, since $A = U + V \in A_{i,i}\mathcal{M} + (1 - A_{i,i})\mathcal{M} = \mathcal{M}$. We prove that

$$A_i = \mathrm{diag}(U) \text{ and } \mathrm{diag}(A) - A_i = \mathrm{diag}(V). \tag{6.35}$$

If $A_{i,i} = 0$ we have $A_i = 0$ since A is positive semidefinite, and (6.35) follows. Hence we may assume that $A_{i,i} > 0$. Notice that $V_{i,i} = 0$ and hence $V_i = 0$. Since $A_{i,i}^{-1}U_{i,i} = 1$ it follows from the positive semidefiniteness of $R(A_{i,i}^{-1}U)$ that $U_i = \mathrm{diag}(U)$. Hence $A_i = U_i + V_i = \mathrm{diag}(U)$ and $\mathrm{diag}(A) - A_i = \mathrm{diag}(U)\ U_i + \mathrm{diag}(V) + V_i = \mathrm{diag}(V)$. □

6.3 Bounds for codes using matrix cuts

Fix integers $1 \leq d \leq n$ and $q \geq 2$, and fix an alphabet $\mathbf{q} = \{0, 1, \ldots, q-1\}$. The Hamming distance $d(x, y)$ of two words x and y is defined as the number of positions in which x and y differ. Let $G = (V, E)$ be the graph with $V = \mathbf{q}^n$, where two different *words* $x, y \in V$ are joined by an edge if x and y differ in at most $d - 1$ position. The stable sets in G are precisely the q-ary codes of length n and minimum distance at most d. The stability number of G equals $A_q(n, d)$. Define

$$\mathcal{M}' := \{A \in \mathcal{R}_V \mid A \geq 0, A_{x,y} = 0 \text{ if } \{x, y\} \in E\}, \tag{6.36}$$

and let

$$\mathrm{TH}'(G) := p(\mathcal{M}') = \{\mathrm{diag}(A) \mid A \in \mathcal{M}'\} \tag{6.37}$$

denote the modified theta body of G. Maximizing the all-one vector over $\mathrm{TH}'(G)$ gives an upper bound on $A_q(n, d)$, which we have seen, equals the Delsarte bound. A tighter upper bound can be found by maximizing the all-one vector over the smaller convex set $N_+(\mathrm{TH}'(G))$:

$$\max\{\mathrm{tr}A \mid A \in N(\mathcal{M})\}. \tag{6.38}$$

Using the symmetries of the graph G, this can be made more explicit as follows.

Denote by $\mathrm{Aut}(q, n)$ the set of permutations of $\mathbf{q}^n$ that preserve the Hamming distance. It is not hard to see that $\mathrm{Aut}(q, n)$ consists of the permutations of $\mathbf{q}^n$ obtained by permuting the n coordinates followed by independently permuting the alphabet $\mathbf{q}$ at each of the n coordinates. The group $\mathrm{Aut}(q, n)$ acts on the set of $V \times V$ matrices in the following way. For $\sigma \in \mathrm{Aut}(q, n)$ and $A \in \mathbb{R}^{V \times V}$ define $\sigma(A)$ by

$$(\sigma(A))_{\sigma x, \sigma y} = A_{x,y}. \tag{6.39}$$

The matrices in $\mathbb{R}^{V \times V}$ that are invariant under this action of $\mathrm{Aut}(q, n)$ are precisely the adjacency matrices $A_0, A_1, \ldots, A_n$ of the Hamming scheme $H(n, q)$ defined by

$$(A_i)_{x,y} : \begin{cases} 1 & \text{if } d(x, y) = i, \\ 0 & \text{otherwise,} \end{cases} \tag{6.40}$$

for $i = 0, 1, \ldots, n$ and the Bose–Mesner algebra of the Hamming scheme.

In the following calculations, it will be convenient do define for a square matrix A and a positive real number c the matrix $R(c; A)$ by

$$R(c; A) := \begin{pmatrix} c & (\mathrm{diag}(A))^{\mathsf{T}} \\ \mathrm{diag}(A) & A \end{pmatrix}. \tag{6.41}$$

Observe that $R(1; A) = R(A)$ and $R(c; A)$ is positive semidefinite if and only if $R(c^{-1}A)$ is positive semidefinite. Since G is invariant under the permutations $\sigma \in \mathrm{Aut}(q, n)$, also $\mathcal{M}'$, $N(\mathcal{M}')$ and $N_+(\mathrm{TH}'(G))$ are invariant under the action of $\mathrm{Aut}(q, n)$. Hence if $A \in N(\mathcal{M}')$ maximizes $\mathrm{tr}M$ over all $M \in N(\mathcal{M}')$, also

$$\frac{1}{|\mathrm{Aut}(q, n)|} \sum_{\sigma \in \mathrm{Aut}(q,n)} \sigma(A) \in N(\mathcal{M}') \tag{6.42}$$

is a maximizer. Hence the maximum in (6.38) is equal to

$$\max\{\mathrm{tr}A \mid A \in N(\mathcal{M}') \text{ is in the Bose–Mesner algebra}\}. \tag{6.43}$$

If A is a matrix in the Bose-Mesner algebra, all rows of A are equal up to permuting by elements of $\mathrm{Aut}(q,n)$. Hence since $\mathcal{M}'$ is invariant under these permutations, the maximum is equal to

$$\begin{aligned}\max\{q^n \cdot x_0 \mid & R(\sum_{i=0}^{n} x_i A_i) \text{ is positive semidefinite} \\ & \text{and there exist } U \in x_0 \cdot \mathcal{M}' \text{ and } V \in (1-x_0)\cdot \mathcal{M}' \text{ such that} \\ & U_{u,u} = x_i \text{ if } d(u,0) = i \text{ and} \\ & V_{u,u} = x_0 - x_i \text{ if } d(u,0) = i\}.\end{aligned} \tag{6.44}$$

Note that if U and V are as in (6.44), and $\sigma \in \mathrm{Aut}(q,n)$ fixes the zero word, then $\sigma(U)$ and $\sigma(V)$ satisfy the same constraints. Hence U may be replaced by

$$\frac{1}{|\mathrm{Aut}_{\mathbf{0}}(q,n)|} \sum_{\sigma \in \mathrm{Aut}_{\mathbf{0}}(q,n)} \sigma(U) \tag{6.45}$$

and similarly for V. Here $\mathrm{Aut}_{\mathbf{0}}(q,n)$ denotes the set $\{\sigma \in \mathrm{Aut}(q,n) \mid \sigma(0) = 0\}$. Hence we may impose that U and V are elements of the Terwilliger algebra without changing the maximum. We obtain

$$\begin{aligned}\max\{q^n \cdot x_0 \mid & R(\sum_{i=0}^{n} x_i A_i) \text{ is positive semidefinite,} \\ & R(\sum_{i,j,t,p} y_{i,j}^{t,p} M_{i,j}^{t,p}), R(\sum_{i,j,t,p} z_{i,j}^{t,p} M_{i,j}^{t,p}) \text{ are positive semidefinite,} \\ & x_i = x_0 y_{i,i}^{i,i}, \quad x_0 - x_i = (1-x_0) z_{i,i}^{i,i} \quad (i = 0, \ldots, n), \\ & y_{i,j}^{t,p}, z_{i,j}^{t,p} \geq 0, \\ & y_{i,j}^{t,p} = z_{i,j}^{t,p} = 0 \text{ if } i + j - t - p \in \{1, \ldots, d-1\}\}.\end{aligned} \tag{6.46}$$

Since $x_i = x_0 \cdot y_{i,i}^{i,i}$ we can eliminate the variables x_i from this program by substituting

$$\begin{aligned} \widetilde{y}_{i,j}^{t,p} &:= x_0 \cdot y_{i,j}^{t,p} \\ \widetilde{z}_{i,j}^{t,p} &:= (1-x_0) z_{i,j}^{t,p}. \end{aligned} \tag{6.47}$$

We obtain the following semidefinite program (where we have dropped all the tilde's from the variables):

$$\begin{aligned}\max\{q^n \cdot y_{0,0}^{0,0} \mid & R(\sum_{i=0}^{n} y_{i,i}^{i,i} A_i) \text{ is positive semidefinite,} \\ & R(y_{0,0}^{0,0}; \sum_{i,j,t,p} y_{i,j}^{t,p} M_{i,j}^{t,p}), R(1 - y_{0,0}^{0,0}; \sum_{i,j}^{t,p} z_{i,j}^{t,p} M_{i,j}^{t,p}) \succeq 0 \\ & y_{0,0}^{0,0} - y_{i,i}^{i,i} = z_{i,i}^{i,i} \quad (i = 0, \ldots, n), \\ & y_{i,j}^{t,p}, z_{i,j}^{t,p} \geq 0, \\ & y_{i,j}^{t,p} = z_{i,j}^{t,p} = 0 \text{ if } i + j - t - p \in \{1, \ldots, d-1\}\}.\end{aligned} \tag{6.48}$$

If we use the stronger operator $\widetilde{N}$ in stead of N we arrive in a similar fashion at the program

$$\begin{aligned}\max\{q^n \cdot x_0 \,|R(x_0; \sum_{i,j,t,p} y_{i,j}^{t,p} M_{i,j}^{t,p}), R(1-x_0; \sum_{i,j,t,p} z_{i,j}^{t,p} M_{i,j}^{t,p}) \succeq 0,\\ y_{0,0}^{0,0} = x_0, y_{i,j}^{t,p} + z_{i,j}^{t,p} = x_{i+j-t-p}\\ y_{i,j}^{t,p}, z_{i,j}^{t,p} \geq 0, y_{i,j}^{t,p} = z_{i,j}^{t,p} = 0 \text{ if } i+j-t-p \in \{1,\ldots,d-1\}\}\end{aligned} \tag{6.49}$$

it follows from $y_{0,0}^{0,0} + z_{0,0}^{0,0} = x_0$ and $y_{0,0}^{0,0} = x_0$ that $z_{0,0}^{0,0} = 0$. Since for each feasible solution the matrix

$$M := \sum_{i,j}^{t,p} z_{i,j}^{t,p} M_{i,j}^{t,p} \tag{6.50}$$

is positive semidefinite, it follows from $M_{\mathbf{0},\mathbf{0}} = z_{0,0}^{0,0} = 0$ that $0 = M_{u,\mathbf{0}} = z_{i,0}^{0,0}$ when $\mathbf{u}$ has weight i. Hence

$$x_i = y_{i,0}^{0,0} + z_{i,0}^{0,0} = y_{i,0}^{0,0}. \tag{6.51}$$

This implies that we can eliminate the variables x_i and $z_{i,j}^{t,p}$ by using

$$x_i = y_{i,0}^{0,0}, \quad z_{i,j}^{t,p} = y_{i+j-t-p,0}^{0,0} - y_{i,j}^{t,p} \tag{6.52}$$

for all i, j, t, p. We obtain the following semidefinite program:

$$\begin{aligned}\max\{q^n \cdot y_{0,0}^{0,0} \,|R(y_{0,0}^{0,0}; \sum_{i,j,t,p} y_{i,j}^{t,p} M_{i,j}^{t,p}), R(1-y_{0,0}^{0,0}; \sum_{i,j,t,p} (y_{i+j-t-p,0}^{0,0} - y_{i,j}^{t,p}) M_{i,j}^{t,p}) \succeq 0,\\ y_{i,j}^{t,p}, y_{i+j-t-p,0}^{0,0} - y_{i,j}^{t,p} \geq 0,\\ y_{i,j}^{t,p} = y_{i+j-t-p,0}^{0,0} = 0 \text{ if } i+j-t-p \in \{1,\ldots,d-1\}\}\end{aligned} \tag{6.53}$$

This program may be further simplified by observing that for a matrix A with $A_{1,1} = 1$

$$R(A) \succeq 0 \quad \text{if and only if} \quad A \succeq 0, A_1 = \operatorname{diag}(A). \tag{6.54}$$

We finally obtain

$$\begin{aligned}\max\{q^n \cdot y_{0,0}^{0,0} \mid \sum_{i,j,t,p} y_{i,j}^{t,p} M_{i,j}^{t,p}, R(1-y_{0,0}^{0,0}; \sum_{i,j,t,p} (y_{i+j-t-p,0}^{0,0} - y_{i,j}^{t,p}) M_{i,j}^{t,p}) \succeq 0,\\ y_{i,j}^{t,p}, y_{i+j-t-p,0}^{0,0} - y_{i,j}^{t,p} \geq 0,\\ y_{i,0}^{0,0} = y_{i,i}^{i,i},\\ y_{i,j}^{t,p} = y_{i+j-t-p,0}^{0,0} = 0 \text{ if } i+j-t-p \in \{1,\ldots,d-1\}\}\end{aligned} \tag{6.55}$$

This bound is very similar to the bound (4.38) derived in Chapter 4, that is to say the impoved version of Schrijver's bound given by Laurent. The main difference is that in (6.55) the symmetry conditions

$$\begin{aligned}y_{i,j}^{t,p} = y_{i',j'}^{t',p'} \quad &\text{when } t-p = t'-p' \text{ and } (i,j,i+j-t-p) \text{ is a}\\ &\text{permutation of } (i',j',i'+j'-t'-p')\end{aligned} \tag{6.56}$$

are lacking. It can be seen from the computational results in given in the next section, that these conditions make a huge difference in the resulting bound.

6.4 Computational results

In this section we give some computational results on the different bounds we obtain and compare them to the bound proposed by Schrijver (see [38], [16]) with the improvement of Laurent. That is, the bound obtained from (4.38). Each of the bounds can be computed in polynomial time in n by block diagonalising the Terwilliger algebra of the Hamming scheme for each q and n.

From the tables below it follows that we can have the strict inequality

$$\widetilde{N}(\mathcal{M}) \subset N(\mathcal{M}). \tag{6.57}$$

Table 6.1: Bounds on $A_3(n, d)$

n	d	best lower bound known	best upper bound previously known	Delsarte bound	bound from (6.48)	bound from (6.55)	bound from (4.38)
6	3	38	38	48	48	48	46
7	3	99	111	145	145	144	136
8	3	243	333	340	340	340	340
9	3	729	937	937	937	937	937
7	4	33	33	48	48	48	44
8	4	99	99	139	139	139	121
9	4	243	297	340	340	339	324
10	4	729	891	937	937	937	914
11	4	1458	2561	2811	2811	2805	2583
12	4	4374	7029	7029	7029	7029	6839
6	5	4	4	5	5	4	4
7	5	10	10	15	15	14	13
8	5	27	27	41	41	41	33
9	5	81	81	90	90	90	86
10	5	243	243	243	243	243	243
11	5	729	729	729	729	729	729
12	5	729	1562	1562	1562	1562	1557
7	6	3	3	4	4	4	4
9	7	6	6	7	7	7	7
10	7	14	14	21	21	21	21
11	7	36	36	63	63	62	49
12	7	54	108	138	138	138	131

Remark: We calculate the Delsarte bound by maximizing $x_0 \cdot q^n$ (the trace of $\sum_i x_i M_i$) under the condition that the x_i are nonnegative and $R(\sum_i x_i M_i)$ is positive semidefinite. This turns out to give a more stable semidefinite program than setting $x_0 = 1$ and maximizing $\sum_i x_i \binom{n}{i} (q-1)^i$.

Table 6.2: Bounds on $A_4(n, d)$

n	d	best lower bound known	best upper bound previously known	Delsarte bound	bound from (6.48)	bound from (6.55)	bound from (4.38)
7	4	128	179	179	179	179	169
8	4	320	614	614	614	614	611
9	4	1024	2340	2340	2340	2340	2314
10	4	4096	9360	9362	9362	9360	8951
7	5	32	32	40	40	40	39
8	5	70	128	160	160	160	147
9	5	256	512	614	614	614	579
10	5	1024	2048	2145	2145	2145	2045
10	6	256	512	512	512	511	496
11	6	1024	2048	2048	2048	2047	1780
12	6	4096	6241	6241	6241	6241	5864
10	7	40	80	112	112	111	106
12	7	256	1280	1280	1280	1280	1167

Table 6.3: Bounds on $A_5(n, d)$

n	d	best lower bound known	best upper bound previously known	Delsarte bound	bound from (6.48)	bound from (6.55)	bound from (4.38)
6	4	125	125	125	125	125	125
7	4	250	554	625	625	623	545
8	4	1125	2291	2291	2291	2291	2291
9	4	3750	9672	9672	9672	9672	9672
10	4	15625	44642	44642	44642	44642	44642
11	4	78125	217013	217013	217013	217013	217013
7	5	53	125	125	125	124	108
8	5	160	554	625	625	623	485
9	5	625	2291	2291	2291	2291	2152
10	5	3125	9672	9672	9672	9672	9559
11	5	15625	44642	44642	44642	44642	44379
8	6	45	75	75	75	75	75
9	6	135	375	375	375	375	375
10	6	625	1875	1875	1875	1875	1855
11	6	3125	9375	9375	9375	9375	8840
11	9	25	35	45	45	45	43

Chapter 7

Further discussion

In this chapter, we present some further observations, and notes related to the methods from previous chapters.

7.1 Bounds for affine caps

Let $\mathrm{AG}(k,q)$ be the k-dimensional affine space over the field GF_q. A subset $A \subseteq \mathrm{AG}(k,q)$ is called an *affine cap* if no three elements of A are on an affine line, that is, any three different vectors in $\{\binom{1}{a} \mid a \in A\}$ are linearly independent. We denote by $C_k(q)$ the maximum cardinality of an affine cap in $\mathrm{AG}(k,q)$.

The effectiveness of the semidefinite programming approach for error correcting codes, suggested that we could, more generally, find good bounds for the size of a code where we forbid the occurence of triples of code words in some prescribed configuration. Indeed the variables $x_{i,j}^{t,p}$ in the semidefinite program correspond exactly to the number of tripes in a code, for each equivalence class under automorphisms of the Hamming space. One may be led to wonder if setting those variables that correspond to forbidden configurations to zero, would yield good upper bounds in general. This is an appealing idea. Unfortunately, it turned out to be false in general.

A prominent structure that might be approached this way are affine caps over the field of three elements. The only known values are $C_1(3) = 2, C_2(3) = 4, C_3(3) = 9, C_4(3) = 20$ and $C_5(3) = 45$. In [4] the general bound $C_k(3) \leq 3^k \frac{k+1}{k^2}$ was shown. A code $A \subseteq \mathrm{AG}(k,3)$ is an affine cap if and only if for any three elements $\mathbf{u}, \mathbf{v}, \mathbf{w} \in A$ we have $d(\mathbf{u}, \mathbf{v}, \mathbf{w}) \neq (i,i,i,0)$ for every $i = 1, \ldots, k$. Recall that

$$\begin{aligned} d(\mathbf{u}, \mathbf{v}, \mathbf{w}) \;:=\; & (i,j,t,p), \text{ where} \\ & i := d(\mathbf{u}, \mathbf{v}), \\ & j := d(\mathbf{u}, \mathbf{w}), \\ & t := |\{i \mid \mathbf{u}_i \neq \mathbf{v}_i \text{ and } \mathbf{u}_i \neq \mathbf{w}_i\}|, \\ & p := |\{i \mid \mathbf{u}_i \neq \mathbf{v}_i = \mathbf{w}_i\}|. \end{aligned} \tag{7.1}$$

Consider the following semidefinite program.

$$\text{maximize } \sum_{i=0}^{n} \binom{n}{i} 2^i x_{i,0}^{0,0} \quad \text{subject to} \tag{7.2}$$

(i) $x_{0,0}^{0,0} = 1$

(ii) $0 \leq x_{i,j}^{t,p} \leq x_{i,0}^{0,0}$

(iii) $x_{i,j}^{t,p} = x_{i',j'}^{t',p'}$ if $t - p = t' - p'$ and
$(i, j, i + j - t - p)$ is a permutation of $(i', j', i' + j' - t' - p')$

(iv) $x_{i,i}^{i,0} = 0$ for $i = 1, \ldots, n$.

(v) $\sum_{i,j,t,p} x_{i,j}^{t,p} M_{i,j}^{t,p}$, $\sum_{i,j,t,p} (x_{i+j-t-p,0}^{0,0} - x_{i,j}^{t,p}) M_{i,j}^{t,p}$ are positive semidefinite.

Clearly, this gives an upper bound on $C_n(3)$. We have the following result.

Proposition 45. *The maximum in (7.2) equals* $1 + \frac{3^n-1}{2}$.

Proof. Setting the variables $x_{i,j}^{t,p}$ as follows:

$$x_{i,j}^{t,p} := \begin{cases} 1 & \text{if } i = j = t = p = 0, \\ \frac{1}{2} & \text{if } i = j = t = p \neq 0 \text{ or exactly one of } i, j \text{ is zero}, \\ 0 & \text{if } i = j = t \neq 0 \text{ and } p = 0, \\ \frac{1}{4} & \text{otherwise} \end{cases} \tag{7.3}$$

gives a feasible solution with objective value equal to $1 + \frac{3^n-1}{2}$.

On the other hand, let any feasible solution be given. Then the matrix $M' := \sum_{i,j,t,p} x_{i,j}^{t,p} M_{i,j}^{t,p}$ is positive semidefinite. Hence for any nonzero word $\mathbf{u}$ the 3×3 principal submatrix indexed by the words $\mathbf{0}, \mathbf{u}, -\mathbf{u}$ is positive semidefinite and equals

$$\begin{pmatrix} 1 & M_{\mathbf{u},\mathbf{u}} & M_{-\mathbf{u},-\mathbf{u}} \\ M_{\mathbf{u},\mathbf{u}} & M_{\mathbf{u},\mathbf{u}} & 0 \\ M_{-\mathbf{u},-\mathbf{u}} & 0 & M_{-\mathbf{u},-\mathbf{u}.} \end{pmatrix} \tag{7.4}$$

This implies that $(M_{\mathbf{u},\mathbf{u}} - M_{\mathbf{u},\mathbf{u}}^2)(M_{-\mathbf{u},-\mathbf{u}} - M_{-\mathbf{u},-\mathbf{u}}^2) \geq (M_{\mathbf{u},\mathbf{u}} M_{-\mathbf{u},-\mathbf{u}})^2$. Hence $M_{\mathbf{u},\mathbf{u}} + M_{-\mathbf{u},-\mathbf{u}} \leq 1$. Since the objective function equals the trace of M, the value is at most $1 + \frac{3^n-1}{2}$. □

This bound is very poor. The same bound already follows from the fact that if $\mathbf{0} \in A$, for every nonzero word $\mathbf{u}$ not both $\mathbf{u}$ and $-\mathbf{u}$ can belong to A.

7.2 Notes on computational results

The computational results from Chapters 4 and 5 have been obtained by using CSDP version 4.7 (see [7]) and SDPT3 (see [42]). Both are *SDP-solvers* and can be accessed also through the NEOS server, see

`www-neos.mcs.anl.gov/`

. The semidefinite programs were generated by perl scripts in the sparse SDPA format, which allows for explicit block structure in the constraint matrices to be exploited by the solver.

In the case of error correcting codes (tables 1,2,3 from Chapter 4), all solutions produced by the solvers have been examined by a perl script to ensure that the produced numbers really do give valid upper bounds on error correcting codes. In none of the instances this has made a diference for the final bound obtained. This was done as follows.

The original problem was to maximize $\sum_i \binom{n}{i}(q-1)^i x_{i,0}^{0,0}$, given certain constraints on the variables $x_{i,j}^{t,p}$ (4.27). By changing the sign of the objective vector, we obtain a semidefinite program of the following form:

$$\begin{array}{rl} \text{minimize} & x_1c_1 + \cdots + x_mc_m \\ \text{subject to} & x_1F_1 + \cdots + x_mF_m - F_0 =: X \succeq 0, \end{array} \tag{7.5}$$

where we minimize over $x^{\mathsf{T}} = (x_1, \ldots, x_m)$, $c^{\mathsf{T}} = (c_1, \ldots, c_m)$ is the objective vector and $F_0, \ldots, F_m$ are given symmetric matrices. The SDP solver not only returns a solution to this (primal) problem, but also to its dual:

$$\begin{array}{rl} \text{maximize} & \langle F_0, Y\rangle \\ \text{subject to} & \langle F_i, Y\rangle = c_i, \quad i = 1, \ldots, m, \\ & Y \succeq 0. \end{array} \tag{7.6}$$

Any genuine feasible matrix Y for the dual problem gives a lower bound on the minimum in the primal problem, and hence an upper bound for our coding problem. However, the produced dual solutions Y usually do not exactly satisfy the linear constraint, but satisfy

$$\langle F_i, Y\rangle = c_i + \epsilon_i, \tag{7.7}$$

for small numbers $\epsilon_1, \ldots, \epsilon_m$. In all cases we did find that $Y \succeq 0$ was satisfied. This yields a lower bound on the optimum of the primal program as follows. Let (x, X) be an optimal solution for the primal program with value O. Then we obtain:

$$\begin{array}{rcl} \langle F_0, Y\rangle & = & \langle x_1F_1 + \cdots + x_mF_m - X, Y\rangle \\ & \leq & \langle x_1F_1 + \cdots + x_mF_m, Y\rangle \\ & = & x_1\langle F_1, Y\rangle + \cdots + x_m\langle F_m, Y\rangle \\ & = & x_1(c_1+\epsilon_1) + \cdots + x_m(c_m+\epsilon_m) \\ & = & O + (x_1\epsilon_1 + \cdots + x_m\epsilon_m). \end{array} \tag{7.8}$$

The numbers $\epsilon_1, \ldots, \epsilon_m$ are easily calculated from the solution Y. Although the numbers $x_1, \ldots, x_m$ are not known, we can say that $x_i \in [0, 1]$ in this case, which allows us to bound the error term by

$$(x_1\epsilon_1 + \cdots + x_m\epsilon_m) \leq \max\{0, \epsilon_1\} + \cdots + \max\{0, \epsilon_m\}. \tag{7.9}$$

This gives lower bound on O, and hence an upper bound on the maximum size of a code.

Bibliography

[1] R. A. Bailey. *Association schemes*, volume 84 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2004. Designed experiments, algebra and combinatorics.

[2] E. Bannai and T. Ito. *Algebraic combinatorics. I.* The Benjamin/Cummings Publishing Co. Inc., Menlo Park, CA, 1984. Association schemes.

[3] G. P. Barker, L. Q. Eifler, and T. P. Kezlan. A non-commutative spectral theorem. *Linear Algebra and Appl.*, 20(2):95–100, 1978.

[4] J. Bierbrauer and Y. Edel. Bounds on affine caps. *J. Combin. Des.*, 10(2):111–115, 2002.

[5] G. T. Bogdanova, A. E. Brouwer, S. N. Kapralov, and P. R. J. Östergård. Error-correcting codes over an alphabet of four elements. *Des. Codes Cryptogr.*, 23(3):333–342, 2001.

[6] G. T. Bogdanova and P. R. J. Östergård. Bounds on codes over an alphabet of five elements. *Discrete Math.*, 240(1-3):13–19, 2001.

[7] B. Borchers. CSDP, a C library for semidefinite programming. *Optim. Methods Softw.*, 11/12(1-4):613–623, 1999. Interior point methods.

[8] R. C. Bose and T. Shimamoto. Classification and analysis of partially balanced incomplete block designs with two associate classes. *J. Amer. Statist. Assoc.*, 47:151–184, 1952.

[9] A. E. Brouwer. Website: `http://www.win.tue.nl/∼aeb`.

[10] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-regular graphs*, volume 18 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1989.

[11] A. E. Brouwer, H. O. Hämäläinen, P. R. J. Östergård, and N. J. A. Sloane. Bounds on mixed binary/ternary codes. *IEEE Trans. Inform. Theory*, 44(1):140–161, 1998.

[12] P. J. Cameron. Coherent configurations, association schemes and permutation groups. In *Groups, combinatorics & geometry (Durham, 2001)*, pages 55–71. World Sci. Publishing, River Edge, NJ, 2003.

[13] W. Chen and I. S. Honkala. Lower bounds for q-ary covering codes. *IEEE Trans. Inform. Theory*, 36(3):664–671, 1990.

[14] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein. *Covering codes*, volume 54 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, 1997.

[15] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, (10):vi+97, 1973.

[16] D. Gijswijt, A. Schrijver, and H. Tanaka. New upper bounds for nonbinary codes based on the terwilliger algebra and semidefinite programming. Submitted, November 2004.

[17] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric algorithms and combinatorial optimization*, volume 2 of *Algorithms and Combinatorics*. Springer-Verlag, Berlin, second edition, 1993.

[18] L. Habsieger. Some new lower bounds for ternary covering codes. *Electron. J. Combin.*, 3(2):Research Paper 23, approx. 14 pp. (electronic), 1996. The Foata Festschrift.

[19] L. Habsieger and A. Plagne. New lower bounds for covering codes. *Discrete Math.*, 222(1-3):125–149, 2000.

[20] H. Hämäläinen, I. Honkala, S. Litsyn, and P. Östergård. Football pools—a game for mathematicians. *Amer. Math. Monthly*, 102(7):579–588, 1995.

[21] I. S. Honkala. Lower bounds for binary covering codes. *IEEE Trans. Inform. Theory*, 34(2):326–329, 1988.

[22] R. A. Horn and C. R. Johnson. *Matrix analysis*. Cambridge University Press, Cambridge, 1990. Corrected reprint of the 1985 original.

[23] S. M. Johnson. A new lower bound for coverings by rook domains. *Utilitas Math.*, 1:121–140, 1972.

[24] G. Kéri. Tables for bounds on covering codes, website: `http://www.sztaki.hu/~keri/codes`.

[25] G. Kéri and P. R. Östergård. Bounds for covering codes over large alphabets. Technical report, Computer and Automation Research Institute, Hungarian Academy of Sciences, Laboratory of Operations Research and Decision Systems, 2004.

[26] E. de Klerk and D.V. Pasechnik. A note on the stability number of an orthogonality graph. ArXiv:math.CO/0505038, May 2005.

[27] S. Lang. *Linear algebra*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, third edition, 1989.

[28] M. Laurent. Strengthened semidefinite bounds for codes. Januari 2005.

[29] D. Li and W. Chen. New lower bounds for binary covering codes. *IEEE Trans. Inform. Theory*, 40(4):1122–1129, 1994.

[30] J. H. van Lint. *Introduction to coding theory*, volume 86 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third edition, 1999.

[31] L. Lovász. On the Shannon capacity of a graph. *IEEE Trans. Inform. Theory*, 25(1):1–7, 1979.

[32] L. Lovász and A. Schrijver. Cones of matrices and set-functions and 0-1 optimization. *SIAM J. Optim.*, 1(2):166–190, 1991.

[33] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. I, II.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[34] Y. Nesterov and A. Nemirovskii. *Interior-point polynomial algorithms in convex programming*, volume 13 of *SIAM Studies in Applied Mathematics*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1994.

[35] M. Rørdam, F. Larsen, and N. Laustsen. *An introduction to K-theory for C^*-algebras*, volume 49 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2000.

[36] A. Schrijver. A comparison of the Delsarte and Lovász bounds. *IEEE Trans. Inform. Theory*, 25(4):425–429, 1979.

[37] A. Schrijver. *Combinatorial optimization. Polyhedra and efficiency. Vol. B*, volume 24 of *Algorithms and Combinatorics*. Springer-Verlag, Berlin, 2003. Matroids, trees, stable sets, Chapters 39–69.

[38] A. Schrijver. New code upper bounds from the terwilliger algebra. *IEEE Trans. Inform. Theory*, To appear.

[39] P. Terwilliger. The subconstituent algebra of an association scheme. I. *J. Algebraic Combin.*, 1(4):363–388, 1992.

[40] P. Terwilliger. The subconstituent algebra of an association scheme. III. *J. Algebraic Combin.*, 2(2):177–210, 1993.

[41] M. J. Todd. Semidefinite optimization. *Acta Numer.*, 10:515–560, 2001.

[42] K. C. Toh, M. J. Todd, and R. H. Tütüncü. SDPT3—a MATLAB software package for semidefinite programming, version 1.3. *Optim. Methods Softw.*, 11/12(1-4):545–581, 1999. Interior point methods.

[43] J. H. M. Wedderburn. *Lectures on matrices*. Dover Publications Inc., New York, 1964.

[44] G. J. M. van Wee. Improved sphere bounds on the covering radius of codes. *IEEE Trans. Inform. Theory*, 34(2):237–245, 1988.

[45] G. J. M. van Wee. *Covering codes, perfect codes, and codes from algebraic curves.* Technische Universiteit Eindhoven, Eindhoven, 1991. Dissertation, Technische Universiteit Eindhoven, Eindhoven, 1991, With a Dutch summary.

[46] Z. Zhang. Linear inequalities for covering codes. I. Pair covering inequalities. *IEEE Trans. Inform. Theory*, 37(3, part 1):573–582, 1991.

[47] Z. Zhang and C. Lo. Linear inequalities for covering codes. II. Triple covering inequalities. *IEEE Trans. Inform. Theory*, 38(6):1648–1662, 1992.

Index

Samenvatting

Dit proefschrift gaat over foutcorrigerende codes en overdekkingscodes. Een code is een collectie woorden van dezelfde lengte n met letters uit een alfabet $\mathbf{q} = \{0, 1, \ldots, q-1\}$ bestaande uit een q-tal symbolen. In het geval dat $q = 2$ bestaat elk woord uit een rijtje van n nullen en enen. We spreken in dat geval van een binaire code. Voor $q \geq 3$ spreken we van niet-binaire codes. De Hamming afstand $d(\mathbf{x}, \mathbf{y})$ tussen twee woorden $\mathbf{x}$ en $\mathbf{y}$ is gedefinieerd als het aantal posities waarin zij verschillen. Zo krijgt de verzameling $\mathbf{q}^n$ van alle woorden de structuur van een metrische ruimte, de Hamming ruimte.

Een centrale vraag in de theorie van foutcorrigerende codes is:

> Gegeven een 'minimum afstand' d, wat is het maximale aantal woorden in een code als we eisen dat van elk tweetal woorden de onderlinge afstand ten minste d moet zijn?

Dit maximum, aangegeven met $A_q(n, d)$ heeft een mooie 'meetkundige' interpretatie in het geval dat $d = 2e + 1$ oneven is. Het getal $A_q(n, d)$ is dan precies het aantal bollen van straal e dat binnen de Hammingruimte kan worden gestapeld. De foutcorrigerende eigenschappen van zo'n code volgen uit het feit dat wanneer een codewoord in hoogstens e posities wordt gewijzigd, het originele woord weer terug wordt gevonden door het dichtsbijzijnde codewoord te nemen.

Een twee vraag, die duaal is aan de vorige, speelt een rol in onder andere datacompressie:

> Gegeven een 'overdekkings straal' r, wat is het minimale aantal woorden in een code als we eisen dat ieder woord afstand ten hoogste r tot een woord in de code heeft?

Dit minimum, aangegeven met $K_q(n, r)$ is het aantal bollen van straal r dat nodig is om de hele Hamming ruimte te bedekken.

In het algemeen zijn de getallen $A_q(n, d)$ en $K_q(n, r)$ erg moeilijk te bepalen en slechts weinig waarden zijn bekend. Daarom is het interessant om goede onder- en bovengrenzen te vinden voor deze getallen. Het meetkundige beeld van het stapelen van en overdekken met bollen geeft al een bovengrens voor $A_q(n, 2r + 1)$ en een ondergrens voor $K_q(n, r)$ door het volume van de gehele Hamming ruimte te delen door het volume van een bol van straal r.

In dit proefschrift geven we nieuwe bovengrenzen voor $A_q(n, d)$ en nieuwe ondergrenzen voor $K_q(n, r)$ met behulp van semidefiniete programmering. Een belangrijke rol wordt gespeeld door een expliciete blokdiagonalisatie van de Terwilliger algebra van het Hamming schema. Deze maakt het mogelijk om de grote symmetriegroep van de Hamming

ruimte te benutten, zowel voor het verkrijgen van scherpere grenzen, als voor het efficient kunnen bepalen van deze grenzen. De beschreven methode voor het begrenzen van $A_q(n,d)$ werd door Schrijver geintroduceerd voor het binaire geval in [38]. In hetzelfde artikel werd ook een blokdiagonalisatie gegeven voor de Terwilliger algebra van het binaire Hamming schema. Een centraal resultaat uit dit proefschrift is een expliciete blokdiagonalisatie van de Terwilliger algebra van het niet-binaire Hamming schema.

In hoofdstuk 2 brengen we de benodigde theorie in herinnering. In het bijzonder stippen we de krachtige methode van Delsarte [15] aan, waarmee met behulp van associatieschemas bovengrenzen voor $A_q(n,d)$ te verkrijgen zijn door middel van lineaire programmering. Het idee is om te kijken naar de afstandsverdeling $1 = x_0, x_1, \ldots, x_n$ van een code, waar x_i het gemiddeld aantal codewoorden op afstand i van een codewoord is. De getallen x_i voldoen aan bepaalde lineaire ongelijkheden. De eerste soort ongelijkheden heeft een directe combinatorische betekenis: de getallen x_i zijn niet-negatief en $x_i = 0$ als er geen twee woorden zijn op afstand i. De andere ongelijkheden, met coefficienten gegeven door de Krawtchouk polynomen, hebben een diepere betekenis. Zij weerspiegelen het feit dat de corresponderende lineaire combinatie $A := x_0A_0 + \cdots + x_nA_n$ van associatiematrices van het Hamming schema positief semidefiniet is. Dat het positief semidefiniet zijn van A kan worden teruggebracht tot een $n+1$ tal lineaire ongelijkheden, is het plezierige gevolg van het feit dat de Bose–Mesner algebra behorende bij het Hamming schema commutatief is, en daardoor in diagonaalvorm kan worden gebracht.

Een van de ideeen achter het onderhavige werk, is om naar de verdeling van *drietallen* codewoorden te kijken in plaats van naar paren. Dit leidt tot de bestudering van een verfijning van de Bose–Mesner algebra in Hoofdstuk 3. De algebra bestaat uit alle matrices die invariant zijn onder die automorfismen van het Hamming schema $H(n,q)$, die een gekozen woord vasthouden. Er is een basis van 0–1 matrices die geparametriseerd wordt door de mogelijke configuraties van drietallen woorden modulo automorfismen. We laten zien dat de algebra overeenkomt met de Terwilliger algebra [39] van het Hamming schema. Deze Terwilliger algebra is niet langer commutatief en kan daarom niet worden gediagonaliseerd. Het analogon voor niet-commutatieve algebras is een blokdiagonalisatie, waarbij de algebra bestaat uit alle matrices met gegeven blok-diagonaal structuur. Een centraal resultaat van dit proefschrift is een expliciete blokdiagonalisatie van de Terwilliger algebra behorende bij het niet-binaire Hamming schema. Hoewel het positief semidefiniet zijn van een matrix in de Terwilliger algebra niet langer kan worden geformuleerd door een klein aantal lineaire ongelijkheden, geeft de blokdiagonalisatie toch een handzame formulering in termen van het positief semidefinitiet zijn van een klein aantal kleine matrices (het aantal is $O(n^2)$ en de grootte $O(n)$).

In hoofdstuk 4 geven we een verscherping van de Delsarte grens voor codes. Met behulp van de expliciete blokdiagonalisatie van de Terwilliger algebra uit hoofdstuk 3, kan deze grens efficient worden bepaald middels semidefinite programmering. Voor $q = 3, 4, 5$ levert dit computationeel een reeks verscherpingen op voor bekende bovengrenzen voor $A_q(n,d)$.

In hoofdstuk 5 beschouwen we overdekkingscodes en geven we nieuwe ondergrenzen voor $K_q(n,r)$. Veel bestaande grenzen voor $K_q(n,r)$ zijn gebaseerd op de afstandsverdeling $A_0(\mathbf{x}), \ldots, A_n(\mathbf{x})$ van de code C gezien vanuit een woord $\mathbf{x}$. Hier is $A_i(\mathbf{x})$ het aantal woorden in C op afstand i van $\mathbf{x}$. Iedere lineaire ongelijkheid in $A_0, \ldots, A_n$ die voor de afstandsverdeling vanuit ieder woord $\mathbf{x}$ geldt, geeft een ondergrens voor $K_q(n,r)$. De voor

de hand liggende ongelijkheid

$$A_0 + A_1 + \cdots + A_r \geq 1 \tag{7.10}$$

leidt op deze manier tot dezelfde grens ('sphere covering bound') als het volume argument als boven. Vanuit polyhedraal oogpunt optimaliseren we een lineare functie over een een polytoop $P \subseteq [0,1]^{\mathbf{q}^n}$ binnen de eenheidskubus, met een groot aantal symmetrieen, namelijk de symmetrieen van de Hamming ruimte $\mathbf{q}^n$. Met behulp van de theorie van matrix snedes [32] kunnen we P vervangen door een kleinere convexe verzameling, en daarmee scherpere grenzen voor $K_q(n,r)$ vinden. Om deze grenzen efficient te kunnen bepalen met lineaire en semidefiniete programmering, is wederom de blokdiagonalisatie van de Terwilliger algebra van het Hamming schema van groot belang. Computationeel levert deze methode voor $q = 3$ en $q = 4$ een aantal verscherpingen op ten opzichte van de ondergrenzen voor $K_q(n,r)$ uit de literatuur.

In hoofdstuk 6 brengen we deze theorie van matrix-snedes in herinnering en bestuderen we de relatie tussen de nieuwe grenzen voor $A_q(n,d)$ en deze theorie van matrix snedes. In het bijzonder blijkt dat de grenzen voor $A_q(n,d)$ uit hoofdstuk 4 scherper zijn dan die afkomstig van het toepassen van matrix-snedes op het 'theta-body'. Dit is (vooral) te danken aan extra relaties die voortvloeien uit de aanwezige symmetrieen.

Dankwoord

Met groot genoegen maak ik hier van de mogelijkheid gebruik om een ieder te bedanken die mij gedurende mijn promotietijd heeft gesteund, met dit proefschrift als resultaat.

Zonder mijn promotor, Lex Schrijver, was dit proefschrift er niet geweest, en zou ik geen promotieonderzoek hebben gedaan in de combinatorische optimalisatie. Graag wil ik hem bedanken voor zijn continue steun en vertrouwen, ook wanneer ik dat laatste schier verloren had. Ik ben blij dat ik zo veel van hem heb kunnen leren.

Dit boekje heb ik opgedragen aan Violeta, mijn partner en moeder van onze twee kinderen Amber en Mark. Hoewel ik soms te weinig tijd voor hen vrij maakte, heeft Violeta mij altijd gesteund. Mark en Amber hebben mij altijd weer weten te verleiden om mijn werk even opzij te schuiven.

Veel heb ik ook te danken aan mijn ouders, en ook mijn schoonouders. Zij hebben mij op zoveel verschillende manieren beinvloed en ondersteund.

Voor de prettige werksfeer dank ik mijn collegas aan de UvA, in het bijzonder mijn kamergenoot Pia Pfluger. Ook aan het CWI heb ik het enorm getroffen met fijne collegas. Ik bedank Monique Laurent voor de gesprekken over het onderwerp van dit proefschrift. Ook wil ik mijn kamergenoot Gabor Maroti bedanken. Zonder hem was het vast niet gelukt om *Theory of Integer and Linear Programming* zo grondig te bestuderen. Ook ging er geen keer voorbij dat hij geen *nice puzzle* had. Ik vermoed dat zijn Hongaarse achtergrond hier deels verantwoordelijk voor was.

Graag wil ik ook Chris Zaal noemen. Ik herinner mij goed de SET-workshop die we aan het APS gegeven hebben, de opnamen van de Nationale Wetenschaps Quiz en diverse andere creativiteiten op het gebied van wiskunde-promotie. In het bijzonder heeft hij mij geintroduceerd bij Pythagoras, waar ik nog steeds de problemenrubriek mag vullen.

Ik dank ook Marco Zwaan. Via hem heb ik mogen proeven hoe het is om wiskundeleraren te onderwijzen aan de eerstegraads opleiding, een bijzondere ervaring.

Tenslotte dank ik de iedereen die ik niet met name heb genoemd, maar aan wie ik niettemin fijne herinneringen dank. Bedankt!

Curriculum Vitae

Dion Camilo Gijswijt is geboren op 20 maart 1978 te Bunschoten. Al vroeg had hij grote interesse in natuurkunde en andere exacte wetenschappen. Tijdens de eerste jaren van zijn middelbareschool-tijd groeide zijn interesse voor kunstmatige intelligentie en wiskunde. Het boek *Gödel, Escher, Bach* van D.R. Hofstadter had daarin een groot aandeel. Uiteindelijk gaf zijn deelname aan de International Wiskunde Olympiade in de laatste jaren van de middelbare school de doorslag om wiskunde te gaan studeren.

In 1996 slaagde hij voor het eindexamen VWO aan het Goois Lyceum in Bussum en begon aan een dubbele studie wiskunde en natuurkunde aan de Universiteit van Amsterdam. Na in 1997 zijn propedeuses wiskunde en natuurkunde cum laude te hebben behaald, besloot hij zich te concentreren op de studie wiskunde. Tijdens zijn studie besteede hij een groot deel van zijn tijd aan het tijdschrift Pythagoras, dat juist onder de bezielende leiding van Chris Zaal nieuw leven was ingeblazen. Nadat hij in 1996 begon met het vullen van de problemenrubriek, werd hij in 1998 tevens redacteur.

In augustus 2001 behaalde hij zijn doctoraaldiploma (cum laude) na het schrijven van een scriptie getiteld *The Colin de Verdière Graph Parameter* μ onder begeleiding van Lex Schrijver. In september 2001 begon hij, eveneens onder supervisie van Lex Schrijver, aan zijn promotie-onderzoek aan het KdVI aan de Universiteit van Amsterdam. Dit onderzoek, met als thema *Spectral Methods for Graph Optimization and Embedding*, mondde in juli 2005 uit in het onderhavige proefschrift.

Gedurende deze vier jaar als promovendus was hij ook in de gelegenheid andere activiteiten te ontplooien. Naast het met plezier begeleiden van diverse werkcolleges, heeft hij vooral veel geleerd van het doceren van een college grafentheorie aan eerstejaars wiskunde studenten, en later aan leraren aan de eerstegraads lerarenopleiding. Ook het begeleiden van twee studenten bij het schrijven van hun kandidaatsscriptie was een grote ervaring.

Daarnaast heeft hij zich beziggehouden met activiteiten ter promotie van de wiskunde. Naast zijn werk voor Pythagoras, was hij actief als lid van de vraagstukkencommissie voor de Nederlandse Wiskunde Olympiade, en was betrokken bij diverse promotionele activiteiten waaronder: de Leve de Wiskunde dag, Nationale Wetenschapsdag, voorlichtingsdagen van de UvA, mastercourse voor wiskundeleraren en workshops voor scholieren en leraren.