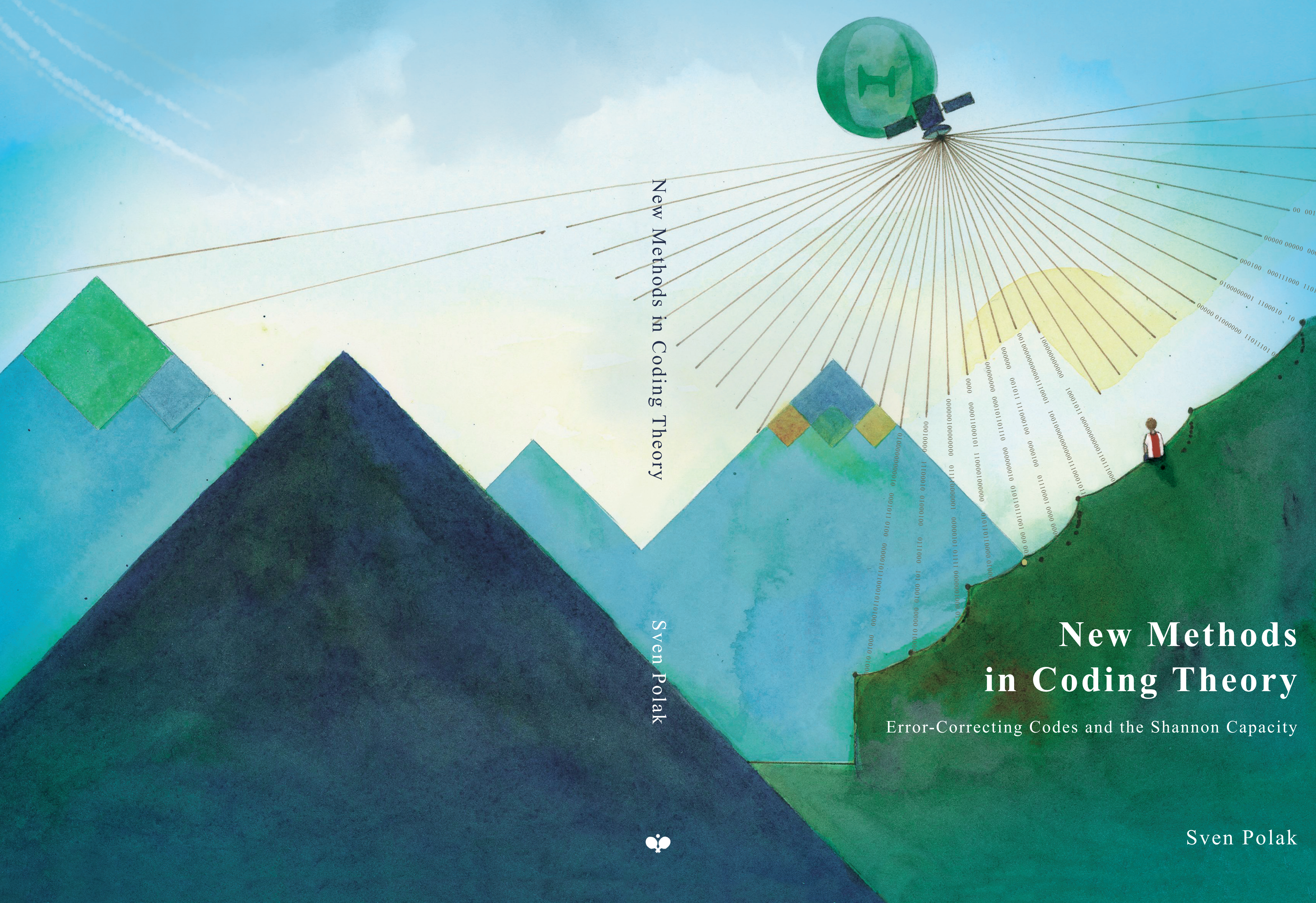
New methods in coding theory

Error-correcting codes and the Shannon capacity

Polak, S.C.



New Methods in Coding Theory

Sven Polak

New Methods in Coding Theory

Error-Correcting Codes and the Shannon Capacity

Sven Polak

New Methods in Coding Theory

Error-Correcting Codes and the Shannon Capacity

Sven Carel Polak

New Methods in Coding Theory

Error-Correcting Codes and the Shannon Capacity

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. ir. K.I.J. Maex
ten overstaan van een door het College voor Promoties
ingestelde commissie,
in het openbaar te verdedigen in de Agnietenkapel
op dinsdag 10 september 2019, te 14:00 uur

door

Sven Carel Polak

geboren te Amsterdam

Promotiecommissie:

Promotor:	
Prof. dr. A. Schrijver	Universiteit van Amsterdam
Copromotor:	
Prof. dr. A.E. Brouwer	Technische Universiteit Eindhoven
Overige leden:	
Prof. dr. N. Bansal	Technische Universiteit Eindhoven
Prof. dr. G.B.M. van der Geer	Universiteit van Amsterdam
Dr. D.C. Gijswijt	Technische Universiteit Delft
Dr. G. Regts	Universiteit van Amsterdam
Prof. dr. J.V. Stokman	Universiteit van Amsterdam

Faculteit der Natuurwetenschappen, Wiskunde en Informatica

Universiteit van Amsterdam

This research has been carried out at the Korteweg-de Vries Institute for Mathematics.

The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement №339109.

Cover design by Evelien Jagtman

Printed by Gildeprint

ISBN: 978-94-6323-747-5

Contents

Dankwoord

Voor u ligt het proefschrift *New Methods in Coding Theory: Error-Correcting Codes and the Shannon Capacity*, het resultaat van een vier jaar durend onderzoek aan het Korteweg-de Vries Instituut voor Wiskunde. Ik ben dankbaar dat ik de mogelijkheid daarvoor heb gekregen. Graag wil ik een aantal mensen persoonlijk bedanken.

De afgelopen vier jaar heeft Lex Schrijver, mijn promotor, mij deskundig en met grote toewijding begeleid. Lex, zonder jou was dit proefschrift er niet geweest. Dank voor je uitstekende begeleiding, voor alle afspraken op het KdvI, voor de vele emails over en weer, voor het nauwkeurig lezen van talloze manuscripten, voor je vertrouwen, en in het algemeen voor de fijne samenwerking. Ik heb heel veel van je geleerd en had me geen betere begeleider kunnen wensen. Bedankt Lex!

Mijn dank gaat ook uit naar copromotor Andries Brouwer, samen met wie ik een artikel over uniciteit van codes heb geschreven. De samenwerking verliep uitsluitend via '*brieven*' (e-mail), maar was zeer nuttig. Bedankt Andries, ook voor het goede commentaar.

Mijn medepromovendi en kamergenoten in F3.28 waren Bart Litjens en Bart Sevenster. Bart Litjens en ik hebben drie jaar lang dagelijks op het CWI getafeltennist. Bart is loyaal, heeft me veel geholpen met praktische zaken, en zonder hem zou ik vast nog nooit carnaval hebben gevierd. We hebben ook wiskundig goed samengewerkt: zo heb ik met Bart en Lex mijn eerste artikel geschreven. Ook met Bart Sevenster heb ik regelmatig over wiskunde gepraat, getafeltennist en – uiteraard – koffie gedronken. Barts directe relativerende opmerkingen waren een verrijking voor de sfeer in kamer F3.28. Bart en Bart, veel dank, het was een prachtige tijd. De *kamerspelen* – waarbij je bijvoorbeeld elastiekjes moest schieten op een bepaald doel, of zo snel mogelijk een artikel van Wikipedia moest overtypen – zullen mij zeker bijblijven. Ik ben ervan overtuigd dat deze activiteiten aan onze wiskundige creativiteit hebben bijgedragen.

Furthermore, I thank my other roommates and direct colleagues, to be specific: Guus, Pjotr, Lluís, Viresh, Jacob, Vaidy, Ewan, Ferenc, Fabian, for interesting discussions (both mathematical and non-mathematical), seminars, conferences, dinners, drinks at the Polder and numerous other fun activities. I thank all colleagues of the KdvI for the lunch conversations and coffee breaks. Marieke, instituutsmanager, en Evelien en Tiny van het secretariaat, jullie zorgden voor uitstekende ondersteuning en ik liep altijd graag bij jullie binnen.

Van het CWI dank ik om te beginnen Guido Schäfer, van wie ik veel geleerd heb in de fase voorafgaand aan het promotieonderzoek. Monique Laurent dank ik voor alle gesprekken en de cursus over semidefiniet programmeren. Verder dank ik al mijn CWI-vrienden voor de tafeltennis- en tafelvoetbalpartijen, vooral nadat Bart en Bart vertrokken waren. In het bijzonder wil ik hiervoor graag Sander, Pieter, Mathé en Ruben bedanken, ook voor de nuttige aanmerkingen op delen van dit proefschrift.

Dion Gijswijt dank ik voor de cursus over geheeltallige programmering en de gesprekken in Toronto over het ‘trifference’-probleem, Jeroen Zuiddam voor de interessante discussies over de Shannoncapaciteit en voor zijn goede commentaar op Hoofdstuk 9 van dit proefschrift, en Carla Groenland voor (alweer) het tafeltennissen en de leuke seminars.

Naast het onderzoek heeft het geven van onderwijs mij de afgelopen vier jaar veel voldoening gegeven. Chris Zaal verdient lof en dank voor het in goede banen leiden van de bacheloropleiding, ook toen ik zelf bachelorstudent was. Verder dank ik de vaste medewerkers die ik mocht assisteren bij het onderwijs: Gerard, Guus, Han, Hessel, Jan, Rob, bedankt voor de fijne samenwerking!

Ik dank de studenten die de afgelopen vier jaar mijn werkcolleges hebben gevolgd. Simon, het was me een genoegen je bachelorproject te begeleiden. Boudewijn, Edward, Helena, Mike, Ruben, Suzanne, Thijs en Wouter, bedankt voor jullie enthousiasme en voor het geven van die fantastische kaart, dat heeft een blijvende indruk op mij gemaakt. Edward en Suzanne dank ik in het bijzonder voor onze sportieve activiteiten. Ook alle andere werkcollegestudenten, bedankt!

Nu richt ik mij tot een aantal andere vrienden die me de afgelopen periode gesteund hebben. Wadim, Jochem, Rob en Hanneke, veel dank voor de avonturen die we tijdens en na onze studie beleefd hebben. Rizky, bedankt voor al het tafeltennissen na werktijd, de Indonesische maaltijden en de reizen om ons aller Ajax aan het werk te zien op vreemde bodem. Ook José voor dit laatste bedankt. Vasily, Wadim and Yana, thank you for our wonderful journeys in Russia and ‘in Europe’. Carlo, Felix, Maarten en Rik, bedankt voor de leuke spelletjesmiddagen. Mijn vrienden van zaalvoetbal, van de teams *FC Barcorona*, *De Echte Mannen* en *Der Angstgegner*, dank ik ook. In het bijzonder dank ik Arne en Joost van *Der Angstgegner* voor twee aanmerkingen op het voorblad van een eerdere versie van dit proefschrift.

Speciale dank gaat uit naar Boudien, mijn voormalige oppas die (in haar eigen woorden) wel oud is, maar er altijd voor me is.

Tot slot dank ik mijn familie. Mijn moeder, die me altijd helpt, me goed begrijpt en die ik zelfs ’s nachts kan bellen. Mijn vader, die me eveneens begrijpt, me praktische en wijze adviezen geeft, en die – zelf gepromoveerd en professor in Leiden – een voorbeeld voor me is bij mijn eigen promotie, maar ook Ajax met me toejuicht in de Arena. Heleen, bij wie ik altijd terecht kan. Mijn zusje Lara, die tijdens mijn PhD aan het Science Park studeerde, met wie ik talloze keren heb geluncht en met wie ik alles kan bespreken. Mijn zusje Noor, die al bijna halverwege het Vossius zit en vroeg of ze wel in het dankwoord kwam: reken maar, Noor! Ook dank ik al mijn andere familieleden en vrienden die hier niet bij naam genoemd zijn, maar wier aanwezigheid ik niettemin zeer waardeer. Bedankt dat jullie er zijn!

Sven Polak
Amsterdam, juli 2019

Chapter 1

Introduction

The art of doing mathematics consists in finding that special case which contains all the germs of generality.
— David Hilbert (1862–1943)

Between 1979 and 1981, the *Voyager* spacecrafts from NASA were travelling close to Jupiter and Saturn. They transmitted detailed images of both planets and their moons back to Earth. When a spacecraft sends a message over such a considerable distance, information gets lost or damaged easily. In other words, the information channel which is used is noisy. *Coding theory* is the branch of mathematics that deals with reliable transmission of information over noisy channels.

Claude Shannon initiated the study of coding theory in his seminal paper *A Mathematical Theory of Communication* from 1948 [85]. Shortly thereafter, Golay [40] and Hamming [44] discovered important codes with good error-correction properties. Moreover, Hamming [44] and Lee [49] introduced two distance functions, now central to coding theory and known as the Hamming and Lee distances. One of Golay's codes, the binary extended Golay code, was later used in the Voyager missions to facilitate the correction of transmission errors.

This thesis contributes to the field of coding theory, focussing in particular on upper bounds on the cardinality of *error-correcting codes* with certain parameters, on symmetry reductions of semidefinite programs in coding theory using representation theory, on uniqueness of certain codes —mostly related to the binary Golay code— and on the *Shannon capacity*, a graph parameter introduced by and named after the founding father of coding theory.

In the following sections we introduce the main topics studied in this thesis and we give historical background and motivation. We conclude this introduction with a description of the organization of the thesis into chapters, which includes a summary of our contributions per chapter.

1.1 Error-correcting codes

Suppose that Q is a finite set of $q \geq 2$ elements and fix a positive integer n. The set Q is our *alphabet*. A *word* is an element of Q^n and a *(q-ary) code* is a subset C of Q^n. For two words $u, v \in Q^n$, their *Hamming distance* $d_H(u, v)$ is the number of i with $u_i \neq v_i$.

For a code $C \subseteq Q^n$, its *minimum distance* $d_{\min}(C)$ is the minimum of $d_H(u,v)$ over all distinct $u, v \in C$. If $|C| \leq 1$, we set $d_{\min}(C) = \infty$. Define, for any integer d,

$$A_q(n,d) := \max\{|C| \mid C \subseteq Q^n,\ d_{\min}(C) \geq d\}. \tag{1.1}$$

Without loss of generality we usually take $Q := [q]$, where $[q]$ denotes the set $\{0, \ldots, q-1\}$. Moreover, if $q = 2$ we often write $A(n,d)$ instead of $A_q(n,d)$.

J.H. van Lint characterized the study of the numbers $A_q(n,d)$ as the *central problem in (combinatorial) coding theory* [50]. The main motivation for studying $A_q(n,d)$ is *error-correction*. Assume that transmitter T aims to send a message to receiver R, but their communication channel is noisy. Every time T sends a word to R at most e symbols change, for some positive integer e. Suppose that T only transmits words from a code C with $d_{\min}(C) \geq 2e+1$ to R, where C is known to both T and R. Then R can recover any transmitted word, since it is the word from C that is closest to the received word in Hamming distance. So in order to maximize the number of distinct words that can be sent over this channel, we should maximize $|C|$ provided that $d_{\min}(C) \geq 2e+1$. So we should find $A_q(n, 2e+1)$.

The numbers $A_q(n,d)$ are hard to compute in general. For many triples (q,n,d), only upper and lower bounds are known. Note that $A_q(n,d)$ can be interpreted as the independent set number of a graph, as follows. (Here the *independent set number* $\alpha(G)$ of a graph G is the maximum cardinality of a set of vertices of G, no two of which are adjacent.) Consider the graph $G(q,n,d)$ with vertex set Q^n, the set of all words, and edges between distinct words if their Hamming distance is strictly less than d. Then $A_q(n,d)$ is the independent set number $\alpha(G(q,n,d))$ of this graph.

Explicit codes yield lower bounds on $A_q(n,d)$ and they can be used for error-correction as explained. In this thesis we will study the problem of finding upper bounds on $A_q(n,d)$, which has received considerable research attention — see for example [12, 15, 16, 31, 67]. A classical upper bound on $A_q(n,d)$ is the *Delsarte bound (in the Hamming scheme)* [31]. The Delsarte bound is equal to a special case of the following general upper bound on the independent set number $\alpha(G)$ of a graph $G = (V, E)$ in the spirit of Lovász [53], introduced by McEliece, Rodemich and Rumsey [59] and Schrijver [79]:

$$\vartheta'(G) := \max\left\{ \textstyle\sum_{u,v \in V} X_{u,v} \,\middle|\, X \in \mathbb{R}^{V \times V}_{\geq 0},\ \mathrm{tr}(X) = 1,\ X_{u,v} = 0 \text{ if } uv \in E,\ X \succeq 0 \right\}. \tag{1.2}$$

Here $X \succeq 0$ denotes the condition that X is *positive semidefinite*, i.e., symmetric with all eigenvalues nonnegative. This optimization problem is an example of a semidefinite programming (SDP) problem.

The upper bound in (1.2) can be computed in time polynomial in the number of vertices of the graph. For some graphs (graphs whose edge set is a union of classes of a symmetric association scheme) it can be reformulated as a linear program, using symmetry reductions. An example of such a graph is the graph $G(q,n,d)$ defined above. In this case, $D_q(n,d) := \vartheta'(G(q,n,d))$ is called the *Delsarte bound (in the Hamming scheme)*, and the linear program can be formulated as follows. Let $K_t(x)$ be the t-th *Krawtchouk polynomial*:

$$K_t(x) := \sum_{j=0}^{t} (-1)^j \binom{x}{j} \binom{n-x}{t-j} (q-1)^{t-j}, \quad \text{for } 0 \leq t \leq n. \tag{1.3}$$

Then $A_q(n,d) \leq D_q(n,d)$, where

$$D_q(n,d) = \max \big\{ \textstyle\sum_{i=0}^{n} a_i \;\big|\; a_0 = 1,\; a_1 = \ldots = a_{d-1} = 0,\;\; a_i \geq 0 \text{ if } d \leq i \leq n, \\ \textstyle\sum_{i=0}^{n} K_t(i) a_i \geq 0 \text{ for all } 0 \leq t \leq n \big\}. \tag{1.4}$$

The optimization problem (1.4) contains only $n+1$ variables, which number is linear in n. By contrast, the number of variables in (1.2), which is the number of edges of $G(q,n,d)$, is exponential in n. So (1.4) gives a considerable reduction. It can be used to compute upper bounds on $A_q(n,d)$ for several triples (q,n,d), cf. [12, 15, 16, 31, 92].

The Delsarte bound is an SDP bound based on pairs of codewords (edges in the underlying graph), as can be seen from (1.2). For binary codes, the Delsarte bound was generalized to an SDP bound based on triples of codewords by Schrijver [81], and later to a quadruple bound by Gijswijt, Mittelmann and Schrijver [37]. Also, a bound for nonbinary codes based on triples of codewords has been studied by Gijswijt, Schrijver and Tanaka [38] — see also Gijswijt's thesis [36].

In this thesis, we consider the following SDP bound based on quadruples of codewords. For any k, let $\mathcal{C}_k$ be the collection of codes of cardinality at most k. For each $x : \mathcal{C}_4 \to \mathbb{R}$ define the $\mathcal{C}_2 \times \mathcal{C}_2$ matrix $M(x)$ by

$$M(x)_{C,C'} := x(C \cup C').$$

Then $A_q(n,d) \leq B_q(n,d)$, with

$$B_q(n,d) := \max \big\{ \textstyle\sum_{v \in [q]^n} x(\{v\}) \mid x : \mathcal{C}_4 \to \mathbb{R}_{\geq 0},\; x(\emptyset) = 1,\;\; x(S) = 0 \text{ if } d_{\min}(S) < d, \\ M(x) \succeq 0 \big\}. \tag{1.5}$$

Indeed, let C be a code with $d_{\min}(C) \geq d$ and $|C| = A_q(n,d)$. Define $x : \mathcal{C}_4 \to \mathbb{R}$ by $x(S) = 1$ if $S \subseteq C$ and $x(S) = 0$ otherwise, for $S \in \mathcal{C}_4$. Then x satisfies the conditions in (1.5): the condition $M(x) \succeq 0$ follows from the fact that for this x one has $M(x)_{S,S'} = x(S)x(S')$ for all $S, S' \in \mathcal{C}_2$. Moreover, we have $\sum_{v \in [q]^n} x(\{v\}) = |C| = A_q(n,d)$, yielding $A_q(n,d) \leq B_q(n,d)$.

We will apply representation theory to reduce the size of the above optimization problem from exponential in n to polynomial in n, with entries (i.e., coefficients) being polynomials in q. We calculate the bound for some values of q, n, d, yielding new upper bounds for five instances of $A_q(n,d)$. In the reduction, we use a general method used in all symmetry reductions throughout this thesis. We outline this method in Section 1.2.

We also explore other methods of finding upper bounds on $A_q(n,d)$, based on combinatorial divisibility arguments. Our most prominent result in this direction gives in certain cases a strengthening of a bound implied by the Plotkin bound (cf. [54, 68, 67]). We prove the following.

Theorem (Theorem 5.2.5)**.** *Suppose that q, n, d, m are positive integers with $q \geq 2$, such that $d = m(qd - (q-1)(n-1))$, and such that $n - d$ does not divide $m(n-1)$. If $r \in \{1, \ldots, q-1\}$ satisfies*

$$n(n-1-d)(r-1)r < (q-r+1)(qm(q+r-2) - 2r),$$

then $A_q(n,d) < q^2 m - r$.

The theorem yields new bounds for the cases $A_5(8,6)$ and $A_4(11,8)$. We also find a number of other new bounds on $A_q(n,d)$ using divisibility arguments.

Before we explain the general method of symmetry reductions to reduce semidefinite programs as in (1.5) in more detail, we first introduce two other types of error-correcting codes: binary *constant weight codes* and q-ary *Lee codes*. For these codes we will formulate SDP bounds in this thesis as well, and show that they can be computed in time polynomially bounded in n (for fixed q in the case of Lee codes). We calculate the bound for some values of q, n, d, yielding explicit new upper bounds for several instances of $A_q^L(n,d)$.

Constant weight codes. Let $Q := \mathbb{F}_2 = \{0,1\}$ be the binary alphabet, where $\mathbb{F}_2$ denotes the field of two elements. For $v \in \mathbb{F}_2^n$, the *weight* of v is $\text{wt}(v) := d_H(v, \mathbf{0})$, where $\mathbf{0} := 0\ldots0$ denotes the all-zeros word. So $\text{wt}(v)$ is the number of 1's in v. Fix a positive integer w. Instead of considering all (unrestricted) words in Q^n, we now restrict to words with a constant weight w. A (binary) *constant weight code* is a code $C \subseteq \mathbb{F}_2^n$ in which all words have a fixed weight w. Define

$$A(n,d,w) := \max\{|C| \mid C \subseteq \mathbb{F}_2^n,\ d_{\min}(C) \geq d,\ \text{wt}(v) = w\ \forall\, v \in C\}. \tag{1.6}$$

Similar to $A_q(n,d)$, the numbers $A(n,d,w)$ are subject to a wide range of research (see for example [1, 12, 31, 81]), and they are also hard to compute in general. Note that $A(n,d,w)$ is the maximum cardinality of a collection $\mathcal{A}$ of subsets of size w of a set X of n elements such that any two subsets in the collection have at most $w - d/2$ elements in common.

Constant weight codes are used in GSM mobile telephone networks to generate 'frequency hopping lists' for cell towers [87]. Suppose that we assign to each cell tower a list of w out of n possible frequencies. Each tower hops between frequencies from its list according to a given rule. Less overlap between the lists from any two cell towers (i.e., larger Hamming distance between the corresponding constant weight w codewords), contributes to less interference, i.e., fewer collisions on one frequency. Larger constant weight codes with a specified minimum distance then permit larger spaces between two towers with the same list in the GSM network, which also leads to less interference.

Delsarte [31] formulated a linear programming upper bound on $A(n,d,w)$, now known as the *Delsarte bound in the Johnson scheme*, which can be interpreted as an SDP bound based on pairs of codewords (as in (1.2)), which again is a linear programming bound. The Delsarte bound was generalized to an SDP bound based on triples of codewords by Schrijver [81]. Schrijver's bound was strengthened by Kim and Toan with extra linear inequalities [47]. In this thesis we consider two SDP upper bounds on $A(n,d,w)$ based on quadruples of codewords, which admit definitions similar to but different from (1.5). Using symmetry reductions, we can compute both bounds in time polynomially bounded in n, resulting in several new upper bounds on $A(n,d,w)$.

The new upper bounds imply the exact values $A(22,8,10) = 616$ and $A(22,8,11) = 672$. Lower bounds on these two instances are obtained from the *shortened binary Golay code*, which is the unique (unrestricted) binary optimal code achieving $A_2(22,7) = 2^{11}$ containing $\mathbf{0}$, up to a permutation of the coordinate positions [20]. From these new values in combination with previously known values of $A(n,d,w)$, it can be concluded that the shortened binary Golay code is a union of constant weight w codes of sizes $A(n,d,w)$.

The Lee distance and Lee codes. The Hamming distance measures how many symbols are different, but not *to what extent* they are different. To give more importance to symbols which are far apart in two words and less importance to symbols which differ only slightly, C.Y. Lee introduced a different distance function [49].

Let $Q := \mathbb{Z}_q$, the cyclic group of order q, which has a natural distance function $\delta : \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{Z}$ given by

$$\delta(x, y) := \min\{|x - y|,\, q - |x - y|\}, \tag{1.7}$$

where we consider x and y as integers in $\{0, \dots, q-1\}$. So $\delta(x, y)$ is the length of a shortest path from x to y in the circuit graph C_q on q points. Fix $n \in \mathbb{N}$. The *Lee distance* of two words $u, v \in \mathbb{Z}_q^n$ is

$$d_L(u, v) := \textstyle\sum_{i=1}^n \delta(u_i, v_i). \tag{1.8}$$

The Lee distance is used in so called 'phase modulated systems' — see [11, Chapter 8]. These are examples of noisy information channels in which a symbol is more likely to change upon transmission into a symbol which is close to it, than into a symbol which is far from it.

The *minimum Lee distance* $d_{\min}^L(C)$ of a code $C \subseteq \mathbb{Z}_q^n$ is the minimum of $d_L(u, v)$ taken over distinct $u, v \in C$. If $|C| \leq 1$, we set $d_{\min}^L(C) = \infty$. For any natural number d, define analogously to (1.1) and (1.6),

$$A_q^L(n, d) := \max\{|C| \mid C \subseteq \mathbb{Z}_q^n,\ d_{\min}^L(C) \geq d\}. \tag{1.9}$$

As is the case with $A_q(n, d)$ and $A(n, d, w)$, it generally is an interesting and nontrivial problem to determine the numbers $A_q^L(n, d)$. The classical Delsarte linear programming bound (in the Lee association scheme) based on pairs of codewords provides upper bounds on $A_q^L(n, d)$ [4, 5, 31]. In [7], the possibility of applying semidefinite programming to Lee codes is mentioned and it is stated that to the best knowledge of the authors, such bounds for Lee codes using triples have not yet been studied. In this thesis we study an SDP bound based on triples of codewords and show that it can be reduced to size bounded by a polynomial in n (for fixed q). The method yields several new upper bounds on $A_q^L(n, d)$ for $q \in \{5, 6, 7\}$. We only consider $q \geq 5$, since for $q = 4$, it holds that $A_4^L(n, d) = A_2(2n, d)$ — this follows by applying the Gray map [28]. Moreover, if $q = 2$ or $q = 3$, the Lee distance coincides with the Hamming distance.

1.2 Symmetry reductions with representation theory

For the sake of exposition, we first sketch how to reduce the optimization problem (1.5). After that, we describe the general method that is used in all symmetry reductions throughout this thesis.

To explain the reduction of (1.5), let H be the wreath product $S_q^n \rtimes S_n$, where S_q and S_n denote the symmetric groups on q and n elements, respectively. For each k, the group H acts naturally on Q^n, hence on the collection $\mathcal{C}_k$ of all codes $C \subseteq Q^n$ with $|C| \leq k$, maintaining minimum distances and cardinalities of elements of $\mathcal{C}_k$ (being codes). Then we can assume that x is invariant under the H-action on $\mathcal{C}_4$. That is, we can assume that $x(C) = x(D)$ whenever $C, D \in \mathcal{C}_2$ and $D = g \cdot C$ for some $g \in H$. Indeed, the conditions in (1.5) are maintained under replacing x by $g \cdot x$. (Note that $M(g \cdot x)$ is obtained from $M(x)$ by simultaneously permuting rows and columns.) Moreover, the objective function does not change by this action. Hence the optimum x can be replaced by the average of all $g \cdot x$ (over all $g \in H$), by the convexity of the set of positive semidefinite matrices. This makes the optimum solution H-invariant.

Let Ω_4 be the set of H-orbits on $\mathcal{C}_4$. Note that Ω_4 is bounded by a polynomial in n (independently of q). As (1.5) has an H-invariant optimum solution, we can replace, for each $\omega \in \Omega_4$ and $C \in \omega$, each variable $x(C)$ by a variable $z(\omega)$. In this way we obtain $M(z)$. Note that $M(z)$ depends only on $|\Omega_4|$ variables $z(\omega)$, which is polynomially bounded in n. Furthermore, $M(z)$ is invariant under the simultaneous action of H on its rows and columns. However, its size is still exponential in n. To reduce the matrix $M(z)$ further, we use a general method for symmetry reductions, which we will give in detail in Chapter 3 and which we sketch now.

The main symmetry reduction. Let G be a finite group acting on a finite set Z. Let $(\mathbb{C}^{Z\times Z})^G$ denote the set of (complex) $Z \times Z$ matrices invariant under the simultaneous action of G on its rows and columns. This means that $(\mathbb{C}^{Z\times Z})^G$ can be identified with the *centralizer algebra* of the action of G on $\mathbb{C}^Z$, i.e., the collection of G-equivariant endomorphisms $\mathbb{C}^Z \to \mathbb{C}^Z$. Then it is a standard fact from representation theory that there exists a *block diagonalization* of $(\mathbb{C}^{Z\times Z})^G$. For our purposes, this is a linear bijection

$$\Phi\,:\,(\mathbb{C}^{Z\times Z})^G \to \bigoplus_{i=1}^{k} \mathbb{C}^{m_i\times m_i}$$

(for some $k, m_1, \ldots, m_k \in \mathbb{N}$), such that M is positive semidefinite if and only if $\Phi(M)$ is positive semidefinite, for each $M \in (\mathbb{C}^{Z\times Z})^G$. The map Φ can be given by $M \mapsto U^*MU$ for a matrix U depending on G but independent of M. Here U^* denotes the conjugate transpose of the matrix U.

Now, let Z be a finite set and let $n \in \mathbb{N}$. Then the wreath product $H := G^n \rtimes S_n$ acts on Z^n, by permuting the n coordinates and by acting with G on the elements of Z in each coordinate separately. Then we can apply the previous considerations to the finite group H acting on the finite set Z^n. So there exists a block diagonalization $M \mapsto U^*MU$ of $M \in (\mathbb{C}^{Z^n\times Z^n})^H$, for a matrix U depending on H but independent of M. In this case the order of U^*MU is polynomial in n.

The matrices M we consider in this thesis are real matrices. Moreover, it turns out that in our applications the matrices U can be taken to be real matrices; so $U^{\mathsf{T}} = U^*$. The issue which is crucial to us is that M is positive semidefinite if and only if each of the smaller matrix blocks in the image $U^{\mathsf{T}}MU$ is positive semidefinite. This will allow us to reduce our semidefinite programs to size polynomially bounded in n.

In this thesis we show how to compute the matrix entries of the image $U^{\mathsf{T}}MU$ of the block diagonalization of $(\mathbb{C}^{Z^n\times Z^n})^H$ explicitly, from a known block diagonalization of $(\mathbb{C}^{Z\times Z})^G$ (with corresponding matrix U). This is the *main symmetry reduction*. An algorithm appeared in a manuscript of Gijswijt [35], but our method is an adaptation of the —more direct— method of [52]. In particular, we consider the following cases.

(i) For q-ary codes with the Hamming distance we take $G := S_q$ and $Z := [q]$ or $Z := [q]^2$. We use the set $Z = [q]$ in the reductions for the Delsarte bound, to illustrate the method (see Section 3.4.2). The set $Z = [q]^2$ is used in the reductions for our quadruple bound $B_q(n, d)$ in Chapter 4.

Note that the matrices $M(z)$ described above are $\mathcal{C}_2 \times \mathcal{C}_2$ matrices, i.e., the rows and columns of the matrices are indexed by *unordered* pairs of codewords. However, the method gives a reduction of $Z^n \times Z^n = ([q]^2)^n \times ([q]^2)^n \cong ([q]^n)^2 \times ([q]^n)^2$ matrices, i.e., matrices whose rows and columns are indexed by *ordered* pairs of codewords. This is not a problem; we could have defined $M(z)$ to be indexed by ordered pairs of codewords in the definition of $B_q(n,d)$. But in the present case we can further reduce the program by a factor 2, since there is an S_2-action on the ordered pairs. See Chapter 4.

(ii) For binary constant weight codes we take $G := \{1\}$, the trivial group and $Z := \mathbb{F}_2$ or $Z := \mathbb{F}_2^2$. So the group acts trivially on the alphabet, as the weight of each word must remain fixed. See Chapter 6.

(iii) For q-ary codes with the Lee distance we take $Z := \mathbb{Z}_q$ and $G := D_q$, the dihedral group of order $2q$, or $G := S_2$. We take the latter group in case the symbol $0 \in \mathbb{Z}_q$ is fixed, which is the case in a matrix occurring in the semidefinite programming bound based on triples of codewords. Here the action of S_2 on $\mathbb{Z}_q$ is the *reflection action*, i.e., we consider $0, \ldots, q-1 \in \mathbb{Z}_q$ as vertices of a regular q-gon, and the non-identity element of S_2 switches the vertices i and $q-i$ (for $i = 1, \ldots, \lfloor (q-1)/2 \rfloor$). See Chapter 8.

We also give a generalization of the method to groups of the form $(G_1^{j_1} \rtimes S_{j_1}) \times \ldots \times (G_s^{j_s} \rtimes S_{j_s})$ acting on sets of the form $Z_1^{j_1} \times \ldots \times Z_s^{j_s}$, where $Z_1, \ldots, Z_s$ are finite sets and $G_1, \ldots, G_s$ are finite groups. In coding theory, this can be used in semidefinite programs to reduce matrices depending on a fixed code D. We use this in the reductions for constant weight codes and in certain reductions for Lee codes — see Sections 6.2.1 and 8.5.2. Other applications of the generalization, which we do not discuss here, include reductions of matrices in semidefinite programs for codes with mixed alphabets [51], ternary (or q-ary) constant weight codes [76], or doubly constant weight codes [1, 90].

1.3 Uniqueness of codes

Until now we have discussed bounds on $A_q(n,d)$, $A(n,d,w)$ and $A_q^L(n,d)$. If we know the value of a certain case of one of these parameters, it is natural to ask if we can *classify* the corresponding optimal codes up to equivalence (see below). An analysis of a complete catalogue of certain objects often provides knowledge regarding the common structure of the objects, and may help in proving theorems. See the book by Kaski and Östergård [46].

Two q-ary codes $C, D \subseteq [q]^n$ are *equivalent* if D can be obtained from C by first permuting the n coordinates and by subsequently permuting the alphabet $[q]$ in each coordinate separately, i.e., if there is a $g \in S_q^n \rtimes S_n$ such that $g \cdot C = D$. Similarly, two binary constant weight codes C, D are *equivalent* if D can be obtained from C by permuting the n coordinates. Finally, two codes $C, D \subseteq \mathbb{Z}_q^n$ are *Lee equivalent* if there is a $g \in D_q^n \rtimes S_n$ such that $g \cdot C = D$.

As mentioned before, a famous code is the binary Golay code, discovered by Marcel J.E. Golay [40]. It is the unique binary code achieving $A(23,7) = 2^{12}$, up to the equivalence relation described above. The uniqueness was proved by Snover [88] and later with a simpler proof by Delsarte and Goethals [32]. The Golay code is *perfect*, which means that the balls with radius 3 (in Hamming distance) around the codewords form a partition of $\mathbb{F}_2^{23}$. It can be extended with a 24th *parity* bit, which equals the weight (mod 2) of the codeword, to obtain the *extended binary Golay code*. This is the unique (up to equivalence) optimal code achieving $A(24,8) = 2^{12}$ [31, 40]. If it contains $\mathbf{0}$, the zero word, then the extended binary Golay code is *linear*, i.e., it is a subspace of $\mathbb{F}_2^{24}$. A basis is given by the rows of the 'generator' matrix in Figure 1.1.

$$\begin{array}{cccccccccccccccccccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&0&0&1&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&1&0&1&1\\
0&0&1&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&1&0&1&1&1\\
0&0&0&1&0&0&0&0&0&0&0&0&1&1&1&0&0&0&1&0&1&1&0&1\\
0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&1&0&1&1&0&1&1\\
0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&1&1&0&1&1&1\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&1&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&1&0&1&1&1&0&1\\
0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&1&0&1&1&1&0&0&1\\
0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&1&0&1&1&1&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&0&1&1&1&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&0
\end{array}$$

Figure 1.1: A generator matrix of the extended binary Golay code (i.e., the 2^{12} codewords are sums mod 2 of the rows of this matrix). The extended binary Golay code was used in the *Voyager* missions to Jupiter and Saturn [94].

The binary Golay code, assuming it contains $\mathbf{0}$, contains 1288 words of weight 11. So $A(23,8,11) \geq 1288$. With semidefinite programming based on triples of codewords, A. Schrijver proved an upper bound matching the lower bound [81]. So $A(23,8,11) = 1288$. Of these 1288 words in the binary Golay code, exactly 616 words have a 1 at any fixed position, and exactly 672 words have a 0 at any position. So $A(22,8,10) \geq 616$ and $A(22,8,11) \geq 672$. As mentioned in Section 1.1, in this thesis we show SDP upper bounds matching these lower bounds.

Using information obtained from the SDP output, we prove that the optimal codes achieving $A(23,8,11) = 1288$, $A(22,8,10) = 616$ and $A(22,8,11) = 672$ are the *unique* codes achieving these values, up to a permutation of the coordinate positions.

Uniqueness of codes related to the binary Golay code has been studied by Brouwer (cf. [20]). He explains that there exist unique codes up to equivalence achieving $A(24-i,8) = 2^{12-i}$ for $i = 0,\ldots,3$. The unique code for the case $i = 0$ is the extended binary Golay code, and the unique codes for the cases $i = 1,\ldots,3$ are obtained by taking subcodes and throwing away coordinates of this code (also called *shortening*). The question whether the statement also holds for the case $i = 4$ was still open. In this thesis, we prove that there exist several nonequivalent codes achieving $A(20,8) = 2^{10}$. So the quadruply shortened binary extended Golay code is not the unique optimal code attaining $A(20,8) = 2^{10}$. We show that there exist precisely 15 equivalence classes of such codes with all distances divisible by 4. We also show that there exist such codes with not all distances divisible by 4.

Kirkman systems and Lee codes. A classic combinatorial problem is *Kirkman's schoolgirl problem*, posed by Thomas P. Kirkman in 1850 in the *Lady's and Gentleman's Diary*.

> *"Fifteen young ladies in a school walk out three abreast for seven days in succession: it is required to arrange them daily, so that no two walk twice abreast."*

There exist 7 nonequivalent solutions to Kirkman's problem (up to a permutation of the girls and a permutation of the days of the week) [29]. It is known that there is a 1-1-correspondence between equivalence classes of solutions to Kirkman's problem and equivalence classes of optimal codes achieving $A_5(7,6) = 15$ [83] (see also Chapter 5). In Chapter 5, we exploit the classification of solutions to Kirkman's problem and the described 1-1-correspondence to prove that $A_5(8,6) \leq 65$, using a divisibility argument (the best previously known upper bound was $A_5(8,6) \leq 75$).

We also explore a connection with Lee codes in Chapter 8. Previously, the upper bound $A_5^L(7,9) \leq 15$ was known [5, 74], but it was not known whether a code attaining this value exists. Any code achieving this upper bound is equivalent to an arrangement of 15 girls 7 days in succession into triples, where the triples are placed at the corners of a pentagon, such that the total Lee distance between any two girls over the 7 days is 9 — see Section 8.3. This problem connects to, but is different from, the above-mentioned Kirkman's schoolgirl problem.

Consider the following $\mathbb{Z}_7 \times \mathbb{Z}_7$ matrix with entries in $\mathbb{Z}_5$:

$$\widetilde{M} := \begin{pmatrix} 0 & 1 & 1 & 3 & 1 & 3 & 3 \\ 1 & 1 & 3 & 1 & 3 & 3 & 0 \\ 1 & 3 & 1 & 3 & 3 & 0 & 1 \\ 3 & 1 & 3 & 3 & 0 & 1 & 1 \\ 1 & 3 & 3 & 0 & 1 & 1 & 3 \\ 3 & 3 & 0 & 1 & 1 & 3 & 1 \\ 3 & 0 & 1 & 1 & 3 & 1 & 3 \end{pmatrix}, \quad \text{so } \widetilde{M}_{i,j} = \begin{cases} 0, & \text{if } i+j \equiv 0 \pmod 7, \\ 1, & \text{if } i+j \text{ is a nonzero square mod } 7, \\ 3, & \text{if } i+j \text{ is not a square mod } 7. \end{cases} \tag{1.10}$$

We show that $A_5^L(7,9) = 15$, and an optimal code proving this is $\widetilde{M} \cup -\widetilde{M} \cup \{\mathbf{0}\}$, where the matrix $\widetilde{M}$ is interpreted as a 5-ary code of size 7 (i.e., the rows are the codewords). We also obtain, using the SDP output and computer experiments, that this is the *unique* code achieving this value, up to Lee equivalence. As the mentioned code has minimum Hamming distance 5, there is no arrangement of 15 girls 7 days in succession into triples which is a solution simultaneously to both problems given above.

1.4 The Shannon capacity

Now we introduce the Shannon capacity, the final topic of study in this thesis. For any graph $G = (V,E)$ and $n \in \mathbb{N}$, let $G^{\boxtimes n}$ denote the graph with vertex set V^n and edges between two distinct vertices $(u_1,\ldots,u_n)$ and $(v_1,\ldots,v_n)$ if and only if for all $i \in \{1,\ldots,n\}$ one has either $u_i = v_i$ or $u_iv_i \in E$. The graph $G^{\boxtimes n}$ is known as the n-th *strong product power* of G. The *Shannon capacity* of G is defined as

$$\Theta(G) := \sup_{n\in\mathbb{N}} \sqrt[n]{\alpha(G^{\boxtimes n})}, \tag{1.11}$$

where $\alpha(G^{\boxtimes n})$ denotes the maximum cardinality of an independent set in $G^{\boxtimes n}$. Since $\alpha(G^{\boxtimes (n_1+n_2)}) \geq \alpha(G^{\boxtimes n_1})\alpha(G^{\boxtimes n_2})$ for any two positive integers n_1 and n_2, Fekete's lemma (cf. [34], see also [80, Corollary 2.2a]) implies that $\Theta(G) = \lim_{n\to\infty} \sqrt[n]{\alpha(G^{\boxtimes n})}$.

The Shannon capacity was introduced by Shannon [86] and is an important and widely studied parameter in information theory (see e.g., [3, 18, 43, 53, 98]). It is the effective size of an alphabet in an information channel represented by the graph G. The input is a set of letters $V(G) = Q := \{0, \dots, q-1\}$ and two letters are 'confusable' when transmitted over the channel if and only if there is an edge between them in G. Then $\alpha(G)$ is the maximum size of a set of pairwise non-confusable single letters. Moreover, $\alpha(G^{\boxtimes n})$ is the maximum size of a set of pairwise non-confusable n-letter words. (Here two n-letter words u, v are confusable if and only if u_i and v_i are confusable for all $1 \leq i \leq n$.) Taking n-th roots and letting n go to infinity, we find the effective size of the alphabet in the information channel: $\Theta(G)$.

A classical upper bound on Θ is Lovász's ϑ-function [53]. For any graph G, the number $\vartheta(G)$ is equal to the maximum (1.2) over all $X \in \mathbb{R}^{V \times V}$ instead of over nonnegative X. The Shannon capacity of C_5, the cycle on 5 vertices, was already discussed by Shannon in 1956 [86], who showed $\sqrt{5} \leq \Theta(C_5) \leq 5/2$. The easy lower bound of $\sqrt{5}$ is obtained from the independent set $\{(0,0), (1,2), (2,4), (3,1), (4,3)\}$ in $C_5^{\boxtimes 2}$. More than twenty years later, Lovász [53] determined that $\Theta(C_5) = \sqrt{5}$ by proving an upper bound matching this lower bound: he showed $\Theta(C_5) \leq \vartheta(C_5) = \sqrt{5}$. More generally, for odd q,

$$\Theta(C_q) \leq \vartheta(C_q) = \frac{q\cos(\pi/q)}{1 + \cos(\pi/q)}. \tag{1.12}$$

Here C_q denotes the cycle on q vertices. For q even it is not hard to see that $\Theta(C_q) = q/2$.

The Shannon capacity of C_7 is still unknown and its determination is a notorious open problem in extremal combinatorics [18, 39]. Many lower bounds have been given by explicit independent sets in some fixed power of C_7 [10, 56, 93], while the best known upper bound is $\Theta(C_7) \leq \vartheta(C_7) < 3.3177$. In this thesis we give an independent set of size 367 in $C_7^{\boxtimes 5}$, which yields $\Theta(C_7) \geq 367^{1/5} > 3.2578$. The best previously known lower bound on $\Theta(C_7)$ is $\Theta(C_7) \geq 350^{1/5} > 3.2271$, found by Mathew and Östergård [56]. They proved that $\alpha(C_7^{\boxtimes 5}) \geq 350$ using stochastic search methods that utilize the symmetry of the problem. We obtained our new lower bound on $\alpha(C_7^{\boxtimes 5})$ and on $\Theta(C_7)$ by considering so-called circular graphs — see Chapter 9 for details.

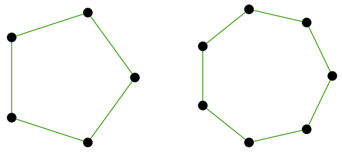


Figure 1.2: The graphs C_5 (left) and C_7 (right).

Next we will define circular graphs, explain the connection of independent sets in strong product powers of these graphs to Lee codes, and we explain which other results about circular graphs are proved in this thesis.

The Shannon capacity of circular graphs. For positive integers q, d with $q \geq 2d$, the *circular graph* $C_{d,q}$ is the graph with vertex set $\mathbb{Z}_q$ (the cyclic group of order q) in which two distinct vertices are adjacent if and only if their distance (mod q) is strictly less than d. So $C_{2,q} = C_q$. A closed formula for $\vartheta(C_{d,q})$, Lovász's upper bound on $\Theta(C_{d,q})$, is given in [8], see (1.16) below.

To study the Shannon capacity of circular graphs, we are interested in the independent set numbers $\alpha(C_{d,q}^{\boxtimes n})$. Independent sets in $C_{d,q}^{\boxtimes n}$ are strongly related to Lee codes, as we will now explain.

If (X, d) is a metric space, then (X^n, d_p) is also a metric space. Here d_p denotes the distance function given by

$$d_p((x_1, \ldots, x_n), (x_1', \ldots, x_n')) := \|(d(x_1, x_1'), \ldots, d(x_n, x_n'))\|_p, \tag{1.13}$$

where p either is a real number at least 1, or $p = \infty$. Now fix $X := \mathbb{Z}_q$ and $d := \delta$ from (1.7). If we take $p = 1$ in (1.13), we obtain the Lee distance as in (1.8). However, if we take $p = \infty$ in (1.13) we obtain the so-called *Lee*$_\infty$ *distance*. So for $u, v \in \mathbb{Z}_q^n$, their Lee$_\infty$ distance is defined as

$$d_{L_\infty}(u, v) = \max_{i \in \{1,\ldots,n\}} \delta(u_i, v_i). \tag{1.14}$$

The *minimum Lee*$_\infty$ *distance* $d_{\text{min}}^{L_\infty}(C)$ of a set $C \subseteq \mathbb{Z}_q^n$ is the minimum Lee$_\infty$ distance between any pair of distinct elements of C. If $|C| \leq 1$, we set $d_{\text{min}}^{L_\infty}(C) = \infty$. Then $d_{\text{min}}^{L_\infty}(C) \geq d$ if and only if C is independent in $C_{d,q}^{\boxtimes n}$. Define

$$A_q^{L_\infty}(n, d) := \alpha(C_{d,q}^{\boxtimes n}) = \max\{|C| \mid C \subseteq \mathbb{Z}_q^n,\ d_{\text{min}}^{L_\infty}(C) \geq d\}. \tag{1.15}$$

Compare with the definition of $A_q^L(n, d)$ in (1.9). The SDP upper bound on $A_q^L(n, d)$ based on triples of codewords is easily adapted to a new SDP upper bound on $A_q^{L_\infty}(n, d) = \alpha(C_{d,q}^{\boxtimes n})$, sharpening ϑ (cf. [53]) and ϑ' (cf. [59, 79]), using the same symmetry reductions as for Lee codes — see Section 9.5.

The circular graphs have the property that $\alpha(C_{d,q}^{\boxtimes n})$ (for fixed n), $\vartheta(C_{d,q})$ and $\Theta(C_{d,q})$ only depend on the fraction q/d. Moreover, the three mentioned quantities are nondecreasing functions in q/d (see Chapter 9 for details). Let us consider the graph of the function

$$q/d \mapsto \vartheta(C_{d,q}) = \frac{q}{d} \sum_{i=0}^{d-1} \prod_{j=1}^{d-1} \frac{\cos\left(\frac{2i\pi}{d}\right) - \cos\left(\lfloor\frac{qj}{d}\rfloor\frac{2\pi}{q}\right)}{1 - \cos\left(\lfloor\frac{qj}{d}\rfloor\frac{2\pi}{q}\right)}, \tag{1.16}$$

where the closed form formula for $\vartheta(C_{d,q})$ is proved by Bachoc, Pêcher and Thiéry [8]. See Figure 1.3.

Lovász's sandwich theorem [53] (see also [48]) implies that

$$\Theta(C_{d,q}) \leq \vartheta(C_{d,q}) \leq q/d \qquad \text{for all } q, d \in \mathbb{N} \text{ with } q \geq 2d. \tag{1.17}$$

Here q/d equals the fractional clique cover number of $C_{d,q}$, which is an upper bound on $\vartheta(C_{d,q})$ cf. [53]. Currently, the only known values of $\Theta(C_{d,q})$ for $q \geq 2d$ are for q/d integer and $q/d = 5/2$, which corresponds with C_5.

For understanding the Shannon capacity of $C_{d,q}$ it may be useful to determine whether $\vartheta(C_{d,q})$ and $\Theta(C_{d,q})$ are continuous functions of q/d. In this thesis, we prove that this is indeed the case at $q/d \geq 3$ integer. Fix an integer $r \geq 3$. Right-continuity of $q/d \mapsto \vartheta(C_{d,q})$ and $q/d \mapsto \Theta(C_{d,q})$ at $q/d = r$ follows immediately from (1.17) in combination with the fact that $\Theta(C_{d,q}) = r$ if $q/d = r$ and the fact that $q/d \mapsto \Theta(C_{d,q})$ is a nondecreasing function in q/d. To prove left-continuity, we prove the following result (using an explicit construction).

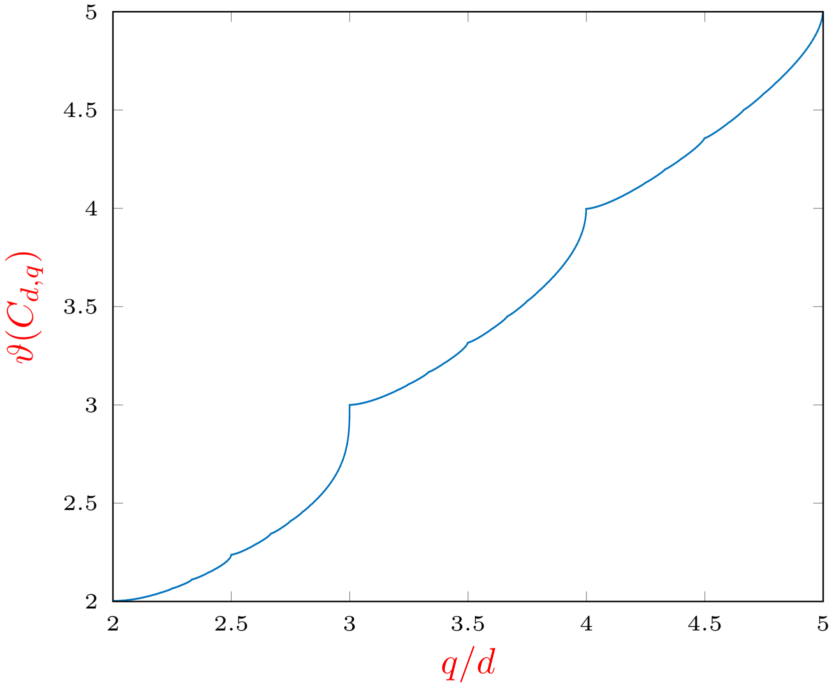


Figure 1.3: A graph of the function $q/d \mapsto \vartheta(C_{d,q})$.

Theorem (Theorem 9.3.1)**.** *For each $r, n \in \mathbb{N}$ with $r \geq 3$,*

$$\max_{\frac{q}{d}<r} \alpha(C_{d,q}^{\boxtimes n}) = \frac{1+r^n(r-2)}{r-1}. \tag{1.18}$$

This theorem can be shown to imply that $\lim_{\frac{q}{d}\uparrow r} \Theta(C_{d,q}) = r$. As $\Theta(C_{d,q}) = r$ if $q/d = r$, it follows that $q/d \mapsto \Theta(C_{d,q})$ is left-continuous at $q/d = r$ (and hence $q/d \mapsto \vartheta(C_{d,q})$, also by (1.17)). Continuity of $q/d \mapsto \Theta(C_{d,q})$ at *non*-integer points q/d seems hard to prove and even continuity of $q/d \mapsto \vartheta(C_{d,q})$ at these points is not yet known, although the latter function *looks* continuous (cf. Figure 1.3).

We also prove that the independent set achieving $\alpha(C_{5,14}^{\boxtimes 3}) = 14$, one of the independent sets used in our proof of Theorem 9.3.1, is unique up to Lee equivalence. Finally, we give the mentioned independent set of size 367 in $C_7^{\boxtimes 5}$, demonstrating the new lower bound on $\Theta(C_7)$. It is obtained by adapting an independent set of size 382 in $C_{108,382}^{\boxtimes 5}$ which we found by computer, inspired by the construction used to prove " $\geq$ " in (1.18).

1.5 An overarching theme: independent sets in graph products

We describe a framework which encompasses the main objects studied in this thesis. First we describe two graph products. Let $G = (V, E)$ and $H = (V', E')$ be graphs.

The *Cartesian product* $G \square H$ is the graph with vertex set $V \times V'$ in which two distinct vertices (u, u') and (v, v') are adjacent if either $uv \in E$ and $u' = v'$, or $u = v$ and $u'v' \in E'$. For $n \in \mathbb{N}$, write

$$G^{\square n} := \underbrace{G \square G \square \ldots \square G}_{n \text{ times}}.$$

So two distinct vertices $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$ of $G^{\square n}$ are adjacent if and only if there is an $i \in \{1, \ldots, n\}$ such that $u_i v_i \in E$, and $u_j = v_j$ for all $j \neq i$.

The *strong product* $G \boxtimes H$ is the graph with vertex set $V \times V'$ in which two distinct vertices (u, u') and (v, v') are adjacent if ($u = v$ or $uv \in E$) and ($u' = v'$ or $u'v' \in E'$). For $n \in \mathbb{N}$, write

$$G^{\boxtimes n} := \underbrace{G \boxtimes G \boxtimes \ldots \boxtimes G}_{n \text{ times}}.$$

Note that this definition coincides with the definition of $G^{\boxtimes n}$ given in Section 1.4, since two distinct vertices $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$ of $G^{\boxtimes n}$ are adjacent if and only if for each $i \in \{1, \ldots, n\}$ one has either $u_i = v_i$ or $u_i v_i \in E$.

For any connected graph $G = (V, E)$ and $u, v \in V$, let $d_G(u, v)$ denote the smallest length (in edges) of a path between u and v in G. So $d_G : V \times V \to \mathbb{R}_{\geq 0}$ is a metric, and (V, d_G) is a metric space. Then, cf. (1.13),

$$d_{G^{\square n}} = (d_G)_1 \quad \text{and} \quad d_{G^{\boxtimes n}} = (d_G)_\infty. \tag{1.19}$$

Define the number

$$\alpha_d(G) := \max\{|U| \mid U \subseteq V,\ d_G(u, v) \geq d \text{ for all distinct } u, v \in U\}. \tag{1.20}$$

So $\alpha_2(G) = \alpha(G)$. Let K_q denote the complete graph on q vertices, and let C_q denote the circuit on q vertices. Then

$$\begin{aligned} A_q(n, d) &= \alpha_d(K_q^{\square n}), \\ A_q^L(n, d) &= \alpha_d(C_q^{\square n}), \\ A_q^{L_\infty}(n, d) = \alpha(C_{d,q}^{\boxtimes n}) &= \alpha_d(C_q^{\boxtimes n}). \end{aligned}$$

So the main objects studied in this thesis are all of the form $\alpha_d(G^n)$, where $G \in \{C_q, K_q\}$, and where G^n denotes either $G^{\boxtimes n}$ or $G^{\square n}$. Only the parameter $A(n, d, w)$ does not fit directly into this framework. We have $A(n, d, w) = \alpha_d(H)$, where H is the subgraph of $K_2^{\square n}$ induced by the vertices $(u_1, \ldots, u_n)$ with $u_i = 1$ for exactly w indices $i \in \{1, \ldots, n\}$ (where the vertices of K_2 are labeled with 0 and 1).

1.6 Publications

This thesis is based on six published papers.

[25] A.E. Brouwer, S.C. Polak, Uniqueness of codes using semidefinite programming, *Designs, Codes and Cryptography* **87** (2019), 1881–1895.

[52] B.M. Litjens, S.C. Polak, A. Schrijver, Semidefinite bounds for nonbinary codes based on quadruples, *Designs, Codes and Cryptography* **84** (2017), 87–100.

[69] S.C. Polak, New nonbinary code bounds based on divisibility arguments, *Designs, Codes and Cryptography* **86** (2018), 861–874.

[70] S.C. Polak, Semidefinite programming bounds for constant weight codes, *IEEE Transactions on Information Theory* **65** (2019), 28–38.

[71] S.C. Polak, Semidefinite programming bounds for Lee codes, *Discrete Mathematics* **342** (2019), 2579–2589.

[72] S.C. Polak, A. Schrijver, New lower bound on the Shannon capacity of C_7, *Information Processing Letters* **143** (2019), 37–40.

To each of the papers mentioned above, the contribution of each of the authors is equivalent.

1.7 Organization of the thesis

Here we give a description of the organization of the thesis into chapters, which includes a summary of our contributions per chapter.

Chapter 2. Preliminaries. We give basic definitions and notation used throughout the thesis. We will also introduce semidefinite programming, one of our main tools. The last section is devoted to the definitions and results from representation theory used in the symmetry reductions in this thesis.

Chapter 3. The main symmetry reduction. We give the main symmetry reduction used in the semidefinite programs throughout the thesis. Suppose that G is a finite group acting on a finite set Z and let $n \in \mathbb{N}$. We consider the natural action of $H := G^n \rtimes S_n$ on Z^n. We show how to obtain a reduction $\Phi(M)$ of matrices $M \in (\mathbb{C}^{Z^n \times Z^n})^H$ to size polynomially bounded in n. The reduction can be derived from a manuscript of Gijswijt [35], but we give a more direct method. Chapter 3 is a generalization of the method of [52], which is joint work with Bart Litjens and Lex Schrijver.

Chapter 4. Semidefinite programming bounds for unrestricted codes. For nonnegative integers q, n, d, let $A_q(n,d)$ denote the maximum size of a code $C \subseteq [q]^n$ with minimum (Hamming) distance at least d. In this chapter we give an SDP upper bound on $A_q(n,d)$ based on quadruples of codewords and we give a reduction of the size of the matrices involved with the method of Chapter 3, so that the upper bound can be computed in time bounded by a polynomial in n. We provide new upper bounds on $A_q(n,d)$ for five triples (q,n,d), that were obtained with this SDP. Chapter 4 is based on joint work with Bart Litjens and Lex Schrijver [52].

Chapter 5. New nonbinary code bounds based on divisibility arguments. We give a divisibility argument that results in new upper bounds on $A_q(n,d)$: we find that $A_5(8,6) \leq 65$, $A_4(11,8) \leq 60$ and $A_3(16,11) \leq 29$. The divisibility argument builds upon the work of Plotkin [67]. Our main result in this chapter is the following. Suppose that q, n, d, m are positive integers with $q \geq 2$, such that $d = m(qd - (q-1)(n-1))$, and such that $n - d$ does not divide $m(n-1)$. If $r \in \{1, \ldots, q-1\}$ satisfies

$$n(n-1-d)(r-1)r < (q-r+1)(qm(q+r-2)-2r),$$

then $A_q(n,d) < q^2m - r$.

In the last part of Chapter 5, we prove that for $\mu, q \in \mathbb{N}$, there is a 1-1-correspondence between symmetric (μ, q)-nets (which are certain designs) and codes $C \subseteq [q]^{\mu q}$ of size μq^2 with minimum distance at least $\mu q - \mu$. We derive the new upper bounds $A_4(9,6) \leq 120$ and $A_4(10,6) \leq 480$ from these 'symmetric net' codes.

Chapter 5 is self-contained and does not use SDP or representation theory, but entirely relies on basic combinatorics. Chapter 5 is based on [69].

Chapter 6. Semidefinite programming bounds for constant weight codes. For nonnegative integers n, d, w, let $A(n,d,w)$ be the maximum size of a code $C \subseteq \{0,1\}^n$ with constant weight w and minimum distance at least d. We consider two SDP upper bounds based on quadruples of code words that yield several new upper bounds on $A(n,d,w)$ and we show that they can be computed in polynomial time by applying symmetry reductions with the method of Chapter 3. The new upper bounds imply the exact values $A(22,8,10) = 616$ and $A(22,8,11) = 672$. Lower bounds on $A(22,8,10)$ and $A(22,8,11)$ are obtained from the $(n,d) = (22,7)$ shortened binary Golay code of size 2048. It can be concluded that the shortened binary Golay code is a union of constant weight w codes of sizes $A(22,8,w)$. Chapter 6 is based on [70].

Chapter 7. Uniqueness of codes using semidefinite programming. With semidefinite programming, some upper bounds on $A(n,d,w)$ have recently been obtained that are equal to the best known lower bounds: it has been established that $A(23,8,11) = 1288$ (see [81]), and that $A(22,8,11) = 672$ and $A(22,8,10) = 616$ (see Chapter 6). We show using the output of the corresponding semidefinite programs that the corresponding codes of maximum size are unique up to coordinate permutations for these n, d, w.

For unrestricted (non-constant weight) binary codes, the bound $A(n,d) = A(20,8) \leq 256$ was obtained by Gijswijt, Schrijver and Mittelmann in [37], implying that the quadruply shortened extended binary Golay code of size 256 is optimal. Up to equivalence the optimal binary codes attaining $A(24-i,8) = 2^{12-i}$ for $i = 0,1,2,3$ are unique, namely they are the i times shortened extended binary Golay codes [20]. We show that there exist several nonequivalent optimal codes achieving $A(20,8) = 256$. We classify such codes under the additional condition that all distances are divisible by 4, and find 15 such codes. Chapter 7 is based on joint work with Andries Brouwer [25].

Chapter 8. Semidefinite programming bounds for Lee codes. For $q, n, d \in \mathbb{N}$, let $A_q^L(n,d)$ denote the maximum cardinality of a code $C \subseteq \mathbb{Z}_q^n$ with minimum Lee distance at least d, where $\mathbb{Z}_q$ denotes the cyclic group of order q. We consider an SDP upper bound based on triples of codewords, which bound can be computed efficiently using symmetry reductions with the method of Chapter 3, resulting in several new upper bounds on $A_q^L(n,d)$. We also give constructions for obtaining lower bounds and derive uniqueness of two instances: $A_5^L(7,9) = 15$ and $A_6^L(4,6) = 18$, using the SDP output. The code achieving $A_5^L(7,9) = 15$ is obtained by arranging 15 girls 7 days in succession into triples in a special way, which is different from but connects to Kirkman's schoolgirl problem. Chapter 8 is based on [71], except for the constructions and uniqueness of $A_5^L(7,9) = 15$ and $A_6^L(4,6) = 18$, which are new.

Chapter 9. The Shannon capacity of circular graphs. We consider the Shannon capacity $\Theta(C_{d,q})$ of circular graphs $C_{d,q}$. The circular graph $C_{d,q}$ is the graph with vertex set $\mathbb{Z}_q$ (the cyclic group of order q) in which two distinct vertices are adjacent if and only if their distance $(\text{mod } q)$ is strictly less than d. The value of $\Theta(C_{d,q})$ can be seen to only depend on the quotient q/d. We show that the function $q/d \mapsto \Theta(C_{d,q})$ is continuous at *integer* points $q/d \geq 3$. We also prove that the independent set achieving $\alpha(C_{5,14}^{\boxtimes 3}) = 14$, one of the independent sets used in our proof, is unique up to Lee equivalence. Furthermore, we adapt the SDP bound of Chapter 8 to an upper bound on $\alpha(C_{d,q}^{\boxtimes n})$ (see (1.15)) based on triples of codewords. The SDP bound does not seem to improve significantly over the bound obtained from Lovász's theta-function, except for very small n. Finally, we give a new lower bound of $367^{1/5}$ on the Shannon capacity of the 7-cycle. Chapter 9 is based on joint work with Lex Schrijver, part of which can be found in [72].

Chapter 2

Preliminaries

Mathematics is the supreme judge;
from its decisions there is no appeal.
— Tobias Dantzig (1884–1956)

In this chapter we give the preliminaries on coding theory, semidefinite programming and representation theory which are used in the other chapters. We start by introducing notation and giving some basic definitions.

2.1 Notation and basic definitions

Sets and graphs. We denote the sets of nonnegative integers and nonnegative real numbers by $\mathbb{Z}_{\geq 0}$ and $\mathbb{R}_{\geq 0}$, respectively. Moreover, we use the notation $\mathbb{N} := \mathbb{Z}_{\geq 0} \setminus \{0\}$. For $m \in \mathbb{Z}_{\geq 0}$ we define $[m] := \{1, \ldots, m\}$. So $[0] = \emptyset$. If $q \in \mathbb{N}$ and $Q := [q]$ denotes an alphabet in coding theory, we follow the convention that $[q] := \{0, 1 \ldots, q-1\}$ in this context. We write $\mathbb{Z}_q$ for the group of integers modulo q. Furthermore, we write $|Z|$ for the cardinality of a set Z.

A *graph* is a pair (V, E), where V is a finite set and E is a collection of unordered pairs from V. The elements of V are called *vertices* and the elements of E are called *edges*. Sometimes we will denote an edge $\{u, v\}$ by uv. If G is a graph, we sometimes write $V(G)$ and $E(G)$ for the vertex and edge sets of G, respectively. For $q \in \mathbb{N}$, the complete graph on q vertices is denoted by K_q, and the circuit on q vertices is denoted by C_q. Finally, for $q, d \in \mathbb{N}$ with $q \geq 2d$, we define the *circular graph* $C_{d,q}$ to be the graph with vertex set $V(C_q) = \mathbb{Z}_q$ in which two distinct vertices are adjacent if and only if their distance (mod q) is strictly less than d. We refer to Section 1.5 for definitions of two often used graph products. Finally, we recall that $U \subseteq V$ is called an *independent set* in a graph $G = (V, E)$ if for all $e \in E$, we have $e \nsubseteq U$. The maximum cardinality of an independent set in G is the *independent set number of* G, denoted by $\alpha(G)$.

Free vector space and group algebra. If Z is a finite set and K is a field, we denote by KZ the *free vector space* of Z over K. It consists of all K-linear combinations of elements in Z, i.e., of all formal sums $\sum_{z \in Z} \lambda_z z$ with $\lambda_z \in K$ for all $z \in Z$. If $\sum_{z \in Z} \lambda_z z$ and $\sum_{z \in Z} \gamma_z z$ are elements of KZ and $\alpha \in K$, then

$$\left(\textstyle\sum_{z \in Z} \lambda_z z\right) + \left(\textstyle\sum_{z \in Z} \gamma_z z\right) = \textstyle\sum_{z \in Z} (\lambda_z + \gamma_z) z \quad \text{and} \quad \alpha \left(\textstyle\sum_{z \in Z} \lambda_z z\right) = \textstyle\sum_{z \in Z} (\alpha \lambda_z) z.$$

If V is a vector space, we denote by V^* its dual vector space. If KZ is the free vector space of Z over K, the dual space $(KZ)^* = K^Z$ is the vector space consisting of all functions $Z \to K$. If G is a finite (multiplicative) group, we write KG for the *group algebra* of G over K. It is the free vector space KG equipped with the product from G, extended bilinearly.

Matrices. For two finite sets Y, Z and a set R, we write $R^{Y\times Z}$ for the set of matrices with entries in R whose rows and columns are indexed by the elements of Y and Z respectively. We call an element of $R^{Y\times Z}$ an $Y \times Z$ *matrix.* It is a function $Y \times Z \to R$, and if $R = K$ is a field, it is an element of the function space $K^{Y\times Z}$ defined above. Moreover, $R^{m\times n} = R^{[m]\times[n]}$ for nonnegative integers m, n, and we write $R^Z := R^{Z\times 1} = R^{Z\times[1]}$.

For a matrix $A \in \mathbb{C}^{Y\times Z}$, the *conjugate transpose* of A is the $Z \times Y$ matrix A^* with $A^*_{i,j} = \overline{A_{j,i}}$ for $i \in Z$ and $j \in Y$, where for any complex number z its complex conjugate is denoted by $\overline{z}$. If $A \in \mathbb{C}^{Z\times Z}$ with $A = A^*$, then A is called *Hermitian.* For two matrices $A, B \in \mathbb{C}^{Y\times Z}$, their *(trace) inner product* $\langle\, ,\rangle$ is defined as

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

If $A \in R^{Y\times Z}$, the *transpose* of A is the $Z \times Y$ matrix A^{T} with $A^{\mathsf{T}}_{i,j} = A_{j,i}$ for $i \in Z$ and $j \in Y$. Finally, for $n \in \mathbb{N}$ we denote by I_n and J_n the $n \times n$ identity and all-ones matrices, respectively.

Polynomials on a vector space. For a $\mathbb{C}$-vector space V, we write $\mathcal{O}(V)$ for the *coordinate ring* of V. It is the algebra of functions $p : V \to \mathbb{C}$ generated by elements of the dual vector space V^* of V, i.e., the algebra consisting of all $\mathbb{C}$-linear combinations of products of elements from V^*. An element of $\mathcal{O}(V)$ is called a *polynomial* on V. If $p \in \mathcal{O}(V)$ is a $\mathbb{C}$-linear combination in which each term is a constant times a product of n elements of V^* (for a fixed integer $n \in \mathbb{Z}_{\geq 0}$), we call p *homogeneous* of degree n. Moreover we write $\mathcal{O}_n(V) := \{p \in \mathcal{O}(v) \mid p \text{ homogeneous of degree } n\}$.

2.2 Coding theory

In this section we give the main definitions from coding theory used throughout the thesis. Many definitions have already passed in Chapter 1, but for convenience of the reader we restate them here.

The parameters $A_q(n, d)$, $A(n, d, w)$ and $A^L_q(n, d)$. Suppose that Q is a finite set of $q \geq 2$ elements and fix a positive integer n. A *word* is an element of Q^n and a *(q-ary) code* is a subset C of Q^n. So Q is our *alphabet.* We call elements of Q *symbols* or *letters.* For two words $u, v \in Q^n$, their *(Hamming) distance* $d_H(u, v)$ is the number of i with $u_i \neq v_i$. For a code $C \subseteq Q^n$, its *minimum distance* $d_{\min}(C)$ is the minimum of $d_H(u, v)$ over all $u, v \in C$. If $|C| \leq 1$, we set $d_{\min}(C) = \infty$. Without loss of generality we usually take $Q := [q]$, where $[q]$ denotes the set $\{0, \ldots, q-1\}$ (in this context). Define, for any integer d,

$$A_q(n,d) := \max\{|C| \mid C \subseteq [q]^n,\ d_{\min}(C) \geq d\}. \tag{2.1}$$

If $q = 2$ we often write $A(n,d)$ instead of $A_q(n,d)$. If $C \subseteq [q]^n$ with $d_{\min}(C) \geq d$, we call C an *$(n,d)_q$-code*, and if $d = 2$ simply an *(n,d)-code.* The weight of a word $v \in [q]^n$ is $\mathrm{wt}(v) := d_H(v, \mathbf{0})$, where $\mathbf{0} = 0 \ldots 0$ denotes the all-zeros word. A classical upper bound on $A_q(n,d)$ is the *Delsarte bound in the Hamming scheme*, which is given in (1.4).

Now, let $Q := \mathbb{F}_2 = [2] = \{0,1\}$ denote the binary alphabet. Here $\mathbb{F}_2$ denotes the field of two elements. A (binary) *constant weight code* is a code $C \subseteq \mathbb{F}_2^n$ in which all words have a fixed weight w. Define, for $n,d,w \in \mathbb{N}$,

$$A(n,d,w) := \max\{|C| \mid C \subseteq \mathbb{F}_2^n\ d_{\min}(C) \geq d,\ \ \mathrm{wt}(v) = w \text{ for all } v \in C\}. \tag{2.2}$$

If $C \subseteq \mathbb{F}_2^n$ is a constant weight w code with $d_{\min}(C) \geq d$, we call C an *(n,d,w)-code.* A classical upper bound on $A(n,d,w)$ is the *Delsarte bound in the Johnson scheme* $D(n,d,w)$. It is defined as follows. We assume without loss of generality that d is even (as any two weight w words have even distance) and that $w \leq n/2$ (as $A(n,d,w) = A(n,d,n-w)$). Define E_i to be the i-th *Eberlein polynomial*:

$$E_i(x) := \sum_{j=0}^{i} (-1)^j \binom{x}{j}\binom{w-x}{i-j}\binom{n-w-x}{i-j}, \qquad \text{for } 0 \leq i \leq w. \tag{2.3}$$

Then $A(n,d,w) \leq D(n,d,w)$, where

$$\begin{aligned} D(n,d,w) := \max\Big\{ \textstyle\sum_{i=0}^{w} a_{2i} \;\Big|\; & a_0 = 1,\ a_2 = a_4 = \ldots = a_{d-2} = 0,\ \ a_{2i} \geq 0 \text{ if } d/2 \leq i \leq w, \\ & \textstyle\sum_{i=0}^{w} \binom{w}{i}^{-1}\binom{n-w}{i}^{-1} E_i(k) a_{2i} \geq 0 \text{ for all } 0 \leq k \leq w \Big\}. \end{aligned} \tag{2.4}$$

Finally, let $Q := \mathbb{Z}_q$. For two words $u,v \in \mathbb{Z}_q^n$, their *Lee distance* is $d_L(u,v) := \sum_{i=1}^{n} \min\{|u_i - v_i|, q - |u_i - v_i|\}$, where we consider u_i and v_i as integers in $\{0,\ldots,q-1\}$. The *minimum Lee distance* $d_{\min}^L(C)$ of a code $C \subseteq \mathbb{Z}_q^n$ is the minimum of $d_L(u,v)$ taken over all distinct $u,v \in C$. If $|C| \leq 1$, we set $d_{\min}^L(C) = \infty$. Define, for $q,n,d \in \mathbb{N}$,

$$A_q^L(n,d) := \max\{|C| \mid C \subseteq \mathbb{Z}_q^n,\ d_{\min}^L(C) \geq d\}. \tag{2.5}$$

If $C \subseteq \mathbb{Z}_q^n$ with $d_{\min}^L(C) \geq d$, we call C an *$(n,d)_q^L$-code.* The Delsarte bound can be adapted to the Lee scheme to obtain a linear programming upper bound on $A_q^L(n,d)$ [4, 31].

Linear codes. Assume that Q is a field (often, $Q = \mathbb{F}_2$). A code $C \subseteq Q^n$ is called *linear* if it is a linear subspace of Q^n. So $|C| = |Q|^k$, with k the dimension of C as a Q-vector space. Any $k \times n$ matrix with a basis of C as rows is called a *generator* matrix of C.

If $C \subseteq \mathbb{F}_2^n$ is a linear code, the minimum distance of C is the minimum of the nonzero weights of the words in C: if $u,v \in C$ also $u - v \in C$ and $d_H(u,v) = \mathrm{wt}(u-v)$ for all $u,v \in C$.

Distance distribution. The *distance distribution* $(a_i)_{i=0}^n$ of a nonempty code $C \subseteq Q^n$ is the sequence $(a_i)_{i=0}^n$ given by

$$a_i := |C|^{-1} \cdot |\{(u,v) \in C \times C \mid d_H(u,v) = i\}|, \qquad \text{for } i = 0, \dots, n.$$

The inequalities on the a_i in the Delsarte bound (1.4) are satisfied by the distance distribution $(a_i)_{i=0}^n$ of any code $C \subseteq Q^n$ with $d_{\min}(C) \geq d$. Similarly, if $C \subseteq \mathbb{F}_2^n$ is a constant weight w code with $d_{\min}(C) \geq d$, its distance distribution $(a_{2i})_{i=0}^w$ satisfies the inequalities in the Delsarte bound in the Johnson scheme (2.4).

Equivalence of codes. Two q-ary codes $C, D \subseteq [q]^n$ are *equivalent* if D can be obtained from C by first permuting the n coordinates and by subsequently permuting the alphabet $[q]$ in each coordinate separately, i.e., if there is a $g \in S_q^n \rtimes S_n$ such that $g \cdot C = D$. Similarly, two binary constant weight codes C, D are *equivalent* if D can be obtained from C by permuting the n coordinates. Two codes $C, D \subseteq \mathbb{Z}_q^n$ are *Lee equivalent* if there is a $g \in D_q^n \rtimes S_n$ such that $g \cdot C = D$. Here D_q denotes the dihedral group of order $2q$ (acting on $\mathbb{Z}_q$).

The binary (extended) Golay code. In Chapters 6 and 7, we will encounter the (extended) binary Golay code. There exists a unique optimal code attaining $A(23,7) = 2^{12}$ up to equivalence [32, 88]. This code is called the *binary Golay code*, discovered by Marcel J.E. Golay [40]. It is *perfect*, i.e., the balls $B(u) := \{v \in \mathbb{F}_2^{23} \mid d_H(u,v) \leq 3)\}$ around the codewords $u \in C$ partition the vector space $\mathbb{F}_2^{23}$. (This follows by counting, as for any $u \in C$ we have $|B(u)| = 1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11}$. Since $|C| = 2^{12}$ and $B(u) \cap B(v) = \emptyset$ if $u, v \in C$ with $u \neq v$, we conclude $\sum_{u \in C} |B(u)| = 2^{12} \cdot 2^{11} = |\mathbb{F}_2^{23}|$.)

We will also need the *extended binary Golay code*. This is the code obtained from the binary Golay code by adding a 24th *parity check* bit to every codeword, which is equal to the sum (mod 2) of the original 23 bits of the respective codeword. So each codeword of the extended binary Golay code has even weight. As two binary words with even weight have even Hamming distance, and the binary Golay code has minimum distance 7 (which is odd), the extended binary Golay code has minimum distance 8. The extended binary Golay code is the unique binary code achieving $A(24,8) = 2^{12}$, up to equivalence.

Usually, we assume that the (extended) binary Golay code has been chosen such as to contain $\mathbf{0} = 0 \dots 0$, the all-zeros word. Then both codes are linear. A generator matrix of the extended binary Golay code is given in Figure 1.1 on page 8.

Also, we will encounter the i-times shortened (extended) binary Golay code (for $i = 1, \dots, 4$). Shortening of a code C means fixing a coordinate position (in $\{1, \dots, n\}$) of C, taking the subcode of C consisting of all codewords having symbol 0 in this coordinate position, and then deleting this fixed coordinate position of this subcode, resulting in a code D. Note that D has word length $n-1$ and that $d_{\min}(D) \geq d_{\min}(C)$. The code D is obtained by *shortening* C.

Since the automorphism groups of the binary Golay and extended binary Golay codes, the *Mathieu groups* M_{23} and M_{24}, act 4- and 5-transitively on the coordinate positions respectively (see [55]), the *i-times shortened (extended) binary Golay code* is well-defined for $i = 1, \dots, 4$ (i.e., these codes do not depend on which coordinate position we chose as 'fixed' coordinate position in each shortening step).

2.3 Semidefinite programming

Recall that a matrix $A \in \mathbb{C}^{n\times n}$ is called *Hermitian* if $A^* = A$. The eigenvalues of an Hermitian matrix are real. Let $A \in \mathbb{C}^{n\times n}$. Then A is called *positive semidefinite* if A is Hermitian and all eigenvalues of A are nonnegative. We use the notation $A \succeq 0$ to denote that A is positive semidefinite. It is known that the following are equivalent:

(i) $A \succeq 0$,
(ii) $A^* = A$ and $v^*Av \geq 0$ for all $v \in \mathbb{C}^n$,
(iii) $A = L^*L$ for some $L \in \mathbb{C}^{n\times n}$.

In case A is real, we may restrict v to real vectors in (ii) and L to real matrices in (iii). Note that if $A = L_1^*L_1$ and $B = L_2^*L_2$ are positive semidefinite matrices, then

$$\langle A, B\rangle = \mathrm{tr}(B^*A) = \mathrm{tr}(L_2^*L_2L_1^*L_1) = \mathrm{tr}(L_1L_2^*L_2L_1^*) = \mathrm{tr}((L_2L_1^*)^*(L_2L_1^*)) \geq 0, \tag{2.6}$$

as $(L_2L_1^*)^*(L_2L_1^*)$ is positive semidefinite by (iii).

We now describe semidefinite programming. Let $m, n \in \mathbb{Z}_{\geq 0}$, $b_1, \ldots, b_m \in \mathbb{R}$ and let $C, F_1, \ldots, F_m \in \mathbb{R}^{n\times n}$ be symmetric real matrices. A *semidefinite program* is an optimization problem of the form

$$\begin{aligned} \text{Maximize: } & b_1z_1 + \ldots + b_mz_m \\ \text{subject to: } & M := C - F_1z_1 + \ldots + F_mz_m \succeq 0. \end{aligned} \tag{2.7}$$

Here $z_1, \ldots, z_m$ are called the *variables*. Any (M, z) satisfying the constraints in (2.7) is called a *feasible solution* to (2.7), with *objective value* $b_1z_1+\ldots+b_mz_m$. The program (2.7) has an associated dual program which reads

$$\begin{aligned} \text{Minimize: } & \langle C, X\rangle \\ \text{subject to: } & \langle F_i, X\rangle = b_i \text{ for all } i = 1, \ldots, m, \\ & X \succeq 0. \end{aligned} \tag{2.8}$$

Any $X \in \mathbb{R}^{n\times n}$ satisfying the constraints in (2.8) is called a *feasible solution* to (2.8) with *objective value* $\langle C, X\rangle$. Note that if (M, y) and X are feasible solutions to (2.7) and (2.8) respectively, then

$$\begin{aligned} \langle C, X\rangle = \langle M + \textstyle\sum_{i=1}^m F_iz_i, X\rangle = \langle M, X\rangle + \textstyle\sum_{i=1}^m \langle F_i, X\rangle z_i = \langle M, X\rangle + \textstyle\sum_{i=1}^m b_iz_i \\ \geq \textstyle\sum_{i=1}^m b_iz_i, \end{aligned} \tag{2.9}$$

where the inequality follows from (2.6). So the maximum in (2.7) is at most the minimum in (2.8). This is called *weak duality*. Under a certain condition (called *Slater's condition*), which is satisfied in the cases when we apply SDP, even *strong duality* holds, that is, the optimal values in (2.8) and (2.7) are equal. To exhibit upper bounds in coding theory using semidefinite programs, we only need weak duality, i.e., the fact that a given feasible dual solution has an objective value greater than or equal to the objective value of *any* primal feasible solution.

Semidefinite programs can be solved approximately —up to any fixed precision— in polynomial time by the ellipsoid method [41]. In practice more recent interior point methods [62] are preferred, which also run in polynomial time. See [91] for more information about semidefinite programming.

2.4 Preliminaries on representation theory

In this section we give the definitions and notation from representation theory used throughout the thesis. For more information, the reader can consult Sagan [77].

A *group action* of a group G on a set Z is a group homomorphism $\phi : G \to S_Z$, where S_Z is the group of bijections of Z to itself. If ϕ is a group action of a group G on a set Z, we say that G *acts* on Z, and we write $g \cdot x := \phi(g)(x)$ for all $g \in G$ and $x \in Z$. Moreover, we write Z^G for the set of elements of Z invariant under the action of G. If Z is a linear space, we restrict S_Z to the linear bijections $Z \to Z$. The action of G on a finite set Z induces an action of G on the linear space $\mathbb{C}Z$ by linear extension. It also induces an action on the linear space $\mathbb{C}^Z$, by $(g \cdot f)(z) := f(g^{-1} \cdot z)$, for $g \in G$, $f \in \mathbb{C}^Z$ and $z \in Z$.

If G is a group acting on a finite dimensional complex vector space V, then V is called a *G-module*. If V is a G-module and $U \subseteq V$ is a G-invariant subspace, the space U is called a *submodule* of V. If V and W are G-modules, then a *G-homomorphism* (or: *G-equivariant map*) $\psi : V \to W$ is a linear map such that $g \cdot \psi(v) = \psi(g \cdot v)$ for all $g \in G$, $v \in V$. Two G-modules V and W are (G-)*isomorphic* or *equivalent* if there exists a bijective G-homomorphism from V to W, which is also called a *G-isomorphism.*

A G-module V is called *irreducible* if $V \neq \{0\}$ and the only submodules of V are $\{0\}$ and V itself. We write $\mathrm{End}_G(V)$ for the *centralizer algebra* of the action of G on V, i.e., the algebra of G-equivariant maps $V \to V$. We recall the well-known Schur's Lemma, which characterizes all G-equivariant maps between irreducible G-modules.

Lemma 2.4.1 (Schur's Lemma)**.** *Let V and W be irreducible G-modules, and let $f : V \to W$ be a G-equivariant map.*

(i) If V and W are nonisomorphic, then $f = 0$.
(ii) If there exists a G-isomorphism $\phi : V \to W$, then $f = \lambda\phi$ for some $\lambda \in \mathbb{C}$.

Let G be a finite group acting on a finite dimensional complex vector space V. Then V can be decomposed as $V = V_1 \oplus \ldots \oplus V_k$ such that each V_i is a direct sum $V_{i,1} \oplus \ldots \oplus V_{i,m_i}$ of irreducible G-modules with the property that $V_{i,j}$ and $V_{i',j'}$ are isomorphic if and only if $i = i'$. The number k and the V_i are unique up to permuting indices. The G-modules $V_1, \ldots, V_k$ are called the *G-isotypical components.*

Now choose, for each $i \leq k$ and $j \leq m_i$, a nonzero vector $u_{i,j} \in V_{i,j}$ so that for each i and all $j, j' \leq m_i$ there exists a G-isomorphism $V_{i,j} \to V_{i,j'}$ mapping $u_{i,j}$ to $u_{i,j'}$. For each $i \leq k$, define U_i to be the m_i-tuple $(u_{i,1}, \ldots, u_{i,m_i})$ of elements $u_{i,j}$ $(j = 1, \ldots, m_i)$. (We order the elements of U_i for later purposes.)

Definition 2.4.2 (Representative set)**.** Any set $\{U_1, \ldots, U_k\}$ obtained in this way is called a *representative set* for the action of G on V.

It is convenient to note that, since $V_{i,j}$ is the linear space spanned by $G \cdot u_{i,j}$ (for each i, j), we have

$$V = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{m_i} \mathbb{C}G \cdot u_{i,j}, \tag{2.10}$$

where $\mathbb{C}G$ denotes the complex group algebra of G. Moreover, note that

$$\dim \operatorname{End}_G(V) = \dim \operatorname{End}_G \left(\bigoplus_{i=1}^{k} \bigoplus_{j=1}^{m_i} V_{i,j} \right) = \sum_{i=1}^{k} m_i^2, \tag{2.11}$$

by Schur's lemma.

Proposition 2.4.3. *Let G be a finite group acting on a finite dimensional complex vector space V. Let k, $m_1, \dots, m_k \in \mathbb{N}$, and $u_{i,j} \in V$ for $i = 1, \dots, k$, $j = 1, \dots, m_i$. Then the set*

$$\{ (u_{i,1}, \dots, u_{i,m_i}) \mid i = 1, \dots, k\} \tag{2.12}$$

is representative for the action of G on V if and only if:

(i) $V = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{m_i} \mathbb{C}G \cdot u_{i,j}$,

(ii) $\forall\ i = 1, \dots, k$ *and* $j, j' = 1, \dots, m_i$, *there exists a G-isomorphism* $\mathbb{C}G \cdot u_{i,j} \to \mathbb{C}G \cdot u_{i,j'}$ *mapping* $u_{i,j}$ *to* $u_{i,j'}$,

(iii) $\sum_{i=1}^{k} m_i^2 \geq \dim(\operatorname{End}_G(V))$.

Proof. The implication "$\Longrightarrow$" follows from the definition and the above observations. To prove "$\Longleftarrow$", suppose that $k, m_1, \dots, m_k \in \mathbb{N}$, and that $u_{i,j} \in V$ for $i = 1, \dots, k$, $j = 1, \dots, m_i$, satisfy the three conditions from the lemma. Set $V_{i,j} := \mathbb{C}G \cdot u_{i,j}$, for $i = 1, \dots, k$, $j = 1, \dots, m_i$. Then by (i) and (ii) the $V_{i,j}$ form a *decomposition* of V into G-modules and $V_{i,j}$ and $V_{i',j'}$ are equivalent representations if $i = i'$. In fact, by (iii) the $V_{i,j}$ form a decomposition of V into *irreducible* representations and $V_{i,j}$ and $V_{i',j'}$ are equivalent representations if and *only if* $i = i'$, as any further representation, or decomposition, or equivalence would yield that the sum of the squares of the multiplicities of the irreducible representations is strictly larger than $\sum_{i=1}^{k} m_i^2 \geq \dim(\operatorname{End}_G(V))$, which is not possible.

So the set in (2.12) is representative for the action of G on V. □

Let G be a finite group acting on a finite dimensional complex vector space V. Let $\langle\, ,\rangle$ be a G-invariant inner product on V. (Note that any inner product $\langle\, ,\rangle$ on V gives rise to a G-invariant inner product $\langle\, ,\rangle_G$ on V via the rule $\langle x, y\rangle_G := \sum_{g\in G} \langle g \cdot x, g \cdot y\rangle$.) If $\{U_1, \dots, U_k\}$ is a representative set for the action of G on V, define the map

$$\Phi : \operatorname{End}_G(V) \to \bigoplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i} \quad \text{with} \quad A \mapsto \bigoplus_{i=1}^{k} \left(\langle A u_{i,j'}, u_{i,j}\rangle \right)_{j,j'=1}^{m_i}. \tag{2.13}$$

Note that Φ is linear. An element $A \in \operatorname{End}(V)$ is called *positive semidefinite* if $\langle Av, w\rangle = \langle v, Aw\rangle$ for all $v, w \in V$ and $\langle Av, v\rangle \geq 0$ for all $v \in V$.

Proposition 2.4.4. *The map Φ is bijective. Moreover, for any $A \in \operatorname{End}_G(V)$:*

$$A \textit{ is positive semidefinite} \iff \Phi(A) \textit{ is positive semidefinite.} \tag{2.14}$$

Proof. It is a standard fact from representation theory that the G-isotypical components $V_1, \dots, V_k$ are orthogonal with respect to $\langle\,,\rangle$. For each $i = 1, \dots, k$, the decomposition $V_i = V_{i,1} \oplus \dots \oplus V_{i,m_i}$ of V_i into irreducible and mutually isomorphic G-modules is not necessarily orthogonal, but there exists an *orthogonal* decomposition $V_i = W_{i,1} \oplus \dots \oplus W_{i,m_i}$ of V_i into irreducible and mutually isomorphic G-modules (and $V_{i,j}$ is isomorphic to $W_{i,j}$ for each $i \in [k]$, $j \in [m_i]$).

By Schur's lemma, $\operatorname{span}\{u_{i,1}, \dots, u_{i,m_i}\} = \{Bu_{i,1} \mid B \in \operatorname{End}_G(V)\}$. For each $i \in [k]$, $j \in [m_i]$, take a $w_{i,j} \in (\{Bu_{i,1} \mid B \in \operatorname{End}_G(V)\} \cap W_{i,j})$ such that $\langle w_{i,j}, w_{i,j}\rangle = 1$. Then there exists a G-invariant map $W_{i,j} \to W_{i,j'}$ mapping $w_{i,j}$ to $w_{i,j'}$ (for each $i \in [k]$, $j, j' \in [m_i]$). Moreover, for each $i \in [k]$, the set $\{w_{i,1}, \dots, w_{i,m_i}\}$ is an orthonormal basis for $\operatorname{span}\{u_{i,1}, \dots, u_{i,m_i}\}$. If $P \in \mathbb{C}^{m_i \times m_i}$ is the invertible change-of-basis matrix from $\{u_{i,1}, \dots, u_{i,m_i}\}$ to $\{w_{i,1}, \dots, w_{i,m_i}\}$, then

$$(\langle Au_{i,j'}, u_{i,j}\rangle)_{j,j'=1}^{m_i} = P^* \, (\langle Aw_{i,j'}, w_{i,j}\rangle)_{j,j'=1}^{m_i} \, P.$$

Hence, it suffices to prove the statements of the theorem for the linear map

$$\Phi' : \operatorname{End}_G(V) \to \bigoplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i} \quad \text{with} \quad A \mapsto \Phi'(A) := \bigoplus_{i=1}^{k} (\langle Aw_{i,j'}, w_{i,j}\rangle)_{j,j'=1}^{m_i}$$

instead of Φ.

For each $i \in [k]$, we write $d_i := \dim W_{i,1}$. Furthermore, for each $i \in [k]$, $j \in [m_i]$, let $\{w_{i,j,l} \mid l \in [d_i]\}$ be an orthonormal basis of $W_{i,j}$ such that for each j, j' there exists a G-equivariant map $W_{i,j} \to W_{i,j'}$ mapping $w_{i,j,l}$ to $w_{i,j',l}$ for each $l \in [d_i]$, and such that $w_{i,j,1} = w_{i,j}$. (The bases can be chosen in this way since any irreducible G-module has a *unique* G-invariant inner product, up to scalar multiplication. This, in turn, is a consequence of Schur's Lemma.)

Then a direct computation (with Schur's lemma) gives that, for $i, i' \in [k]$, $j \in [m_i]$, $j' \in [m_{i'}]$, $l \in [d_i]$, $l' \in [d_{i'}]$:

$$\langle Aw_{i',j',l'}, w_{i,j,l}\rangle = \begin{cases} \langle Aw_{i,j'}, w_{i,j}\rangle & \text{if } i = i' \text{ and } l = l', \\ 0 & \text{otherwise.} \end{cases} \tag{2.15}$$

Since $\{w_{i,j,l} \,|\, i \in [k], j \in [m_i], l \in [d_i]\}$ is a basis of V, the linear map A is positive semidefinite if and only if the matrix

$$M := (\langle Aw_{i',j',l'}, w_{i,j,l}\rangle)_{i\in[k],l\in[d_i],j\in[m_i],i'\in[k],l'\in[d_{i'}],j'\in[m_{i'}]}$$

is positive semidefinite, and $A = 0$ if and only if $M = 0$. By (2.15), the matrix M is the direct sum

$$M = \bigoplus_{i=1}^{k} \bigoplus_{l=1}^{d_i} (\langle Aw_{i,j'}, w_{i,j}\rangle)_{j,j'=1}^{m_i},$$

and M contains d_i identical blocks (for $i = 1, \dots, k$). So A is positive semidefinite if and only if $\Phi'(A)$ is positive semidefinite. Moreover, $A = 0$ if and only if $\Phi'(A) = 0$, so Φ' is injective. Bijectivity of Φ' now follows from the fact that $\dim \operatorname{End}_G(V) = \sum_{i=1}^{k} m_i^2 = \dim(\oplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i})$. □

This result is basic in our symmetry reductions. Firstly, $\dim(\mathrm{End}_G(V)) = \sum_{i=1}^{k} m_i^2$, which can be considerably smaller than $\dim V$. Secondly, any $A \in \mathrm{End}_G(V)$ is positive semidefinite if and only if the image $\Phi(A)$ is positive semidefinite, i.e., if and only if each of the matrices $(\langle Au_{i,j'}, u_{i,j}\rangle)_{j,j'=1}^{m_i}$ is positive semidefinite.

We will often apply the previous theory to the following situation. Suppose that G is a finite group acting on a finite set Z, hence on $V := \mathbb{C}^Z$. Consider the standard inner product $\langle x, y\rangle := y^* x$ for $x, y \in \mathbb{C}^Z$, where y^* denotes the conjugate transpose of $y \in \mathbb{C}^Z$. This inner product is G-invariant, since for each $g \in G$ the $Z \times Z$ matrix L_g with $g \cdot x = L_g x$ for all $x \in V$ is unitary, since in this case L_g is a permutation matrix.

Definition 2.4.5 (Representative set for the action of G on Z)**.** We call any representative set $\{U_1, \ldots, U_k\}$ for the action of G on $V = \mathbb{C}^Z$ induced by the action of G on Z a *representative set for the action of G on Z.*

Let $\{U_1, \ldots, U_k\}$ be a representative set for the action of G on Z. Then each U_i is an ordered set of m_i elements from $\mathbb{C}^Z$ (for $i = 1, \ldots, k$), hence it is a $Z \times m_i$ matrix. We will often call $\{U_1, \ldots, U_k\}$ a *representative matrix set* for the action of G on Z (or on $\mathbb{C}^Z$). Moreover, we will regularly write $U_i = [u_{i,1}, \ldots, u_{i,m_i}]$ instead of $U_i = (u_{i,1}, \ldots, u_{i,m_i})$, to emphasize the fact that U_i is a matrix (here $i = 1, \ldots, k$).

The action of G on Z induces an action of G on $Z \times Z$, hence on $\mathbb{C}^{Z\times Z}$. So $(\mathbb{C}^{Z\times Z})^G$ is the algebra of complex $Z \times Z$-matrices invariant under the action of G on $Z \times Z$. Since for each $g \in G$ there is a permutation $Z \times Z$ matrix L_g such that $g \cdot x = L_g x$ for all $x \in \mathbb{C}^Z$, the algebra $(\mathbb{C}^{Z\times Z})^G$ can be identified with the algebra $\mathrm{End}_G(\mathbb{C}^Z)$ of G-equivariant maps $\mathbb{C}^Z \to \mathbb{C}^Z$. Since $\{U_1, \ldots, U_k\}$ is a representative matrix set for the action of G on $\mathbb{C}^Z$, (2.13) implies that

$$\Phi : (\mathbb{C}^{Z\times Z})^G \to \bigoplus_{i=1}^{k} \mathbb{C}^{m_i\times m_i} \quad \text{with} \quad A \mapsto \bigoplus_{i=1}^{k} U_i^* A U_i \tag{2.16}$$

is bijective.

It turns out that all representative sets determined in this thesis consist of real matrices. Then

$$\Phi(A) = \bigoplus_{i=1}^{k} U_i^{\mathsf{T}} A U_i \text{ for } A \in (\mathbb{R}^{Z\times Z})^G, \quad \text{and } \Phi\left((\mathbb{R}^{Z\times Z})^G\right) = \bigoplus_{i=1}^{k} \mathbb{R}^{m_i\times m_i}. \tag{2.17}$$

Also, $A \in (\mathbb{R}^{Z\times Z})^G$ is positive semidefinite if and only if each of the matrices $U_i^{\mathsf{T}} A U_i$ is positive semidefinite ($i = 1, \ldots, k$). As mentioned, this is very useful for checking whether A is positive semidefinite.

Finally, we note that if G_1 and G_2 are finite groups and if $\{U_1^{(1)}, \ldots, U_{k_1}^{(1)}\}$ and $\{U_1^{(2)}, \ldots, U_{k_2}^{(2)}\}$ are representative matrix sets for the actions of G_1 and G_2 on finite sets Z_1 and Z_2 respectively, then

$$\left\{U_i^{(1)} \otimes U_j^{(2)} \mid i = 1, \ldots, k_1,\ j = 1, \ldots, k_2\right\} \tag{2.18}$$

is representative for the action of $G_1 \times G_2$ on $Z_1 \times Z_2$. Moreover, if $M_1 \in (\mathbb{C}^{Z_1\times Z_1})^{G_1}$,

$M_2 \in (\mathbb{C}^{Z_2\times Z_2})^{G_2}$, and $i \in [k_1]$, $j \in [k_2]$, then

$$\begin{aligned}
&\left(\left(U_i^{(1)} \otimes U_j^{(2)}\right)^{\mathsf{T}} (M_1 \otimes M_2) \left(U_i^{(1)} \otimes U_j^{(2)}\right)\right)_{(a,b),(a',b')} \\
&= \left(U_i^{(1)}(a) \otimes U_j^{(2)}(b)\right)^{\mathsf{T}} (M_1 \otimes M_2) \left(U_i^{(1)}(a') \otimes U_j^{(2)}(b')\right) \\
&= \left(U_i^{(1)}(a)^{\mathsf{T}} M_1 U_i^{(1)}(a')\right) \left(U_j^{(2)}(b)^{\mathsf{T}} M_2 U_j^{(2)}(b')\right). \qquad (2.19)
\end{aligned}$$

So the entries in the matrix blocks of $\Phi(M_1 \otimes M_2)$ are products of entries in the matrix blocks of $\Phi(M_1)$ and $\Phi(M_2)$. This will be useful in explicitly calculating the blocks.

2.4.1 A representative set for the action of S_n on $V^{\otimes n}$

Fix $n \in \mathbb{N}$ and a finite-dimensional vector space V. We consider the natural action of the symmetric group S_n on $V^{\otimes n}$ by permuting the indices. Based on classical representation theory of the symmetric group, we describe a representative set for the action of S_n on $V^{\otimes n}$. It will be used repeatedly in the reductions throughout this thesis.

A *partition* λ of n is a sequence $(\lambda_1, \ldots, \lambda_h)$ of natural numbers with $\lambda_1 \geq \ldots \geq \lambda_h > 0$ and $\lambda_1 + \ldots + \lambda_h = n$. The number h is called the *height* of λ. We write $\lambda \vdash n$ if λ is a partition of n. The *Young shape* (or *Ferrers diagram*) $Y(\lambda)$ of λ is the set

$$Y(\lambda) := \{(i,j) \in \mathbb{N}^2 \mid 1 \leq j \leq h,\ 1 \leq i \leq \lambda_j\}. \qquad (2.20)$$

(Here French notation is used, cf. [73].) Fixing an index $j_0 \leq h$, the set of elements (i, j_0) (for $1 \leq i \leq \lambda_{j_0}$) in $Y(\lambda)$ is called the *j_0-th row* of $Y(\lambda)$. Similarly, fixing an element $i_0 \leq \lambda_1$, the set of elements (i_0, j) (where j varies) in $Y(\lambda)$ is called the *i_0-th column* of $Y(\lambda)$. Then the *row stabilizer* R_λ of λ is the group of permutations P of $Y(\lambda)$ with $P(L) = L$ for each row L of $Y(\lambda)$. Similarly, the *column stabilizer* C_λ of λ is the group of permutations P of $Y(\lambda)$ with $P(L) = L$ for each column L of $Y(\lambda)$.

A *Young tableau with shape* λ (also called a *λ-tableau*) is a function $\tau : Y(\lambda) \to \mathbb{N}$. A Young tableau with shape λ is *semistandard* if the entries are nondecreasing in each row and strictly increasing in each column. Let $T_{\lambda,m}$ be the collection of semistandard λ-tableaux with entries in $[m]$. Then $T_{\lambda,m} \neq \emptyset$ if and only if m is at least the height of λ. We write $\tau \sim \tau'$ for λ-tableaux τ, τ' if $\tau' = \tau r$ for some $r \in R_\lambda$.

Let $B = (B(1), \ldots, B(m))$ be an ordered basis of V. For any $\tau \in T_{\lambda,m}$, define

$$u_{\tau,B} := \sum_{\tau' \sim \tau} \sum_{c \in C_\lambda} \operatorname{sgn}(c) \bigotimes_{y \in Y(\lambda)} B\left(\tau'(c(y))\right) \quad \in V^{\otimes n}. \qquad (2.21)$$

Here the Young shape $Y(\lambda)$ is ordered by concatenating its rows. Then (cf. [77] and [52]) the set

$$\left\{ \left(u_{\tau,B} \mid \tau \in T_{\lambda,m}\right) \mid \lambda \vdash n \right\}, \qquad (2.22)$$

is a representative set for the natural action of S_n on $V^{\otimes n}$, for any ordering of the elements of $T_{\lambda,m}$. So if Z is a finite set and $V = \mathbb{C}^Z$, then (2.22) gives a representative set for the natural action of S_n on Z^n via the natural isomorphism $\mathbb{C}^{Z^n} \cong (\mathbb{C}^Z)^{\otimes n}$.

Chapter 3

Main symmetry reduction

Beauty is bound up with symmetry.
— Hermann Weyl (1885–1955)

Suppose that G is a finite group acting on a finite set Z and let $n \in \mathbb{N}$. We consider the natural action of $H := G^n \rtimes S_n$ on Z^n. If $U_1, \ldots, U_k$ form a representative set of matrices for the action of H on Z^n, then with (2.13) we obtain a reduction $\Phi(M)$ of matrices $M \in (\mathbb{C}^{Z^n \times Z^n})^H$ to size polynomially bounded in n.

First, we give in Section 3.1 a representative set for the action of $H = G^n \rtimes S_n$ on $V^{\otimes n}$ (for any finite dimensional complex vector space V), with the help of the representative set for the natural action of S_n on $V^{\otimes n}$ from Section 2.4.1. Here we assume that a representative set $\boldsymbol{B} = \{B_1, \ldots, B_k\}$ for the action of G on V is given. If the given representative set is real, also the representative set for the action of H on $V^{\otimes n}$ turns out to be real. So if $V = \mathbb{C}^Z$, then our method yields a representative set for the action of H on Z^n via the natural isomorphism $\mathbb{C}^{Z^n} \cong (\mathbb{C}^Z)^{\otimes n} = V^{\otimes n}$.

Subsequently, we show in Section 3.2 how to compute $\Phi(M)$ in polynomial time. In Section 3.3 we give a generalization to groups of the form $(G_1^{j_1} \rtimes S_{j_1}) \times \ldots \times (G_s^{j_s} \rtimes S_{j_s})$ acting on sets of the form $Z_1^{j_1} \times \ldots \times Z_s^{j_s}$. The chapter is concluded with two appendices. The first appendix gives two subroutines to compute a polynomial used in the computation of $\Phi(M)$. In the second appendix we show as an illustration how to apply the symmetry reduction of this chapter to the matrix occurring in the analytical definition of the Delsarte bound for error-correcting codes with the Hamming distance.

The reduction explained in this chapter can also be derived from a manuscript of Gijswijt [35], but we give a more direct approach. Our method is a generalization of the method of [52], which is joint work with Bart Litjens and Lex Schrijver.

3.1 A representative set for the action of $G^n \rtimes S_n$ on $V^{\otimes n}$

Let G be a finite group acting on a finite dimensional vector space V. Suppose that a representative set $\boldsymbol{B} = \{B_1, \ldots, B_k\}$ for the action of G on V is given. Here each B_i is an ordered m_i-tuple of elements from V, for some integers $m_1, \ldots, m_k$.

Let $n \in \mathbb{N}$ and let $\boldsymbol{N}$ be the collection of all k-tuples $(n_1, \ldots, n_k)$ of nonnegative integers adding up to n. For $\boldsymbol{n} = (n_1, \ldots, n_k) \in \boldsymbol{N}$, let $\boldsymbol{\lambda} \vdash \boldsymbol{n}$ mean that $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_k)$ with $\lambda_i \vdash n_i$ for $i = 1, \ldots, k$. (So each λ_i is equal to a partition $(\lambda_{i,1}, \ldots, \lambda_{i,h_i})$ of n_i, for some h_i.) Define $\boldsymbol{m} := (m_1, \ldots, m_k)$.

For $\boldsymbol{\lambda} \vdash \boldsymbol{n}$ define

$$\boldsymbol{T_{\lambda,m}} := T_{\lambda_1,m_1} \times \cdots \times T_{\lambda_k,m_k}, \tag{3.1}$$

and for $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_k) \in \boldsymbol{T_{\lambda,m}}$ define

$$\boldsymbol{u_{\tau,B}} := \bigotimes_{i=1}^{k} u_{\tau_i,B_i} = \bigotimes_{i=1}^{k} \sum_{\tau_i' \sim \tau_i} \sum_{c_i \in C_{\lambda_i}} \operatorname{sgn}(c_i) \bigotimes_{y \in Y(\lambda_i)} B_i\left(\tau_i'(c_i(y))\right) \qquad \in V^{\otimes n}. \tag{3.2}$$

Proposition 3.1.1. *The set*

$$\{ \quad (\boldsymbol{u_{\tau,B}} \mid \boldsymbol{\tau} \in \boldsymbol{T_{\lambda,m}}) \quad \mid \boldsymbol{n} \in \boldsymbol{N}, \boldsymbol{\lambda} \vdash \boldsymbol{n}\} \tag{3.3}$$

is representative for the action of $H := G^n \rtimes S_n$ on $V^{\otimes n}$ (for any ordering of the elements of $\boldsymbol{T_{\lambda,m}}$).

Proof. For $i = 1, \ldots, k$, let L_i denote the $\mathbb{C}$-linear space spanned by $B_i(1), \ldots, B_i(m_i)$. Then

$$\begin{aligned} V^{\otimes n} &\overset{(2.10)}{=} \left(\bigoplus_{i=1}^{k} \bigoplus_{j=1}^{m_i} \mathbb{C}G \cdot B_i(j) \right)^{\otimes n} = \mathbb{C}S_n \cdot \bigoplus_{\boldsymbol{n} \in \boldsymbol{N}} \bigotimes_{i=1}^{k} \left(\bigoplus_{j=1}^{m_i} \mathbb{C}G \cdot B_i(j) \right)^{\otimes n_i} \\ &= \mathbb{C}S_n \cdot (\mathbb{C}G)^{\otimes n} \cdot \bigoplus_{\boldsymbol{n} \in \boldsymbol{N}} \bigotimes_{i=1}^{k} L_i^{\otimes n_i} \overset{(2.10),\ (2.22)}{=} \mathbb{C}H \cdot \bigoplus_{\boldsymbol{n} \in \boldsymbol{N}} \bigotimes_{i=1}^{k} \bigoplus_{\lambda_i \vdash n_i} \bigoplus_{\tau_i \in T_{\lambda_i,m_i}} \mathbb{C}S_{n_i} \cdot u_{\tau_i,B_i} \\ &= \bigoplus_{\boldsymbol{n} \in \boldsymbol{N}} \bigoplus_{\boldsymbol{\lambda} \vdash \boldsymbol{n}} \bigoplus_{\boldsymbol{\tau} \in \boldsymbol{T_{\lambda,m}}} \mathbb{C}H \cdot \boldsymbol{u_{\tau,B}}. \end{aligned} \tag{3.4}$$

Now for each $\boldsymbol{n}, \boldsymbol{\lambda}$ and $\boldsymbol{\tau}, \boldsymbol{\sigma} \in \boldsymbol{T_{\lambda,m}}$, there is an H-isomorphism $\mathbb{C}H \cdot \boldsymbol{u_{\tau,B}} \to \mathbb{C}H \cdot \boldsymbol{u_{\sigma,B}}$ bringing $\boldsymbol{u_{\tau,B}}$ to $\boldsymbol{u_{\sigma,B}}$, since for each $i = 1, \ldots, k$, setting $H_i := G^{n_i} \rtimes S_{n_i}$, there is an H_i-isomorphism $\mathbb{C}H_i \cdot u_{\tau_i,B_i} \to \mathbb{C}H_i \cdot u_{\sigma_i,B_i}$, since for each $j, j' \in [m_i]$ there is a G-isomorphism $\mathbb{C}G \cdot B_i(j) \to \mathbb{C}G \cdot B_i(j')$ and by the results in Section 2.4.1, there is an S_{n_i}-isomorphism $\mathbb{C}S_{n_i} \cdot u_{\tau_i,B_i} \to \mathbb{C}S_{n_i} \cdot u_{\sigma_i,B_i}$. Hence (where $\operatorname{Sym}_t(X) := (X^{\otimes t})^{S_t}$ for any $t \in \mathbb{Z}_{\geq 0}$ and any linear space X, with the natural action of S_t on $X^{\otimes t}$)

$$\begin{aligned} \dim\left((V^{\otimes n} \otimes V^{\otimes n})^H\right) &\geq \sum_{\boldsymbol{n} \in \boldsymbol{N}} \sum_{\boldsymbol{\lambda} \vdash \boldsymbol{n}} |\boldsymbol{T_{\lambda,m}}|^2 = \sum_{\boldsymbol{n} \in \boldsymbol{N}} \sum_{\boldsymbol{\lambda} \vdash \boldsymbol{n}} \prod_{i=1}^{k} |T_{\lambda_i,m_i}|^2 \\ &= \sum_{\boldsymbol{n} \in \boldsymbol{N}} \prod_{i=1}^{k} \sum_{\lambda_i \vdash n_i} |T_{\lambda_i,m_i}|^2 = \sum_{\boldsymbol{n} \in \boldsymbol{N}} \prod_{i=1}^{k} \dim \operatorname{Sym}_{n_i}(\mathbb{C}^{m_i} \otimes \mathbb{C}^{m_i}), \end{aligned}$$

where the last equality follows from the fact that the set in (2.22) is representative for the action of S_{n_i} on $(\mathbb{C}^{m_i})^{\otimes n_i}$. So

$$\begin{aligned} \dim\left((V^{\otimes n} \otimes V^{\otimes n})^H\right) &\geq \sum_{\boldsymbol{n} \in \boldsymbol{N}} \prod_{i=1}^{k} \dim \operatorname{Sym}_{n_i}(\mathbb{C}^{m_i} \otimes \mathbb{C}^{m_i}) \\ &= \sum_{\boldsymbol{n} \in \boldsymbol{N}} \prod_{i=1}^{k} \binom{m_i^2 + n_i - 1}{n_i - 1} = \binom{\sum_{i=1}^{k} m_i^2 + n - 1}{n - 1} \\ &= \dim \operatorname{Sym}_n((V \otimes V)^G) \\ &= \dim\left((V^{\otimes n} \otimes V^{\otimes n})^H\right), \end{aligned} \tag{3.5}$$

as $\sum_{i=1}^{k} m_i^2 = \dim((V \otimes V)^G)$. So we have equality throughout in (3.5), and hence each $\mathbb{C}H \cdot \boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}$ is irreducible, and if $\boldsymbol{\lambda} \neq \boldsymbol{\lambda}'$, then for each $\boldsymbol{\tau} \in \boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}$ and $\boldsymbol{\tau}' \in \boldsymbol{T}_{\boldsymbol{\lambda}',\boldsymbol{m}}$, the spaces $\mathbb{C}H \cdot \boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}$ and $\mathbb{C}H \cdot \boldsymbol{u}_{\boldsymbol{\tau}',\boldsymbol{B}}$ are not H-isomorphic. □

Note that the representative set in (3.3) is real if we start with a real representative set $\boldsymbol{B} = \{B_1, \ldots, B_k\}$. Moreover, if G is a finite group acting on a finite set Z and $V = \mathbb{C}^Z$, then (3.3) gives a representative set for the action of $G^n \rtimes S_n$ on Z^n via the natural isomorphism $\mathbb{C}^{Z^n} \cong (\mathbb{C}^Z)^{\otimes n} = V^{\otimes n}$.

3.2 Computation

If G is a finite group acting on a finite set Z, we often tacitly identify $\mathbb{C}Z$ and $\mathbb{C}^Z = (\mathbb{C}Z)^*$ via the standard inner product.[1] It will turn out that we only need this identification for real vectors.

Let G be a finite group acting on a finite set Z, hence on $Z \times Z$. Set $\Lambda := (Z \times Z)/G$ and $W := (\mathbb{C}Z \otimes \mathbb{C}Z)^G$. For each $P \in \Lambda$, define

$$a_P := \sum_{(x,y) \in P} x \otimes y \quad \in W. \tag{3.6}$$

Then the set $A := \{a_P \mid P \in \Lambda\}$ is a basis of W.

Let $n \in \mathbb{N}$ and set again $H := G^n \rtimes S_n$. There is a natural bijection $\Lambda^n/S_n \to (Z \times Z)^n/H$ given by

$$\omega \mapsto \{P_1 \times \cdots \times P_n \mid (P_1, \ldots, P_n) \in \omega\}, \tag{3.7}$$

for $\omega \in \Lambda^n/S_n$. For each $\omega \in \Lambda^n/S_n$, let K_ω be the *adjacency matrix* of ω, i.e., the $Z^n \times Z^n$ matrix with

$$(K_\omega)_{(\alpha,\beta)} := \begin{cases} 1 & \text{if } (\alpha,\beta) \in \omega, \\ 0 & \text{otherwise,} \end{cases} \tag{3.8}$$

for $\alpha, \beta \in Z^n$. Using the natural identification of $Z^n \times Z^n$ and $(Z \times Z)^n$, we have

$$K_\omega = \sum_{(P_1,\ldots,P_n) \in \omega} a_{P_1} \otimes \cdots \otimes a_{P_n} \quad \in W^{\otimes n}. \tag{3.9}$$

Then any matrix in $(\mathbb{C}^{Z^n \times Z^n})^H$ can be written as

$$M(z) := \sum_{\omega \in \Lambda^n/S_n} z(\omega) K_\omega, \qquad \text{for } z : \Lambda^n/S_n \to \mathbb{C}.$$

A representative matrix set for the action of H on Z^n is given by (3.3) (with $V := \mathbb{C}^Z$). Given $\boldsymbol{n} \in \boldsymbol{N}$, for each $\boldsymbol{\lambda} \vdash \boldsymbol{n}$ we write $U_{\boldsymbol{\lambda}}$ for the matrix in (3.3) that corresponds with $\boldsymbol{\lambda}$. For any $z : \Lambda^n/S_n \to \mathbb{C}$ we obtain with (2.16) that

$$\Phi(M(z)) = \Phi\left(\sum_{\omega \in \Lambda^n/S_n} z(\omega) K_\omega\right) = \bigoplus_{\boldsymbol{n} \in \boldsymbol{N}} \bigoplus_{\boldsymbol{\lambda} \vdash \boldsymbol{n}} \sum_{\omega \in \Lambda^n/S_n} z(\omega) U_{\boldsymbol{\lambda}}^* K_\omega U_{\boldsymbol{\lambda}}. \tag{3.10}$$

[1] The standard inner product on the free vector space $\mathbb{C}Z$ is the unique inner product (linear in the first coordinate, conjugate-linear in the second coordinate) on $\mathbb{C}Z$ with respect to which Z is an orthonormal basis.

The matrices $M(z)$ we consider in this thesis are all real. Moreover, in all our applications the representative sets turn out to be real, i.e., all $U_{\boldsymbol{\lambda}}$ are real matrices. So we can write $U_{\boldsymbol{\lambda}}^{\mathsf{T}}$ instead of $U_{\boldsymbol{\lambda}}^{*}$. In the remainder of this chapter, we assume that $M(z)$ and all $U_{\boldsymbol{\lambda}}$ are real matrices. We leave the adaptations for the case that $U_{\boldsymbol{\lambda}}$ is not real to the reader.

So in our case, for any $z : \Lambda^n/S_n \to \mathbb{R}$ we obtain with (2.17) that

$$\Phi(M(z)) = \Phi\left(\sum_{\omega\in\Lambda^n/S_n} z(\omega)K_\omega\right) = \bigoplus_{\boldsymbol{n}\in\boldsymbol{N}}\bigoplus_{\boldsymbol{\lambda}\vdash\boldsymbol{n}}\sum_{\omega\in\Lambda^n/S_n} z(\omega)U_{\boldsymbol{\lambda}}^{\mathsf{T}}K_\omega U_{\boldsymbol{\lambda}}. \tag{3.11}$$

Fixing G and Z, the number of $\boldsymbol{n}\in\boldsymbol{N}$, $\boldsymbol{\lambda}\vdash\boldsymbol{n}$, and the numbers $|\boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}|$ and $|\Lambda^n/S_n|$ are all bounded by a polynomial in n. This implies that the number of blocks in (3.11), the size of each block and the number of variables occurring in all blocks are polynomially bounded in n.

We still need to show how to compute the entries in the blocks $\sum_{\omega\in\Lambda^n/S_n} z(\omega)U_{\boldsymbol{\lambda}}^{\mathsf{T}}K_\omega U_{\boldsymbol{\lambda}}$ for $\boldsymbol{n}\in\boldsymbol{N}$, $\boldsymbol{\lambda}\vdash\boldsymbol{n}$ in (3.11) in polynomial time, since the orders of $\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}$, $\boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}$ and K_ω are exponential in n. That is, we must compute $\sum_{\omega\in\Lambda^n/S_n} z(\omega)\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}}K_\omega\boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}$, for $\boldsymbol{\tau},\boldsymbol{\sigma}\in\boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}$, $\boldsymbol{\lambda}\vdash\boldsymbol{n}$ and $\boldsymbol{n}\in\boldsymbol{N}$.

How to compute $\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}}K_\omega\boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}$

First we examine a relation between S_n-orbits on Λ^n and monomials of degree n expressed in the dual basis A^* of A, which will be used in the computations.

For each $\omega\in\Lambda^n/S_n$, the monomial $\mu(\omega)$ is defined as

$$\mu(\omega) := a_{P_1}^{*}\cdots a_{P_n}^{*}\in\mathcal{O}_n(W), \tag{3.12}$$

where $(P_1,\ldots,P_n)$ is an arbitrary element of ω (this does not depend on the choice of $(P_1,\ldots,P_n)$). Note that this gives a bijection between Λ^n/S_n and the set of degree n monomials expressed in the basis A^*.

Let $w\mapsto\widehat{w}$ be the linear function $(W^*)^{\otimes n}\to\mathcal{O}_n(W)$ satisfying

$$(w_1^*\otimes\cdots\otimes w_n^*)\mapsto w_1^*\cdots w_n^*$$

for all $w_1^*,\ldots,w_n^*\in W^*$.

Define for $i=1,\ldots,k$, the $m_i\times m_i$ matrix $F_i\in(W^*)^{m_i\times m_i}$ by

$$(F_i)_{j,h} := (B_i(j)\otimes B_i(h))|_W = \sum_{P\in\Lambda}(B_i(j)\otimes B_i(h))(a_P)a_P^{*}. \tag{3.13}$$

For any $n',m'\in\mathbb{Z}_{\geq 0}$, $\lambda\vdash n'$, and $\tau,\sigma\in T_{\lambda,m'}$, define the polynomial $p_{\tau,\sigma}\in\mathbb{C}[x_{j,h}\mid j,h=1,\ldots,m']$ by

$$p_{\tau,\sigma}(X) := \sum_{\substack{\tau'\sim\tau\\ \sigma'\sim\sigma}}\sum_{c,c'\in C_\lambda}\operatorname{sgn}(cc')\prod_{y\in Y(\lambda)}x_{\tau'c(y),\sigma'c'(y)}, \tag{3.14}$$

for $X=(x_{j,h})_{j,h=1}^{m'}\in\mathbb{C}^{m'\times m'}$. This polynomial can be computed (expressed as a linear combination of monomials in $x_{j,h}$) in polynomial time, as proven in [35, 52] — see Section 3.4.1.

Proposition 3.2.1. *We have*

$$\sum_{\omega\in\Lambda^n/S_n} \left(\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}} K_\omega \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}\right)\mu(\omega) = \prod_{i=1}^{k} p_{\tau_i,\sigma_i}(F_i). \tag{3.15}$$

Proof. For each $\omega \in \Lambda^n/S_n$ we can write $\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}} K_\omega \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}} = (\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}} \otimes \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}})(K_\omega)$, using the fact that $\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}, \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}} \in ((\mathbb{C}Z)^{\otimes n})^*$ and $K_\omega \in (\mathbb{C}Z)^{\otimes n} \otimes (\mathbb{C}Z)^{\otimes n}$. Set

$$f := (\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}} \otimes \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}})|_{W^{\otimes n}} = \bigotimes_{i=1}^{k} \sum_{\substack{\tau_i'\sim\tau_i\\ \sigma_i'\sim\sigma_i}} \sum_{c_i,c_i'\in C_{\lambda_i}} \operatorname{sgn}(c_ic_i') \bigotimes_{y\in Y(\lambda_i)} (F_i)_{\tau_i'c_iy,\,\sigma_i'c_i'y}.$$

Then, as $K_\omega \in W^{\otimes n}$,

$$\begin{aligned}
\sum_{\omega\in\Lambda^n/S_n} (\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}} \otimes \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}})(K_\omega)\mu(\omega) &= \sum_{\omega\in\Lambda^n/S_n} f(K_\omega)\mu(\omega)\\
&\overset{(3.9),\,(3.12)}{=} \sum_{(P_1,\ldots,P_n)\in\Lambda^n} f(a_{P_1}\otimes\cdots\otimes a_{P_n})\, a_{P_1}^*\cdots a_{P_n}^*\\
&= \sum_{(P_1,\ldots,P_n)\in\Lambda^n} f(a_{P_1}\otimes\cdots\otimes a_{P_n})\, \widehat{a_{P_1}^*\otimes\ldots\otimes a_{P_n}^*} = \widehat{f}\\
&= \prod_{i=1}^{k} \sum_{\substack{\tau_i'\sim\tau_i\\ \sigma_i'\sim\sigma_i}} \sum_{c_i,c_i'\in C_{\lambda_i}} \operatorname{sgn}(c_ic_i') \prod_{y\in Y(\lambda_i)} (F_i)_{\tau_i'c_iy,\,\sigma_i'c_i'y}\\
&= \prod_{i=1}^{k} p_{\tau_i,\sigma_i}(F_i),
\end{aligned}$$

which gives the desired equality. □

So it remains to compute the entries of the matrices F_i, i.e., to express each $(B_i(j)\otimes B_i(h))|_W$ as a linear function into the basis A^*. So we must calculate the numbers $(B_i(j)\otimes B_i(h))(a_P)$ for all $i = 1,\ldots,k$ and $j,h = 1,\ldots,m_i$, and $P \in \Lambda$.

Now one computes the entry $\sum_{\omega\in\Lambda^n/S_n} z(\omega)\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}} K_\omega \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}$ by replacing each monomial $\mu(\omega)$ in $\prod_{i=1}^{k} p_{\tau_i,\sigma_i}(F_i)$ with the variable $z(\omega)$.

3.3 Generalization: multiple Z_i and G_i

Let $s \in \mathbb{N}$ be fixed. For $i = 1,\ldots,s$, let G_i be a finite group acting on a finite set Z_i and let $j_i \in \mathbb{N}$ be such that $j_1 + \ldots + j_s = n$. Set

$$H := (G_1^{j_1} \rtimes S_{j_1}) \times \ldots \times (G_s^{j_s} \rtimes S_{j_s}) \quad\text{and}\quad R := Z_1^{j_1} \times \ldots \times Z_s^{j_s}. \tag{3.16}$$

For $i = 1,\ldots,s$, let $\Lambda_i := (Z_i \times Z_i)/G_i$ and $W_i := (\mathbb{C}Z_i \otimes \mathbb{C}Z_i)^{G_i}$. By (3.7), there is a natural bijection $\Lambda_i^{j_i}/S_{j_i} \to (Z_i \times Z_i)^{j_i}/(G_i^{j_i} \rtimes S_{j_i})$ for each $i = 1,\ldots,s$. Also, there is a bijection

$$\prod_{i=1}^{s} \left((Z_i \times Z_i)^{j_i}/(G_i^{j_i} \rtimes S_{j_i})\right) \to R^2/H,$$

obtained by identifying $(Z_1 \times Z_1)^{j_1} \times \ldots \times (Z_s \times Z_s)^{j_s}$ and R^2 in the natural way. So this gives is a bijection between the set $(\Lambda_1^{j_1}/S_{j_1}) \times \ldots \times (\Lambda_s^{j_s}/S_{j_s})$ and the set of H-orbits on R^2. So we can write each $\omega \in R^2/H$ as

$$\omega = \omega_1 \times \ldots \times \omega_s, \quad \text{where } \omega_i \in \Lambda_i^{j_i}/S_{j_i} \text{ for each } 1 \leq i \leq s. \tag{3.17}$$

For each $P \in \Lambda_i$, define $a_P := \sum_{(x,y)\in P} x \otimes y \in W_i$. Then the set $A_i := \{a_P \mid P \in \Lambda_i\}$ is a basis of W_i. As before, let for each orbit $\omega_i \in \Lambda_i^{j_i}/S_{j_i}$ the matrix $K_{\omega_i}^{(i)}$ be the *adjacency matrix* of ω_i, i.e., the $Z_i^{j_i} \times Z_i^{j_i}$ matrix with

$$(K_{\omega_i}^{(i)})_{\alpha,\beta} := \begin{cases} 1 & \text{if } (\alpha,\beta) \in \omega_i, \\ 0 & \text{otherwise,} \end{cases} \tag{3.18}$$

for $\alpha, \beta \in Z^{j_i}$. Using the natural identification of $Z_i^{j_i} \times Z_i^{j_i}$ and $(Z_i \times Z_i)^{j_i}$, we have

$$K_{\omega_i}^{(i)} = \sum_{(P_1,\ldots,P_{j_i})\in\omega_i} a_{P_1} \otimes \cdots \otimes a_{P_{j_i}} \quad \in W_i^{\otimes j_i}. \tag{3.19}$$

Next, we define for each $\omega \in R^2/H$ the $R \times R$ adjacency matrix K_ω of ω by

$$(K_\omega)_{\alpha,\beta} := \begin{cases} 1 & \text{if } (\alpha,\beta) \in \omega, \\ 0 & \text{otherwise,} \end{cases} \tag{3.20}$$

for $\alpha, \beta \in R$. So

$$K_\omega = K_{\omega_1}^{(1)} \otimes \ldots \otimes K_{\omega_s}^{(s)}, \tag{3.21}$$

if $\omega = \omega_1 \times \ldots \times \omega_s$. The matrix $M(z) := \sum_{\omega\in R^2/H} z(\omega)K_\omega$ (for any $z : R^2/H \to \mathbb{R}$) can be reduced to size polynomially bounded in n. We sketch the reduction.

With Proposition 3.1.1, we obtain representative sets for the separate actions of of $G_i^{j_i} \rtimes S_{j_i}$ on $Z_i^{j_i}$, for each $i = 1, \ldots, s$. Subsequently, with (2.18) we find a representative set for the action of $(G_1^{j_1} \rtimes S_{j_1}) \times \ldots \times (G_s^{j_s} \rtimes S_{j_s})$ on $(\mathbb{C}^{Z_1^{j_1}}) \otimes \ldots \otimes (\mathbb{C}^{Z_s^{j_s}}) \cong \mathbb{C}^R$. The computation of $\Phi(M(z))$ now entirely follows from (2.19) in combination with the results described in Section 3.2, as

$$(u_1 \otimes \ldots \otimes u_s)^\mathsf{T} \left(K_{\omega_1}^{(1)} \otimes \ldots \otimes K_{\omega_s}^{(s)}\right)(v_1 \otimes \ldots \otimes v_s) = \prod_{i=1}^{s} \left(u_i^\mathsf{T} K_{\omega_i}^{(i)} v_i\right), \tag{3.22}$$

for all vectors $u_i, v_i \in \mathbb{C}^{Z_i^{j_i}} \cong (\mathbb{C}^{Z_i})^{\otimes j_i}$.

3.4 Appendices

3.4.1 Appendix 1: Two algorithms to compute $p_{\tau,\sigma}$

For any $n, m \in \mathbb{Z}_{\geq 0}$, $\lambda \vdash n$, and $\tau, \sigma \in T_{\lambda,m}$, recall that the polynomial $p_{\tau,\sigma} \in \mathbb{C}[x_{j,h} \mid j, h = 1, \ldots, m]$ is defined by

$$p_{\tau,\sigma}(X) := \sum_{\substack{\tau'\sim\tau \\ \sigma'\sim\sigma}} \sum_{c,c'\in C_\lambda} \operatorname{sgn}(cc') \prod_{y\in Y(\lambda)} x_{\tau'c(y),\sigma'c'(y)} \quad \text{(as in (3.14))},$$

for $X = (x_{j,h})_{j,h=1}^m \in \mathbb{C}^{m\times m}$. Note that in this way $p_{\tau,\sigma}(X)$ is described with an exponential number of terms. However:

Proposition 3.4.1. *Expressing $p_{\tau,\sigma}(X)$ as a linear combination of monomials can be done in time polynomial in n, for fixed m.*

Proof. First observe that

$$\begin{aligned} p_{\tau,\sigma}(X) &= |C_\lambda| \sum_{\substack{\tau'\sim\tau\\ \sigma'\sim\sigma}} \sum_{c\in C_\lambda} \operatorname{sgn}(c) \prod_{y\in Y(\lambda)} x_{\tau'(y),\sigma'c(y)} \\ &= |C_\lambda| \sum_{\substack{\tau'\sim\tau\\ \sigma'\sim\sigma}} \prod_{i=1}^{\lambda_1} \det((x_{\tau'(i,j),\sigma'(i,j')})_{j,j'=1}^{\lambda_i^*}). \end{aligned}$$

(λ^* is the dual partition of λ; that is, λ_i^* is the height of column i.)

For fixed m, when n grows, there will be several columns of $Y(\lambda)$ that are the same both in τ' and in σ'. More precisely, for given τ', σ' let the 'count function' κ be defined as follows: for $t \in \mathbb{Z}_{\geq 0}$ and $v, w \in [m]^t$, $\kappa(v, w)$ is the number of columns i of height t such that $\tau'(i, j) = v_j$ and $\sigma'(i, j) = w_j$ for all $j = 1, \ldots, t$. Furthermore, write for each $j \leq h :=$ height(λ) and each $s \in [m]$:

$$\begin{aligned} r(s, j) &:= \#\text{ symbols } s \text{ in row } j \text{ of } \tau, \\ u(s, j) &:= \#\text{ symbols } s \text{ in row } j \text{ of } \sigma. \end{aligned} \tag{3.23}$$

Then for each $j \leq h$ and each $s \in [m]$:

$$\begin{aligned} &\sum_{t=j}^{h} \sum_{\substack{v,w\in[m]^t\\ v_j=s}} \kappa(v, w) = r(s, j), \text{ and} \\ &\sum_{t=j}^{h} \sum_{\substack{v,w\in[m]^t\\ w_j=s}} \kappa(v, w) = u(s, j). \end{aligned} \tag{3.24}$$

For any given function $\kappa : \bigcup_{j=1}^{h} [m]^j \times [m]^j \to \mathbb{Z}_{\geq 0}$ satisfying (3.24), there are precisely

$$\prod_{t=1}^{h} \frac{(\lambda_t - \lambda_{t+1})!}{\prod_{v,w\in[m]^t} \kappa(v, w)!} \tag{3.25}$$

pairs $\tau' \sim \tau$ and $\sigma' \sim \sigma$ having count function κ (setting $\lambda_{h+1} := 0$). (Note that (3.24) implies $\lambda_t - \lambda_{t+1} = \sum_{v,w\in[m]^t} \kappa(v, w)$, for each t, so that for each t, the factor in (3.25) is a Newton multinomial coefficient.) Hence

$$p_{\tau,\sigma}(X) = |C_\lambda| \sum_{\kappa} \prod_{t=1}^{h} (\lambda_t - \lambda_{t+1})! \prod_{v,w\in[m]^t} \frac{\det((x_{v_j,w_{j'}})_{j,j'=1}^{t})^{\kappa(v,w)}}{\kappa(v, w)!},$$

where κ ranges over functions $\kappa : \bigcup_{t=1}^{h}([m]^t \times [m]^t) \to \mathbb{Z}_{\geq 0}$ satisfying (3.24). □

This is the algorithm we gave in [52]. We now also state a different method (due to Gijswijt [35]) which is easy to implement. Define the operators

$$d_{s\to j} := \sum_{i=1}^{m} x_{s,i} \frac{\partial}{\partial x_{j,i}}, \quad \text{and } d^*_{j\to s} := \sum_{i=1}^{m} x_{i,s} \frac{\partial}{\partial x_{i,j}}. \tag{3.26}$$

Also define the polynomial (here $\lambda_{m+1} := 0$)

$$P_\lambda(X) := \prod_{k=1}^{m} \left(k! \det\left((x_{i,j})_{i,j=1}^{k}\right)\right)^{\lambda_k - \lambda_{k+1}}, \tag{3.27}$$

which is a polynomial in the variables $x_{i,j}$, where $i, j = 1, \ldots, m$. Then $P_\lambda(X)$ can be computed in time polynomially bounded in n (for fixed m, note that $\det((x_{i,j})_{i,j=1}^{m})$ has $m!$ terms).

Recall that $r(s,j)$ and $u(s,j)$ are defined in (3.23) for each $1 \leq j \leq h$ and each $s \in [m]$. We set $r(s,j) := 0$ and $u(s,j) := 0$ if $h < j \leq m$ and $s \in [m]$, so that $r(s,j)$ and $u(s,j)$ are defined for each $j \in [m]$ and $s \in [m]$. Now it holds, as is proved in [35, Theorem 7], that

$$p_{\tau,\sigma}(X) = \left(\prod_{j=1}^{m-1} \prod_{s=j+1}^{m} \frac{1}{r(s,j)!\, u(s,j)!} (d_{s \to j})^{r(s,j)} (d^*_{j \to s})^{u(s,j)} \right) \cdot P_\lambda(X). \tag{3.28}$$

Expression (3.28) gives a method to compute $p_{\tau,\sigma}(X)$ in polynomial time (for fixed m), using only methods for polynomial addition, multiplication and differentiation.

3.4.2 Appendix 2: The Delsarte bound

To illustrate the method of this chapter, we consider the Delsarte bound (cf. McEliece, Rodemich and Rumsey [59] and Schrijver [79]). The analytic definition can be given as a semidefinite programming problem of large size, as a matrix of order $q^n \times q^n$ is involved. We show how the matrix occurring in the semidefinite program can be reduced. A semidefinite programming description of the Delsarte bound $D_q(n,d)$ is the following:

$$\begin{aligned} D_q(n,d) = \max \big\{ \textstyle\sum_{u,v \in [q]^n} X_{u,v} \;\big|\; & X \in \mathbb{R}_{\geq 0}^{[q]^n \times [q]^n},\ \operatorname{tr}(X) = 1, \\ & X_{u,v} = 0 \text{ if } 0 < d_H(u,v) < d,\ X \succeq 0 \big\}. \end{aligned} \tag{3.29}$$

If $C \subseteq [q]^n$ is a code with $|C| = A_q(n,d)$ and $d_{\min}(C) \geq d$, then the matrix X with $X_{u,v} = |C|^{-1}$ if $u, v \in C$ and $X_{u,v} = 0$ otherwise is a feasible solution (positive semidefiniteness of this X follows from $X = |C|^{-1}\chi_C\chi_C^{\mathsf{T}}$, with $\chi_C \in \mathbb{R}^V$ the $0,1$-vector with $(\chi_C)_v = 1 \iff v \in C$) with objective value $|C|$. This shows that $A_q(n,d) \leq D_q(n,d)$.

The group $H := S_q^n \rtimes S_n$ acts on $[q]^n$ and preserves distances, which means that $d_H(u,v) = d_H(\pi(u), \pi(v))$ for all $\pi \in H$ and $u, v \in [q]^n$. If X is an optimum solution, also $\pi \cdot X$ is an optimum solution (where $\pi \cdot X$ denotes the matrix with $(\pi \cdot X)_{u,v} = X_{\pi(u),\pi(v)}$) as $\pi \cdot X$ is feasible with the same objective value as X. Since the set of feasible solutions is convex, we may replace any optimum solution X by $(1/|H|) \sum_{\pi \in H} \pi \cdot X$, which is an H-invariant optimum solution. So we may assume that the optimum in (3.29) is H-invariant.

In that case, the value $X_{u,v}$ only depends on the distance i between u and v, so we can write $z(\omega_i)$ for the common value of $X_{u,v}$ for all $u, v \in [q]^n$ with $d_H(u,v) = i$. With notation as in the previous subsections, set $Z := [q]$ and $G := S_q$, so that $\Lambda := ([q] \times [q])/S_q$.

As explained in (3.7), there is a natural bijection between Λ^n/S_n and $(Z \times Z)^n/H \cong (Z^n \times Z^n)/H$. In the present case, an H-orbit of $Z^n \times Z^n$ is determined by the distance i between two elements of Z^n. So we can write ω_i for the element in Λ^n/S_n that corresponds with the H-orbit of two words at distance i. Then the bound $D_q(n,d)$ from (3.29) is equal to

$$\max\Big\{\textstyle\sum_{i=0}^{n}\binom{n}{i}(q-1)^i q^n z(\omega_i) \;\Big|\; z:\Lambda^n/S_n \to \mathbb{R},\; z(\omega_0)=q^{-n},\; z(\omega_1)=\ldots=z(\omega_{d-1})=0, \\ z(\omega_i)\geq 0 \text{ for all } d\leq i\leq n,\; M(z)\succeq 0\Big\}, \tag{3.30}$$

where $M(z) := \sum_{i=0}^{n} z(\omega_i)K_{\omega_i}$.

Now we compute $\Phi(M(z))$ with the method from this chapter. First we find a representative set for the natural action of $G = S_q$ on $Z = [q]$. It is well known that $V := \mathbb{C}^Z = \mathbb{C}^{[q]}$ decomposes into pairwise orthogonal irreducible representations as $V_{1,1}\oplus V_{2,1}$ where $V_{1,1} = \{\lambda\mathbf{1} \mid \lambda\in\mathbb{C}\}$ is the trivial representation (here $\mathbf{1}$ denotes the all-ones vector in $\mathbb{C}^{[q]}$) and $V_{2,1} = V_{1,1}^{\perp}$ is the $(q-1)$-dimensional standard representation [77]. So a representative set for the action of G on V is $\boldsymbol{B} = \{B_1, B_2\}$, where $B_1 \in V_{1,1}$ and $B_2 \in V_{2,1}$ arbitrary. We take

$$B_1 := \tfrac{1}{\sqrt{q}}\mathbf{1}, \quad B_2 := \tfrac{1}{\sqrt{2}}(e_0 - e_1), \tag{3.31}$$

where e_i denotes the ith standard basis vector in $\mathbb{C}^{[q]}$, for $i\in[q]$.

Now Proposition 3.1.1 gives a representative set (3.3) for the action of $H = S_q^n \rtimes S_n$ on $Z^n = [q]^n$. For convenience of the reader, we restate the main definitions of Chapter 3 and the main facts about representative sets applied to the context of this section in a separate frame — see Figure 3.1.

FACTS.

$G := S_q$.
$Z := [q]$.

$k := 2$, $\boldsymbol{m} = (m_1, m_2) = (1,1)$.

A representative set for the action of G on Z is $\boldsymbol{B} = \{B_1, B_2\}$ from (3.31).
A representative set for the action of H on Z^n follows from Proposition 3.1.1.

$\Lambda = ([q]\times[q])/S_q$.
$a_P = \sum_{(x,y)\in P} x\otimes y$ for $P\in\Lambda$.
$A := \{a_P \,|\, P\in\Lambda\}$, a basis of $W := (\mathbb{C}[q]\otimes\mathbb{C}[q])^{S_q}$.
$K_\omega = \sum_{(P_1,\ldots,P_n)\in\omega} a_{P_1}\otimes\cdots\otimes a_{P_n}$ for $\omega\in\Lambda^n/S_n$.

Figure 3.1: The main definitions of Chapter 3 and the main facts about representative sets applied to the context of Section 3.4.2.

With the notation as in Section 3.1, we have in this case that $\boldsymbol{m} = (m_1, m_2) = (1,1)$, and that $\boldsymbol{N} = \{(n-t,t) \mid t = 0,\ldots,n\}$. For each $(n-t,t)\in\boldsymbol{N}$, there is only one $\boldsymbol{\lambda}\vdash(n-t,t)$ with $\text{height}(\lambda_1)\leq m_1 = 1$ and $\text{height}(\lambda_2)\leq m_2 = 1$, namely $\boldsymbol{\lambda} = (\lambda_1,\lambda_2)$ with $\lambda_1 = (n-t)$ and $\lambda_2 = (t)$. Moreover, for this $\boldsymbol{\lambda}$, the set $\boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}} = T_{\lambda_1,1}\times T_{\lambda_2,1}$ has only one element $\boldsymbol{\tau}$, namely $\boldsymbol{\tau} = (\tau_1,\tau_2)$ with

$$\tau_1 = \underbrace{\boxed{1}\ldots\boxed{1}}_{n-t}, \quad \tau_2 = \underbrace{\boxed{1}\ldots\boxed{1}}_{t},$$

i.e., both τ_1 and τ_2 are Young tableaux of height 1 which only contain ones. So the blocks $U_{\boldsymbol{\lambda}}^{\mathsf{T}} M(z) U_{\boldsymbol{\lambda}}$ all have size 1, and $U_{\boldsymbol{\lambda}}^{\mathsf{T}} M(z) U_{\boldsymbol{\lambda}} = \boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}} M(z) \boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}$ for the unique element $\boldsymbol{\tau} \in \boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}$ with $\boldsymbol{\lambda} \vdash (n-t,t)$. By Proposition 3.2.1 we have for this $\boldsymbol{\tau}$ that

$$\sum_{i=0}^{n} (\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}} K(\omega_i) \boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}) \mu(\omega_i) = \prod_{i=1}^{2} p_{\tau_i,\tau_i}(F_i) = ((F_1)_{1,1})^{n-t}((F_2)_{1,1})^t.$$

Recall that each $B_i \in \mathbb{C}^{[q]}$ is a linear function on $\mathbb{C}[q]$, and that each a_P is an element of $\mathbb{C}[q] \otimes \mathbb{C}[q]$, where $P \in \Lambda$. We express each $(F_i)_{1,1} = (B_i \otimes B_i)|_W$ in the dual basis $A^* := \{a_P^* \mid P \in \Lambda\}$ of A. The coefficient of a_P^* is obtained by evaluating $(B_i \otimes B_i)(a_P)$. We denote an equivalence class in $\Lambda = [q]^2/S_q$ by its lexicographically smallest element, representing vectors in $[q]^2$ as words, i.e., a vector in $[q]^2$ is represented as a string of symbols in $[q]$ of length 2. We find

$$\begin{aligned}(F_1)_{1,1} &= (B_1(1) \otimes B_1(1))|_W = a_{00}^* + (q-1)a_{01}^*,\\ (F_2)_{1,1} &= (B_2(1) \otimes B_2(1))|_W = a_{00}^* - a_{01}^*,\end{aligned} \tag{3.32}$$

as $(B_1(1) \otimes B_1(1))(a_{00}) = 1$, $(B_1(1) \otimes B_1(1))(a_{01}) = q-1$, $(B_2(1) \otimes B_2(1))(a_{00}) = 1$ and $(B_2(1) \otimes B_2(1))(a_{01}) = -1$. So we obtain

$$\begin{aligned}((F_1)_{1,1})^{n-t}((F_2)_{1,1})^t &= (a_{00}^* + (q-1)a_{01}^*)^{n-t}(a_{00}^* - a_{01}^*)^t\\ &= \sum_{l=0}^{n-t} \binom{n-t}{l} (a_{00}^*)^{n-t-l}(q-1)^l (a_{01}^*)^l \sum_{j=0}^{t} \binom{t}{j} (a_{00}^*)^{t-j}(-1)^j (a_{01}^*)^j\\ &= \sum_{l=0}^{n-t}\sum_{j=0}^{t} \binom{t}{j}\binom{n-t}{l} (-1)^j (q-1)^l (a_{00}^*)^{n-j-l}(a_{01}^*)^{j+l}.\end{aligned}$$

Now we replace each monomial $\mu(\omega)$ by the variable $z(\omega)$, so $(a_{00}^*)^{n-i}(a_{01}^*)^i$ gets replaced by $z(\omega_i)$ for each $0 \le i \le n$. We obtain:

$$U_{\boldsymbol{\lambda}}^{\mathsf{T}} M(z) U_{\boldsymbol{\lambda}} = \sum_{l=0}^{n-t}\sum_{j=0}^{t} \binom{t}{j}\binom{n-t}{l} (-1)^j (q-1)^l z(\omega_{j+l}). \tag{3.33}$$

Put $a_i := \binom{n}{i}(q-1)^i q^n z(\omega_i)$ for $0 \le i \le n$. Here we note that $|\omega_i| = \binom{n}{i}(q-1)^i q^n$, so $a_i = |\omega_i| z(\omega_i)$. Moreover, note that $\binom{n}{t}\binom{t}{j}\binom{n-t}{l} = \binom{n}{j+l}\binom{n-j-l}{t-j}\binom{j+l}{j}$ for nonnegative integers n,t,j,l satisfying $j \le t \le n$ and $l \le n-t$. So we obtain from (3.33) that

$$\begin{aligned}U_{\boldsymbol{\lambda}}^{\mathsf{T}} M(z) U_{\boldsymbol{\lambda}} &= \frac{1}{\binom{n}{t} q^n} \sum_{l=0}^{n-t}\sum_{j=0}^{t} \binom{n-j-l}{t-j}\binom{j+l}{j} (-1)^j (q-1)^{-j} a_{j+l}\\ &= \frac{1}{\binom{n}{t}(q-1)^t q^n} \sum_{i=0}^{n}\sum_{j=0}^{t} \binom{n-i}{t-j}\binom{i}{j} (-1)^j (q-1)^{t-j} a_i\\ &= \frac{1}{|\omega_t|} \sum_{i=0}^{n} K_t(i) a_i,\end{aligned} \tag{3.34}$$

where K_t is the t-th *Krawtchouk polynomial* defined in (1.3). So $M(z) \succeq 0$ if and only if $\sum_{i=0}^{n} K_t(i)a_i \geq 0$ for each $t = 0, \ldots, n$. This allows us to rewrite (3.30) as a linear program as follows:

$$\begin{aligned} D_q(n,d) = \max \Big\{ \textstyle\sum_{i=0}^{n} a_i \;\Big|\; & a_0 = 1,\; a_1 = \ldots = a_{d-1} = 0,\;\; a_i \geq 0 \text{ if } d \leq i \leq n, \\ & \textstyle\sum_{i=0}^{n} K_t(i)a_i \geq 0 \text{ for all } 0 \leq t \leq n \;\Big\}, \end{aligned} \tag{3.35}$$

which coincides with the definition given in the introduction. Hence we obtain the Delsarte bound as an application of the method of this chapter.

Note that the fact that we obtain a *linear* program stems from the fact that the G-module $\mathbb{C}^Z$ decomposes into irreducible modules each of multiplicity ≤ 1. In this case the matrices $U_{\boldsymbol{\lambda}}^{\mathsf{T}} M(z) U_{\boldsymbol{\lambda}}$ are of order 1×1.

Chapter 4

Semidefinite programming bounds for unrestricted codes

The purpose of computation is insight, not numbers.
— Richard Hamming (1915–1998)

For $q, n, d \in \mathbb{N}$, let $A_q(n,d)$ denote the maximum cardinality of a q-ary code of word length n and minimum distance at least d. We will consider a semidefinite programming upper bound on $A_q(n,d)$ based on quadruples of codewords. By the symmetry of the problem, we can apply representation theory to reduce the problem to a semidefinite programming problem with order bounded by a polynomial in n. The method yields the new upper bounds $A_4(6,4) \leq 176$, $A_4(7,3) \leq 596$, $A_4(7,4) \leq 155$, $A_5(7,4) \leq 489$ and $A_5(7,5) \leq 87$. This chapter is based on joint work with Bart Litjens and Lex Schrijver [52] and relies on the method explained in Chapter 3.

4.1 Introduction

We will assume throughout that $q \geq 2$. For $q = 2$, semidefinite programming bounds based on quadruples of codewords have been studied by Gijswijt, Mittelmann and Schrijver [37]. While this chapter is mainly meant to handle the case $q \geq 3$, the results also hold for $q = 2$. We will study the following upper bound on $A_q(n,d)$, sharpening Delsarte's classical linear programming bound [31].

For $k \in \mathbb{Z}_{\geq 0}$, let $\mathcal{C}_k$ be the collection of subsets C of $[q]^n$ with $|C| \leq k$. For each $x : \mathcal{C}_4 \to \mathbb{R}$ define the $\mathcal{C}_2 \times \mathcal{C}_2$ matrix $M(x)$ by

$$M(x)_{C,C'} := x(C \cup C') \tag{4.1}$$

for $C, C' \in \mathcal{C}_2$. Then define

$$B_q(n,d) := \max \left\{ \textstyle\sum_{v \in [q]^n} x(\{v\}) \mid x : \mathcal{C}_4 \to \mathbb{R}_{\geq 0},\ x(\emptyset) = 1, \quad x(S) = 0 \text{ if } d_{\min}(S) < d, \right.$$
$$\left. M(x) \succeq 0 \right\}. \tag{4.2}$$

Proposition 4.1.1. *$A_q(n,d) \leq B_q(n,d)$.*

Proof. Let $C \subseteq [q]^n$ have minimum distance at least d and satisfy $|C| = A_q(n,d)$. Define $x : \mathcal{C}_4 \to \mathbb{R}$ by $x(S) = 1$ if $S \subseteq C$ and $x(S) = 0$ otherwise, for $S \in \mathcal{C}_4$. Then x satisfies the conditions in (4.2): the condition that $M(x) \succeq 0$ follows from the fact that for this x one has $M(x)_{S,S'} = x(S)x(S')$ for all $S, S' \in \mathcal{C}_2$. Moreover, $\sum_{v \in [q]^n} x(\{v\}) = |C| = A_q(n,d)$. □

The optimization problem (4.2) is huge, but, with the representation theory of Chapters 2 and 3, it can be reduced to a size bounded by a polynomial in n, with entries (i.e., coefficients) being polynomials in q.

To explain the reduction, let H be the wreath product $S_q^n \rtimes S_n$. For each k, the group H acts naturally on $\mathcal{C}_k$, maintaining minimum distances and cardinalities of elements of $\mathcal{C}_k$ (being codes). Then we can assume that x in (4.2) is invariant under the H-action on $\mathcal{C}_4$. That is, we can assume that $x(C) = x(D)$ whenever $C, D \in \mathcal{C}_2$ and $D = g \cdot C$ for some $g \in H$. Indeed, the conditions in (4.2) are maintained under replacing x by $g \cdot x$. (Note that $M(g \cdot x)$ is obtained from $M(x)$ by simultaneously permuting rows and columns.) Moreover, the objective function does not change by this action. Hence the optimum x can be replaced by the average of all $g \cdot x$ (over all $g \in H$), by the convexity of the set of positive semidefinite matrices. This makes the optimum solution H-invariant.

Let Ω_4 be the set of H-orbits on $\mathcal{C}_4$. Note that Ω_4 is bounded by a polynomial in n (independently of q). As there exists an H-invariant optimum solution, we can replace, for each $\omega \in \Omega_4$ and $C \in \omega$, each variable $x(C)$ by a variable $z(\omega)$. In this way we obtain $M(z)$.

Then $M(z)$ is invariant under the simultaneous action of H on the set $\mathcal{C}_2$ of its rows and columns. Hence $M(z)$ can be block-diagonalized (as explained in Sect. 1.2) by $M(z) \mapsto U^{\mathsf{T}} M(z) U$, where U is a matrix independent of z, such that the order of $U^{\mathsf{T}} M(z) U$ is polynomial in n and such that the original matrix $M(z)$ is positive semidefinite if and only if each of the blocks is positive semidefinite. The entries in each block are linear functions of the variables $z(\omega)$.

In this chapter we will describe the blocks that reduce the problem. We make use of the framework developed in Chapter 3. With the reduced semidefinite program, we found the following improvements on the known bounds for $A_q(n,d)$ (see Table 4.1), with thanks to Hans D. Mittelmann for his help in solving the larger-sized programs.

q	n	d	best lower bound known	**new upper bound**	best upper bound previously known	Delsarte bound
4	6	3	164	**176**	179	179
4	7	3	512	**596**	614	614
4	7	4	128	**155**	169	179
5	7	4	250	**489**	545	625
5	7	5	53	**87**	108	125

Table 4.1: The new upper bounds on $A_q(n,d)$.

The best upper bounds previously known for $A_4(6,3)$ and $A_4(7,3)$ are Delsarte's linear programming bound [31]; the other three best upper bounds previously known were given by Gijswijt, Schrijver, and Tanaka [38] (semidefinite programming bounds based on triples). We refer to the most invaluable tables maintained by Andries Brouwer [23] with the best known lower and upper bounds for the size of error-correcting codes (see also Bogdanova, Brouwer, Kapralov, and Östergård [15] and Bogdanova and Östergård [16] for studies of bounds for codes over alphabets of size $q = 4$ and $q = 5$, respectively).

4.1.1 Comparison with earlier bounds

The bound $B_q(n, d)$ described above is a sharpening of Delsarte's classical linear programming bound [31]. The value of the Delsarte bound is equal to our bound after replacing $\mathcal{C}_4$ and $\mathcal{C}_2$ by $\mathcal{C}_2$ and $\mathcal{C}_1$, respectively, which generally yields a less strict bound.

We can add to (4.2) the condition that, for each $D \in \mathcal{C}_4$, the $\mathcal{C}_4(D) \times \mathcal{C}_4(D)$ matrix

$$(x(C \cup C'))_{C,C' \in \mathcal{C}_4(D)} \text{ is positive semidefinite,} \tag{4.3}$$

where $\mathcal{C}_4(D) := \{C \in \mathcal{C}_4 \mid C \supseteq D, |D| + 2|C \setminus D| \leq 4\}$. (So $M(x)$ in (4.2) is the case $D = \emptyset$.) Also the addition of (4.3) allows a reduction of the optimization problem to polynomial size as above. (It can be seen that adding (4.3) for $|D| = 2$ suffices.) For $q = 2$ we obtain in this way the bound given by Gijswijt, Mittelmann and Schrijver [37].

A bound intermediate to the Delsarte bound and the currently investigated bound is based on considering functions $x : \mathcal{C}_3 \to \mathbb{R}_{\geq 0}$ and the related matrices — see Schrijver [81] for binary codes and Gijswijt, Schrijver, and Tanaka [38] for nonbinary codes.

4.2 Reduction of the optimization problem

In this section we describe reducing the optimization problem (4.2) conceptually. In Section 4.3 we consider this reduction computationally. For the remainder of this chapter we fix n and q.

We consider the natural action of $H = S_q^n \rtimes S_n$ on $\mathcal{C}_2$. If $U_1, \ldots, U_k$ form a representative set of matrices for this action, then with (2.16) we obtain a reduction of the size of the optimization problem to polynomial size. To make this reduction explicit in order to apply semidefinite programming, we need to express each $m_i \times m_i$ matrix $U_i^{\mathsf{T}} M(z) U_i$ as an explicit matrix in which each entry is a linear combination of the variables $z(\omega)$ for $\omega \in \Omega_4$ (the set of H-orbits of $\mathcal{C}_4$).

For $\omega \in \Omega_4$, let N'_ω be the $\mathcal{C}_2 \times \mathcal{C}_2$ matrix with $0, 1$ entries satisfying

$$(N'_\omega)_{\{\alpha,\beta\},\{\gamma,\delta\}} = 1 \text{ if and only if } \{\alpha, \beta, \gamma, \delta\} \in \omega \tag{4.4}$$

for $\alpha, \beta, \gamma, \delta \in [q]^n$. Then

$$U_i^{\mathsf{T}} M(z) U_i = \sum_{\omega} z(\omega) U_i^{\mathsf{T}} N'_\omega U_i.$$

So to get the reduction, we need to obtain the matrices $U_i^{\mathsf{T}} N'_\omega U_i$ explicitly, for each $\omega \in \Omega_4$ and for each $i = 1, \ldots, k$. We do this in a number of steps, using the main symmetry reduction in Chapter 3.

We first describe in Section 4.2.1 a representative set for the natural action of S_q on $[q] \times [q]$. Proposition 3.1.1 (with $V := \mathbb{C}^Z$, where $Z := [q] \times [q]$, and $G := S_q$) then yields a representative set for the action of the wreath product $H = S_q^n \rtimes S_n$ on the set $([q]^n)^2$ of *ordered* pairs of words in $[q]^n$, in other words, on $\mathbb{C}^{([q]^n)^2} \cong (\mathbb{C}^{[q]\times[q]})^{\otimes n}$. From this we derive in Section 4.2.3 a representative set for the action of H on the set $\mathcal{C}_2 \setminus \{\emptyset\}$ of *unordered* pairs $\{v, w\}$ (including singleton) of words v, w in $[q]^n$. Then in Section 4.2.4 we derive a representative set for the action of H on the set $\mathcal{C}_2^d \setminus \{\emptyset\}$, where $\mathcal{C}_2^d$ is the set of codes in $\mathcal{C}_2$ of minimum distance at least d. (So each singleton word belongs to $\mathcal{C}_2^d$.) Finally, in Section 4.2.4 we include the empty set $\emptyset$, by an easy representation-theoretic argument.

4.2.1 A representative set for the action of of S_q on $[q] \times [q]$

We now consider the natural action of S_q on $\mathbb{C}^{[q]\times[q]}$. Let e_j be the j-th unit basis vector in $\mathbb{C}^q$, I_q be the $q \times q$ identity matrix, J_q be the all-one $q \times q$ matrix, $\mathbf{1}$ be the all-one column vector in $\mathbb{C}^q$, $N := (e_0 - e_1)\mathbf{1}^\mathsf{T}$, and $E_{i,j} := e_i e_j^\mathsf{T}$. We furthermore define the following matrices, where we consider matrices in $\mathbb{C}^{q\times q}$ as *columns* of the matrices B_i:

$$\begin{aligned}
B_1 &:= [I_q, J_q - I_q],\\
B_2 &:= [E_{0,0} - E_{1,1}, N - N^\mathsf{T}, N + N^\mathsf{T} - 2(E_{0,0} - E_{1,1})],\\
B_3 &:= [E_{0,1} + E_{1,2} + E_{2,0} - E_{1,0} - E_{2,1} - E_{0,2}],\\
B_4 &:= [E_{0,2} - E_{2,1} + E_{1,3} - E_{3,0} + E_{2,0} - E_{1,2} + E_{3,1} - E_{0,3}]. \qquad (4.5)
\end{aligned}$$

The matrices in $\mathbb{C}^{q\times q}$ are elements of the dual space $(\mathbb{C}([q] \times [q]))^*$, so they are elements of the algebra $\mathcal{O}(\mathbb{C}([q] \times [q]))$ of polynomials on the linear space $\mathbb{C}([q] \times [q])$.

Proposition 4.2.1. *The matrix set* $\boldsymbol{B} := \{B_1, \ldots, B_4\}$ *is representative for the natural action of* S_q *on* $\mathbb{C}^{[q]\times[q]}$, *if* $q \geq 4$. *If* $q \leq 3$, *we delete* B_4, *and if* $q = 2$ *we moreover delete* B_3 *and the last column of* B_2 *(as this column is* 0 *if* $q = 2$*).*

Proof. For $a \in \mathbb{C}^q$, let Δ_a be the $q \times q$ diagonal matrix with diagonal a. Define

$$\begin{aligned}
V_{1,1} &:= \{\lambda I_q \mid \lambda \in \mathbb{C}\},\\
V_{1,2} &:= \{\lambda(J_q - I_q) \mid \lambda \in \mathbb{C}\},\\
V_{2,1} &:= \{\Delta_a \mid a \in \mathbb{C}^q, a^\mathsf{T}\mathbf{1} = 0\},\\
V_{2,2} &:= \{a\mathbf{1}^\mathsf{T} - \mathbf{1}a^\mathsf{T} \mid a \in \mathbb{C}^q, a^\mathsf{T}\mathbf{1} = 0\},\\
V_{2,3} &:= \{a\mathbf{1}^\mathsf{T} + \mathbf{1}a^\mathsf{T} - 2\Delta_a \mid a \in \mathbb{C}^q, a^\mathsf{T}\mathbf{1} = 0\},\\
V_{3,1} &:= \{X \in \mathbb{C}^{q\times q} \mid X \text{ skew-symmetric}, X\mathbf{1} = 0\},\\
V_{4,1} &:= \{X \in \mathbb{C}^{q\times q} \mid X \text{ symmetric}, X\mathbf{1} = 0, X_{i,i} = 0 \text{ for all } i \in [q]\}.
\end{aligned}$$

Observe that each $V_{i,j}$ is S_q-stable, and that $V_{i,j}$ and $V_{i',j'}$ are orthogonal whenever $(i, j) \neq (i', j')$ (with respect to the inner product $X, Y \mapsto \operatorname{tr}(Y^*X)$). Moreover $\lambda I_q \mapsto \lambda(J_q - I_q)$ gives an S_q-isomorphism $V_{1,1} \to V_{1,2}$, $\Delta_a \mapsto a\mathbf{1}^\mathsf{T} - \mathbf{1}a^\mathsf{T}$ gives an S_q-isomorphism $V_{2,1} \to V_{2,2}$, and $\Delta_a \mapsto a\mathbf{1}^\mathsf{T} + \mathbf{1}a^\mathsf{T} - 2\Delta_a$ gives an S_q-isomorphism $V_{2,1} \to V_{2,3}$.

Let $q \geq 4$. Then $\dim(V_{i,j}) > 0$ for all i, j. Set, as before, $m_1 = 2$, $m_2 = 3$, $m_3 = m_4 = 1$. Then $\sum_{i=1}^4 m_i^2 = 15$, which is equal to the number of partitions of $\{1, 2, 3, 4\}$, hence to the dimension of $(\mathbb{C}^{[q]\times[q]} \otimes \mathbb{C}^{[q]\times[q]})^{S_q}$. This implies that the $V_{i,j}$

in fact form an orthogonal *decomposition* of $\mathbb{C}^{[q]\times[q]}$ into *irreducible* representations and that $V_{i,j}$ and $V_{i',j'}$ are equivalent representations if and *only if* $i = i'$ (as any further representation, or decomposition, or equivalence would yield that the sum of the squares of the multiplicities of the irreducible representations is strictly larger than 15, contradicting the fact that Φ in (2.16) is bijective).

Now $B_{1,1}$ and $B_{1,2}$ are the elements of $V_{1,1}$ and $V_{1,2}$ with $\lambda = 1$. Moreover, $B_{2,1}$, $B_{2,2}$, and $B_{2,3}$ are the elements of $V_{2,1}$, $V_{2,2}$, and $V_{2,3}$ with $a = e_0 - e_1$. Finally, $B_{3,1}$ and $B_{4,1}$ are (arbitrary) nonzero elements of $V_{3,1}$ and $V_{4,1}$. This implies that $\{B_1, \dots, B_4\}$ is a representative matrix set.

If $q = 3$, then $\dim(V_{4,1}) = 0$, while the dimension of $(\mathbb{C}^{[3]\times[3]} \otimes \mathbb{C}^{[3]\times[3]})^{S_3}$ is equal to the number of partitions of $\{1, 2, 3, 4\}$ into at most 3 classes, which is $2^2+3^2+1^2 = 14$. If $q = 2$, then moreover $\dim(V_{2,3}) = \dim(V_{3,1}) = 0$, while the dimension of $(\mathbb{C}^{[2]\times[2]} \otimes \mathbb{C}^{[2]\times[2]})^{S_2}$ is equal to the number of partitions of $\{1, 2, 3, 4\}$ into at most 2 classes, which is $2^2 + 2^2 = 8$. Similarly as above, this implies that also for $q \leq 3$, $B_1, \dots, B_k$ form a representative matrix set. □

Note that the above representative set is real.

If $q \geq 4$, set $k := 4$ and $\boldsymbol{m} := (m_1, \dots, m_k) := (2, 3, 1, 1)$. If $q = 3$, set $k := 3$ and $\boldsymbol{m} := (m_1, \dots, m_k) := (2, 3, 1)$. If $q = 2$, set $k := 2$ and $\boldsymbol{m} := (m_1, m_2) := (2, 2)$. For the remainder of this chapter we fix k, $\boldsymbol{m} = (m_1, \dots, m_k)$, and $\boldsymbol{B} = \{B_1, \dots, B_k\}$.

4.2.2 A representative set for the action of H on $([q] \times [q])^n$

Recall that $H = S_q^n \rtimes S_n$ and that we have fixed k, $\boldsymbol{m} = (m_1, \dots, m_k)$, and $\boldsymbol{B} = \{B_1, \dots, B_k\}$ in Section 4.2.1. We use the notation and definitions of Chapter 3. So $\boldsymbol{N}$ denotes the collection of all k-tuples $(n_1, \dots, n_k)$ of nonnegative integers adding up to n. Moreover, for $\boldsymbol{n} = (n_1, \dots, n_k) \in \boldsymbol{N}$, by $\boldsymbol{\lambda} \vdash \boldsymbol{n}$ it is meant that $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_k)$ with $\lambda_i \vdash n_i$ for $i = 1, \dots, k$. (So each λ_i is equal to a partition $(\lambda_{i,1}, \dots, \lambda_{i,h_i})$ of n_i, for some h_i.)

Now Proposition 3.1.1 (with $V := \mathbb{C}^Z$, where $Z := [q] \times [q]$, and $G := S_q$) gives a representative set for the action of H on $([q] \times [q])^n$: it is the set

$$\{ \ [\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}} \mid \boldsymbol{\tau} \in \boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}] \quad | \, \boldsymbol{n} \in \boldsymbol{N}, \boldsymbol{\lambda} \vdash \boldsymbol{n} \}$$

where $\boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}$ and $\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}$ are defined in (3.1) and (3.2) respectively.

For convenience of the reader, we restate the main definitions of Chapter 3 and the main facts about representative sets applied to the context of this chapter — see Figure 4.1.

4.2.3 Unordered pairs

We now go over from the set $([q]^n)^2$ of ordered pairs of code words to the set $\mathcal{C}_2 \setminus \{\emptyset\}$ of unordered pairs (including singletons) of code words. For this we consider the action of the group S_2 on $\mathbb{C}^{[q]^n \times [q]^n} \cong \mathbb{C}^{([q]^n)^2} \cong (\mathbb{C}^{[q]\times[q]})^{\otimes n}$, where the nonidentity element σ in S_2 acts as taking the transpose. The actions of S_2 and H commute.

Let L be the $(\mathcal{C}_2 \setminus \{\emptyset\}) \times ([q]^n)^2$ matrix with $0, 1$ entries satisfying

$$L_{\{\alpha,\beta\},(\gamma,\delta)} = 1 \text{ if and only if } \{\gamma, \delta\} = \{\alpha, \beta\},$$

FACTS.

$G := S_q$.
$Z := [q] \times [q]$.

If $q \geq 4$, set $k := 4$ and $\boldsymbol{m} := (m_1, \ldots, m_k) := (2, 3, 1, 1)$.
If $q = 3$, set $k := 3$ and $\boldsymbol{m} := (m_1, \ldots, m_k) := (2, 3, 1)$.
If $q = 2$, set $k := 2$ and $\boldsymbol{m} := (m_1, m_2) := (2, 2)$.

A representative set for the action of G on Z is $\boldsymbol{B} = \{B_1, \ldots, B_k\}$ from Prop. 4.2.1.
A representative set for the action of H on Z^n follows from Proposition 3.1.1.

$\Lambda = ([q]^2 \times [q]^2)/S_q \cong [q]^4/S_q$.
$a_P = \sum_{(x,y)\in P} x \otimes y$ for $P \in \Lambda$.
$A := \{a_P \mid P \in \Lambda\}$, a basis of $W := (\mathbb{C}[q]^2 \otimes \mathbb{C}[q]^2)^{S_q}$.
$K_{\omega'} = \sum_{(P_1,\ldots,P_n)\in\omega'} a_{P_1} \otimes \cdots \otimes a_{P_n}$ for $\omega' \in \Lambda^n/S_n$.

Figure 4.1: The main definitions of Chapter 3 and the main facts about representative sets applied to the context of Chapter 4.

for $\alpha, \beta, \gamma, \delta \in [q]^n$. Then the function $x \mapsto Lx$ is an H-isomorphism $(\mathbb{C}^{([q]^n)^2})^{S_2} \to \mathbb{C}^{\mathcal{C}_2 \setminus \{\emptyset\}}$.

Now note that each $B_i(j)$, as matrix in $\mathbb{C}^{q\times q}$, is S_2-invariant (i.e., symmetric) except for $B_2(2)$ and $B_3(1)$, while $\sigma \cdot B_2(2) = -B_2(2)$ and $\sigma \cdot B_3(1) = -B_3(1)$ (as $B_2(2)$ and $B_3(1)$ are skew-symmetric). So for any $\boldsymbol{n} \in \boldsymbol{N}$, $\boldsymbol{\lambda} \vdash \boldsymbol{n}$, and $\boldsymbol{\tau} \in \boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}$, we have

$$\sigma \cdot \boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}} = (-1)^{|\tau_2^{-1}(2)|+|\tau_3^{-1}(1)|}\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}.$$

Therefore, let $\boldsymbol{T}'_{\boldsymbol{\lambda},\boldsymbol{m}}$ be the set of those $\boldsymbol{\tau} \in \boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}$ with $|\tau_2^{-1}(2)| + |\tau_3^{-1}(1)|$ even. Then the matrix set

$$\{ \ \ [\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}} \mid \boldsymbol{\tau} \in \boldsymbol{T}'_{\boldsymbol{\lambda},\boldsymbol{m}}] \ \ \mid \ \ \boldsymbol{n} \in \boldsymbol{N}, \boldsymbol{\lambda} \vdash \boldsymbol{n}\} \tag{4.6}$$

is representative for the action of H on $(\mathbb{C}^{([q]^n)^2})^{S_2}$. Hence the matrix set

$$\{ \ \ [L\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}} \mid \boldsymbol{\tau} \in \boldsymbol{T}'_{\boldsymbol{\lambda},\boldsymbol{m}}] \ \mid \ \boldsymbol{n} \in \boldsymbol{N}, \boldsymbol{\lambda} \vdash \boldsymbol{n}\} \tag{4.7}$$

is representative for the action of H on $\mathcal{C}_2 \setminus \{\emptyset\}$.

4.2.4 Restriction to pairs of words at distance at least d

Let $d \in \mathbb{Z}_{\geq 0}$, and let $\mathcal{C}_2^d$ be the collection of elements of $\mathcal{C}_2$ of minimum distance at least d. Note that each singleton code word belongs to $\mathcal{C}_2^d$, and that H acts on $\mathcal{C}_2^d$. From (4.7) we derive a representative set for the action of H on $\mathcal{C}_2^d \setminus \{\emptyset\}$.

To see this, let for each $t \in \mathbb{Z}_{\geq 0}$, L_t be the subspace of $\mathbb{C}^{\mathcal{C}_2}$ spanned by the elements $e_{\{\alpha,\beta\}}$ with $\alpha, \beta \in [q]^n$ and $d_H(\alpha, \beta) = t$. (For any $C \in \mathcal{C}_2$, e_C denotes the unit base vector in $\mathbb{C}^{\mathcal{C}_2^d}$ for coordinate C.)

Then for any $\boldsymbol{n} \in \boldsymbol{N}$, $\boldsymbol{\lambda} \vdash \boldsymbol{n}$, and $\boldsymbol{\tau} \in \boldsymbol{T}'_{\boldsymbol{\lambda},\boldsymbol{m}}$, the irreducible representation $H \cdot L\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}$ is contained in L_t, where

$$t := n - |\tau_1^{-1}(1)| - |\tau_2^{-1}(1)|,$$

since $B_1(1) = I_q$ and $B_2(1) = E_{0,0} - E_{1,1}$ are the only two entries $B_i(j)$ in the B_i that have nonzeros on the diagonal of the matrix $B_i(j)$. Let $\boldsymbol{T}''_{\boldsymbol{\lambda},\boldsymbol{m}}$ be the set of those $\boldsymbol{\tau}$ in $\boldsymbol{T}'_{\boldsymbol{\lambda},\boldsymbol{m}}$ with

$$n - |\tau_1^{-1}(1)| - |\tau_2^{-1}(1)| \in \{0, d, d+1, \ldots, n\}.$$

Then a representative set for the action of H on $\mathcal{C}_2^d \setminus \{\emptyset\}$ is

$$\Big\{ \ [L\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}} \mid \boldsymbol{\tau} \in \boldsymbol{T}''_{\boldsymbol{\lambda},\boldsymbol{m}}] \quad \Big| \quad \boldsymbol{n} \in \boldsymbol{N}, \boldsymbol{\lambda} \vdash \boldsymbol{n} \Big\}. \tag{4.8}$$

4.2.5 Adding $\emptyset$

To obtain a representative set for the action of H on $\mathcal{C}_2^d$, note that H acts trivially on $\emptyset$. So $\emptyset$ belongs to the H-isotypical component of $\mathbb{C}^{\mathcal{C}_2}$ that consists of H-invariant elements. Now the H-isotypical component of $\mathbb{C}^{\mathcal{C}_2 \setminus \{\emptyset\}}$ that consists of the H-invariant elements corresponds to the matrix in the representative set indexed by indexed by $\boldsymbol{n} = (n, 0, 0, 0)$ and $\boldsymbol{\lambda} = ((n), (), (), ())$, where $() \vdash 0$. So to obtain a representative set for $\mathbb{C}^{\mathcal{C}_2}$, we just add the vector $e_\emptyset$ as column to this matrix.

4.3 How to compute $(L\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}})^{\mathsf{T}} N'_\omega L\boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}$

We currently have a reduction of the original problem to matrix blocks with coefficients $(L\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}})^{\mathsf{T}} N'_\omega L\boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}$ (where N'_ω is as in (4.4)), for $\boldsymbol{n} \in \boldsymbol{N}$, $\boldsymbol{\lambda} \vdash \boldsymbol{n}$, $\boldsymbol{\tau}, \boldsymbol{\sigma} \in \boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}$, and $\omega \in \Omega_4$. The number and orders of these blocks are bounded by a polynomial in n, but computing these coefficients still must be reduced in time, since the orders of L, $\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}$, $\boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}$, and N'_ω are exponential in n.

Fix $\boldsymbol{n} \in \boldsymbol{N}$, $\boldsymbol{\lambda} \vdash \boldsymbol{n}$, and $\boldsymbol{\tau}, \boldsymbol{\sigma} \in \boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}$. For any $\omega \in \Omega_4$, let $N_\omega := L^{\mathsf{T}} N'_\omega L$. So N_ω is a $([q]^n \times [q]^n) \times ([q]^n \times [q]^n)$ matrix with 0,1 entries satisfying

$$(N_\omega)_{(\alpha,\beta),(\gamma,\delta)} = 1 \text{ if and only if } \{\alpha, \beta, \gamma, \delta\} \in \omega,$$

for all $\alpha, \beta, \gamma, \delta \in [q]^n$. By definition of N_ω,

$$(L\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}})^{\mathsf{T}} N'_\omega L\boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}} = \boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}} N_\omega \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}.$$

So it suffices to evaluate the latter value.

Recall that $\Lambda = ([q]^4)/S_q$. By (3.7), there is a natural bijection between Λ^n/S_n and the set of H-orbits on $([q]^n)^4 \cong ([q]^4)^n$. The function $([q]^n)^4 \to \mathcal{C}_4$ with $(\alpha_1, \ldots, \alpha_4) \mapsto \{\alpha_1, \ldots, \alpha_4\}$ then gives a surjective function $r : \Lambda^n/S_n \to \Omega_4 \setminus \{\{\emptyset\}\}$.

Lemma 4.3.1. *For each $\omega \in \Omega_4$:*

$$N_\omega = \sum_{\substack{\omega' \in \Lambda^n/S_n \\ r(\omega') = \omega}} K_{\omega'}.$$

Proof. Choose $\alpha, \beta, \gamma, \delta \in [q]^n$. Then

$$\begin{aligned}\sum_{\substack{\omega' \in \Lambda^n/S_n \\ r(\omega')=\omega}} (K_{\omega'})_{(\alpha,\beta),(\gamma,\delta)} &= \sum_{\substack{\omega' \in \Lambda^n/S_n \\ r(\omega')=\omega}} \sum_{\substack{P_1,\dots,P_n \in \Lambda \\ (P_1,\dots,P_n)\in\omega'}} \left(\bigotimes_{i=1}^n a_{P_i} \right)_{\alpha,\beta,\gamma,\delta} \\ &= \sum_{\substack{\omega' \in \Lambda^n/S_n \\ r(\omega')=\omega}} \sum_{\substack{P_1,\dots,P_n \in \Lambda \\ (P_1,\dots,P_n)\in\omega'}} \prod_{i=1}^n (a_{P_i})_{\alpha_i,\beta_i,\gamma_i,\delta_i}.\end{aligned}$$

The latter value is 1 if $r(\omega') = \omega$ where ω' is the S_n-orbit of $(\pi(\alpha_1\beta_1\gamma_1\delta_1), \dots, \pi(\alpha_n\beta_n\gamma_n\delta_n))$ (here $\pi(\alpha_i\beta_i\gamma_i\delta_i)$ denotes the equivalence class in Λ containing $(\alpha_i, \beta_i, \gamma_i, \delta_i)$), and is 0 otherwise. So it is equal to $(N_\omega)_{(\alpha,\beta),(\gamma,\delta)}$. □

By this lemma, it suffices to compute $\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}} K_{\omega'} \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}$ for each $\omega' \in \Lambda^n/S_n$. By Proposition 3.2.1, we have $\sum_{\omega' \in \Lambda^n/S_n} \left(\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}} K_{\omega'} \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}\right) \mu(\omega') = \prod_{i=1}^k p_{\tau_i,\sigma_i}(F_i)$, where the matrices $F_i \in (W^*)^{m_i \times m_i}$ are defined in (3.13) and the polynomial p_{τ_i,σ_i} is defined in (3.14). So it suffices to calculate the matrices F_i, that is, to express each $(B_i(j) \otimes B_i(h))|_W$ as linear function into the dual basis A^* of A. So we must calculate the numbers $(B_i(j) \otimes B_i(h))(a_P)$ for all $i = 1, \dots, k$, $j, h = 1, \dots, m_i$, and $P \in \Lambda$ — see Appendix 1 (Section 4.4.1 below).

Now one computes the entry $\sum_{\omega \in \Omega_4} z(\omega) \boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}} N_\omega \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}$ by first expressing $\prod_{i=1}^k p_{\tau_i,\sigma_i}(F_i)$ as a linear combination of degree n monomials expressed in the dual basis A^* of A and subsequently replacing each monomial $\mu(\omega')$ in $\prod_{i=1}^k p_{\tau_i,\sigma_i}(F_i)$ with the variable $z(r(\omega'))$.

We finally consider the entries in the row and column indexed by $\emptyset$ in the matrix associated with $\boldsymbol{\lambda} = ((n), (), (), ())$ (cf. Section 4.2.5). Trivially, $e_\emptyset^{\mathsf{T}} M(x) e_\emptyset = (M(x))_{\emptyset,\emptyset} = x(\emptyset)$, which is set to 1 in the optimization problem. Any $\boldsymbol{\tau} \in \boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}$ is determined by the number t of 2's in the row of the Young shape $Y((n))$. Then

$$\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}} = \sum_{\substack{v,w \in [q]^n \\ d_H(v,w)=t}} e_{(v,w)} \quad \text{and hence} \quad L\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}} = \sum_{\substack{v,w \in [q]^n \\ d_H(v,w)=t}} e_{\{v,w\}}.$$

Hence, as $\emptyset \cup \{v, w\} = \{v, w\}$,

$$e_\emptyset^{\mathsf{T}} M(x) L\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}} = \sum_{\substack{v,w \in [q]^n \\ d_H(v,w)=t}} x(\{v,w\}) = \binom{n}{t} q^n (q-1)^t z(\omega), \tag{4.9}$$

where ω is the H-orbit of $\mathcal{C}_4$ consisting of all pairs $\{\alpha, \beta\}$ with $d_H(\alpha, \beta) = t$.

4.4 Appendices

4.4.1 Appendix 1: The formulas $(F_i)_{j,h}$

Recall that each $B_i(j) \in \mathbb{C}^{[q]\times[q]}$ is a linear function on $\mathbb{C}([q] \times [q])$, and that each a_P is an element of $\mathbb{C}([q] \times [q]) \otimes \mathbb{C}([q] \times [q])$, where $P \in \Lambda$. We compute

$$(F_i)_{j,h} := (B_i(j) \otimes B_i(h))|_W = \sum_{P \in \Lambda} (B_i(j) \otimes B_i(h))(a_P) a_P^* \quad \in W^*$$

for each $i = 1, \dots, 4$ and $j, h = 1, \dots, m_i$. The coefficient of a_P^* is obtained by evaluating $(B_i(j) \otimes B_i(h))(a_P)$. This is routine, but we display the expressions. We denote an equivalence class in $\Lambda = [q]^4/S_q$ by its lexicographically smallest element, representing vectors in $[q]^4$ as words, i.e., a vector in $[q]^4$ is represented as a string of symbols in $[q]$ of length 4.

$$\begin{aligned}
(F_1)_{1,1} &= qa^*_{0000} + q(q-1)a^*_{0011},\\
(F_1)_{1,2} &= q(q-1)(a^*_{0001} + a^*_{0010} + (q-2)a^*_{0012}),\\
(F_1)_{2,1} &= q(q-1)(a^*_{0111} + a^*_{0100} + (q-2)a^*_{0122}),\\
(F_1)_{2,2} &= q(q-1)(a^*_{0101} + a^*_{0110} + (q-2)(a^*_{0102} + a^*_{0120} + a^*_{0112} + a^*_{0121} + (q-3)a^*_{0123})).
\end{aligned}$$

$$\begin{aligned}
(F_2)_{1,1} &= 2a^*_{0000} - 2a^*_{0011},\\
(F_2)_{1,2} &= 2q(a^*_{0001} - a^*_{0010}),\\
(F_2)_{1,3} &= 2(q-2)(a^*_{0010} + a^*_{0001} - 2a^*_{0012}),\\
(F_2)_{2,1} &= 2q(a^*_{0100} - a^*_{0111}),\\
(F_2)_{2,2} &= 2q(2a^*_{0101} - 2a^*_{0110} + (q-2)(a^*_{0102} - a^*_{0120} - a^*_{0112} + a^*_{0121})),\\
(F_2)_{2,3} &= 2q(q-2)(a^*_{0102} + a^*_{0120} - a^*_{0112} - a^*_{0121}),\\
(F_2)_{3,1} &= 2(q-2)(a^*_{0111} + a^*_{0100} - 2a^*_{0122}),\\
(F_2)_{3,2} &= 2q(q-2)(a^*_{0102} - a^*_{0120} + a^*_{0112} - a^*_{0120}),\\
(F_2)_{3,3} &= 2(q-2)(2a^*_{0101} + 2a^*_{0110} + (q-4)(a^*_{0102} + a^*_{0120} + a^*_{0112} + a^*_{0121}) - 4(q-3)a^*_{0123}).
\end{aligned}$$

$$(F_3)_{1,1} = 6(a^*_{0101} - a^*_{0110} - a^*_{0102} + a^*_{0120} + a^*_{0112} - a^*_{0121}).$$

$$(F_4)_{1,1} = 8(a^*_{0101} + a^*_{0110} - a^*_{0102} - a^*_{0120} - a^*_{0112} - a^*_{0121}) + 16a^*_{0123}.$$

4.4.2 Appendix 2: An overview of the program

In this section we give a high-level overview of the program, to help the reader with implementing the method. See Figure 4.2 for an outline of the method. We write $\omega_t \in \Omega_4$ for the (unique) $S_q^n \rtimes S_n$-orbit of a pair of code words of distance t, and $\omega_\emptyset$ for the orbit $\{\emptyset\}$. Also, we write $\Omega_4^d \subseteq \Omega_4$ for the set of $S_q^n \rtimes S_n$-orbits on $\mathcal{C}_4^d$, where $\mathcal{C}_4^d$ denotes the collection of elements of $\mathcal{C}_4$ of minimum distance at least d.

```
Input:  Natural numbers $q, n, d$
Output: Semidefinite program to compute $B_q(n, d)$

print Maximize $q^n z(\omega_0)$
print Subject to:
foreach $\boldsymbol{n} = (n_1, \ldots, n_k) \in \boldsymbol{N}$
    foreach $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_k) \vdash \boldsymbol{n}$ with height$(\lambda_i) \leq m_i \quad \forall\, i = 1, \ldots, k$
        start a new block $M_{\boldsymbol{\lambda}}$
        foreach $\boldsymbol{\tau} \in \boldsymbol{T}''_{\boldsymbol{\lambda},\boldsymbol{m}}$ from Section 4.2.4
            foreach $\boldsymbol{\sigma} \in \boldsymbol{T}''_{\boldsymbol{\lambda},\boldsymbol{m}}$ from Section 4.2.4
                compute $\prod_{i=1}^{k} p_{\tau_i,\sigma_i}(F_i)$ (cf. the definitions in (3.14) and (3.13))
                replace each degree $n$ monomial $\mu(\omega')$ in variables $a_P^*$
                    by a variable $z(r(\omega'))$ if $r(\omega') \in \Omega_4^d$ and by 0 otherwise
                $(M_{\boldsymbol{\lambda}})_{\boldsymbol{\tau},\boldsymbol{\sigma}}$ := the resulting linear expression in $z(\omega)$
            end
        end
        if $\boldsymbol{n} = (n, 0, 0, 0)$ and $\boldsymbol{\lambda} = ((n), (), (), ())$  //Add $\emptyset$.
            add a row and column to $M_{\boldsymbol{\lambda}}$ indexed by $\emptyset$
            put $(M_{\boldsymbol{\lambda}})_{\emptyset,\emptyset} := 1$ and the entries $(M_{\boldsymbol{\lambda}})_{\emptyset,\boldsymbol{\tau}}$ and $(M_{\boldsymbol{\lambda}})_{\boldsymbol{\tau},\emptyset}$ as in (4.9)
        end
        print $M_{\boldsymbol{\lambda}} \succeq 0$
    end
end
foreach $\omega \in \Omega_4^d$ //Now nonnegativity of all variables.
    print $z(\omega) \geq 0$
end
```

Figure 4.2: Algorithm to generate semidefinite programs for computing $B_q(n, d)$.

Chapter 5

Nonbinary code bounds based on divisibility arguments

We all believe that mathematics is an art.
— Emil Artin (1898–1962)

For $q, n, d \in \mathbb{N}$, let again $A_q(n, d)$ denote the maximum size of a code $C \subseteq [q]^n$ with minimum distance at least d. We give a divisibility argument resulting in the new upper bounds $A_5(8, 6) \leq 65$, $A_4(11, 8) \leq 60$ and $A_3(16, 11) \leq 29$. These in turn imply the new upper bounds $A_5(9, 6) \leq 325$, $A_5(10, 6) \leq 1625$, $A_5(11, 6) \leq 8125$ and $A_4(12, 8) \leq 240$.

Furthermore, we prove that for $\mu, q \in \mathbb{N}$, there is a 1-1-correspondence between so-called symmetric (μ, q)-nets (which are certain designs) and codes $C \subseteq [q]^{\mu q}$ of size μq^2 with minimum distance at least $\mu q - \mu$. From this, we derive the new upper bounds $A_4(9, 6) \leq 120$ and $A_4(10, 6) \leq 480$.

This chapter is based on [69].

5.1 Introduction

Recall that for $q, n, d \in \mathbb{N}$, an *$(n, d)_q$-code* is a set $C \subseteq [q]^n$ that satisfies $d_{\min}(C) \geq d$. As before, define

$$A_q(n, d) := \max\{|C| \mid C \text{ is an } (n, d)_q\text{-code}\}. \tag{5.1}$$

In this chapter we find new upper bounds on $A_q(n, d)$ (for some q, n, d), based on a *divisibility*-argument. In some cases, it will sharpen a combination of the following two well-known upper bounds on $A_q(n, d)$. Fix $q, n, d \in \mathbb{N}$. Then

$$qd > (q-1)n \implies A_q(n, d) \leq \frac{qd}{qd - (q-1)n}. \tag{5.2}$$

This is the q-ary *Plotkin bound*. Moreover,

$$A_q(n, d) \leq q \cdot A_q(n-1, d). \tag{5.3}$$

A proof of these statements can be found in [55]. The Plotkin bound can be proved by comparing the leftmost and rightmost terms in (5.4) below. The second bound follows from the observation that in a $(n,d)_q$-code any symbol can occur at most $A_q(n-1,d)$ times at the first position.

We view an $(n,d)_q$-code C of size M as an $M \times n$ matrix with the words as rows. Two codes $C, D \subseteq [q]^n$ are *equivalent* (or *isomorphic*) if D can be obtained from C by first permuting the n columns of C and subsequently applying to each column a permutation of the q symbols in $[q]$ (we will write '*renumbering a column*' instead of 'applying a permutation to the symbols in a column').

q	n	d	best lower bound known [15, 16, 54, 92]	**new upper bound**	best upper bound previously known [15, 16, 38, 92]	Delsarte bound
5	8	6	50	**65**	75	75
5	9	6	135	**325**	375	375
5	10	6	625	**1625**	1855	1875
5	11	6	3125	**8125**	8840	9375
4	9	6	64	**120**	128	128
4	10	6	256	**480**	496	512
4	11	8	48	**60**	64	64
4	12	8	128	**240**	242	242
3	16	11	18	**29**	30	33

Table 5.1: An overview of the new upper bounds on $A_q(n,d)$. The previous lower and upper bounds are taken from references [15, 16, 92], except for the upper bounds $A_5(10,6) \leq 1855$, $A_5(11,6) \leq 8840$ and $A_4(10,6) \leq 496$ (cf. [38]), and the lower bounds $A_5(8,6) \geq 50$ and $A_4(11,8) \geq 48$.[1] These lower bounds follow from the exact values $A_5(10,8) = 50$ and $A_4(12,9) = 48$ ([54]). For updated tables with all most recent code bounds, we refer to [23].

If an $(n,d)_q$-code C is given, then for $j = 1, \dots, n$, let $c_{\alpha,j}$ denote the number of times symbol $\alpha \in [q]$ appears in column j of C. For any two words $u, v \in [q]^n$, we define $g(u,v) := n - d_H(u,v)$. So $g(u,v)$ is the number of i with $u_i = v_i$. In our divisibility arguments, we will use the following observations (which are well known and often used in coding theory and combinatorics).

Proposition 5.1.1. *If C is an $(n,d)_q$-code of size M, then*

$$\binom{M}{2}(n-d) \geq \sum_{\substack{\{u,v\} \subseteq C \\ u \neq v}} g(u,v) = \sum_{j=1}^{n} \sum_{\alpha \in [q]} \binom{c_{\alpha,j}}{2} \geq n \cdot \left((q-r)\binom{m}{2} + r\binom{m-1}{2} \right), \tag{5.4}$$

where $m := \lceil M/q \rceil$ and $r := qm - M$, so that $M = qm - r$ and $0 \leq r < q$. Moreover, writing L and R for the leftmost term and the rightmost term in (5.4), respectively, we have

$$|\{\{u,v\} \subseteq C \mid u \neq v,\ d_H(u,v) \neq d\}| \leq L - R, \tag{5.5}$$

[1] In [15, 16], the lower bounds $A_5(8,6) \geq 45$ and $A_4(11,8) \geq 34$ are given.

i.e., the number of pairs of distinct words $\{u,v\} \subseteq C$ with distance unequal *to d is at most the leftmost term minus the rightmost term in (5.4).*

Proof. The first inequality in (5.4) holds because $n-d \geq g(u,v)$ for all $u,v \in C$. The equality is obtained by counting the number of equal pairs of entries in the same columns of C in two ways. The second inequality follows from the (strict) convexity of the binomial coefficient $F(x) := x(x-1)/2$. Fixing a column j, the quantity $\sum_{\alpha \in [q]} F(c_{\alpha,j})$, under the condition that $\sum_{\alpha\in[q]} c_{\alpha,j} = M$, is minimal if the $c_{\alpha,j}$ are as equally divided as possible, i.e., if $c_{\alpha,j} \in \{\lceil M/q \rceil, \lfloor M/q \rfloor\}$ for all $\alpha \in [q]$. The desired inequality follows.

To prove the second assertion, note that (5.4) implies that $\sum_{\{u,v\}\subseteq C,\, u\neq v} g(u,v) \geq R$, so

$$\begin{aligned} |\{\{u,v\} \subseteq C \mid u \neq v,\ d_H(u,v) \neq d\}| &\leq \sum_{\substack{\{u,v\}\subseteq C \\ u\neq v}} (n-d-g(u,v)) \qquad (5.6) \\ &\leq \binom{M}{2}(n-d) - R = L - R. \qquad \square \end{aligned}$$

A code $C \subseteq [q]^n$ is *equidistant with distance d* if the distance between any two distinct codewords in C is equal to d. A code is *equidistant* if there exists a $d \in \mathbb{N}$ such that C is equidistant with distance d. Define, for $q,n,d,M \in \mathbb{N}$,

$$h(q,n,d,M) := L - R, \qquad (5.7)$$

where L and R denote the leftmost and rightmost terms in (5.4), respectively. So if C is an $(n,d)_q$-code of size M, then (5.5) states that

$$|\{\{u,v\} \subseteq C \mid u \neq v,\ d_H(u,v) \neq d\}| \leq h(q,n,d,M). \qquad (5.8)$$

Corollary 5.1.2. *If $h(q,n,d,M) = 0$ for some q,n,d and M (so the leftmost term equals the rightmost term in (5.4)), then for any $(n,d)_q$-code C of size M,*

(i) $d_H(u,v) = d$ for all $u,v \in C$ with $u \neq v$, i.e., C is equidistant with distance d, and

(ii) for each column C_j of C, there are $q-r$ symbols in $[q]$ that occur m times in C_j and r symbols in $[q]$ that occur $m-1$ times in C_j.

In the next sections we will use (i), (ii) and the bound in (5.8) to give (for some q,n,d) new upper bounds on $A_q(n,d)$, based on divisibility arguments. Furthermore, in Section 5.5, we will prove that, for $\mu, q \in \mathbb{N}$, there is a 1-1-correspondence between symmetric (μ,q)-nets (which are certain designs) and $(n,d)_q = (\mu q, \mu q - \mu)_q$-codes C with $|C| = \mu q^2$. We derive some new upper bounds from these 'symmetric net' codes.

5.2 The divisibility argument

In this section, we describe the divisibility argument and illustrate it by an example. Next, we show how the divisibility argument can be applied to obtain upper bounds on $A_q(n,d)$ for certain q,n,d. In subsequent sections, we will see how we can improve upon these bounds for certain fixed q,n,d. We will use the following notation.

Definition 5.2.1 (k-block)**.** Let C be an $(n,d)_q$-code in which a symbol $\alpha \in [q]$ is contained exactly k times in column j. The $k \times n$ matrix B formed by the k rows of C that have symbol α in column j is called a (k-)*block* (for column j). In that case, columns $\{1,\dots,n\} \setminus \{j\}$ of B form an $(n-1,d)_q$-code of size k.

At the heart of the divisibility arguments that will be used throughout this chapter lies the following observation.

Proposition 5.2.2 (Divisibility argument)**.** *Suppose that C is an $(n,d)_q$-code and that B is a block in C (for some column j) containing every symbol exactly m times in every column except for column j. If $n-d$ does not divide $m(n-1)$, then for each $u \in C \setminus B$ there is a word $v \in B$ with $d_H(u,v) \notin \{d,n\}$.*

Proof. Let $u \in C \setminus B$. We renumber the symbols in each column such that u is $\mathbf{0} := 0\dots0$, the all-zeros word. The total number of 0's in B is $m(n-1)$ (as the block B does not contain 0's in column j since $u \notin B$ and since B consists of all words in C that have the same symbol in column j). Since $n-d$ does not divide $m(n-1)$, there must be a word $v \in B$ that contains a number of 0's not divisible by $n-d$. In particular, the number of 0's in v is different from 0 and $n-d$. So $d_H(u,v) \notin \{d,n\}$. □

Example 5.2.3. We apply Proposition 5.2.2 to the case $(n,d)_q = (8,6)_5$. The best known upper bound[2] is $A_5(8,6) \leq 75$, which can be derived from (5.2) and (5.3), as the Plotkin bound yields $A_5(7,6) \leq 15$ and hence $A_5(8,6) \leq 5 \cdot 15 = 75$. Since $h(5,7,6,15) = 0$ (where h is defined in (5.7)), any $(7,6)_5$-code D of size 15 is equidistant with distance 6 and each symbol appears exactly $m = 3$ times in every column of D.

Suppose there exists a $(8,6)_5$-code C of size 75. As $A_5(7,6) \leq 15$, each column of C yields a division of C into five 15-blocks. Let B be a 15-block for the jth column and let $u \in C \setminus B$. By the above, the other columns of B contain each symbol 3 times, and $3(n-1) = 3 \cdot 7 = 21$ is not divisible by $n-d = 2$. So by Proposition 5.2.2, there must be a word $v \in B$ with $d_H(u,v) \notin \{6,8\}$.

However, since all $(7,6)_5$-codes of size 15 are equidistant with distance 6, all distances in C belong to $\{6,8\}$: either two words are contained together in some 15-block (hence their distance is 6) or there is no column for which the two words are contained in a 15-block (hence their distance is 8). This implies that an $(8,6)_5$-code C of size 75 cannot exist. Hence $A_5(8,6) \leq 74$. Theorem 5.2.5 and Corollary 5.2.6 below will imply that $A_5(8,6) \leq 70$ and in Section 5.3 we will show that, with some computer assistance, the bound can be pushed down to $A_5(8,6) \leq 65$.

To exploit the idea of Proposition 5.2.2, we will count the number of so-called irregular pairs of words occurring in a code.

Definition 5.2.4 (Irregular pair)**.** Let C be an $(n,d)_q$-code and $u,v \in C$ with $u \neq v$. If $d_H(u,v) \notin \{d,n\}$, we call $\{u,v\}$ an *irregular pair*.

For any code $C \subseteq [q]^n$, we write

$$X := \text{ the set of irregular pairs } \{u,v\} \text{ for } u,v \in C. \tag{5.9}$$

[2] The Delsarte bound [31] on $A_5(8,6)$, the bound based on (5.2), and the semidefinite programming bound $B_5(8,6)$ based on quadruples of codewords from (4.2) all are equal to 75.

Using Proposition 5.2.2, we can for some cases derive a lower bound on $|X|$. If we can also compute an upper bound on $|X|$ that is smaller than the lower bound, we derive that the code C cannot exist. The proof of the next theorem uses this idea.

Theorem 5.2.5. *Suppose that q, n, d, m are positive integers with $q \geq 2$, such that $d = m(qd-(q-1)(n-1))$, and such that $n-d$ does not divide $m(n-1)$. If $r \in \{1, \dots, q-1\}$ satisfies*

$$n(n-1-d)(r-1)r < (q-r+1)(qm(q+r-2)-2r), \tag{5.10}$$

then $A_q(n,d) < q^2m - r$.

Proof. By the Plotkin bound (5.2) we have

$$A_q(n-1,d) \leq qm. \tag{5.11}$$

Let D be an $(n-1,d)_q$-code of size $qm-t$ with $0 \leq t < q$. Note that $d = (q-1)m(n-1)/(qm-1)$, so

$$n-1-d = \frac{(qm-1)n-(qm-1)-(q-1)m(n-1)}{qm-1} = \frac{(m-1)(n-1)}{qm-1}.$$

Then we have (where h is defined cf. (5.7))

$$\begin{aligned} h(q,n-1,d,qm-t) &= \binom{qm-t}{2}(n-1-d) - (n-1)\left((q-t)\binom{m}{2} + t\binom{m-1}{2}\right) \\ &= \binom{qm-t}{2}(n-1-d) \\ &\quad - \tfrac{1}{2}(n-1-d)(qm-1)\left((q-t)m + t(m-2)\right) \\ &= \tfrac{1}{2}(n-1-d)((qm-t)(qm-t-1)-(qm-1)(qm-2t)) \\ &= (n-1-d)\binom{t}{2}. \end{aligned}$$

Hence

$$D \text{ contains at most } (n-1-d)\binom{t}{2} \text{ pairs of words with distance } \neq d. \tag{5.12}$$

Therefore, all $(n-1,d)_q$-codes D of size qm are equidistant with distance d (then $t=0$) and each symbol occurs m times in every column of D.

Now let C be an $(n,d)_q$-code of size $M := q^2m - r$ with $r \in \{1, \dots, q-1\}$ and suppose that (5.10) holds. Consider a qm-block B for some column of C. As $n-d$ does not divide $m(n-1)$, by Proposition 5.2.2 we know

$$\text{if } u \in C \setminus B, \text{ then there exists } v \in B \text{ with } d_H(u,v) \notin \{d,n\}. \tag{5.13}$$

Let $B_1, \dots, B_s$ be qm-blocks in C for some fixed column. Since $|C| = q^2m - r$, the number of qm-blocks for any fixed column is at least $q-r$ (so we can take $s = q-r$). Then, with (5.13), one obtains a lower bound on the number $|X|$ of irregular pairs in C. Every pair $\{B_i, B_k\}$ of qm-blocks gives rise to qm irregular pairs: for each word $u \in B_i$, there is a word $v \in B_k$ such that $\{u,v\} \in X$. This implies that in $\cup_{i=1}^{s} B_i \subseteq C$ there are at least $\binom{s}{2}qm$ irregular pairs. Moreover, for each word u in $C \setminus \cup_{i=1}^{s} B_i$ (there are $M - qm \cdot s$ of such words) there is, for each $i = 1, \dots, s$, a word $v_i \in B_i$ with $\{u, v_i\} \in X$. This gives an additional number of at least $(M - qms)s$ irregular pairs in C. Hence:

$$\begin{aligned} |X| &\geq \binom{s}{2}qm + (M - qms)s \\ &= \tfrac{1}{2}s(qm(2q - s - 1) - 2r) =: \psi(s). \end{aligned} \tag{5.14}$$

On the other hand, note that the ith block for the jth column has size $qm - r_{i,j}$ for some integer $r_{i,j} \geq 0$ by (5.11), where $\sum_{i=1}^{q} r_{i,j} = r \leq q - 1$ (hence each $r_{i,j} < q$). So by (5.12), the number of irregular pairs in C that have the same entry in column j is at most

$$(n - 1 - d)\sum_{i=1}^{q}\binom{r_{i,j}}{2}. \tag{5.15}$$

As each irregular pair $\{u, v\}$ has $u_j = v_j$ for at least one column j, we conclude

$$|X| \leq (n - 1 - d)\sum_{j=1}^{n}\sum_{i=1}^{q}\binom{r_{i,j}}{2} \leq n(n - 1 - d)\binom{r}{2}. \tag{5.16}$$

Here the last inequality follows by convexity of the binomial function, since (for fixed j) the sum $\sum_{i=1}^{q}\binom{r_{i,j}}{2}$ under the condition that $\sum_{i=1}^{q} r_{i,j} = r$ is maximal if one of the $r_{i,j}$ is equal to r and the others are equal to 0.

Suppose each $r_{i,j} \in \{0, 1\}$, then $|X| = 0$ by (5.16). However, as $q - r \geq 1$, there is at least one qm-block for any fixed column, so $|X| \geq 1$ by (5.13), which is not possible. Hence we can assume that $r_{i,j} \geq 2$ for some i, j (this also implies $A_q(n,d) \leq q^2m - 2$). Then the number s of qm-blocks for column j satisfies $s \geq q - r + 1$. This gives by (5.14) and (5.16) that

$$\psi(q - r + 1) \leq |X| \leq n(n - 1 - d)\binom{r}{2}, \tag{5.17}$$

where the function ψ is defined in (5.14). Multiplying (5.17) by 2 yields

$$n(n - 1 - d)(r - 1)r \geq (q - r + 1)(qm(q + r - 2) - 2r),$$

contradicting (5.10).

So if (5.10) holds, then $A_q(n,d) < q^2m - r$, as was needed to prove. □

We give two interesting applications of Theorem 5.2.5.

Corollary 5.2.6. *If* $q \equiv 1 \pmod 4$ *and* $q \neq 1$, *then*

$$A_q(q + 3, q + 1) \leq \tfrac{1}{2}q^2(q + 1) - q = \tfrac{1}{2}(q - 1)q(q + 2). \tag{5.18}$$

Proof. Apply Theorem 5.2.5 to $n = q+3$, $d = q+1$, $m = d/(qd-(q-1)(n-1)) = (q+1)/2 \in \mathbb{N}$ and $r = q - 1$. Then $n - d = 2$ does not divide $m(n - 1) = (q + 1)(q + 2)/2$, as $q \equiv 1 \pmod 4$. Furthermore, the left hand side minus the right hand side in (5.10) is equal to $-(q^3 - q^2 - 2) < 0$, so (5.10) is satisfied. Hence $A_q(q+3, q+1) < q^2(q+1)/2 - (q-1)$. □

Applying Corollary 5.2.6 to $q = 5$ gives $A_5(8,6) \leq 70$. In Section 5.3 we will improve this to $A_5(8,6) \leq 65$.

Remark 5.2.7. Note that for bound (5.18) to hold it is necessary that $q \equiv 1 \pmod 4$. If $q \equiv 3 \pmod 4$ the statement does *not* hold in general. For example, $A_3(6,4) = 18$ (see [23]), which is larger than bound (5.18).

Theorem 5.2.5 also gives an upper bound on $A_q(n,d) = A_q(kq+k+1, kq)$, where $q \geq 2$ and $k+1$ does not divide $q(q+1)$ (which is useful for $k < q-1$; for $k \geq q+1$ the Plotkin bound gives a better bound). One new upper bound for such q, n, d is obtained:

Proposition 5.2.8. *$A_4(11,8) \leq 60$.*

Proof. This follows from Theorem 5.2.5 with $q = 4$, $n = 11$, $d = 8$, $m = d/(qd-(q-1)(n-1)) = 4 \in \mathbb{N}$ and $r = 3$. Then $n - d = 3$ does not divide $m(n-1) = 40$. Furthermore, the left hand side minus the right hand side in (5.10) is equal to $-16 < 0$, so (5.10) is satisfied. Therefore $A_4(11,8) < 61$. □

This implies the following bound, which is also new:

Corollary 5.2.9. *$A_4(12,8) \leq 240$.*

Proof. By Proposition 5.2.8 and (5.3). □

5.3 Kirkman triple systems and $A_5(8,6)$

In this section we consider the case $(n,d)_q = (8,6)_5$ from Example 5.2.3. Corollary 5.2.6 implies that $A_5(8,6) \leq 70$. Using small computer checks, we will obtain $A_5(8,6) \leq 65$.

As in the proof of Theorem 5.2.5, we will compare upper and lower bounds on $|X|$. But since an $(8,6)_5$-code C of size at most 70 does not necessarily contain a 15-block (as $70 = 5 \cdot 14$), we need information about 14-blocks. To this end we show, using an analogous approach as in [17] (based on occurrences of symbols in columns of an equidistant code):

Proposition 5.3.1. *Any $(7,6)_5$-code C of size 14 can be extended to a $(7,6)_5$-code of size 15.*

Proof. Let C be a $(7,6)_5$-code of size 14. Since $h(5,7,6,14) = 0$ (where h is defined cf. (5.7)), Corollary 5.1.2 yields that C is equidistant with distance 6 and that for each $j \in \{1,\ldots,7\}$ there exists a unique $\beta_j \in [q]$ with $c_{\beta_j,j} = 2$ and $c_{\alpha,j} = 3$ for all $\alpha \in [q] \setminus \{\beta_j\}$. Define a 15-th codeword u by putting $u_j := \beta_j$ for all $j = 1,\ldots,7$. We claim that $C \cup \{u\}$ is a $(7,6)_5$-code of size 15.

To establish the claim we must prove that $d_H(u,w) \geq 6$ for all $w \in C$. Suppose that there is a word $w \in C$ with $d_H(u,w) < 6$. We can renumber the symbols in each column of C such that $w = \mathbf{0}$. Since C is equidistant with distance 6, each word in $C \setminus \{w\}$ contains precisely one 0. On the other hand, there are two column indices j_1 and j_2 with $u_{j_1} = 0$ and $u_{j_2} = 0$. Then $C \setminus \{w\}$ contains at most $1 + 1 + 5 \cdot 2 = 12$ occurrences of the symbol 0 (since in columns j_1 and j_2 there is precisely one 0 in $C \setminus \{w\}$). But in that case, since $|C \setminus \{w\}| = 13 > 12$, there is a row in C that contains zero occurrences of the symbol 0, contradicting the fact that C is equidistant with distance 6. □

Note that a code of size more than 65 must have at least one 15- or 14-block, and therefore it must have a subcode of size 65 containing at least one 14-block. We shall now prove that this is impossible because

$$\text{each } (8,6)_5\text{-code of size 65 only admits 13-blocks.} \tag{5.19}$$

It follows that $A_5(8,6) \leq 65$. In order to prove (5.19), let C be a $(8,6)_5$-code of size 65. We first compute a lower bound on the number of irregular pairs in C. Define, for $x, y \in \mathbb{Z}_{\geq 0}$,

$$\begin{aligned} f(x,y) := (3x+y)(65-15x-14y) + 3\cdot 15\binom{x}{2} + 14\binom{y}{2} + 3\cdot 14xy \\ - 2\cdot 21x - 8y + \mathbf{1}_{\{y>0 \text{ and } x=0\}}(65-14-39). \end{aligned} \tag{5.20}$$

Proposition 5.3.2 (Lower bound on $|X|$)**.** *Let C be an $(n,d)_q = (8,6)_5$-code of size 65 and let $j \in \{1,\dots,n\}$. Let x and y be the number of symbols that appear 15 and 14 times (respectively) in column j. Then the number $|X|$ of irregular pairs in C is at least $f(x,y)$.*

Proof. First consider a $(7,6)_5$-code D of size 15 or size 14 and define

$$S := \{u \in [5]^7 \mid d_H(u,w) \geq 5 \ \ \forall\, w \in D\}. \tag{5.21}$$

For any $u \in S$, define

$$\alpha(u) := |\{w \in D \mid d_H(u,w) = 6\}|. \tag{5.22}$$

Then

$$\begin{array}{ll} \text{if } |D| = 15, \text{ then} & \text{if } |D| = 14, \text{ then} \\ \quad |\{u \in S \mid \alpha(u) = 0\}| = 0, & \quad |\{u \in S \mid \alpha(u) = 0\}| \leq 8, \\ \quad |\{u \in S \mid \alpha(u) = 1\}| \leq 21, & \quad |\{u \in S \mid \alpha(u) \leq 1\}| \leq 39. \\ \quad |\{u \in S \mid \alpha(u) = 2\}| = 0, & \end{array} \tag{5.23}$$

This can be checked efficiently with a computer[3] by checking all possible $(7,6)_5$-codes of size 15 and 14 up to equivalence. Here we note that a $(7,6)_5$-code D of size 15 (which is equidistant with distance 6, see Example 5.2.3) corresponds to a solution to *Kirkman's school girl problem* [83].[4] So to establish (5.23), it suffices to check[5] all $(7,6)_5$-codes of size 15, that is, Kirkman systems (there are 7 nonisomorphic Kirkman systems [29]), and all $(7,6)_5$-codes of size 14, of which there are at most $7 \cdot 15$ by Proposition 5.3.1.

Recall that C is an $(8,6)_5$-code of size 65. Let $G = (C,X)$ be the graph with vertex set $V(G) := C$ and edge set $E(G) := X$. Consider a 15-block B determined by column j. By (5.23), each $u \in C \setminus B$ has ≥ 1 neighbor in B.

[3] All computer tests in this chapter are small and can be executed within a minute on modern personal computers.

[4] Kirkman's school girl problem asks to arrange 15 girls 7 days in a row in groups of 3 such that no two girls appear in the same group twice. The 1-1-correspondence between $(7,6)_5$-codes D of size 15 and solutions to Kirkman's school girl problem is given by the rule: girls i_1 and i_2 walk in the same triple on day $j \iff D_{i_1,j} = D_{i_2,j}$.

[5] By 'check' we mean that given a $(7,6)_5$-code D of size 14 or 15, we first compute S, then $\alpha(u)$ for all $u \in S$, and subsequently verify (5.23).

Furthermore, (5.23) gives that all but ≤ 21 elements $u \in C \setminus B$ have ≥ 3 neighbors in B. So by adding $\leq 2 \cdot 21$ new edges, we obtain that each $u \in C \setminus B$ has ≥ 3 neighbors in B.

Similarly, for any 14-block B determined by column j, by adding ≤ 8 new edges we achieve that each $u \in C \setminus B$ has ≥ 1 neighbor in B. Hence, by adding $\leq (2 \cdot 21 \cdot x + 8 \cdot y)$ edges to G, we obtain a graph G' with

$$|E(G')| \geq (3x+y)(65-15x-14y) + 3 \cdot 15\binom{x}{2} + 14\binom{y}{2} + 3 \cdot 14xy. \tag{5.24}$$

This results in the required bound, except for the term with the indicator function. That term can be added because $|\{u \in S \mid \alpha(u) \leq 1\}| \leq 39$ if $|D| = 14$, by (5.23). □

Theorem 5.3.3 ($A_5(8,6) \leq 65$)**.** *Suppose that C is an $(n,d)_q = (8,6)_5$-code with $|C| = 65$. Then each symbol appears exactly* 13 *times in each column of C. Hence, $A_5(8,6) \leq 65$.*

Proof. If D is any $(7,6)_5$-code of size k, then $h(5,7,6,k)$ (where h is defined cf. (5.7)) is an upper bound on the number of pairs $\{u,v\} \subseteq D$ with $u \neq v$ and $d_H(u,v) \neq 6$ (hence $d_H(u,v) = 7$), cf. (5.8). The values $h(5,7,6,k)$ are given in Table 5.2.

k	15	14	13	12	11	10	9	8	7	6	5
$h(5,7,6,k)$	0	0	1	3	6	10	8	7	7	8	10

Table 5.2: Upper bound $h(5,7,6,k)$ on the number of pairs $\{u,v\} \subseteq D$ with $d_H(u,v) = 7$ for a $(7,6)_5$-code D with $|D| = k$.

Recall that C is an $(n,d)_q = (8,6)_5$-code with $|C| = 65$. We now give an upper bound on $|X|$. Let $a_k^{(j)}$ be the number of symbols that appear exactly k times in column j of C. Then the number of irregular pairs that have the same entry in column j is at most $\sum_{k=5}^{15} a_k^{(j)} h(5,7,6,k)$. It follows that

$$|X| \leq U := \sum_{j=1}^{8} \sum_{k=5}^{15} a_k^{(j)} h(5,7,6,k). \tag{5.25}$$

One may check that if $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_{\geq 0}^{15}$ are 15-tuples of nonnegative integers, with $\sum_k a_k k = 65$, $\sum_k b_k k = 65$, $\sum_k a_k = 5$, $\sum_k b_k = 5$, and $f(a_{15}, a_{14}) \leq f(b_{15}, b_{14}) \neq 0$, then

$$\sum_{k=5}^{15} (7a_k + b_k) h(5,7,6,k) < f(b_{15}, b_{14}). \tag{5.26}$$

(There are 30 $\mathbf{a} \in \mathbb{Z}_{\geq 0}^{15}$ with $\sum_k a_k k = 65$ and $\sum_k a_k = 5$. So there are 900 possible pairs $\mathbf{a}, \mathbf{b}$. A computer now quickly verifies (5.26).)

By permuting the columns of C we may assume that $\max_j f(a_{15}^{(j)}, a_{14}^{(j)}) = f(a_{15}^{(1)}, a_{14}^{(1)})$. Hence if $f(a_{15}^{(1)}, a_{14}^{(1)}) > 0$, then

$$U = \sum_{j=1}^{8} \sum_{k=5}^{15} a_k^{(j)} h(5,7,6,k) = \frac{1}{7} \sum_{j=2}^{8} \left(\sum_{k=5}^{15} \left(7a_k^{(j)} + a_k^{(1)}\right) h(5,7,6,k) \right) \tag{5.27}$$
$$< f(a_{15}^{(1)}, a_{14}^{(1)}) \leq |X|$$

(where we used Prop. 5.3.2 in the last inequality), contradicting (5.25). So $f(a_{15}^{(j)}, a_{14}^{(j)}) = 0$ for all j, which implies (for $\mathbf{a}^{(j)} \in \mathbb{Z}_{\geq 0}^{15}$ with $\sum_k a_k^{(j)} k = 65$, $\sum_k a_k^{(j)} = 5$) that $a_{15}^{(j)} = a_{14}^{(j)} = 0$ for all j, hence each symbol appears exactly 13 times in each column of C. □

Corollary 5.3.4. *$A_5(9,6) \leq 325$, $A_5(10,6) \leq 1625$ and $A_5(11,6) \leq 8125$.*

Proof. By Theorem 5.3.3 and (5.3). □

5.4 Improved bound on $A_3(16, 11)$

We show that $A_3(16, 11) \leq 29$ using a surprisingly simple argument.

Proposition 5.4.1. $A_3(16, 11) \leq 29$.

Proof. Suppose that C is an $(n,d)_q = (16,11)_3$-code of size 30. We can assume that $\mathbf{0} \in C$. It is known that $A_3(15,11) = 10$, so the symbol 0 is contained at most 10 times in every column of C. Since $|C| = 30$, the symbol 0 appears exactly 10 times in every column of C, so the number of 0's in C is divisible by 5. On the other hand, Corollary 5.1.2 yields that any $(15,11)_3$-code of size 10 is equidistant with distance 10, since $h(3,15,11,10) = 0$. This implies that all distances in a $(16,11)_3$-code of size 30 belong to $\{11,16\}$. So the number of 0's in any code word $\neq \mathbf{0}$ is 0 or 5. As $\mathbf{0}$ contains 16 0's, it follows that the total number of 0's is not divisible by 5, a contradiction. □

5.5 Codes from symmetric nets

In this section we will show that there is a 1-1-correspondence between *symmetric* (μ, q)-*nets* and $(n,d)_q = (\mu q, \mu q - \mu)_q$-codes of size μq^2. From this, we derive in Section 5.6 the new upper bound $A_4(9,6) \leq 120$, implying $A_4(10,6) \leq 480$.

Definition 5.5.1 (Symmetric net)**.** Let $\mu, q \in \mathbb{N}$. A *symmetric* (μ, q)*-net* (also called *symmetric transversal design* [13]) is a set X of μq^2 elements, called *points*, together with a collection $\mathcal{B}$ of subsets of X of size μq, called *blocks*, such that:

(s1) $\mathcal{B}$ can be partitioned into μq partitions (*block parallel classes*) of X.

(s2) Any two blocks that belong to different parallel classes intersect in exactly μ points.

(s3) X can be partitioned into μq sets of q points (*point parallel classes*), such that any two points from different classes occur together in exactly μ blocks, while any two points from the same class do not occur together in any block.[6]

Remark 5.5.2. From the 1-1-correspondence between symmetric (μ, q)-nets and $(n,d)_q = (\mu q, \mu q - \mu)_q$-codes C of size μq^2 in Theorem 5.5.6 below it follows that (s2) and (s3) can be replaced by the single condition:

(s') Each pair of points is contained in at most μ blocks,

since the only condition posed on such a code is that $g(u,v) \leq \mu$ for all distinct $u, v \in C$.

[6] That is, a symmetric (μ, q)-net is a $1 - (\mu q^2, \mu q, \mu q)$ design D, which is resolvable (s1), affine (s2), and the dual design D^* of D is affine resolvable (s3).

Example 5.5.3. Let $X = \{1, 2, 3, 4\}$ and $\mathcal{B} = \{\{1, 3\}, \{2, 4\}, \{1, 4\}, \{2, 3\}\}$. Then $(X, \mathcal{B})$ is a symmetric $(1, 2)$-net. The block parallel classes are $\{\{1, 3\}, \{2, 4\}\}$ and $\{\{1, 4\}, \{2, 3\}\}$. The point parallel classes are $\{1, 2\}$ and $\{3, 4\}$.

By labeling the points as $x_1, \dots, x_{\mu q^2}$ and the blocks as $B_1, \dots, B_{\mu q^2}$, the $\mu q^2 \times \mu q^2$-*incidence matrix* N of a symmetric (μ, q)-net is defined by

$$N_{i,j} := \begin{cases} 1 & \text{if } x_i \in B_j, \\ 0 & \text{otherwise.} \end{cases} \tag{5.28}$$

If $(X, \mathcal{B})$ and $(X', \mathcal{B}')$ are symmetric nets, an *isomorphism* of $(X, \mathcal{B})$ and $(X', \mathcal{B}')$ is a bijection $\phi : X \to X'$ with the property that $\{\{\phi(x) \,|\, x \in B\} \,|\, B \in \mathcal{B}\} = \mathcal{B}'$. That is, two symmetric nets are isomorphic if and only if their incidence matrices are the same up to row and column permutations. Symmetric nets are a generalization of *generalized Hadamard matrices.*

Definition 5.5.4 (Generalized Hadamard matrix)**.** Let M be an $n \times n$ matrix with entries from a finite group G. Then M is called a *generalized Hadamard matrix* $\mathrm{GH}(n, G)$ (or $\mathrm{GH}(n, |G|)$) if for any two different rows i and k, the n-tuple $(M_{ij} M_{kj}^{-1})_{j=1}^{n}$ contains each element of G exactly $n/|G|$ times.

$$\begin{pmatrix} e & e & e & e & e & e & e & e \\ e & e & a & a & b & b & c & c \\ e & b & e & b & c & a & c & a \\ e & c & c & e & a & b & b & a \\ e & a & b & c & e & a & b & c \\ e & c & b & a & c & e & a & b \\ e & b & a & c & a & c & e & b \\ e & a & c & b & b & c & a & e \end{pmatrix}$$

Figure 5.1: An incidence matrix of the unique (up to isomorphism) symmetric $(2, 4)$-net is obtained by writing the elements e, a, b, c as 4×4-permutation matrices in the generalized Hadamard matrix $\mathrm{GH}(8, V_4)$ (with V_4 the Klein 4-group). See Al-Kenani [2].

Each generalized Hadamard matrix $\mathrm{GH}(n, G)$ gives rise to a symmetric $(n/|G|, |G|)$-net: by replacing each element g of G by the $G \times G$ (permutation) matrix of the linear map $\mathbb{C}G \to \mathbb{C}G$ determined by $h \mapsto gh$ $(\forall h \in G)$, one obtains the incidence matrix of a symmetric net. Not every symmetric $(n/q, q)$-net gives rise to a generalized Hadamard matrix $\mathrm{GH}(n, q)$, see [57]. But if the group of automorphisms (*bitranslations*) of a symmetric $(n/q, q)$-net has order q, then one can construct a generalized Hadamard matrix $\mathrm{GH}(n, q)$ from it. See [13] for details.

Assumption 5.5.5. In this section we consider triples $(n, d)_q$ of natural numbers for which

$$qd = (q - 1)n, \tag{5.29}$$

hence $n - d = n/q =: \mu$ and $\mu \in \mathbb{N}$. So $(n, d)_q = (\mu q, \mu q - \mu)_q$.

The fact that a generalized Hadamard matrix $\mathrm{GH}(n,q)$ gives rise to an $(n,d)_q$-code of size qn, was proved in [54] and for some parameters it can also be deduced from [84]. Using a result by Bassalygo, Dodunekov, Zinoviev and Helleseth [9] about the structure of $(n,d)_q$-codes of size qn,[7] we prove that such codes are in 1-1-relation with symmetric $(n/q,q)$-nets.

Theorem 5.5.6. *Let $\mu, q \in \mathbb{N}$. There is a 1-1-relation between symmetric (μ,q)-nets (up to isomorphism) and $(n,d)_q = (\mu q, \mu q - \mu)_q$-codes C of size μq^2 (up to equivalence).*

Proof. Given an $(n,d)_q = (\mu q, \mu q-\mu)_q$-code C of size μq^2, we construct a $\{0,1\}$-matrix M of order $\mu q^2 \times \mu q^2$ with the following properties:

(I) M is a $\mu q^2 \times \mu q^2$ matrix that consists of $q \times q$ blocks $\sigma_{i,j}$ (so M is a $\mu q \times \mu q$ matrix of blocks $\sigma_{i,j}$), where each $\sigma_{i,j}$ is a permutation matrix.

(II) $MM^\mathsf{T} = M^\mathsf{T}M = A$, where A is the $\mu q^2 \times \mu q^2$ matrix that consists of $q \times q$ blocks $A_{i,j}$ (so A is an $\mu q \times \mu q$ matrix of blocks $A_{i,j}$), with

$$A_{i,j} = \begin{cases} \mu q \cdot I_q & \text{if } i = j, \\ \mu \cdot J_q & \text{if } i \neq j. \end{cases} \tag{5.30}$$

Here J_q denotes the $q \times q$ all-ones matrix.

By Proposition 4 of [9], since $d = n(q-1)/q$ and $|C| = qn$, C can be partitioned as

$$C = V_1 \cup V_2 \cup \ldots \cup V_n, \tag{5.31}$$

where the union is disjoint, $|V_i| = q$ for all $i = 1, \ldots, n$, and where $d_H(u,v) = n$ if $u, v \in C$ are together in one of the V_i, and $d_H(u,v) = d$ if $u \in V_i$ and $v \in V_j$ with $i \neq j$.

Now we write each word $w \in [q]^n$ as a $\{0,1\}$-row vector of size $qn = \mu q^2$ by putting a 1 on positions $(i, w_i) \in \{1,\ldots,n\} \times [q]$ (for $i = 1,\ldots,n$) and 0's elsewhere. The q words in any of the V_i then form a $q \times qn$ matrix consisting of n permutation matrices $\sigma_{i,j}$ of size $q \times q$.

By placing the matrices obtained in this way from all n tuples $V_1, \ldots, V_n$ underneath each other, we obtain a $qn \times qn$ matrix M consisting of n^2 permutation matrices of order $q \times q$, so (I) is satisfied. Property (II) also holds, since for any $u, v \in C$ written as row vectors of size qn, with the V_i as in (5.31), it holds that

$$\sum_{k \in \{1,\ldots,n\} \times [q]} u_k v_k = g(u,v) = \begin{cases} n = \mu q & \text{if } u = v, \\ 0 & \text{if } u \neq v \text{ and } u, v \in V_i, \\ n - d = \mu & \text{if } u \neq v \text{ and } u \in V_i, v \in V_j \text{ with } i \neq j. \end{cases} \tag{5.32}$$

So $MM^\mathsf{T} = A$. Moreover, for any $j_1 := (j_1', a_1) \in \{1,\ldots,n\} \times [q]$ and $j_2 := (j_2', a_2) \in \{1,\ldots,n\} \times [q]$,

$$\begin{aligned} \sum_{k \in \{1,\ldots,qn\}} M_{k,j_1} M_{k,j_2} &= |\{w \in C \mid w_{j_1'} = a_1,\ w_{j_2'} = a_2\}| \\ &= \begin{cases} n = \mu q & \text{if } j_1' = j_2' \text{ and } a_1 = a_2, \\ 0 & \text{if } j_1' = j_2' \text{ and } a_1 \neq a_2, \\ n/q = \mu & \text{if } j_1' \neq j_2', \end{cases} \end{aligned} \tag{5.33}$$

[7] Note that $A_q(n,d) \leq qn$, since by the Plotkin bound (5.2), $A_q(n-1,d) \leq n$, hence $A_q(n,d) \leq qn = \mu q^2$ by (5.3).

where the statement that $|\{w \in C \,|\, w_{j_1'} = a_1,\, w_{j_2'} = a_2\}| = n/q$ if $j_1' \neq j_2'$ follows by considering the words in C that have a_1 at the j_1'-th position. (The remaining columns form an n-block for the j_1'-th column. In this n-block, each symbol occurs exactly n/q times at each position, since $h(q, n-1, d, n) = 0$ (where h is defined in (5.7)).) We see that also $M^{\mathsf{T}} M = A$. Hence, M is the incidence matrix of a symmetric (μ, q)-net (see [13], Proposition I.7.6 for the net and its dual).

Note that one can do the reverse construction as well: given a symmetric (μ, q)-net, the incidence matrix of M can be written (after possible row and column permutations) as a matrix of permutation matrices such that $MM^{\mathsf{T}} = M^{\mathsf{T}} M = A$, with A as defined in (5.30). From M we obtain a code C of size μq^2 of the required minimum distance by mapping the rows $(i, w_i) \in \{1, \ldots, \mu q\} \times [q]$ to $w \in [q]^{\mu q}$. Observe that equivalent codes yield isomorphic incidence matrices M and vice versa. □

w_0	0	0	0
w_1	1	1	1
w_2	2	2	2
w_4	0	2	1
w_5	1	0	2
w_6	2	1	0
w_7	0	1	2
w_8	1	2	0
w_9	2	0	1

$\longleftrightarrow$

	0	1	2	0	1	2	0	1	2
w_1	1	0	0	1	0	0	1	0	0
w_2	0	1	0	0	1	0	0	1	0
w_3	0	0	1	0	0	1	0	0	1
w_4	1	0	0	0	0	1	0	1	0
w_5	0	1	0	1	0	0	0	0	1
w_6	0	0	1	0	1	0	1	0	0
w_7	1	0	0	0	1	0	0	0	1
w_8	0	1	0	0	0	1	1	0	0
w_9	0	0	1	1	0	0	0	1	0

Figure 5.2: An $(n,d)_q = (3,2)_3$-code $C = \{w_1, \ldots, w_9\}$ of size 9 (left table) gives rise to an incidence matrix of a symmetric $(1,3)$-net (right table) and vice versa.

5.6 New upper bound on $A_4(9,6)$

In this section we use the 1-1-correspondence between symmetric (μ, q)-nets and $(n,d)_q = (\mu q, \mu q - \mu)_q$-codes of size μq^2 in combination with a known result about symmetric $(2,4)$-nets [2] to derive that $A_4(9,6) \leq 120$.

As $A_4(8,6) = 32$, any $(9,6)_4$-code of size more than 120 must contain at least one 31- or 32-block, and therefore it contains a subcode of size 120 containing at least one 31-block. We will show (using a small computer check) that this is impossible because

$$\text{each } (9,6)_4\text{-code of size 120 only admits 30-blocks.} \tag{5.34}$$

Therefore $A_4(9,6) \leq 120$. To prove (5.34), we need information about $(8,6)_4$-codes of size 31.

Proposition 5.6.1. *Let $q, n, d \in \mathbb{N}$ satisfy $qd = (q-1)n$. Any $(n,d)_q$-code C of size $qn-1$ can be extended to an $(n,d)_q$-code of size qn.*

Proof. Let C be an $(n,d)_q$-code of size $qn - 1$. Recall that $c_{\alpha,j}$ denotes the number of times symbol $\alpha \in [q]$ appears in column $j \in \{1, \ldots, n\}$ of C. By the Plotkin bound, $A_q(n-1, d) \leq n$, so each symbol occurs at most n times in each column of C, hence there exists for each $j \in \{1, \dots, n\}$ a unique $\beta_j \in [q]$ with $c_{\beta_j,j} = n-1$, implying $c_{\alpha,j} = n$ for all $\alpha \in [q] \backslash \{\beta_j\}$. We can define a qn-th codeword u by putting $u_j := \beta_j$ for all $j = 1, \dots, n$. We claim that $C \cup \{u\}$ is an $(n,d)_q$-code of size qn.

To establish the claim we must prove that $d_H(u,w) \geq d$ for all $w \in C$. Let $w \in C$ with $d_H(u,w) < n$. We can renumber the symbols in each column of C such that $w = \mathbf{0}$. Then w is contained in an $(n-1)$-block B for some column in C (otherwise $d_H(u,w) = n$). The number of 0's in B is $n + (n-2)(n-d) = n + (n-2)n/q$ (since any $(n-1,d)_q$-code of size $n-1$ is equidistant with distance d by Corollary 5.1.2, as $h(q,n-1,d,n-1) = 0$).

Moreover, the number of 0's in $C \setminus B$ is $(q-1)(n-1)n/q$ (since in any $(n-1,d)_q$-code of size n, each symbol appears exactly n/q times in each column by Corollary 5.1.2, as $h(q,n-1,d,n) = 0$). Adding these two numbers we see that the total number of 0's in C is $n^2 - n/q$. Since $C \cup \{u\}$ contains each symbol n^2 times by construction, u contains symbol 0 exactly n/q times, hence $d_H(u,w) = n - n/q = d$, which gives the desired result. □

Proposition 5.6.2. *$A_4(9,6) \leq 120$.*

Proof. The $(n,d)_q = (8,6)_4$-code of size 32 is unique up to equivalence, since the symmetric $(2,4)$-net is unique up to equivalence (see Al-Kenani [2]). By checking all $(8,6)_4$-codes D of size 31 (of which there are at most 32 up to equivalence since each $(8,6)_4$-code of size 31 arises by removing one word from an $(8,6)_4$-code of size 32 by Proposition 5.6.1) we find that for each $(8,6)_4$-code D of size 31:

$$|\{u \in [4]^8 \mid d_H(u,w) \geq 5 \ \ \forall\, w \in D\}| \leq 25. \tag{5.35}$$

So any $(9,6)_4$ code with a 31- or 32-block contains at most $31 + 25 = 56$ words. Hence a $(9,6)_4$-code of size 120 cannot contain a 31- or 32-block. So (5.34) holds, hence $A_4(9,6) \leq 120$. □

Corollary 5.6.3. *$A_4(10,6) \leq 480$.*

Proof. By Proposition 5.6.2 and (5.3). □

Chapter 6

Semidefinite programming bounds for constant weight codes

Further study of this function is being pursued.
— Selmer Martin Johnson (1916–1996)

For nonnegative integers n, d, w, let $A(n, d, w)$ be the maximum size of a code $C \subseteq \mathbb{F}_2^n$ with constant weight w and minimum distance at least d. We consider two semidefinite programs based on quadruples of code words that yield several new upper bounds on $A(n, d, w)$. The new upper bounds imply the exact values $A(22, 8, 10) = 616$ and $A(22, 8, 11) = 672$. Lower bounds on $A(22, 8, 10)$ and $A(22, 8, 11)$ are obtained from the $(n, d)_2 = (22, 7)_2$ shortened binary Golay code of size 2048. It can be concluded that the shortened binary Golay code is a union of constant weight w codes of sizes $A(22, 8, w)$. This chapter is based on [70].

6.1 Introduction

In this chapter we consider two semidefinite programming upper bounds on $A(n, d, w)$. Both upper bounds sharpen the classical Delsarte linear programming bound [31], as well as Schrijver's semidefinite programming bound based on a block diagonalization of the Terwilliger algebra [81].

The chapter serves the following purposes. Firstly, the quadruple bound for unrestricted binary codes from [37], which is a slight sharpening of the bound $B_2(n, d)$ from (4.2), is adapted to a bound $A_k(n, d, w)$ for binary constant weight codes. Subsequently, a relaxation $B_k(n, d, w)$ is formulated, which might also be of interest for unrestricted binary codes. By studying $A_4(n, d, w)$ and $B_4(n, d, w)$, a sharpening of the Schrijver bound [81] for constant weight codes is obtained that is in most cases sharper than the bound from [47] (in which linear inequalities were added to the Schrijver bound). The constructed semidefinite programs are very large, but a symmetry reduction (using representation theory of the symmetric group) based on the method of Section 2.4 and Chapter 3 is given to reduce them to polynomial size. This finally leads to many new upper bounds on $A(n, d, w)$, including the exact values $A(22, 8, 10) = 616$ and $A(22, 8, 11) = 672$ — see Table 6.2.

The once shortened binary Golay code (see Section 2.2) which is an $(n, d) = (22, 7)$-code of size 2048, contains the numbers of words of a given weight w (and no words of other weights) which are given in Table 6.1.

weight w	0	7	8	11	12	15	16
# words	1	176	330	672	616	176	77

Table 6.1: Number of words of a given weight w contained in the once shortened binary Golay code.

While it was already known that $A(22,8,6) = 77$, $A(22,8,7) = 176$, and $A(22,8,8) = 330$ (here note that $A(n,d,w) = A(n,d,n-w)$), the results of this chapter imply that $A(22,8,10) = 616$ and $A(22,8,11) = 672$. So if one collects all words of a given weight w in the (once) shortened binary Golay code, the resulting code (if nonempty) is a constant weight code of maximum size. In other words, the shortened binary Golay code is a union of constant weight w codes of sizes $A(22,8,w)$. The value $A(22,8,10) = 616$ together with the already known values implies that also the twice shortened extended binary Golay code (which is an $(n,d) = (22,8)$-code of size 1024) has this property, since it contains 1, 330, 616, and 77 words of weight 0, 8, 12, and 16, respectively. It was already known that the binary Golay code, the extended binary Golay code and the once shortened extended binary Golay code have this property, i.e., that they are unions of constant weight codes of sizes $A(n,d,w)$.

Several tables with bounds on $A(n,d,w)$ have been given in the literature [1, 12, 26]. Tables with best currently known upper and lower bounds can be found on the website of Andries Brouwer [22].

6.1.1 The upper bounds $A_k(n,d,w)$ and $B_k(n,d,w)$

We describe two upper bounds on $A(n,d,w)$ based on quadruples of code words. Fix $n,d,w \in \mathbb{N}$ and let $N \subseteq \mathbb{F}_2^n$ be the set of all words of constant weight w. For $k \in \mathbb{Z}_{\geq 0}$, let $\mathcal{C}_k$ be the collection of codes $C \subseteq N$ with $|C| \leq k$. For any $D \in \mathcal{C}_k$, we define

$$\mathcal{C}_k(D) := \{C \in \mathcal{C}_k \mid C \supseteq D,\ |D| + 2|C \setminus D| \leq k\}. \tag{6.1}$$

Note that then $|C \cup C'| = |C| + |C'| - |C \cap C'| \leq 2|D| + |C \setminus D| + |C' \setminus D| - |D| \leq k$ for all $C, C' \subseteq \mathcal{C}_k(D)$. Furthermore, for any function $x : \mathcal{C}_k \to \mathbb{R}$ and $D \in \mathcal{C}_k$, we define the $\mathcal{C}_k(D) \times \mathcal{C}_k(D)$ matrix $M_{k,D}(x)$ by

$$M_{k,D}(x)_{C,C'} := x(C \cup C'),$$

for $C, C' \in \mathcal{C}_k(D)$. Define the following number, which is an adaptation to constant weight codes of the upper bound for unrestricted codes based on quadruples of codewords from Gijswijt, Mittelmann and Schrijver [37]:

$$A_k(n,d,w) := \max\left\{\textstyle\sum_{v \in N} x(\{v\}) \mid x : \mathcal{C}_k \to \mathbb{R},\ x(\emptyset) = 1, x(S) = 0 \text{ if } d_{\min}(S) < d,\right.$$
$$\left. M_{k,D}(x) \succeq 0 \text{ for each } D \text{ in } \mathcal{C}_k\right\}. \tag{6.2}$$

In this chapter, we first consider $A_4(n,d,w)$. Even after reductions (see the next subsection), the semidefinite program for computing $A_4(n,d,w)$ is large in practice, although $A_k(n,d,w)$ can be computed in polynomial time for fixed k. In computing $A_k(n,d,w)$, the matrix blocks coming from the matrices $M_{k,D}(x)$ for $D = \emptyset$ if k is even, and for $|D| = 1$ if k is odd, are often larger (in size and importantly, more variables occur in each matrix entry, yielding large semidefinite programs) than the blocks coming from $M_{k,D}(x)$ for D with $|D| \geq 2$. This observation has suggested the following relaxation of $A_k(n,d,w)$, which is sharper than $A_{k-1}(n,d,w)$ for $k \geq 4$ (while it equals $A_{k-1}(n,d,w)$ for $k = 3$, so assume $k \geq 3$ in the following definition).

$$\begin{aligned} B_k(n,d,w) := \max \big\{ \textstyle\sum_{v \in N} x(\{v\}) \mid\ & x : \mathcal{C}_k \to \mathbb{R},\ x(\emptyset) = 1, x(S) = 0 \text{ if } d_{\min}(S) < d, \\ & M_{k-1,D}(x|_{\mathcal{C}_{k-1}}) \succeq 0 \text{ for each } D \in \mathcal{C}_{k-1} \text{ with } |D| < 2, \\ & M_{k,D}(x) \succeq 0 \text{ for each } D \in \mathcal{C}_k \text{ with } |D| \geq 2 \big\}. \end{aligned} \tag{6.3}$$

Proposition 6.1.1. *For all $k, n, d, w \in \mathbb{N}$ with $k \geq 3$, we have that $A_{k-1}(n,d,w) \geq B_k(n,d,w) \geq A_k(n,d,w) \geq A(n,d,w)$.*

Proof. It is not hard to see that $B_k(n,d,w) \geq A_k(n,d,w)$, as all constraints in (6.3) follow from (6.2). Similarly, it follows that $A_{k-1}(n,d,w) \geq B_k(n,d,w)$.

To see $A_k(n,d,w) \geq A(n,d,w)$, let $C \subseteq \mathbb{F}_2^n$ be a constant weight w code with $d_{\min}(C) \geq d$ and $|C| = A(n,d,w)$. Define $x : \mathcal{C}_k \to \mathbb{R}$ by $x(S) = 1$ if $S \subseteq C$ and $x(S) = 0$ else, for $S \in \mathcal{C}_k$. Then x satisfies the conditions in (6.2), where the condition that $M_{k,D}(x) \succeq 0$ is satisfied since $M_{k,D}(x)_{C,C'} = x(C)x(C')$ for all $C, C' \in \mathcal{C}_k(D)$. Moreover, the objective value equals $\sum_{v \in N} x(\{v\}) = |C| = A(n,d,w)$, which gives $A_k(n,d,w) \geq A(n,d,w)$. □

This chapter considers $A_4(n,d,w)$ and $B_4(n,d,w)$, that is, $k = 4$. By symmetry we assume throughout that $w \leq n/2$ (otherwise, add the all-ones word to each word in $\mathbb{F}_2^n$, where the addition is in the vector space $\mathbb{F}_2^n$, and replace w by $n - w$). For computing $A_4(n,d,w)$, it suffices to require that the matrices $M_{4,D}(x)$ with $|D|$ even are positive semidefinite. To see this, note that if $D \subseteq C$ with $|D|$ even and $|C| = |D|+1$, then $\mathcal{C}_4(C) \subseteq \mathcal{C}_4(D)$, i.e., $M_{4,C}(x)$ is a principal submatrix of $M_{4,D}(x)$ and hence positive semidefiniteness of $M_{4,D}(x)$ implies positive semidefiniteness of $M_{4,C}(x)$. For computing $B_4(n,d,w)$, it suffices to require that the matrices $M_{3,D}(x|_{\mathcal{C}_3})$ for each $D \in \mathcal{C}_3$ with $|D| \leq 1$ and the matrices $M_{4,D}(x)$ for each $D \in \mathcal{C}_4$ with $|D| \in \{2,4\}$ are positive semidefinite.

If $|D| = 4$, then $M_{4,D}(x)$ is a matrix of order 1×1, so positive semidefiniteness of $M_{4,D}(x)$ is equivalent to $x(D) \geq 0$. We can assume in (6.2) and (6.3) that $x : \mathcal{C}_4 \to \mathbb{R}_{\geq 0}$, since if $|D| \leq 4$ then $x(D)$ occurs on the diagonal of $M_{4,D}(x)$ and if $|D| \leq 1$ then $x(D)$ occurs on the diagonal of $M_{3,D}(x|_{\mathcal{C}_3})$.

6.1.2 Exploiting the symmetry of the problem

Fix $k \in \mathbb{N}$ with $k \geq 2$. The group $H := S_n$ acts naturally on $\mathcal{C}_k$ by simultaneously permuting the indices $1, \ldots, n$ of each code word in $C \in \mathcal{C}_k$ (since the weight of each codeword is invariant under this action), and this action maintains minimum distances and cardinalities of codes $C \in \mathcal{C}_k$. We can assume that the optimum x in (6.2) (or (6.3)) is H-invariant. To see this, let x be an optimum solution for (6.2) (or (6.3)). For each $g \in H$, the function $g \cdot x$ is again an optimum solution, since the objective value of $g \cdot x$ equals the objective value of x and $g \cdot x$ still satisfies all constraints in (6.2) (or (6.3)). Since the feasible region is convex, the optimum x can be replaced by the average of $g \cdot x$ over all $g \in H$. This yields an H-invariant optimum solution.

			best		best upper		
			lower		bound		
			bound	**new upper**	previously		Delsarte
n	d	w	known	**bound**	known	$\lfloor A_3(n,d,w) \rfloor$	bound
17	6	7	166	**206***	207	228	249
18	6	7	243	**312***	318	353	408
19	6	7	338	**463***	503	526	553
19	6	8	408	**693**	718	718	751
20	6	8	588	**1084**	1106	1136	1199
21	6	8	775	**1665**	1695	1772	1938
21	6	9	1186	**2328**	2359	2359	2364
25	8	8	759	**850**	856	926	948
21	8	9	280	**294**	302	314	358
22	8	9	280	**440**	473	473	597
23	8	9	400	**662**	703	707	830
24	8	9	640	**968**	1041	1041	1160
25	8	9	829	**1366**	1486	1486	1626
26	8	9	887	**1901**	2104	2108	2282
27	8	9	1023	**2616**	2882	2918	3203
22	8	10	616	**616**	630	634	758
22	8	11	672	**672**	680	680	805
27	10	9	118	**291**	293	299	299
22	10	10	46	**71**	72	72	82
23	10	10	54	**116**	117	117	117
26	10	10	130	**397**	406	406	412
27	10	10	162	**555**	571	571	579
22	10	11	46	**79**	80	80	88

Table 6.2: An overview of the new upper bounds for constant weight codes. The best previously known bounds are taken from Brouwer's table [22]. The unmarked new upper bounds are instances of $B_4(n,d,w)$ (rounded down), and the new upper bounds marked with * are instances of $A_4(n,d,w)$ (rounded down). For comparison: $\lfloor B_4(17,6,7) \rfloor = 213$, $\lfloor B_4(18,6,7) \rfloor = 323$ and $\lfloor B_4(19,6,7) \rfloor = 486$. The best previously known upper bounds on $A(22,8,10)$ and $A(22,8,11)$ are from [47] and [81], respectively. The new upper bounds imply that $A(22,8,10) = 616$ and $A(22,8,11) = 672$ (marked in red).

Let Ω_k be the set of H-orbits on $\mathcal{C}_k$. Then $|\Omega_k|$ is bounded by a polynomial in n. Since there exists an H-invariant optimum solution, we can replace, for each $\omega \in \Omega_k$ and $C \in \omega$, each variable $x(C)$ by a variable $z(\omega)$. Hence, the matrices $M_{k,D}(x)$ become matrices $M_{k,D}(z)$ and we have considerably reduced the number of variables in (6.2) and (6.3).

It is only required that we check positive semidefiniteness of $M_{k,D}(z)$ for one code D in each H-orbit of $\mathcal{C}_k$, as for each $g \in H$, the matrix $M_{k,g(D)}(z)$ can be obtained by simultaneously permuting rows and columns of $M_{k,D}(z)$.

We sketch how to reduce these matrices in size. For $D \in \mathcal{C}_k$, let H'_D be the subgroup of H consisting of all $g \in H$ that leaves each element of D invariant. Then the action of H on $\mathcal{C}_k$ gives an action of H'_D on $\mathcal{C}_k(D)$. The simultaneous action of H'_D on the rows and columns of $M_{k,D}(z)$ leaves $M_{k,D}(z)$ invariant. Therefore, there exists a block-diagonalization (as explained in Section 1.2) given by $M_{k,D}(z) \mapsto U^* M_{k,D}(z) U$ of $M_{k,D}(z)$, for a matrix U depending on H'_D but not depending on z, such that the order of $U^* M_{k,D}(z) U$ is polynomial in n and such that $M_{k,D}(z)$ is positive semidefinite if and only if each of the blocks of $U^* M_{k,D}(z) U$ is positive semidefinite. In our case the matrix U can be taken to be real; so $U^* = U^\mathsf{T}$. The entries in each block of $U^\mathsf{T} M_{k,D}(z) U$ are linear functions in the variables $z(\omega)$ (with coefficients bounded polynomially in n). Hence, we have reduced the size of the matrices involved in our semidefinite program to polynomial size.

Note that, after reductions, the number of variables involved in the semidefinite programs for computing $A_k(n,d,w)$ and $B_k(n,d,w)$ are the same. However, the program for computing $B_k(n,d,w)$ contains fewer blocks than the program for computing $A_k(n,d,w)$, and the blocks are smaller and contain fewer variables per matrix entry. This is important, as the semidefinite programs for computing $A_4(n,d,w)$ for moderate values of n,d,w —for example for the cases given in Table 6.2 below— even after reductions turn out to be very large in practice (although they are of polynomial size).

For particular weights w (in the case of constant weight codes), the group of distance-preserving permutations of $\mathcal{C}_k$ can be larger than S_n. If $w = n/2$ there is a further action of S_2 on $\mathcal{C}_k$ by adding the all-ones word $\mathbf{1}$ to each word in each code S in $\mathcal{C}_k$. (This operation is called 'taking complements'; if $S \in \mathcal{C}_k$, we write $S^c := \{u + \mathbf{1} \mid u \in S\}$.) Since the corresponding reduction of the semidefinite program can only be used for specific weights w, we do not consider the reduction in this chapter, although it was used for reducing the number of variables in computing $B_4(22,8,11)$ (as we can assume $x(S) = x(S^c)$ in (6.3)).

The reductions of the optimization problem will be described in detail in Section 6.2. Table 6.2 contains new upper bounds for $n \leq 28$, which is the range of n usually considered. We did not compute bounds for all cases of n,d,w with $n \leq 28$. Only cases for which finding $B_4(n,d,w)$ did not require excessive computing time or memory are considered in the present work. Since some tables on Brouwer's website [22] also consider n in the range $29 \leq n \leq 32$, we give some new bounds for these cases (many of which are computed with the smaller program $A_3(n,d,w)$) in Section 6.3 in Table 6.3. All improvements have been found using multiple precision versions of SDPA [96], where the largest program (for computing $B_4(22,8,10)$) took approximately three weeks to compute on a modern desktop pc.

6.1.3 Comparison with earlier bounds

In this chapter we will consider $B_4(n,d,w)$ and $A_4(n,d,w)$, that is, $k = 4$. It can be proved that $A_2(n,d,w)$ is equal to the Delsarte bound [31]. The bound $A_4(n,d,w)$ is an adaptation of the bound for unrestricted binary codes based on quadruples considered in [37]. (In [37], this quadruple bound on $A(n,d)$ is called $A_4(n,d)$, which must not be confused with the parameter $A_q(n,d)$ from (2.1).) The semidefinite programming bound for constant weight codes introduced by Schrijver in [81] is a slight sharpening of $A_3(n,d,w)$ (in almost all cases it is equal to $A_3(n,d,w)$). The bound $B_4(n,d,w)$, which is based on quadruples of code words, is a bound 'in between' $A_3(n,d,w)$ and $A_4(n,d,w)$: it is the bound $A_3(n,d,w)$ with constraints for matrices $M_{4,D}(x)$ with $|D| = 2$ (based on quadruples of code words) added. Or it can be seen as a bound obtained from $A_4(n,d,w)$ by removing the positive semidefiniteness of the (large) matrix $M_{4,\emptyset}(x)$ and replacing it by the positive semidefiniteness of $M_{3,\emptyset}(x|_{\mathcal{C}_3}) = M_{2,\emptyset}(x|_{\mathcal{C}_2})$.

Recently, Kim and Toan [47] added linear inequalities to the Schrijver bound [81]. As it restricts to triples of codewords, their method has the advantage that the semidefinite programs are small and can be solved fast. The bound $B_4(n, d, w)$ is often sharper than their bound, but it takes much more time to compute.

6.2 Reduction of the optimization problem

In this section we give the reduction of optimization problem (6.3) for computing the bound $B_4(n, d, w)$, using the representation theory from Chapters 2 and 3. Also, we give a reduction for computing $A_4(n, d, w)$. First we consider block diagonalizing $M_{4,D}(z)$ for $D \in \mathcal{C}_4$ with $|D| = 1$ or $|D| = 2$, applied in computing both $B_4(n, d, w)$ and $A_4(n, d, w)$.[1] Subsequently we consider the cases $M_{3,\emptyset}(z|_{\Omega_3}) = M_{2,\emptyset}(z|_{\Omega_2})$ or $M_{4,\emptyset}(z)$, applied in computing $B_4(n, d, w)$ or $A_4(n, d, w)$, respectively. Note that for the cases $|D| = 3$ and $|D| = 4$ the matrix $M_{4,D}(z) = (z(D))$ is its own block diagonalization, so then $M_{4,D}(z)$ is positive semidefinite if and only if $z(D) \geq 0$.

Remark 6.2.1. If $z : \Omega_k \to \mathbb{R}$, $j \leq k$ and $D \in \mathcal{C}_j$, we will from now on omit the restriction sign in $M_{j,D}(z|_{\Omega_j})$. That is, we will write $M_{j,D}(z)$ to denote the matrix $M_{j,D}(z|_{\Omega_j})$.

6.2.1 The cases $|D| = 1$ and $|D| = 2$

In this section we consider one code $D \in \mathcal{C}_4$ with $|D| = 1$ or $|D| = 2$. We can assume that $D = \{v_1, v_2\}$ with

$$\begin{aligned} v_1 &= \overbrace{1 \dots 1\, 1 \dots 1}^{w}\overbrace{0 \dots 0\; 0 \dots 0}^{n-w} \\ v_2 &= \underbrace{0 \dots 0}_{t}\underbrace{1 \dots 1\, 1 \dots 1}_{w}\underbrace{0 \dots 0}_{n-t-w}, \end{aligned} \tag{6.4}$$

where $t \in \mathbb{Z}_{\geq 0}$ with $t = 0$ or $d/2 \leq t \leq w$. For the remainder of this section, fix $t \in \{0\} \cup \{t \mid d/2 \leq t \leq w\}$ (recall that $w \leq n/2$, so $t \leq n - w$). If $t = 0$, then $|D| = 1$ and if $d/2 \leq t \leq w$, then $|D| = 2$. The rows and the columns of $M_{4,D}(z)$ are parametrized by codes $C \supseteq D$ of size at most 3 (if $|D| = 2$) or size at most 2 (if $|D| = 1$).

Let H'_D be the group of distance-preserving permutations of $\mathcal{C}_4$ that fix v_1 and v_2. So

$$H'_D \cong S_t \times S_{w-t} \times S_t \times S_{n-t-w}. \tag{6.5}$$

We first describe a representative set for the action of H'_D on $(\mathbb{C}^{\mathbb{F}_2})^{\otimes j_1} \otimes \ldots \otimes (\mathbb{C}^{\mathbb{F}_2})^{\otimes j_4} \cong \mathbb{C}^{\mathbb{F}_2^n}$ and then restrict to words of weight w and distance at least d to both words in D. Let e_j denote the j-th standard basis vector of $\mathbb{C}^{\mathbb{F}_2}$, for $j = 0, 1$.

We use the notation of Section 2.4 and Chapter 3, most importantly of Section 3.3. Let

$$(j_1, j_2, j_3, j_4) := (t, w - t, t, n - t - w).$$

[1] Note that if $|D| = 1$ then $M_{4,D}(z) = M_{3,D}(z|_{\Omega_3})$. For computing $A_4(n, d, w)$, it is not necessary to consider the case $|D| = 1$ separately, as $M_{4,D}(z)$ for $|D| = 1$ is a principal submatrix of $M_{4,\emptyset}(z)$.

For $i = 1, \ldots, 4$, set $Z_i := \mathbb{F}_2$, $G_i := \{1\}$ (the trivial group) and $B_1^{(i)} := [e_0, e_1]$. For convenience of the reader, we restate the main definitions of Section 3.3 and the main facts about representative sets applied to the context of this section — see Figure 6.1.

FACTS.

$s = 4$, $(j_1, j_2, j_3, j_4) := (t, w - t, t, n - t - w)$.

for $i = 1, \ldots, 4$:
$G_i := \{1\}$, the trivial group.
$Z_i := \mathbb{F}_2$.
$m_i := 2$, so $\boldsymbol{m} := (m_1, \ldots, m_4) = (2, 2, 2, 2)$.

A representative set for the action of G_i on Z_i is $\{B_1^{(i)}\} = \{[e_0, e_1]\}$.
A representative set for the action of H'_D on $(\mathbb{C}^{Z_1})^{\otimes j_1} \otimes \ldots \otimes (\mathbb{C}^{Z_4})^{\otimes j_4}$ follows from (2.22) and (2.18).

$\Lambda_i := (Z_i \times Z_i)/G_i = \mathbb{F}_2 \times \mathbb{F}_2$.
$a_P := x \otimes y$ for $P = (x, y) \in \Lambda_i$.
$A_i := \{a_P \mid P \in \Lambda_i\}$, a basis of $W_i := \mathbb{C}\mathbb{F}_2 \otimes \mathbb{C}\mathbb{F}_2$.
$K_{\omega_i}^{(i)} := \sum_{(P_1,\ldots,P_{j_i}) \in \omega_i} a_{P_1} \otimes \cdots \otimes a_{P_{j_i}}$ for $\omega_i \in \Lambda_i^{j_i}/S_{j_i}$.

Figure 6.1: The main definitions of Section 3.3 and the main facts about representative sets applied to the context of Section 6.2.1.

A representative set for the action of H'_D on $(\mathbb{C}^{\mathbb{F}_2})^{\otimes j_1} \otimes \ldots \otimes (\mathbb{C}^{\mathbb{F}_2})^{\otimes j_4} \cong \mathbb{C}^{\mathbb{F}_2^n}$ is, cf. (2.22) and (2.18), given by

$$\left\{ \left[\bigotimes_{i=1}^{4} u_{\tau_i, B_1^{(i)}} \mid \forall\, i = 1, \ldots, 4 \,:\, \tau_i \in T_{\lambda_i, 2} \right] \;\middle|\; \forall\, i = 1, \ldots, 4 \,:\, \lambda_i \vdash j_i \right\}. \tag{6.6}$$

We restrict to words of weight w and distance contained in $\{0, d, d+1, \ldots, n\}$ to both words in D. For $d_1, d_2 \in \{0, 1, \ldots, n\}$, let L_{w,d_1,d_2} denote the linear subspace of $\mathbb{C}^{\mathbb{F}_2^n}$ spanned by the unit vectors e_v, with v a word of weight w and distances d_1 and d_2 to v_1 and v_2, respectively. Note that L_{w,d_1,d_2} is H'_D-invariant. If for all $i = 1, \ldots, 4$ we have $\lambda_i \vdash j_i$ and $\tau_i \in T_{\lambda_i,2}$, then the irreducible representation $\mathbb{C}H'_D \cdot \bigotimes_{i=1}^{4} u_{\tau_i, B_1^{(i)}}$ is contained in L_{w,d_1,d_2}, where

$$\begin{aligned} w &= |\tau_1^{-1}(2)| + |\tau_2^{-1}(2)| + |\tau_3^{-1}(2)| + |\tau_4^{-1}(2)|, \\ d_1 &= |\tau_1^{-1}(1)| + |\tau_2^{-1}(1)| + |\tau_3^{-1}(2)| + |\tau_4^{-1}(2)|, \\ d_2 &= |\tau_1^{-1}(2)| + |\tau_2^{-1}(1)| + |\tau_3^{-1}(1)| + |\tau_4^{-1}(2)|. \end{aligned} \tag{6.7}$$

Let for $\boldsymbol{\lambda} := (\lambda_1, \ldots, \lambda_4) \vdash (j_1, \ldots, j_4)$,

$$\begin{aligned} \boldsymbol{T'_{\lambda,m}} := \Big\{(\tau_1, \ldots, \tau_4) \,\Big|\, & \text{ for all } i = 1, \ldots, 4 : \tau_i \in T_{\lambda_i, 2}, \\ & |\tau_1^{-1}(2)| + |\tau_2^{-1}(2)| + |\tau_3^{-1}(2)| + |\tau_4^{-1}(2)| = w, \\ & |\tau_1^{-1}(1)| + |\tau_2^{-1}(1)| + |\tau_3^{-1}(2)| + |\tau_4^{-1}(2)| \in \{0, d, d+1, \ldots, n\}, \\ & |\tau_1^{-1}(2)| + |\tau_2^{-1}(1)| + |\tau_3^{-1}(1)| + |\tau_4^{-1}(2)| \in \{0, d, d+1, \ldots, n\}\Big\}. \end{aligned} \tag{6.8}$$

(Note that $\boldsymbol{T}'_{\boldsymbol{\lambda},\boldsymbol{m}}$ is a subset of $\boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}$ from (3.1).) Then

$$\left\{ \left[\bigotimes_{i=1}^{4} u_{\tau_i, B_1^{(i)}} \mid (\tau_1, \ldots, \tau_4) \in \boldsymbol{T}'_{\boldsymbol{\lambda},\boldsymbol{m}} \right] \ \middle| \ \boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_4) \vdash (j_1, \ldots, j_4) \right\} \tag{6.9}$$

is a representative set for the action of H'_D on N', where N' denotes the set of words $v \in N$ such that $C := \{v_1, v_2, v\} \in \mathcal{C}_4(D)$ with $d_{\min}(C) \geq d$.

Computations for $|D| = 1$ or $|D| = 2$

Fix $D = \{v_1, v_2\} \in \mathcal{C}_4$. Let $\Omega_4(D)$ denote the set of all S_n-orbits of codes in $\mathcal{C}_4$ containing $D = \{v_1, v_2\}$. For each $\omega \in \Omega_4(D)$, we define the $\mathbb{F}_2^n \times \mathbb{F}_2^n$ matrix N_ω by

$$(N_\omega)_{\alpha,\beta} := \begin{cases} 1 & \text{if } \{v_1, v_2, \alpha, \beta\} \in \omega, \\ 0 & \text{otherwise,} \end{cases} \tag{6.10}$$

for $\alpha, \beta \in \mathbb{F}_2^n$. Then, for each $z : \Omega_4(D) \to \mathbb{R}$, one has $M_{4,D}(z) \succeq 0$ if and only if $\sum_{\omega \in \Omega_4(D)} z(\omega) N_\omega \succeq 0$. (The implication "$\Longleftarrow$" is trivial, as $M_{4,D}(z)$ is a principal submatrix of $\sum_{\omega \in \Omega_4(D)} z(\omega) N_\omega$. The implication "$\Longrightarrow$" follows from the fact that $L^{\mathsf{T}} M_{4,D}(z) L = \sum_{\omega \in \Omega_4(D)} z(\omega) N_\omega$, where L is the $\mathcal{C}_4(D) \times \mathbb{F}_2^n$ matrix with $0,1$ entries satisfying $L_{C,\alpha} = 1$ if and only if $C = \{v_1, v_2, \alpha\}$, for $C \in \mathcal{C}_4(D)$ and $\alpha \in \mathbb{F}_2^n$.)

Then we obtain with (2.17) and (6.9) that, for each $z : \Omega_4(D) \to \mathbb{R}$,

$$\Phi\left(\sum_{\omega \in \Omega_4(D)} z(\omega) N_\omega \right) = \bigoplus_{\substack{\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_4) \\ \lambda_i \vdash j_i \ \forall\ 1 \leq i \leq 4}} \sum_{\omega \in \Omega_4(D)} z(\omega) U_{\boldsymbol{\lambda}}^{\mathsf{T}} N_\omega U_{\boldsymbol{\lambda}}, \tag{6.11}$$

where $U_{\boldsymbol{\lambda}}$ is the matrix in (6.9) that corresponds with $\boldsymbol{\lambda} := (\lambda_1, \ldots, \lambda_4)$. For each $i = 1, \ldots, 4$, the number of $\lambda_i \vdash j_i$, and the numbers $|\boldsymbol{T}'_{\boldsymbol{\lambda},\boldsymbol{m}}|$ and $|\Omega_4(D)|$ are all bounded by a polynomial in n. This implies that the number of blocks in (6.11), the size of each block and the number of variables occurring in all blocks are polynomially bounded in n. Next we will show how to compute each entry $(\bigotimes_{i=1}^{4} u_{\tau_i, B_1^{(i)}})^{\mathsf{T}} N_\omega (\bigotimes_{i=1}^{4} u_{\sigma_i, B_1^{(i)}})$ in polynomial time, for $(\tau_1, \ldots, \tau_4)$ and $(\sigma_1, \ldots, \sigma_4)$ in $\boldsymbol{T}'_{\boldsymbol{\lambda},\boldsymbol{m}}$.

As in Section 3.3, let $R := Z_1^{j_1} \times \ldots \times Z_4^{j_4}$, so $R = \mathbb{F}_2^t \times \mathbb{F}_2^{w-t} \times \mathbb{F}_2^t \times \mathbb{F}_2^{n-w-t}$. Write $\mathcal{C}'_4$ for the collection of codes $C \subseteq \mathbb{F}_2^n$ of size ≤ 4 (so not necessarily of constant weight w). Then the function

$$\begin{aligned} R^2 = \left(\mathbb{F}_2^t \times \mathbb{F}_2^{w-t} \times \mathbb{F}_2^t \times \mathbb{F}_2^{n-w-t} \right)^2 &\to \mathcal{C}'_4, \\ ((\alpha^1, \alpha^2, \alpha^3, \alpha^4), (\beta^1, \beta^2, \beta^3, \beta^4)) &\mapsto \{v_1, v_2, \alpha^1\alpha^2\alpha^3\alpha^4, \beta^1\beta^2\beta^3\beta^4\}, \end{aligned} \tag{6.12}$$

induces a surjective function $r : R^2/H'_D \to \Omega'_4(D)$, where $\Omega'_4(D) \supseteq \Omega_4(D)$ denotes the set of all H'_D-orbits of codes in $\mathcal{C}'_4$ that contain $D = \{v_1, v_2\}$.

For any $\omega' \in R^2/H'_D$, the matrix $K_{\omega'}$ is defined in (3.20). If $\omega \in \Omega_4(D)$, then a basic calculation as in Lemma 4.3.1 gives

$$N_\omega = \sum_{\substack{\omega' \in R^2/H'_D \\ r(\omega') = \omega}} K_{\omega'}. \tag{6.13}$$

So it suffices to compute $\left(\bigotimes_{i=1}^4 u_{\tau_i,B_1^{(i)}}\right)^{\mathsf{T}} K_{\omega'} \left(\bigotimes_{i=1}^4 u_{\sigma_i,B_1^{(i)}}\right)$. Note that $K_{\omega'} = K_{\omega_1}^{(1)} \otimes \ldots \otimes K_{\omega_4}^{(4)}$, cf. (3.21), where for each $\omega' \in R^2/H'_D$ we write $\omega' = \omega_1 \times \ldots \times \omega_4$, with $\omega_i \in \Lambda_i^{j_i}/S_{j_i}$ for $1 \leq i \leq 4$. Then, as in (2.19),

$$\left(\bigotimes_{i=1}^4 u_{\tau_i,B_1^{(i)}}\right)^{\mathsf{T}} \left(\bigotimes_{i=1}^4 K_{\omega_i}^{(i)}\right) \left(\bigotimes_{i=1}^4 u_{\sigma_i,B_1^{(i)}}\right) = \prod_{i=1}^4 \left(u_{\tau_i,B_1^{(i)}}^{\mathsf{T}} K_{\omega_i}^{(i)} u_{\sigma_i,B_1^{(i)}}\right). \tag{6.14}$$

Hence

$$\sum_{\omega' \in R^2/H'_D} \left(\left(\bigotimes_{i=1}^4 u_{\tau_i,B_1^{(i)}}\right)^{\mathsf{T}} \left(\bigotimes_{i=1}^4 K_{\omega_i}^{(i)}\right) \left(\bigotimes_{i=1}^4 u_{\sigma_i,B_1^{(i)}}\right)\right) \mu(\omega_1) \cdots \mu(\omega_4)$$
$$= \prod_{i=1}^4 \sum_{\omega_i \in \Lambda^{j_i}/S_{j_i}} \left(u_{\tau_i,B_1^{(i)}}^{\mathsf{T}} K_{\omega_i}^{(i)} u_{\sigma_i,B_1^{(i)}}\right) \mu(\omega_i).$$

Moreover, by Proposition 3.1.1 , for $1 \leq i \leq 4$, one has

$$\sum_{\omega_i \in \Lambda_i^{j_i}/S_{j_i}} \left(u_{\tau_i,B_1^{(i)}} K_{\omega_i}^{(i)} u_{\sigma_i,B_1^{(i)}}\right) \mu(\omega_i) = p_{\tau_i,\sigma_i}(F_1^{(i)}),$$

where p_{τ_i,σ_i} is defined in (3.14) and where $F_1^{(i)}$ is the $\mathbb{F}_2 \times \mathbb{F}_2$ matrix with

$$(F_1^{(i)}) := \left(B_1^{(i)}(j) \otimes B_1^{(i)}(h)\right)\Big|_{W_i} = a^*_{(j,h)}, \quad \text{for } j,h \in \mathbb{F}_2 \text{ (so that } (j,h) \in \Lambda_i). \tag{6.15}$$

So one computes the entry $\sum_{\omega \in \Omega_4(D)} z(\omega) \left(\bigotimes_{i=1}^4 u_{\tau_i,B_1^{(i)}}\right)^{\mathsf{T}} N_\omega \left(\bigotimes_{i=1}^4 u_{\sigma_i,B_1^{(i)}}\right)$ by first expressing each polynomial $p_{\tau_i,\sigma_i}(F_1^{(i)})$ as a linear combination of $\mu(\omega_i)$ and subsequently replacing each $\mu(\omega_1) \cdots \mu(\omega_4)$ in the product $\prod_{i=1}^4 p_{\tau_i,\sigma_i}(F_1^{(i)})$ with the variable $z(r(\omega_1 \times \ldots \times \omega_4))$ if $r(\omega_1 \times \ldots \times \omega_4) \in \Omega_4$ and with zero otherwise. (Here $\omega_1 \times \ldots \times \omega_4 \in R^2/H'_D$, cf. (3.17).)

6.2.2 The case $D = \emptyset$

Next, we consider how to block diagonalize $M_{3,\emptyset}(z) = M_{2,\emptyset}(z)$ for computing $B_4(n,d,w)$. We also give a reduction of the matrix $M_{4,\emptyset}(z)$ for computing $A_4(n,d,w)$. So we will reduce the matrices $M_{2\xi,\emptyset}(z)$ for $\xi \in \{1,2\}$, where we consider $\xi = 1$ for computing $B_4(n,d,w)$ and $\xi = 2$ for computing $A_4(n,d,w)$. We start by giving a representative set for the natural action of S_n on $(\mathbb{C}^{\mathbb{F}_2^\xi})^{\otimes n} \cong \mathbb{C}^{(\mathbb{F}_2^n)^\xi}$, using the results described in Section 2.4. For the computations, we will use the framwork from Chapter 3.

Let $B_1 := [e_j \mid j \in \mathbb{F}_2^\xi]$ be an $\mathbb{F}_2^\xi \times \mathbb{F}_2^\xi$ matrix containing the unit basis vectors of $\mathbb{C}^{\mathbb{F}_2^\xi}$ as columns, in lexicographic order (from left to right). So if $\xi = 1$ then $B_1 = [e_0, e_1]$ and if $\xi = 2$ then $B_1 = [e_{(0,0)}, e_{(0,1)}, e_{(1,0)}, e_{(1,1)}]$. Then B_1 is an ordered basis of $\mathbb{C}^{\mathbb{F}_2^\xi}$. For convenience of the reader, we restate the main definitions of Chapter 3 and the main facts about representative sets applied to the context of this section — see Figure 6.2.

Proposition 2.22 gives a representative set for the action of S_n on $(\mathbb{C}^{\mathbb{F}_2^\xi})^{\otimes n}$: it is the set

$$\{ \ [u_{\tau,B_1} \mid \tau \in T_{\lambda,2^\xi}] \ \mid \lambda \vdash n\}. \tag{6.16}$$

FACTS.

$G := \{1\}$, the trivial group.
$Z := \mathbb{F}_2^{\xi}$.

$k := 1$, $m_1 := 2^{\xi}$ and $m := 2^{\xi}$.

A representative set for the action of G on Z is $\{B_1\} := \{[e_j \mid j \in \mathbb{F}_2^{\xi}]\}$.
A representative set for the action of S_n on Z^n is given by (2.22).

$\Lambda := (Z \times Z)/G = \mathbb{F}_2^{\xi} \times \mathbb{F}_2^{\xi}$.
$a_P := x \otimes y$ for $P = (x, y) \in \Lambda$.
$A := \{a_P \,|\, P \in \Lambda\}$, a basis of $W := \mathbb{C}\mathbb{F}_2^{\xi} \otimes \mathbb{C}\mathbb{F}_2^{\xi}$.
$K_{\omega'} := \sum_{(P_1,\ldots,P_n)\in\omega'} a_{P_1} \otimes \cdots \otimes a_{P_n}$ for $\omega' \in \Lambda^n/S_n$.

Figure 6.2: The main definitions of Chapter 3 and the main facts about representative sets applied to the context of Section 6.2.2.

For computing $B_4(n, d, w)$, we consider $\xi = 1$. We restrict the representative set (6.16) for the action of S_n on $(\mathbb{C}^{\mathbb{F}_2})^{\otimes n} \cong \mathbb{C}^{\mathbb{F}_2^n}$ to $\mathbb{C}^N$ (recall: $N \subseteq \mathbb{F}_2^n$ is the set of all words of constant weight w). Note that for any $\tau \in T_{\lambda,2}$, the number of times $B_1(2) = e_1$ appears in the tensor in each summand of u_{τ,B_1} (cf. (2.21)) is equal to $|\tau^{-1}(2)|$. Similarly, $|\tau^{-1}(1)|$ is equal to the number of times $B_1(1) = e_0$ appears in the tensor in each summand of u_{τ,B_1}. Let

$$T_{\lambda,2}^{(1)} := \{\tau \in T_{\lambda,2} \,|\; |\tau^{-1}(2)| = w\}, \quad \text{for } \lambda \vdash n. \tag{6.17}$$

Then

$$\left\{ \left[u_{\tau,B_1} \mid \tau \in T_{\lambda,2}^{(1)}\right] \mid \lambda \vdash n \right\} \tag{6.18}$$

is representative for the action of S_n on $N = \mathcal{C}_1 \setminus \{\emptyset\} \subseteq \mathbb{F}_2^n$.

For computing $A_4(n, d, w)$, we consider $\xi = 2$. We proceed by restricting the representative set (6.16) of the action of S_n on $\mathbb{C}^{(\mathbb{F}_2^n)^2}$ to pairs of words in N^2 with distance contained in $\{0, d, d+1, \ldots, n\}$. Given $w_1, w_2, d_1 \in \{0, 1, \ldots, n\}$, let $L_{w_1,w_2,d_1}^{(2)}$ denote the linear subspace of $\mathbb{C}^{(\mathbb{F}_2^n)^2}$ spanned all the unit vectors $e_{\alpha,\beta}$, with α and β words of weight w_1 and w_2 respectively, and $d_H(\alpha, \beta) = d_1$. Then $L_{w_1,w_2,d_1}^{(2)}$ is S_n-invariant. Moreover, for any $\lambda \vdash n$ and $\tau \in T_{\lambda,4}$, the irreducible representation $\mathbb{C}S_n \cdot u_{\tau,B_1}$ is contained in $L_{w_1,w_2,d_1}^{(2)}$, with

$$\begin{aligned} w_1 &= |\tau^{-1}(3)| + |\tau^{-1}(4)|, \\ w_2 &= |\tau^{-1}(2)| + |\tau^{-1}(4)|, \\ d_1 &= |\tau^{-1}(2)| + |\tau^{-1}(3)|. \end{aligned} \tag{6.19}$$

So let

$$\begin{aligned} T_{\lambda,4}^{(2)} := \{\tau \in T_{\lambda,4} \,|\; & |\tau^{-1}(2)| + |\tau^{-1}(4)| = w,\ |\tau^{-1}(3)| + |\tau^{-1}(4)| = w, \\ & |\tau^{-1}(2)| + |\tau^{-1}(3)| \in \{0, d, d+1, \ldots, n\}\}, \quad \text{for } \lambda \vdash n. \end{aligned} \tag{6.20}$$

Then

$$\left\{ \left[u_{\tau,B_1} \mid \tau \in T^{(2)}_{\lambda,4} \right] \mid \lambda \vdash n \right\} \tag{6.21}$$

is representative for the action of S_n on $(N^2)_d \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^n$, where $(N^2)_d$ denotes the set of all pairs of words in $N \times N$ with distance contained in $\{0, d, d+1, \ldots, n\}$.

It is possible to further reduce the program (by a factor 2) by giving a reduction from ordered pairs to *unordered* pairs of words. We will not consider this reduction in the present chapter. Regardless of a further reduction by a factor 2, the programs for computing $A_4(n, d, w)$ are considerably larger (although they have polynomial size) than the ones for computing $B_4(n, d, w)$.

Note that S_n acts trivially on $\emptyset$. The S_n-isotypical component of $\mathbb{C}^{N^\xi}$ that consists of the S_n-invariant elements corresponds to the matrix in the representative set (6.18) or (6.21) indexed by $\lambda = (n)$. So to obtain a representative set for the action of S_n on $(N^\xi)_d \cup \{\emptyset\}$ (here $(N^1)_d := N$), we add a new unit base vector $e_\emptyset$ to this matrix (as a column).

Computations for $D = \emptyset$

We consider $\xi = 1$ and $\xi = 2$ for computing $B_4(n, d, w)$ and $A_4(n, d, w)$, respectively. If $\xi = 1$, then for all $\omega \in \Omega_2 \subseteq \Omega_4$, we define the $\mathbb{F}_2^n \times \mathbb{F}_2^n$ matrix $N^{(1)}_\omega$ by

$$(N^{(1)}_\omega)_{\alpha,\beta} := \begin{cases} 1 & \text{if } \{\alpha, \beta\} \in \omega, \\ 0 & \text{otherwise,} \end{cases} \tag{6.22}$$

for $\alpha, \beta \in \mathbb{F}_2^n$. Similarly, if $\xi = 2$, then for all all $\omega \in \Omega_4$, we define the $(\mathbb{F}_2^n \times \mathbb{F}_2^n) \times (\mathbb{F}_2^n \times \mathbb{F}_2^n)$ matrix $N^{(2)}_\omega$ by

$$(N^{(2)}_\omega)_{(\alpha,\beta),(\gamma,\delta)} := \begin{cases} 1 & \text{if } \{\alpha, \beta, \gamma, \delta\} \in \omega, \\ 0 & \text{otherwise,} \end{cases} \tag{6.23}$$

for $\alpha, \beta, \gamma, \delta \in \mathbb{F}_2^n$. Let $M'_{2\xi,\emptyset}(z)$ denote the matrix $M_{2\xi,\emptyset}(z)$ with the row and column indexed by $\emptyset$ removed. Then, for each $z : \Omega_{2\xi} \to \mathbb{R}$, one has $M'_{2\xi,\emptyset}(z) \succeq 0$ if and only if $\sum_{\omega \in \Omega_{2\xi} \setminus \{\{\emptyset\}\}} z(\omega) N^{(\xi)}_\omega \succeq 0$. With (2.17) and (6.18) or (6.21) we obtain that, for any $z : \Omega_{2\xi} \setminus \{\{\emptyset\}\} \to \mathbb{R}$,

$$\Phi \left(\sum_{\omega \in \Omega_{2\xi} \setminus \{\{\emptyset\}\}} z(\omega) N^{(\xi)}_\omega \right) = \bigoplus_{\lambda \vdash n} \sum_{\omega \in \Omega_{2\xi} \setminus \{\{\emptyset\}\}} z(\omega) U_\lambda^\mathsf{T} N^{(\xi)}_\omega U_\lambda, \tag{6.24}$$

where U_λ is the matrix in (6.18) or (6.21) that corresponds with λ. The number of $\lambda \vdash n$ with height$(\lambda_1) \leq 2^\xi$, and the numbers $|T^{(\xi)}_{\lambda,2^\xi}|$, $|\Omega_{2\xi}|$, for $\xi = 1$ and $\xi = 2$, respectively, are all polynomially bounded in n. Hence the number of blocks in (6.24), as well as the size of each block and the number of variables occurring in all blocks are bounded by a polynomial in n. We now explain how to compute the coefficients $u_{\tau,B_1}^\mathsf{T} N^{(\xi)}_\omega u_{\sigma,B_1}$ in polynomial time, for $\tau, \sigma \in T^{(\xi)}_{\lambda,2^\xi}$ and $\xi \in \{1, 2\}$.

Recall that $\Lambda = \mathbb{F}_2^\xi \times \mathbb{F}_2^\xi$. Since naturally $(\mathbb{F}_2^n)^{2\xi} \cong (\mathbb{F}_2^\xi \times \mathbb{F}_2^\xi)^n$, there is a natural bijection between Λ^n / S_n and the set of S_n-orbits on $(\mathbb{F}_2^n)^{2\xi}$. The function $(\mathbb{F}_2^n)^{2\xi} \to \mathcal{C}_{2\xi}$

with $(x_1,\dots,x_{2\xi}) \mapsto \{x_1,\dots,x_{2\xi}\}$ then induces a surjective function $r' : \Lambda^n/S_n \to \Omega'_{2\xi} \setminus \{\{\emptyset\}\}$, where $\Omega'_{2\xi} \supseteq \Omega_{2\xi}$ denotes the set of all S_n-orbits of codes in $\mathcal{C}'_{2\xi}$ (so not necessarily of constant weight w) and $\xi \in \{1,2\}$.

In view of Lemma 4.3.1, we have for each $\omega \in \Omega_{2\xi} \setminus \{\{\emptyset\}\}$ that

$$N^{(\xi)}_\omega = \sum_{\substack{\omega' \in \Lambda^n/S_n \\ r'(\omega')=\omega}} K_{\omega'}. \tag{6.25}$$

So it suffices to compute $\left(u^{\mathsf{T}}_{\tau,B_1} K_{\omega'} u_{\sigma,B_1}\right)$ for each $\omega' \in \Lambda^n/S_n$ and $\tau,\sigma \in T^{(\xi)}_{\lambda,2^\xi}$. By Proposition 3.2.1, it holds that $\sum_{\omega'\in\Lambda^n/S_n} \left(u^{\mathsf{T}}_{\tau,B_1} K_{\omega'} u_{\sigma,B_1}\right) \mu(\omega') = p_{\tau,\sigma}(F_1)$, where the polynomial $p_{\tau,\sigma}$ is defined in (3.14) and where F_1 is an $\mathbb{F}_2^\xi \times \mathbb{F}_2^\xi$ matrix with

$$(F_1)_{j,h} = (B_1(j) \otimes B_1(h))|_W = a^*_{(j,h)}, \quad \text{for } j,h \in \mathbb{F}_2^\xi \text{ (so that } (j,h)\in\Lambda). \tag{6.26}$$

Hence one computes the entry $\sum_{\omega\in\Omega_{2\xi}\setminus\{\{\emptyset\}\}} z(\omega) u^{\mathsf{T}}_{\tau,B_1} N^{(\xi)}_\omega u_{\sigma,B_1}$ by first expressing $p_{\tau,\sigma}(F_1)$ as a linear combination of degree n monomials expressed in the dual basis A^* of A and subsequently replacing each monomial $\mu(\omega')$ in $p_{\tau,\sigma}(F_1)$ with the variable $z(r'(\omega'))$ if $r'(\omega') \in \Omega_{2\xi}$ and with zero otherwise.

At last, we compute the entries in the row and column indexed by $\emptyset$ in the matrix for $\lambda = (n)$. Then $e_\emptyset^{\mathsf{T}} M_{2\xi,\emptyset}(z) e_\emptyset = M_{2\xi,\emptyset}(z)_{\emptyset,\emptyset} = x(\emptyset) = 1$ by definition, see (6.2) and (6.3). For computing the other entries we distinguish between the cases $\xi = 1$ and $\xi = 2$. If $\xi = 1$, then for $\lambda = (n)$, we have $|T^{(1)}_{\lambda,2}| = 1$, so there is only one coefficient to compute. If τ is the unique element in $T^{(1)}_{\lambda,2}$ (note that the tableau τ contains w times symbol 2 and $n-w$ times symbol 1), then $u_{\tau,B_1} = \sum_{v\in\mathbb{F}_2^n, \mathrm{wt}(v)=w} e_v$, so

$$e_\emptyset^{\mathsf{T}} M_{2,\emptyset}(z) u_{\tau,B_1} = \binom{n}{w} z(\omega_0), \tag{6.27}$$

where $\omega_0 \in \Omega_2$ is the (unique) S_n-orbit of a code of size 1.

If $\xi = 2$, then for $\lambda = (n)$, any $\tau \in T^{(2)}_{\lambda,4}$ is determined by the number t of 2's in the row of the Young shape $Y((n))$ of tableau τ (this determines also the number of 1's, 3's and 4's, by (6.19)). Then

$$u_{\tau,B_1} = \sum_{\substack{v_1,v_2\in\mathbb{F}_2^n, \\ \mathrm{wt}(v_1)=\mathrm{wt}(v_2)=w \\ d_H(v_1,v_2)=2t}} e_{(v_1,v_2)}. \tag{6.28}$$

Hence

$$e_\emptyset^{\mathsf{T}} M_{4,\emptyset}(z) u_{\tau,B_1} = \sum_{\substack{v_1,v_2\in\mathbb{F}_2^n, \\ \mathrm{wt}(v_1)=\mathrm{wt}(v_2)=w \\ d_H(v_1,v_2)=2t}} x(\{v_1,v_2\}) = \binom{n}{w}\binom{w}{t}\binom{n-w}{t} z(\omega_t), \tag{6.29}$$

where $\omega_t \in \Omega_4$ is the (unique) S_n-orbit of a pair of constant weight code words at distance $2t$.

6.3 Concluding remarks

Recently, also new upper bounds for constant weight codes for some values of n larger than 28 have been given, see [87] and [22]. We therefore also provide a table with improved upper bounds for n in the range $29 \leq n \leq 32$ and $d \geq 10$ (cf. Brouwer's table [22]) — see Table 6.3. Most of our new upper bounds for these cases are instances of $A_3(n,d,w)$, which can computed by using the block diagonalization of $M_{2,\emptyset}(z)$ from Section 6.2.2 and from $M_{3,D}(z) = M_{4,D}(z)$ for $|D| = 1$ from Section 6.2.1 (use only the blocks for $t = 0$ from this section). The bound $A_3(n,d,w)$ is in almost all cases equal to the Schrijver bound [81].

n	d	w	best lower bound known	**new upper bound**	best upper bound previously known	Delsarte bound
31	10	8	124	$\mathbf{322^B}$	329	344
32	10	8	145	$\mathbf{402^B}$	436	442
29	10	9	168	$\mathbf{523^B}$	551	565
30	10	9	203	$\mathbf{657^B}$	676	725
31	10	9	232	$\mathbf{822^B}$	850	936
30	10	10	322	**1591**	1653	1696
31	10	10	465	**2074**	2095	2247
32	10	10	500	**2669**	2720	2996
29	10	11	406	**2036**	2055	2055
30	10	11	504	**2924**	2945	2945
31	10	11	651	**4141**	4328	4328
32	10	11	992	**5696**	6094	6538
29	10	12	539	**3091**	3097	3097
30	10	12	768	**5008**	5139	5139
31	10	12	930	**7259**	7610	7610
32	10	12	1395	**10446**	11541	11541
29	10	13	756	**4282**	4420	4420
30	10	13	935	**6724**	7149	7149
31	10	13	1395	**10530**	12254	12254
32	10	13	1984	**16755**	18608	18608
29	10	14	1458	**4927**	5051	5051
30	10	14	1458	**8146**	9471	9471
31	10	14	1538	**13519**	15409	15409
32	10	14	2325	**22213**	24679	24679
30	10	15	1458	**8948**	10053	10053
31	10	15	1922	**15031**	17337	17337
32	10	15	2635	**26361**	29770	29770
32	10	16	3038	**27429**	30316	30316
29	12	9	42	$\mathbf{59^B}$	66	67
30	12	9	42	$\mathbf{74^B}$	94	96
31	12	9	50	**94**	103	112
29	12	10	66	**126**	129	129
32	12	11	186	**573**	574	574
30	12	12	190	**492**	493	493
31	12	12	310	**679**	692	692
32	12	12	496	**952**	1014	1014
30	12	13	236	**642**	689	689
31	12	13	400	**958**	1177	1177
32	12	13	434	**1497**	1669	1669
29	12	14	173	**492**	507	507
30	12	14	288	**801**	952	952
31	12	14	510	**1238**	1455	1455
32	12	14	900	**2140**	2143	2143
30	12	15	302	**894**	1008	1008
31	12	15	572	**1435**	1605	1605
32	14	11	39	**68**	89	90
29	14	12	29	**47**	50	52
30	14	12	36	**62**	72	80
31	14	12	45	**80**	103	104
32	14	12	55	**118**	134	134
29	14	13	35	**58**	66	74
30	14	13	45	**78**	101	101
31	14	13	60	**129**	137	137
29	14	14	58	**63**	82	82
30	14	14	58	**95**	116	116
30	14	15	62	**104**	122	122

Table 6.3: An overview of the new upper bounds for constant weight codes for $29 \leq n \leq 32$ and $d \geq 10$. The unmarked new upper bounds are instances of $A_3(n,d,w)$ (rounded down), the ones marked with ^{B} are instances of $B_4(n,d,w)$ (rounded down). The best previously known bounds are taken from Brouwer's table [22].

Upper bound (6.3) could also be useful for unrestricted binary codes: one can define $B_k(n,d)$ just as $B_k(n,d,w)$ in (6.3), where $\mathcal{C}_k$ now is defined to be the collection of all codes $C \subseteq \mathbb{F}_2^n$ of size $\leq k$ and $N := \mathbb{F}_2^n$. Note that $B_k(n,d)$ in this context has a different meaning than $B_q(n,d)$ from (4.2). To compute $B_k(n,d)$ in case $k=5$, one must block diagonalize $M_{4,\emptyset}(x|_{\mathcal{C}_4})$ (the block diagonalization can be found explicitly in [37] or more conceptually in Chapter 4) and the matrices $M_{5,D}(x)$ with $|D|=3$ and $|D|=2$. One can assume that $D=\{v_1,v_2,v_3\}$ with

$$\begin{aligned} v_1 &= \overbrace{0\dots0\,0\dots0}^{w}\overbrace{0\dots0\;\,0\dots0}^{n-w} \\ v_2 &= 1\dots1\,1\dots1\,0\dots0\;\,0\dots0 \\ v_3 &= \underbrace{0\dots0}_{t_1}\underbrace{1\dots1}_{w-t_1}\underbrace{1\dots1}_{t_2}\;\underbrace{0\dots0}_{n-w-t_2}, \end{aligned} \tag{6.30}$$

for $0 \leq w \leq n$, $t_1 \leq w$, $t_2 \leq n-w$ and such that the weight of v_3 is at least the weight of v_2, so $t_2 \geq t_1$. Then $S_{t_1} \times S_{w-t_1} \times S_{t_2} \times S_{n-w-t_2}$ acts on $\mathcal{C}_5$ fixing D, and a block diagonalization of $M_{5,D}(x)$ for $|D|=3$ and $|D|=2$ for non-constant weight codes is obtained by a straightforward adaptation of the block diagonalization of $M_{4,D}(x)$ for $|D|=2$ and $|D|=1$ for constant weight codes given in Section 6.2.1.[2] However, for small cases in which $A(n,d)$ is unsettled (with n around 20), the program $B_5(n,d)$ is large in practice, even after reductions. The program to compute the bound from [37] (which is defined analogously to $A_k(n,d,w)$ in (6.2)) for $k=5$ is still larger after reductions (although of size polynomial in n). Using a lot of computing time, one may be able to compute $B_5(n,d)$ for some small unknown cases of n,d, possibly sharpening recent semidefinite programming bounds for binary codes [37, 47]. This is material for further research.

6.4 Appendix: An overview of the program

See Figure 6.3 for an outline of the method. Here we write $\omega_0 \in \Omega_4$ for the (unique) S_n-orbit of a constant weight w code of size 1, and $\omega_\emptyset$ for the orbit $\{\emptyset\}$. Also, we write Ω_4^d for the set orbits in Ω_4 that correspond to a code with minimum distance at least d.

[2] To compute the bound from [37] for $k=5$, we additionally must compute a block diagonalization of the (large) matrix $M_{5,D}(x)$ for $|D|=1$ (so we can assume $D=\{0\dots0\}$, the singleton zero word). This block diagonalization can be obtained by adapting the block diagonalization of $M_{4,\emptyset}$ for constant weight codes given in Section 6.2.2.

```
Input:  Natural numbers $n, d, w$ and $\xi \in \{1, 2\}$
Output: Semidefinite program to compute $B_4(n, d, w)$ ($\xi = 1$) or $A_4(n, d, w)$ ($\xi = 2$)

print Maximize $\binom{n}{w} z(\omega_0)$
print Subject to:
//Start with $|D| = 1$ and $|D| = 2$.
foreach $t \in \mathbb{Z}_{\geq 0}$ with $t = 0$ or $d/2 \leq t \leq w$ //Recall: $(j_1, \ldots, j_4) = (t, w - t, t, n - w - t)$.
    foreach $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_4) \vdash (j_1, \ldots, j_4)$ with height$(\lambda_i) \leq 2$ for all $i$
        start a new block $M_{\boldsymbol{\lambda}}$
        foreach $(\tau_1, \ldots, \tau_4) \in \boldsymbol{T'_{\lambda,m}}$ from (6.8)
            foreach $(\sigma_1, \ldots, \sigma_4) \in \boldsymbol{T'_{\lambda,m}}$ from (6.8)
                compute $p_{\tau_i,\sigma_i}(F_1^{(i)})$ for $i = 1, \ldots, 4$ (with $p_{\tau_i,\sigma_i}$ cf. (3.14), $F_1^{(i)}$ cf. (6.15))
                replace each $\mu_1(\omega_1) \cdots \mu(\omega_4)$ in $\prod_{i=1}^{4} p_{\tau_i,\sigma_i}(F_1^{(i)})$ by a variable
                    $z(r(\omega_1 \times \ldots \times \omega_4))$ if $r(\omega_1 \times \ldots \times \omega_4) \in \Omega_4^d$ and by 0 otherwise
                $(M_{\boldsymbol{\lambda}})_{(\tau_1,\ldots,\tau_4),(\sigma_1,\ldots,\sigma_4)}$ := the resulting linear expression in $z(\omega)$
            end
        end
        print $M_{\boldsymbol{\lambda}} \succeq 0$
    end
end
//Now $D = \emptyset$.
foreach $\lambda \vdash n$ with height$(\lambda) \leq 2^{\xi}$
    start a new block $M_{\lambda}$
    foreach $\tau \in T^{(\xi)}_{\lambda,2^{\xi}}$ from (6.17) or (6.20)
        foreach $\sigma \in T^{(\xi)}_{\lambda,2^{\xi}}$ from (6.17) or (6.20)
            compute $p_{\tau,\sigma}(F_1)$ in variables $a_P^*$ (with $p_{\tau,\sigma}$ cf. (3.14) and $F_1$ cf. (6.26))
            replace each monomial $\mu(\omega')$ by a variable $z(r'(\omega))$ if $r'(\omega') \in \Omega_4^d$
                and by 0 otherwise
            $(M_{\lambda})_{\tau,\sigma}$ := the resulting linear expression in $z(\omega)$
        end
    end
    if $\lambda = (n)$ //Add a row and a column corresponding to $\emptyset$.
        add a row and column to $M_{\lambda}$ indexed by $\emptyset$
        put $(M_{\lambda})_{\emptyset,\emptyset} := 1$ and the entries $(M_{\lambda})_{\emptyset,\tau}$ and $(M_{\lambda})_{\tau,\emptyset}$ as in (6.27) or (6.29)
    end
    print $M_{\lambda} \succeq 0$
end
//Now nonnegativity of all variables (this includes the cases $|D| = 3$ and $|D| = 4$).
foreach $\omega \in \Omega_4^d$
    print $z(\omega) \geq 0$
end
```

Figure 6.3: Algorithm to generate semidefinite programs for computing $A_4(n, d, w)$ and $B_4(n, d, w)$.

Chapter 7

Uniqueness of codes using semidefinite programming

Writing briefly takes far more
time than writing at length.
— Carl Friedrich Gauss (1777–1855)

For $n, d, w \in \mathbb{N}$, let $A(n, d, w)$ again denote the maximum size of a binary code of word length n, minimum distance d and constant weight w. Schrijver recently showed, using semidefinite programming, that $A(23, 8, 11) = 1288$, and we obtained in Chapter 6 that $A(22, 8, 11) = 672$ and $A(22, 8, 10) = 616$. In this chapter we show uniqueness of the codes achieving these bounds.

Let $A(n, d)$ again denote the maximum size of a binary code of word length n and minimum distance d. Gijswijt, Mittelmann and Schrijver showed that $A(20, 8) = 256$, implying that the quadruply shortened extended binary Golay code is optimal. We show that there are several nonisomorphic codes achieving this bound, and classify all such codes under the additional condition that all distances are divisible by 4.

This chapter is based on joint work with Andries Brouwer [25].

7.1 Introduction

Recall that a binary constant weight w code $C \subseteq \mathbb{F}_2^n$ with $d_{\min}(C) \geq d$ is called an (n, d, w)-code. Moreover, a binary code $C \subseteq \mathbb{F}_2^n$ and $d_{\min}(C) \geq d$ is called an (n, d)-code.

Using semidefinite programming, some upper bounds on $A(n, d, w)$ have recently been obtained that are equal to the best known lower bounds: it has been established that $A(23, 8, 11) = 1288$ (see [81]), and that $A(22, 8, 11) = 672$ and $A(22, 8, 10) = 616$ (see Chapter 6, which is based on [70]). We show using the output of the corresponding semidefinite programs that the constant weight codes codes of maximum size are unique (up to coordinate permutations) for these n, d, w.

For unrestricted (non-constant weight) binary codes, the bound $A(n, d) = A(20, 8) \leq 256$ was obtained by Gijswijt, Mittelmann and Schrijver in [37], implying that the quadruply shortened extended binary Golay code is optimal. The quadruply shortened extended binary Golay code is a linear $(n, d) = (20, 8)$-code of size 256 and has all distances divisible by 4.

Up to equivalence, there is a unique optimum $(24-i,8)$-code of size 2^{12-i}, for $i = 0,1,2,3$, namely the i times shortened extended binary Golay code [20]. We show that the 4 times shortened extended binary Golay code is not the only $(20,8)$-code of size 256. We classify such codes under the additional condition that all distances are divisible by 4, and find that there exist 15 such codes.

7.2 The semidefinite programming upper bound

Following [37, 81] and Chapter 6, we recall semidefinite programming upper bounds on $A(n,d)$ and $A(n,d,w)$. Fix $n,d,w \in \mathbb{N}$ and let N be either $\mathbb{F}_2^n$ or the set of words in $\mathbb{F}_2^n$ of weight w. For $k \in \mathbb{Z}_{\geq 0}$, let $\mathcal{C}_k$ be the collection of codes $C \subseteq N$ with $|C| \leq k$. For any $D \in \mathcal{C}_k$, we define

$$\mathcal{C}_k(D) := \{C \in \mathcal{C}_k \mid C \supseteq D,\ |D| + 2|C \setminus D| \leq k\}. \tag{7.1}$$

Note that then $|C \cup C'| = |C| + |C'| - |C \cap C'| \leq 2|D| + |C \setminus D| + |C' \setminus D| - |D| \leq k$ for all $C, C' \subseteq \mathcal{C}_k(D)$. Furthermore, for any function $x : \mathcal{C}_k \to \mathbb{R}$ and $D \in \mathcal{C}_k$, we define the $\mathcal{C}_k(D) \times \mathcal{C}_k(D)$ matrix $M_{k,D}(x)$ by $M_{k,D}(x)_{C,C'} := x(C \cup C')$, for $C, C' \in \mathcal{C}_k(D)$. Recall the parameter $A_k(n,d,w)$ from (6.2):

$$\begin{aligned} A_k(n,d,w) := \max \big\{ \textstyle\sum_{v \in N} x(\{v\}) \mid x : \mathcal{C}_k \to \mathbb{R}_{\geq 0},\ x(\emptyset) = 1, x(S) = 0 \text{ if } d_{\min}(S) < d, \\ M_{k,D}(x) \succeq 0 \text{ for each } D \text{ in } \mathcal{C}_k \big\}, \end{aligned} \tag{7.2}$$

where N is the set of words in $\mathbb{F}_2^n$ of weight w. (Here $X \succeq 0$ means: X positive semidefinite.) Then $A_k(n,d,w)$ is an upper bound on $A(n,d,w)$. Similarly, one obtains an upper bound $A_k(n,d)$ on $A(n,d)$ by setting $N := \mathbb{F}_2^n$ in (7.2), so that $\mathcal{C}_k$ is the collection of unrestricted (not necessarily constant weight) codes of size at most k. It can be proved that $A_2(n,d)$ and $A_2(n,d,w)$ are equal to the classical Delsarte linear programming bound in the Hamming and Johnson schemes respectively [31].

Remark 7.2.1. In this chapter, we use $A_k(n,d)$ to denote the described bound on $A(n,d)$. It must not be confused with the parameter $A_q(n,d)$ from (2.1).

Let H be the group of distance-preserving permutations of N. In case of constant weight-codes, $H = S_n$, except if $n = 2w$; in this case the group H is twice as large, since then taking complements is also a distance-preserving permutation of N. (Here the *complement* of a word $v \in N$ is the word $v + \mathbf{1}$, where the addition is in $\mathbb{F}_2^n$ and where $\mathbf{1}$ denotes the all-ones word.) In case of non-constant weight codes, $H = S_2^n \rtimes S_n$, where S_2^n denotes the direct product of n copies of S_2.

Let Ω_k be the set of H-orbits of codes in $\mathcal{C}_k$ and let $\Omega_k^d \subseteq \Omega_k$ be those orbits that correspond to codes with minimum distance at least d. By averaging an optimum x over all $g \cdot x$ for $g \in H$, one obtains the existence of a H-invariant optimum solution to (7.2).

The original problem (7.2) is equivalent to the much smaller problem in which the constraint is added that x is H-invariant. We will write $z(\omega)$ for the common value of a H-invariant function x on codes C in orbit ω. Hence, the matrices $M_{k,D}(x)$ become matrices $M_{k,D}(z)$ and we have considerably reduced the number of variables in (7.2). Moreover, a block diagonalization $M_{k,D}(z) \mapsto U_{k,D}^{\mathsf{T}} M_{k,D}(z) U_{k,D}$ can be obtained reducing the sizes of the matrices involved to make the computations in (7.2) tractable (see Chapter 6 and [37, 81] for the reductions).

It can be seen (cf. [37, 70]) that the nonnegativity condition on x, and hence on z, is already implied by the positive semidefiniteness of all matrices $M_{k,D}(x)$. When solving the semidefinite program with a computer, we add separate 1×1 blocks $(z(\omega))$ which are required to be positive semidefinite as constraints (although nonnegativeness of z is already implied by positive semidefiniteness of the matrices $M_{k,D}(x)$). As explained in the next section, this will allow us to easily determine which variables $z(\omega)$ will be necessarily zero in any optimum solution. This may yield necessary conditions on all optimal codes, which may classify the optimal codes, in some cases implying uniqueness.

7.2.1 Information about maximum size codes

Suppose that we have an instance of n, d, w or n, d for which $A_k(n,d,w) = A(n,d,w)$ or $A_k(n,d) = A(n,d)$. We want to obtain information about codes attaining these bounds from the semidefinite programming output. The semidefinite program (7.2) can be written as follows:

$$A_k(n,d,w) = \max \left\{ \sum_{\omega \in \Omega_k^d \setminus \{\{\emptyset\}\}} b_\omega z(\omega) \;\middle|\; M = F_\emptyset - \sum_{\omega \in \Omega_k^d \setminus \{\{\emptyset\}\}} F_\omega z(\omega) \succeq 0 \right\}. \tag{7.3}$$

Here $b_{\omega_0} = |N|$, where $\omega_0 \in \Omega_k^d$ corresponds to the orbit of a code of size 1 in $\mathcal{C}_k$, and $b_\omega = 0$ for all other $\omega \in \Omega_k^d \setminus \{\{\emptyset\}\}$. Moreover, M is a (large) block diagonal matrix that consists of blocks $U_{k,D}^{\mathsf{T}} M_{k,D}(z) U_{k,D}$ (which are reduced versions of the blocks $M_{k,D}(z)$ that are required to be positive semidefinite in (7.2)) and blocks $(z(\omega))$. For each orbit $\omega \in \Omega_k^d \setminus \{\{\emptyset\}\}$, the matrix F_ω is a matrix of the same size as M with entries the coefficients of $-z(\omega)$ in the corresponding entries of M. The matrix $F_\emptyset$ is a matrix of the same size as M with entries the constant coefficients in the corresponding entries of M. Recall that for two real-valued square matrices A, B of the same size, we write $\langle A, B \rangle := \operatorname{tr}(B^{\mathsf{T}} A)$. The dual program of (7.3) then reads

$$\min \left\{ \langle F_\emptyset, X \rangle \;\middle|\; \langle F_\omega, X \rangle = b_\omega \text{ for all } \omega \in \Omega_k^d \setminus \{\{\emptyset\}\},\;\; X \succeq 0 \right\}. \tag{7.4}$$

If (M, z) is any optimum solution for (7.3) and X is an optimum solution for (7.4) with the same values, then $\langle M, X \rangle = 0$. This is called *complementary slackness*. As $M \succeq 0$ and $X \succeq 0$, we have in particular $z(\omega) X_\omega = 0$ for the separate 1×1 blocks $(z(\omega))$ in M and (X_ω) in X, where (X_ω) denotes the 1×1 block in X corresponding to the 1×1 block $(z(\omega))$ in M. Thus

$$\begin{gathered} X_\omega > 0 \text{ in some optimum solution to (7.3)} \\ \Longrightarrow \\ z(\omega) = 0 \text{ in each optimum solution to (7.4).} \end{gathered}$$

If $z(\omega) = 0$ for all solutions to (7.2) with objective value $A_k(n,d,w) = A(n,d,w)$, then for any code C of maximum size there is no subcode $D \subset C$ with $D \in \omega$. (Suppose otherwise; then one constructs a feasible solution to (7.2) by putting $x(S) = 1$ for $S \in \mathcal{C}_k$ with $S \subseteq C$ and $x(S) = 0$ else, and hence by averaging over H there exists a feasible H-invariant solution with $z(\omega) > 0$, a contradiction.) So orbit ω does not appear in any code of maximum size. Hence we can identify some orbits $\omega \in \Omega_k^d$ that cannot occur in any code of maximum size. We will call these orbits *forbidden orbits*.

We used the solver SDPA-GMP [61, 96] to conclude which orbits are forbidden. The semidefinite programming solver does not produce exact solutions, but approximations up to a certain precision. In our case the approximations are precise enough to verify (with certainty) that certain orbits are forbidden. See the appendix for details.

7.3 Self-orthogonal codes

If $u, v \in \mathbb{F}_2^n$, we define $(u \cap v) \in \mathbb{F}_2^n$ to be the word that has 1 at position i if and only if $u_i = v_i = 1$. The following easy equality is well-known and will be used often throughout this chapter:

$$d_H(u, v) = \mathrm{wt}(u) + \mathrm{wt}(v) - 2\,\mathrm{wt}(u \cap v), \quad \text{for all } u, v \in \mathbb{F}_2^n. \tag{7.5}$$

The function $(u, v) \mapsto \mathrm{wt}(u \cap v) \pmod 2$ is a non-degenerate symmetric $\mathbb{F}_2$-bilinear form on $\mathbb{F}_2^n$. If $(u, v) = 0$, then u and v are called *orthogonal*. A code C is *self-orthogonal* if $(u, v) = 0$ for all $u, v \in C$. Given a code $C \subseteq \mathbb{F}_2^n$, the *dual code* $C^\perp$ is the set of all $v \in \mathbb{F}_2^n$ that are orthogonal to all $u \in C$. A code C is called *self-dual* if $C = C^\perp$. For small n, self-dual codes are classified by Pless and Sloane [66].

7.4 Constant weight codes

With semidefinite programming three exact values of $A(n, d, w)$ have been obtained. In [81], it is found that $A_3(23, 8, 11) \le 1288$, matching the known lower bound and thereby proving that $A(23, 8, 11) = 1288$. Similarly, in Chapter 6 (which is based on [70]), the upper bounds $A(22, 8, 10) \le 616$ and $A(22, 8, 11) \le 672$ are obtained, which imply $A(22, 8, 10) = 616$ and $A(22, 8, 11) = 672$. The latter two upper bounds are in fact instances of the bound $B_4(n, d, w)$ defined in (6.3), which is a bound (not necessarily strictly) in between $A_3(n, d, w)$ and $A_4(n, d, w)$.

Definition 7.4.1 ($B_4(n, d, w)$)**.** The bound $B_4(n, d, w)$ from (6.3) is defined by replacing in the definition of $A_4(n, d, w)$ from (7.2) the matrix $M_{4,\emptyset}(x)$ by (the much smaller matrix) $M_{2,\emptyset}(x|_{\mathcal{C}_2})$.

In this section we show that the codes attaining these bounds are unique up to coordinate permutations, using the information about forbidden orbits obtained from the semidefinite programming output. In order to prove uniqueness of the $(23, 8, 11)$-code of maximum size, we start by proving uniqueness of the $(24, 8, 12)$-code of maximum size. The uniqueness of this code can already be obtained from the classical linear programming bound by complementary slackness. Recall that the *distance distribution* $(a_i)_{i=0}^n$ of a code $C \subseteq \mathbb{F}_2^n$ is the sequence given by

$$a_i := |C|^{-1} \cdot |\{(u, v) \in C \times C \mid d_H(u, v) = i\}|, \quad \text{for } i = 0, \ldots, n.$$

The complementary slackness based on computational results that we used to conclude uniqueness of the mentioned codes, is displayed (in (7.6), (7.7), (7.8) and (7.9) below) at the beginning of each proof.

7.4.1 $A(24, 8, 12)$

Proposition 7.4.2. *Up to coordinate permutations there is a unique* $(24, 8, 12)$*-code of size* 2576*. It is given by the set of words of weight* 12 *in the extended binary Golay code.*

Proof. Let C be a $(24, 8, 12)$-code of size 2576. The classical Delsarte linear programming bound in the Johnson scheme (which is equal to $A_2(n, d, w)$) gives maximum 2576. Moreover, one has by complementary slackness,[1]

$$a_i = 0 \text{ for } \ i \notin \{0, 8, 12, 16, 24\}. \tag{7.6}$$

To derive uniqueness, consider the $\mathbb{F}_2$-linear span $F := \langle C \rangle$ of C. Note that C (by (7.6)), hence F, is self-orthogonal. So $|F| \leq 2^{24/2} = 2^{12}$. Since $|F| \geq |C| > 2^{11}$ and since F is linear, we must have $|F| = 2^{12}$. So F is self-dual. Let $u \in F$, $u \neq 0$. The sets $\{u + x \mid x \in C\} \subseteq F$ and $C \subseteq F$ have non-empty intersection, because both sets have size $2576 > |F|/2$. So $u + x = y$ for some $x, y \in C$. But then $\text{wt}(u) = d_H(x, y) \geq 8$, as C has minimum distance 8. It follows that F has minimum distance 8, and we conclude that F is the extended binary Golay code. So C is the set of weight 12 words in the extended binary Golay code. □

7.4.2 $A(23, 8, 11)$

Proposition 7.4.3. *Up to coordinate permutations there is a unique* $(23, 8, 11)$*-code of size* 1288*. It is given by the set of words of weight* 11 *in the binary Golay code.*

Proof. Let C be a $(23, 8, 11)$-code of size 1288. With the solution of the semidefinite program $A_3(23, 8, 11)$ (which is 1288) from [81] one obtains, by considering the forbidden orbits from the semidefinite programming output:[2]

$$\text{if } x, y \in C \text{ then } d_H(x, y) \leq 16. \tag{7.7}$$

Construct a code D of length 24, weight 12 and size 2576 as follows: add a symbol 1 to every codeword of C, put it in D and put also the complement of the resulting word in D. Then D has minimum distance 8 by (7.7). Hence D is the set of weight 12 words in the extended Golay code F, by Proposition 7.4.2. The automorphism group of the extended binary Golay code acts transitively on the coordinate positions [55]. Hence, C is the set of weight 11 words in the binary Golay code. □

7.4.3 $A(22, 8, 11)$

Proposition 7.4.4. *Up to coordinate permutations there is a unique* $(22, 8, 11)$*-code of size* 672.

[1] We used SDPA-GMP to solve this LP. The approximate dual solution allows us, with a computation similar to the computation in the Appendix in (7.14)-(7.18) below, to give a very small $\varepsilon > 0$ such that in any optimum solution, $a_i < \varepsilon$ for $i \notin \{0, 8, 12, 16, 24\}$. But if $a_i > 0$ for some $(n, d, w) = (24, 8, 12)$-code C with $|C| = 2576$, then for this code $a_i \geq 2/2576$, by definition of the distance distribution of C. Since $\varepsilon < 10^{-90} < 2/2576$ for $i \notin \{0, 8, 12, 16, 24\}$ it follows that $a_i = 0$ for any $(24, 8, 12)$-code C of size 2576.

[2] Note that the LP does not give this information: the Delsarte bound is 1417, which is not optimal.

Proof. Let C be a $(22, 8, 11)$-code of size 672. First one concludes that $a_{14} = 0$ using the semidefinite program $B_4(22, 8, 11)$ from [70]. This is explained in more detail in the appendix: if $a_{14} > 0$, then $a_{14} \geq 2/672$ and $a_{10} + a_{14} + a_{18} + a_{22} \geq 318/672$ (by Proposition 7.6.2 below). We add these two constraints to the program $B_4(22, 8, 11)$. The resulting bound is strictly smaller than 672, so $a_{14} = 0$ in any $(22, 8, 11)$-code of size 672.

Subsequently, by considering the forbidden orbits in the solution of the semidefinite program $A_3(22, 8, 11)$ from [81] with the added constraint that $a_{14} = 0$ (the solution of $A_3(22, 8, 11)$ with this added constraint is 672) one obtains:

$$\text{if } x, y, z \in C \text{ then } d_H(x, y) \in \{0, 8, 12, 16\} \text{ and } \mathrm{wt}(x + y + z) \in \{7, 11, 15\}. \tag{7.8}$$

Let D be the collection of $672 + 672 = 1344$ codewords of length 24 of the form $10x$ with $x \in C$ together with their complements, and let $F := \langle D \rangle$ be the $\mathbb{F}_2$-linear span of D. All distances in D belong to $\{8, 12, 16\}$ by (7.8), so D, and hence also F, is self-orthogonal, which implies $|F| \leq 2^{24/2} = 2^{12}$. Since all words in D have weight divisible by 4 and F is self-orthogonal, all words in F also have weight divisible by 4.

The code F contains words of forms $01x$, $10y$, $11z$ and $00u$. Each form occurs at least 672 times, so $|F| \geq 4 \cdot 672 > 2^{11}$, hence $|F| = 2^{12}$ and F is self-dual.

To show that F is the extended binary Golay code, it suffices to prove that all words in F have weight ≥ 8, i.e., that no word in F has weight 4. Words of F are sums of words $10x$ with $x \in C$, possibly together with the all-ones word. So we must prove that sums of words $10x$ do not have weight 4 or 20. A sum of words $10x$ starts with 00 or 10 and is the sum of an even or odd number of words $10x$, respectively.

Words in F starting with 00 form a subcode F_{00} of F of size $2^{10} = 1024$. If $u \in F_{00}$, then $\{u + 10y \mid y \in C\} \cap \{10x \mid x \in C\} \neq \emptyset$, as there are 1024 words in F starting with 10 but $|C| = 672 > 1024/2$. So $u = 10x + 10y$ for some $x, y \in C$, hence $F_{00} = \{10x + 10y \mid x, y \in C\}$. However, distances 4 and 20 do not occur in C, so words in F_{00} do not have weight 4 or 20.

The 1024 words in F starting with 10 are formed by the coset $10x + F_{00}$ (with $x \in C$ arbitrary but fixed) and hence are a sum of three elements of the form $10x$ with $x \in C$. But such a sum has weight 8, 12 or 16 by (7.8), implying that words in F starting with 10 do not have weight 4 or 20.

Therefore weights 4 and 20 do not appear in F, so F is indeed the extended binary Golay code. As the automorphism group of the extended binary Golay code F acts 2-transitively on the coordinate positions [55], this implies that C is unique. □

7.4.4 $A(22, 8, 10)$

Proposition 7.4.5. *Up to coordinate permutations there is a unique* $(22, 8, 10)$*-code of size* 616.

Proof. Let C be a $(22, 8, 10)$-code of size 616. First one concludes that $a_{14} = 0$ using the semidefinite program $B_4(22, 8, 10)$ from [70]. This is explained in more detail in the appendix: if $a_{14} > 0$, then $a_{14} \geq 2/616$ and $a_{10} + a_{14} + a_{18} \geq 208/616$ (by Proposition 7.6.1 below). We add these two constraints to the program $B_4(22, 8, 10)$. The resulting bound is strictly smaller than 616, so $a_{14} = 0$ in any $(22, 8, 10)$-code of size 616.

Subsequently, by considering the forbidden orbits in the solution of the semidefinite program $A_3(22, 8, 10)$ from [81] with the added constraint that $a_{14} = 0$ (the solution of

$A_3(22, 8, 10)$ with this added constraint is 616) one obtains:

$$\text{if } x, y, z \in C \text{ then } d_H(x, y) \in \{0, 8, 12, 16\} \text{ and } \operatorname{wt}(x + y + z) \in \{6, 10, 14, 22\}. \tag{7.9}$$

Let $F := \langle C\rangle$. Since C is self-orthogonal and has words of weights divisible by 2 but not by 4, F is self-orthogonal and has half of the weights divisible by 4 and half of the weights divisible by 2 but not by 4. Both halves of F have size $\geq |C| = 616$, but F has size ≤ 2048 as it is self-orthogonal. So $|F| = 2048$ and F is self-dual.

Let $E \subseteq F$ be the subcode of F consisting of all words with weight divisible by 4. For each $u \in E$, we have $C \cap \{u + y \,|\, y \in C\} \neq \emptyset$ (as $|C| = 616 > 1024/2$), so $u = x + y$ for some $x, y \in C$. Hence $E = \{x + y \,|\, x, y \in C\}$. By (7.9), no word in E has weight 4. So weight 4 does not occur in F.

If any word u in F has weight 2 then it is in $F \setminus E = x + E$ (with $x \in C$ arbitrary). So it is the sum of three words in C. But such sums do not have weight 2 by (7.9), hence no word in F has weight 2. So F is a self-dual code of minimum distance 6. As the self-dual $(n, d) = (22, 6)$-code is unique (cf. [66]), F is unique. Hence also C is unique, as it is the collection of weight 10 words of F. (Note that two weight 10 words in F have distance 0 (mod 4), so distance at least 8, since $d_H(u, v) = \operatorname{wt}(u) + \operatorname{wt}(v) - 2\operatorname{wt}(u \cap v)$ for any two words $u, v \in F$.) □

7.5 The quadruply shortened binary Golay code

Recently, Gijswijt, Mittelmann and Schrijver [37] proved that $A(20, 8) = 256$, with the semidefinite program $A_4(n, d)$ from (7.2). An example of a code attaining this bound is the four times shortened extended binary Golay code, which has distance distribution

$$a_0 = 1,\ a_8 = 130,\ a_{12} = 120,\ a_{16} = 5,\ a_i = 0 \text{ for all other } i. \tag{7.10}$$

This code is formed by the words starting with 0000 in the extended binary Golay code with these first four coordinate positions removed.

Recall that two binary codes $C, D \subseteq \mathbb{F}_2^n$ are *equivalent* if D can be obtained from C by first permuting the n coordinates and by subsequently permuting the alphabet $\{0, 1\}$ in each coordinate separately.

Up to equivalence there are unique $(24 - i, 8)$-codes of size 2^{12-i} for $i = 0, 1, 2, 3$, namely the i times shortened extended binary Golay codes [20]. In this section we show that there exist several nonisomorphic $(20, 8)$-codes of size 256. First we show that there exist such codes with different distance distributions. Subsequently we classify such codes under the additional condition that all distances are divisible by 4.

We start by recovering information about possible distance distributions from the semidefinite program $A_4(20, 8)$. Write $\omega_t \in \Omega_4$ for the orbit of two words at Hamming distance t. From a code C with distance distribution (a_i), one constructs a feasible solution to (7.2) by putting $x(S) = 1$ for $S \in \mathcal{C}_k$ with $S \subseteq C$ and $x(S) = 0$ else, and hence by averaging over H one obtains a feasible H-invariant solution with variables $z(\omega)$. This solution has

$$\begin{aligned} z(\omega_t) &= \frac{1}{|H|}\sum_{g\in H} g \cdot x(\{y_1, y_2\}) = \frac{t!(20-t)!}{|H|}|\{(u, v) \in C^2 \ :\ d_H(u, v) = t\}| \\ &= \frac{|\{(u, v) \in C^2 \ :\ d_H(u, v) = t\}|}{2^{20}\binom{20}{t}} = \frac{|C|a_t}{2^{20}\binom{20}{t}}, \end{aligned}$$

where $\{y_1, y_2\}$ is any pair of words with distance t and $H = S_2^{20} \rtimes S_{20}$. So we can add linear constraints on the a_i as linear constraints on the variables $z(\omega_t)$ to our semidefinite program.

The distance distribution (a_i) is not determined uniquely by the requirement that the sequence $(z(\omega))_{\omega\in\Omega_4}$ is an optimal solution of the semidefinite program $A_4(20, 8)$ (from (7.2) and (7.3)).[3] We find minimum possible values for some of the a_i for the case where all distances are even as follows. For any code C, the a_i $(i \neq 0)$ are integer multiples of $2/|C|$. So for any $(20, 8)$-code of size 256,

$$\text{if } a_{16} < 1 \text{ then } a_{16} \leq 254/256.$$

With the constraint $a_{16} \leq 254/256$ the semidefinite program returns an objective value strictly smaller than 256. So $a_{16} \geq 1$. Similarly, we find $a_8 \geq 126$ and $a_{12} \geq 96$. If we simultaneously add the constraints $a_8 \leq 126$, $a_{12} \leq 96$ and $a_{16} \leq 1$, the semidefinite program returns 256 as objective value, and the values of $z(\omega_{10})$ and $z(\omega_{14})$ force $a_{10} = a_{14} = 16$. Therefore, apart from the 4 times shortened extended binary Golay code, also a code with

$$a_1 = 1,\ a_8 = 126,\ a_{10} = 16,\ a_{12} = 96,\ a_{14} = 16,\ a_{16} = 1,\ a_i = 0 \text{ for all other } i, \tag{7.11}$$

is allowed by the program $A_4(20, 8)$. Such a code exists, as the following construction demonstrates.

Start with the extended binary Golay code F containing the weight 8 word u with all 1s in the first eight positions. As $A(24 - 8, 8) = A(16, 8) = 32$ (see [21]), there can be at most 32 words in F starting with 8 zeros. These form a linear subcode E of F. As any word in F has an even number of 1s at the first eight positions, there are at most $2^7 = 128$ distinct cosets $E + v$ in F. As $32 \cdot 128 = 2^{12} = |F|$ it follows that $|E| = 32$ and there are exactly 128 distinct cosets $E + v$.

So if we specify a string of 8 symbols with an even number of ones and take all words in F having these 8 fixed symbols in the first 8 positions, we obtain a subcode D of F of size 32 and minimum distance at least 8. Choose the following 8 specifications, each giving a subcode D of size 32 and minimum distance 8.

$$\begin{array}{l} 00000000\\ 11000000\\ 10100000\\ 10010000\\ 10001000\\ 10000100\\ 10000010\\ 10000001 \end{array} \quad \text{and then replace the first 8 coordinates by} \quad \begin{array}{l} 0000\\ 1100\\ 1010\\ 1001\\ 0110\\ 0101\\ 0011\\ 1111 \end{array}.$$

This yields a $(20, 8)$-code of size $8 \cdot 32 = 256$ in which distances 10 and 14 occur. Note that this code indeed has minimum distance at least 8: first observe that each code D has minimum distance at least 8. Then note that for two different specifications the first

[3] By contrast, in all constant weight cases considered in this chapter, the values of the $z(\omega_t)$ give the unique distance distribution of the (unique up to coordinate permutations) (n, d, w)-codes of maximum size.

part (the first 8 positions) had distance at most 2 before the replacement, so the second part has distance at least 6. After the replacement of the first part, the first 4 positions have distance at least 2, so two words obtained from different specifications have, after the replacement, in total distance at least $2+6=8$. One verifies by computer that its distance distribution is given by (7.11). So, there exist $(20,8)$-codes of maximum size with distance distribution (7.10) as well as with (7.11).

7.5.1 Unrestricted $(20,8)$-codes of maximum size with all distances divisible by 4

In this section we give a classification of the $(20,8)$-codes of size 256 with all distances divisible by 4. An example of such a code is the quadruply shortened extended binary Golay code B, which is linear. There is, up to equivalence, only one such code, since the automorphism group of the extended Golay code acts 5-transitively on the coordinate positions [20]. (Moreover, Dodunekov and Encheva [33] have proved that there exists, up to equivalence, only one *linear* $(20,8)$-code of size 256.) The quadruply shortened extended binary Golay code contains 5 words of weight 16, forming a subcode D. Since the minimum distance is 8, each of those words must have the 0's at different positions. So we can assume that

$$D = \begin{array}{l} 00001111111111111111 \\ 11110000111111111111 \\ 11111111000011111111, \\ 11111111111100001111 \\ 11111111111111110000 \end{array} \tag{7.12}$$

with linear span $\langle D\rangle \subseteq B$ of dimension 4. So B is a union of 16 cosets $u+\langle D\rangle$. If we replace a coset $u+\langle D\rangle$ by its complement $\mathbf{1}+u+\langle D\rangle$, we obtain another $(20,8)$-code of maximum size that is not linear, so this is really a different code. Note that all distances remain divisible by —but not equal to— 4, as $d_H(x,y) \in \{8,12\}$ for any $x \in u+\langle D\rangle$ and $y \in B\setminus(u+\langle D\rangle)$, so $d_H(\mathbf{1}+x,y) \in \{8,12\}$. By replacing any of the 16 cosets $u+\langle D\rangle$ in B with $\mathbf{1}+u+\langle D\rangle$, we obtain $2^{16}=65536$ codes with all distances divisible by 4.

In this section we will first prove that any maximum-size $(20,8)$-code with all distances divisible by 4 is equivalent to one of the 2^{16} thus obtained codes. Secondly, we will obtain (by computer) that these 2^{16} codes can be partitioned into 15 equivalence classes.

In order to prove the first result, we start by proving two auxiliary propositions. Let C be any $(20,8)$-code of size 256 with all distances divisible by 4 and containing $\mathbf{0}$, the zero word. Define $E := \langle C\cup\{\mathbf{1}\}\rangle$ to be the linear span of C together with the all-ones vector.

Proposition 7.5.1. *Up to a permutation of the coordinate positions, the codes E and $\langle B\cup\{\mathbf{1}\}\rangle$ are the same.*

Proof. After the constraints $a_i=0$ if $4\nmid i$ and $a_{20}\geq 2/256$ are added to the Delsarte bound for $(n,d)=(20,8)$, the linear program (LP) returns a solution strictly smaller than 256. Therefore $a_{20}=0$ in any $(20,8)$-code of size 256 with all distances divisible by 4. As $A(20,8,8)=130$ (cf. [22]) and $A(20,8,4)=\lfloor 20/4\rfloor=5$, one has $a_8\leq 130$ and $a_{16}\leq 5$. Moreover, the LP-bound contains the inequalities $a_8-a_{12}-3a_{16}+5\geq 0$

and $-a_8 - a_{12} + 31a_{16} + 95 \geq 0$ (given that $a_{20} = 0$). We add those two equations and use that $a_{16} \leq 5$ to obtain that $a_{12} \leq 120$. As $256 = 1 + a_8 + a_{12} + a_{16}$, the distance distribution of any $(20, 8)$-code of size 256 with all distances divisible by 4 is given by (7.10). Moreover, the values in (7.10) are not mere averages: as $A(20, 8, 8) = 130$ and $A(20, 8, 4) = 5$, the number of words at distance i from *any* word $u \in C$ is specified by (7.10).

Since C is self-orthogonal and has all distances divisible by 4, also E is self-orthogonal and has all distances divisible by 4. Furthermore, E has dimension 9. To see this, note that $\mathbf{1} \notin C$ since $a_{20} = 0$, so $|E| \geq 257$, so $|E| \geq 512$. On the other hand, $\dim E < 10$, as E is self-orthogonal with all distances divisible by 4, but there does not exist a self-dual code of length 20 with all distances divisible by 4 (cf. [65]). So $\dim E = 9$ and $|E| = 512$, implying that

$$\text{for every word } u \in E \text{ one has } u \in C \text{ or } \mathbf{1} + u \in C. \tag{7.13}$$

For any code we write A_i for the number of words of weight i. Since C has weights $A_0 = 1$, $A_8 = 130$, $A_{12} = 120$, $A_{16} = 5$, we conclude that E has weights

$$A_0 = 1,\ A_4 = 5,\ A_8 = 250,\ A_{12} = 250,\ A_{16} = 5,\ A_{20} = 1.$$

The orthogonal complement $E^\perp$ of E has dimension 11, and is a union $E \cup (a + E) \cup (b + E) \cup (c + E)$. Here a, b, c have even weight (because $\mathbf{1} \in E$), so each of $\langle \{a\} \cup E \rangle$ and $\langle \{b\} \cup E \rangle$ and $\langle \{c\} \cup E \rangle$ is self-dual. This means that a, b, c are mutually non-orthogonal.

Look at Pless [65] to find the self-dual codes of length $n = 20$ and dimension 10. There are 16 such codes, but we can forget about those with $A_8 < 250$. There is a unique self-dual code of length $n = 20$ and dimension 10 with $A_8 \geq 250$, namely M_{20} with weight enumerator

$$A_0 = 1,\ A_4 = 5,\ A_6 = 80,\ A_8 = 250,\ A_{10} = 352,\ A_{12} = 250,\ A_{14} = 80,\ A_{16} = 5,\ A_{20} = 1,$$

and E is the subcode of M_{20} consisting of the words of weight divisible by 4, hence is unique. This means that E does not depend on the particular choice of C (up to a permutation of the coordinates), proving the desired result. □

Proposition 7.5.2. *Let C be any $(20, 8)$-code of size 256 with all distances divisible by 4 containing $\mathbf{0}$. Then C is invariant under translations by weight 16 words from C.*

Proof. Clearly, if $a, b, c \in \mathbb{F}_2^{20}$ with $\mathrm{wt}(a) = 16$ and $a + b + c = \mathbf{1}$, then $d_H(b, c) = 4$. Now let $b \in C$ be arbitrary, and $a \in C$ a weight 16 vector. Then we have $a + b + c \neq \mathbf{1}$ for all $c \in C$. So $\mathbf{1} + a + b \notin C$ while $\mathbf{1} + a + b \in \langle C \cup \{\mathbf{1}\} \rangle$. Hence, $a + b \in C$, by (7.13). So indeed, C is invariant under translations by weight 16 words from C. (This in particular implies that C contains the 4-dimensional linear span of the weight 16 vectors.) □

Fix representatives $u_1, \ldots, u_{16}$ for the cosets $u_i + \langle D \rangle$ of the linear quadruply shortened binary extended Golay code B (see Table 7.1 for a possible choice). Using Propositions 7.5.1 and 7.5.2, we obtain the first main result of this section.

Proposition 7.5.3. *Let C be any $(20, 8)$-code of size 256 with all distances divisible by 4. Then C is equivalent to B with some of the cosets $u_i + \langle D \rangle$ replaced by $\mathbf{1} + u_i + \langle D \rangle$.*

Proof. We may assume, by applying a distance-preserving permutation to C, that C contains $\mathbf{0}$ and that $\langle C \cup \{\mathbf{1}\}\rangle = \langle B \cup \{\mathbf{1}\}\rangle$ (by Proposition 7.5.1). Then C contains 5 weight 16 vectors of the form (7.12). By Proposition 7.5.2, the code C is a union of 16 cosets $u + \langle D\rangle$, for some vectors u. The code $\langle B \cup \{\mathbf{1}\}\rangle = \langle C \cup \{\mathbf{1}\}\rangle$ is a union of cosets $u_i + \langle D\rangle$ together with their complements $\mathbf{1} + u_i + \langle D\rangle$. This implies by (7.13) that each coset of C has the form $u_i + \langle D\rangle$ or $\mathbf{1} + u_i + \langle D\rangle$ (and C cannot contain both u_i and $\mathbf{1} + u_i$ at the same time as $a_{20} = 0$), as required. □

Coset representative	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}
$u_1 = 00000000000000000000$		1	1	1	1	1	1	1	1	1				1	
$u_2 = 00000101010101011010$			1	1	1	1	1	1	1	1	1	1	1		1
$u_3 = 00001001011001101100$				1	1		1			1	1	1	1	1	
$u_4 = 00001100001100110110$					1						1				1
$u_5 = 10100000010101101001$						1	1	1	1	1	1	1	1		
$u_6 = 10100101000000110011$								1				1		1	1
$u_7 = 10101001001100000101$									1				1	1	1
$u_8 = 10101100011001011111$															
$u_9 = 11000000011000110101$										1	1	1	1	1	1
$u_{10} = 11000101001101101111$													1	1	1
$u_{11} = 11001001000001011001$															
$u_{12} = 11001100010100000011$															
$u_{13} = 01100000001101011100$															
$u_{14} = 01100101011000000110$															
$u_{15} = 01101001010100110000$															
$u_{16} = 01101100000001101010$															

Table 7.1: The $(20, 8)$-codes of size 256 with all distances divisible by 4. The quadruply shortened extended binary Golay code $B = C_1$ is the union $\cup_{i=1}^{16}(u_i + \langle D\rangle)$. The other codes C_j $(j = 2, \ldots, 15)$ are obtained from B by replacing the coset $u_i + \langle D\rangle$ by $\mathbf{1} + u_i + \langle D\rangle$ if there is a 1 in entry (u_i, C_j) in the above table.

It remains to classify the $2^{16} = 65536$ codes obtained from B by replacing some of the cosets $u_i + \langle D\rangle$ by $\mathbf{1} + u_i + \langle D\rangle$. For this we use the graph isomorphism program `nauty` [60]. For any code C of word length n containing m codewords, a graph with $2n+m$ vertices is created: one vertex for each codeword $u \in C$ and two vertices 0_i and 1_i for each coordinate position. Each code word u has neighbor 0_i if $u_i = 0$ and 1_i if $u_i = 1$ $(i = 1, \ldots, n)$. Moreover, there are edges $\{0_i, 1_i\}$ $(i = 1, \ldots, n)$.

All code words have degree n and the coordinate positions have (in this case) larger degree. An automorphism of this graph permutes the codewords and permutes the coordinate positions. In this way one finds a subgroup of $S_2^n \rtimes S_n$ that fixes C and the question of code equivalence is transformed into a question of graph isomorphism. With the program `nauty` we compute a canonical representative for each of the 2^{16} mentioned codes. In this way we find that the 2^{16} codes from Proposition 7.5.3 can be partitioned into 15 equivalence classes. See Table 7.1 for the classification.

Proposition 7.5.4. *There are* 15 *different* $(20, 8)$*-codes of size* 256 *with all distances divisible by* 4 *up to equivalence.* □

7.6 Appendix: Approximate solutions

The semidefinite programming solver does not produce exact solutions, but approximations up to a certain precision. Here we show that we have enough precision to conclude (7.7), (7.8) and (7.9).

Let (M, z) be feasible for (7.3) with optimum value at least $A(n, d, w)$ and suppose that X is an approximation of the dual program. That is, we have $X \succeq 0$[4] and for all $\omega \in \Omega_k^d \setminus \{\{\emptyset\}\}$:

$$\langle X, F_\omega \rangle = b_\omega + \epsilon_\omega, \tag{7.14}$$

for small ϵ_ω. Consider one particular $\omega \in \Omega_k^d \setminus \{\{\emptyset\}\}$. There is a 1×1 block $(z(\omega))$ in M and hence also a corresponding 1×1 block (X_ω) in X. Remove these 1×1 blocks from M and X and call the resulting matrices M' and X'. Then

$$\begin{aligned} 0 \leq \langle M', X' \rangle &= \langle M, X \rangle - z(\omega) X_\omega \\ &= \langle F_\emptyset, X \rangle - \sum_{\omega \in \Omega_k^d \setminus \{\{\emptyset\}\}} z(\omega) b_\omega + \sum_{\omega \in \Omega_k^d \setminus \{\{\emptyset\}\}} z(\omega)\epsilon_\omega - X_\omega z(\omega), \end{aligned} \tag{7.15}$$

as M' and X' are positive semidefinite, where we used (7.14) and the definition of M from (7.4) in the second equality. Note that $\sum_{\omega \in \Omega_k^d \setminus \{\{\emptyset\}\}} z(\omega) b_\omega$ is bounded from below by $|C|$, and each $z(\omega)$ is bounded from above by $z(\omega_0)$ (this can be done since all 2×2 principal submatrices in the semidefinite program (7.3) are positive semidefinite), which is bounded from above by 1. Hence

$$X_\omega z(\omega) \leq \langle F_\emptyset, X \rangle - |C| + \sum_{\omega \in \Omega_k^d \setminus \{\{\emptyset\}\}} \epsilon_\omega. \tag{7.16}$$

The numbers ϵ_ω are easily calculated from the dual solution, just as the dual approximate objective value $\langle F_\emptyset, X \rangle$. So we find a constant c_ω from the semidefinite programming dual approximation X such that

$$X_\omega z(\omega) \leq c_\omega. \tag{7.17}$$

In the case of $A(23, 8, 11)$ one can conclude with the semidefinite program $A_3(23, 8, 11)$, which can be solved with SDPA-GMP [61, 96] within minutes, that

$$z(\omega) \leq 10^{-90} \tag{7.18}$$

for all orbits corresponding to codes not satisfying (7.7). Let ω be an orbit for which (7.18) holds. If there exists a code C of maximum size containing a subcode $D \subset C$ with $D \in \omega$, then one constructs a feasible solution to (7.2) by putting $x(S) = 1$ for $S \in \mathcal{C}_k$ with $S \subseteq C$ and $x(S) = 0$ else, and hence by averaging over H there exists a feasible H-invariant solution with $z(\omega) \geq 1/|H|$ (this lower bound is not best possible, but sufficient). In our case, $H = S_{23}$, so $z(\omega) \geq 1/23! > 10^{-23}$, which gives a contradiction with (7.18). In this way, one verifies that all orbits not satisfying (7.7) are forbidden, thereby establishing (7.7). We used a separate java program to check that $X \succeq 0$ (in fact, $X \succ 0$) and to compute the error terms as in (7.14) and (7.16).

[4] We used a separate java program to verify that $X \succeq 0$ (in fact, $X \succ 0$) in the SDP-outputs used in this chapter.

Next, we consider the cases $A(22,8,10) = 616$ and $A(22,8,11) = 672$. First we assume that $a_{14} = 0$ for all maximum-size $(22,8,10) = 616$ and $(22,8,11)$-codes C. We write ω_t for the orbit of two words at Hamming distance t. Adding the constraint $z(\omega_{14}) = 0$ to the programs $A_3(n,d,w)$ for these two cases of n,d,w gives $A_3(n,d,w) = A(n,d,w)$. In this way one shows, in the same way as in the previous paragraph, that all orbits not satisfying (7.8) and (7.9) are forbidden, provided that $a_{14} = 0$. So in order to establish (7.8) and (7.9), it remains to prove that

$$\text{if } C \text{ is a maximum-size } (22,8,10)\text{- or } (22,8,11)\text{-code, then } a_{14} = 0. \tag{7.19}$$

Suppose to the contrary that C is a code as in (7.19), yet $a_{14} > 0$. Then $a_{14} \geq 2/|C|$. We will show that this is not possible by adding constraints to the (large) program $B_4(n,d,w)$. The semidefinite program will then give $\lfloor B_4(n,d,w) \rfloor < A(n,d,w)$ and we will arrive at a contradiction, as $B_4(n,d,w)$ is an upper bound for $A(n,d,w)$. To find a better lower bound on some of the a_i, we use the following two propositions. We use in both propositions that for two words u,v in a constant weight w code C,

$$d_H(u,v) \equiv 2 \pmod 4 \iff \mathrm{wt}(u \cap v) \not\equiv w \pmod 2, \tag{7.20}$$

which follows from (7.5). In the next two propositions we will call $\mathrm{wt}(u \cap v)$ the *inner product* of u and v.

Proposition 7.6.1. *Let C be a $(22,8,10)$-code of size 616 with $a_{14} \geq 2/616$. Then $a_{10} + a_{14} + a_{18} \geq 208/616$.*

Proof. Suppose that $a_{10} + a_{14} + a_{18} < 208/616$ (note that $a_{22} = 0$ as two weight 10 words cannot have distance 22). Then, by (7.20), there are at most $206/2 = 103$ pairs of words in C with odd inner product. Let $\{b, b'\} \subseteq C$ be such a pair of words. Starting with $b \in C$, and greedily picking vectors $d \in C$ such that the inner product of d with the already chosen vectors is even, we end with a self-orthogonal subcode B of C of size $\geq 616 - 103 = 513$. Starting with b', we repeat the same process to end up with a self-orthogonal subcode B' of C (containing b') of size ≥ 513. Furthermore, $D := B \cap B'$ has $|D| \geq 512$. (To see this, note that $b, b' \notin D$ with odd inner product. Every word $v \in C \setminus (D \cup \{b, b'\})$ has odd inner product with some word in C so there are at most $103 - 1 = 102$ of such words v, as b, b' is already a pair with odd inner product.) Write $F := \langle D \rangle$. Then F is self-orthogonal, as D is self-orthogonal.

Since $\langle B \rangle$ and $\langle B' \rangle$ are self-orthogonal codes, they have dimension at most 11. Since $\langle B \rangle \neq \langle B' \rangle$, as $b \notin \langle B' \rangle$, we have $\dim F = \dim \langle B \cap B' \rangle \leq \dim(\langle B \rangle \cap \langle B' \rangle) \leq 10$. On the other hand, we have $|F| > 512$ (as $D \subseteq F$ and the zero word is contained in F). So $\dim F = 10$. Moreover, F has minimum distance 8. To see this, let u be any nonzero word in $F \setminus D$. Then $D \cap (u + D) \neq \emptyset$, as both D and $u + D$ have size 512 and are contained in $F \setminus \{\mathbf{0}\}$, a set of size 1023. So u is the sum of two words of D, and hence has weight at least 8 (as D has minimum distance at least 8).

So F is a self-orthogonal code of word length 22, dimension 10 and minimum distance 8. Such a code is the twice shortened extended binary Golay code (see [20]), which does not contain words of weight 10. But all words in $D \subseteq F$ have weight 10, a contradiction. □

Proposition 7.6.2. *Let C be an $(22,8,11)$-code of size 672 with $a_{14} \geq 2/672$. Then $a_{10} + a_{14} + a_{18} + a_{22} \geq 318/672$.*

Proof. Suppose that $a_{10} + a_{14} + a_{18} + a_{22} < 318/616$. Then, by (7.20), there are at most $316/2 = 158$ pairs of words in C with even inner product. Let $\{b, b'\} \subseteq C$ be such a pair of words. Starting with $b \in C$, and greedily picking vectors $d \in C$ such that the inner product of d with the already chosen vectors is odd, we end with a subcode B of C of size $\geq 672 - 158 = 514$. Now, add an extra symbol 1 to every codeword in B, to obtain a self-orthogonal code D of length 23. As D is self-orthogonal, $\dim\langle D\rangle \leq \lfloor 23/2 \rfloor = 11$.

Starting with $b' \in C$, we repeat the same process to end up with a subcode B' of C (containing b') of size ≥ 514 such that all pairs of words in B' have odd inner product. Add an extra symbol 1 to every code word in B' to obtain a self-orthogonal code D' of length 23, so $\dim\langle D'\rangle \leq 11$. Note that $\langle D\rangle \neq \langle D'\rangle$, as $1b' \notin \langle D\rangle$.

Furthermore, $E := D \cap D'$ has $|E| \geq 513$ and all words start with 1. (To see this, note that $b, b' \notin B \cap B'$ with even inner product. Every word $v \in C \setminus ((B \cap B') \cup \{b, b'\})$ has even inner product with some word in C so there are at most 157 of such words v.) Hence $|\langle E\rangle| \geq 2{\cdot}513$, so $\dim\langle E\rangle \geq 11$. But $\langle D\rangle$ and $\langle D'\rangle$ are distinct codes of dimension $\leq$ 11, so their intersection has dimension < 11, hence

$$\dim\langle E\rangle = \dim\langle D \cap D'\rangle \leq \dim(\langle D\rangle \cap \langle D'\rangle) < 11,$$

a contradiction. □

From a code C with distance distribution (a_i), one constructs a feasible solution to (7.2) by putting $x(S) = 1$ for $S \in \mathcal{C}_k$ with $S \subseteq C$ and $x(S) = 0$ else, and hence by averaging over H there exists a feasible H-invariant solution. This solution has

$$\begin{aligned} z(\omega_t) &= \tfrac{1}{|H|}\sum_{g \in H} x \cdot g(\{x, y\}) = \frac{(\frac{t}{2})!(w - \frac{t}{2})!(\frac{t}{2})!(22 - w - \frac{t}{2})!}{|H|} |\{(u, v) \in C^2 \ : \ d_H(u, v) = t\}| \\ &= \frac{|\{(u, v) \in C^2 \ : \ d_H(u, v) = t\}|}{\binom{22}{w} \cdot \binom{22-w}{t/2}\binom{w}{t/2}} = \frac{|C| a_t}{\binom{22}{w}\binom{22-w}{t/2}\binom{w}{t/2}} = \frac{z(\omega_0) a_t}{\binom{22-w}{t/2}\binom{w}{t/2}}, \end{aligned}$$

where $\{x, y\}$ is any pair of constant weight w words with distance t and $H = S_{22}$, the symmetric group on 22 elements.

So we can add linear constraints on the a_i as linear constraints on the variables $z(\omega_t)$ to our semidefinite program. To the program $B_4(22, 8, 10)$ we add the constraints $a_{14} \geq 2/616$ and $a_{10} + a_{14} + a_{18} \geq 208/616$. To $B_4(22, 8, 11)$ we add the constraints $a_{14} \geq 2/672$ and $a_{10} + a_{14} + a_{18} + a_{22} \geq 318/672$. Write $B_4^*(n, d, w)$ for the resulting bound after adding these constraints. We find $B_4^*(n, d, w) < A(n, d, w)$ in both cases (which we verified using the dual solution), which is not possible.[5] This establishes (7.19) and hence completes the verification of (7.8) and (7.9).

The time needed to solve the semidefinite programs $B_4^*(22, 8, 11)$ and $B_4^*(22, 8, 10)$ varied from one to three weeks with sufficient precision to conclude that $B_4^*(n, d, w) < A(n, d, w)$ in these two cases (with SDPA-DD). By contrast, the semidefinite programs for $A_3(22, 8, 10)$ and $A_3(22, 8, 11)$ can be solved withvery high precision within minutes (with SDPA-GMP).

The computer programs we used to generate input for the SDP-solver can be found in [24]. Also, the input and output files for the SDP solver can be found in this folder, and a java program to inspect the outputs.

[5] The SDP-solutions show $B_4^*(22, 8, 11) < 671.885 < 672$ and $B_4^*(22, 8, 10) < 615.935 < 616$.

Chapter 8

Semidefinite programming bounds for Lee codes

Nothing takes place in the universe in which some relation of maximum and minimum does not appear.
— Leonhard Euler (1707–1783)

For nonnegative integers q, n, d, let $A_q^L(n,d)$ denote the maximum cardinality of a code $C \subseteq \mathbb{Z}_q^n$ with minimum Lee distance at least d. We consider a semidefinite programming upper bound on $A_q^L(n,d)$ based on triples of codewords, which bound can be computed efficiently using symmetry reductions, resulting in new upper bounds for several triples (q,n,d). We also give constructions for obtaining lower bounds and prove uniqueness of two instances for which upper bounds were already known: $A_5^L(7,9) = 15$ and $A_6^L(4,6) = 18$, using the semidefinite programming output. The code achieving the first value is obtained by arranging 15 girls 7 days in succession into triples in a special way, which is different from but connects to Kirkman's schoolgirl problem.

This chapter is based on [71], except for the constructions and uniqueness for $A_5^L(7,9) = 15$ and $A_6^L(4,6) = 18$, which are new.

8.1 Introduction

Fix $q, n \in \mathbb{N}$. Recall that the *Lee distance* of two words $u, v \in \mathbb{Z}_q^n$ is

$$d_L(u,v) := \textstyle\sum_{i=1}^n \min\{|u_i - v_i|,\, q - |u_i - v_i|\}, \tag{8.1}$$

where we consider u_i and v_i as integers in $\{0, \ldots, q-1\}$. The *minimum Lee distance* $d_{\text{min}}^L(C)$ of a code $C \subseteq \mathbb{Z}_q^n$ is the minimum of $d_L(u,v)$ taken over distinct $u, v \in C$. If $|C| \leq 1$, we set $d_{\text{min}}^L(C) = \infty$. For $d \in \mathbb{N}$, recall the definition of $A_q^L(n,d)$ cf. (2.5):

$$A_q^L(n,d) := \max\{|C| \mid C \subseteq \mathbb{Z}_q^n,\ d_{\text{min}}^L(C) \geq d\}. \tag{8.2}$$

Generally, it is an interesting and nontrivial problem to determine $A_q^L(n,d)$ for given q, n, d. Quistorff made a table of upper bounds on $A_q^L(n,d)$ based on analytic arguments [74]. H. Astola and I. Tabus calculated several new upper bounds by linear programming [5], using the classical Delsarte bound in the Lee scheme based on pairs of codewords [4, 31]. In [7], the possibility of applying semidefinite programming to Lee codes is mentioned and it is stated that to the best knowledge of the authors, such bounds for Lee codes using triples have not yet been studied.

In this chapter, we describe how to efficiently compute a semidefinite programming upper bound $B_3^L(q,n,d)$ on $A_q^L(n,d)$ based on triples of codewords, using symmetry reductions, and we calculate this bound for several values of q, n, d. We find several new upper bounds on $A_q^L(n,d)$, see Table 8.1. We only consider $q \geq 5$, since $A_4^L(n,d) = A_2(2n,d)$ — this follows by applying the Gray map [28].

q	n	d	**new upper bound**	best upper bound previously known
5	4	3	**62**	64^l
5	4	4	**27**	30^l
5	4	5	**10**	11^l
5	5	3	**270**	276^l
5	5	5	**36**	39^l
5	5	6	**15**	18^l
5	6	3	**1170**	1176^l
5	6	4	**494**	520^b
5	6	5	**149**	155^l
5	6	6	**60**	63^l
5	6	7	**25**	28^l
5	7	3	**5180**	5208^{bl}
5	7	4	**2183**	2232^b
5	7	5	**590**	608^l
5	7	6	**250**	284^l
5	7	7	**79**	81^l
5	7	8	**35**	41^l
6	3	3	**27**	29^l
6	3	4	**14**	17^l
6	4	4	**78**	79^l
6	4	5	**22**	26^l
6	5	3	**693**	699^l
6	5	4	**366**	378^l
6	5	5	**107**	114^l
6	5	6	**61**	67^l
6	5	7	**22**	24^{bl}
6	6	6	**273**	293^l
6	6	7	**79**	85^l
6	6	8	**48**	52^l
6	6	9	**16**	17^l
7	3	4	**21**	24^{bl}
7	3	5	**10**	11^l
7	4	3	**256**	263^l
7	4	4	**121**	128^b
7	4	5	$\mathbf{49}^*$	50^l
7	4	6	**23**	27^l
7	4	7	**11**	13^l
7	4	8	**6**	7^{bl}
7	5	3	**1499**	1512^l
7	5	4	**686**	720^b
7	5	5	**240**	249^l
7	5	6	**116**	130^l
7	5	7	**49**	54^l
7	5	8	**25**	28^l
7	5	9	**13**	14^l
7	6	10	**26**	31^l
7	6	11	**13**	14^b

Table 8.1: An overview of the new upper bounds for Lee codes. The new upper bounds are instances of the bound $B_3^L(q,n,d)$ from (8.4) below. The superscript ^{l} refers to a bound obtained by Astola and Tabus using linear programming [5]. The superscript ^{b} refers to a bound from Quistorff [74]. The superscript * refers to an upper bound matching the known lower bound: $A_7^L(4,5) = 49$ is achieved by a linear code [6]. No tables of lower bounds are given in [5, 74].

Recall that two codes $C, D \subseteq \mathbb{Z}_q^n$ are *Lee equivalent* if D can be obtained from C by first permuting the n coordinates and by subsequently acting on the alphabet $\mathbb{Z}_q$ with an element of the dihedral group D_q in each coordinate separately. Here the dihedral group D_q of order $2q$ is the group of symmetries of a regular q-gon with vertices $0, \ldots, q-1$. It was already known that $A_5^L(7,9) \leq 15$ and $A_6^L(4,6) \leq 18$, cf. [74]. In Sections 8.3 and 8.4 we will give codes achieving those bounds, and we also show that in both cases there is only one code (up to Lee equivalence) of maximum size, using the semidefinite programming output.

8.1.1 The semidefinite programming bound

We define a hierarchy of semidefinite programming upper bounds on $A_q^L(n,d)$, which is an adaptation of the semidefinite programming hierarchy for binary codes defined by Gijswijt, Mittelmann and Schrijver in [37]. For $k \in \mathbb{Z}_{\geq 0}$, let $\mathcal{C}_k$ be the collection of codes $C \subseteq \mathbb{Z}_q^n$ with $|C| \leq k$. For any $D \in \mathcal{C}_k$, we define

$$\mathcal{C}_k(D) := \{C \in \mathcal{C}_k \mid C \supseteq D,\, |D| + 2|C \setminus D| \leq k\}. \tag{8.3}$$

Note that then $|C \cup C'| = |C| + |C'| - |C \cap C'| \leq 2|D| + |C \setminus D| + |C' \setminus D| - |D| \leq k$ for all $C, C' \subseteq \mathcal{C}_k(D)$. Furthermore, for any function $x : \mathcal{C}_k \to \mathbb{R}$ and $D \in \mathcal{C}_k$, we define the $\mathcal{C}_k(D) \times \mathcal{C}_k(D)$ matrix $M_{k,D}(x)$ by

$$M_{k,D}(x)_{C,C'} := x(C \cup C'),$$

for $C, C' \in \mathcal{C}_k(D)$. Now define the following number:

$$\begin{aligned} B_k^L(q,n,d) := \max \big\{ \textstyle\sum_{v \in \mathbb{Z}_q^n} x(\{v\}) \mid x : \mathcal{C}_k \to \mathbb{R},\ x(\emptyset) = 1,\ x(S) = 0 \text{ if } d_{\text{min}}^L(S) < d,& \\ M_{k,D}(x) \succeq 0 \text{ for each } D \text{ in } \mathcal{C}_k \big\}.& \end{aligned} \tag{8.4}$$

Proposition 8.1.1. *For all $k, q, n, d \in \mathbb{N}$, we have $A_q^L(n,d) \leq B_k^L(q,n,d)$.*

Proof. Let $C \subseteq \mathbb{Z}_q^n$ be a code with $d_{\text{min}}^L(C) \geq d$ and $|C| = A_q^L(n,d)$. Define $x : \mathcal{C}_k \to \mathbb{R}$ by $x(S) = 1$ if $S \subseteq C$ and $x(S) = 0$ else, for $S \in \mathcal{C}_k$. Then x satisfies the conditions in (8.4), where the condition that $M_{k,D}(x) \succeq 0$ is satisfied since $M_{k,D}(x)_{C,C'} = x(C)x(C')$ for all $C, C' \in \mathcal{C}_k(D)$. Moreover, the objective value equals $\sum_{v \in \mathbb{Z}_q^n} x(\{v\}) = |C| = A_q^L(n,d)$, which gives $B_k^L(q,n,d) \geq A_q^L(n,d)$. □

It can be shown that the bound $B_2^L(q,n,d)$ is equal to the Delsarte bound in the Lee scheme, which was calculated for several instances by Astola and Tabus in [5]. In this chapter we consider the bound $B_3^L(q,n,d)$. The method for obtaining a symmetry reduction, using representation theory of the dihedral and symmetric groups, is an adaptation of the method in Chapter 3.

8.1.2 Symmetry reductions

Fix $k \in \mathbb{N}$. Let D_q be the dihedral group of order $2q$ and let S_n be the symmetric group on n elements. The group $H := D_q^n \rtimes S_n$ acts naturally on $\mathcal{C}_k$, and this action maintains minimum distances and cardinalities of codes $C \in \mathcal{C}_k$. We can assume that the optimum x in (8.4) is H-invariant, i.e., $g \cdot x = x$ for all $g \in H$. Indeed, if x is any optimum solution for (8.4), then for each $g \in H$, the function $g \cdot x$ is again an optimum solution, since the objective value of $g \cdot x$ equals the objective value of x and $g \cdot x$ still satisfies all constraints in (8.4). Since the feasible region is convex, the optimum x can be replaced by the average of $g \cdot x$ over all $g \in H$. This gives an H-invariant optimum solution.

Let Ω_k be the set of H-orbits on $\mathcal{C}_k$. Then $|\Omega_k|$ is bounded by a polynomial in n, for fixed k and q. Since there exists an H-invariant optimum solution, we can replace, for each $\omega \in \Omega_k$ and $C \in \omega$, each variable $x(C)$ by a variable $z(\omega)$. Hence, the matrices $M_{k,D}(x)$ become matrices $M_{k,D}(z)$ and we have considerably reduced the number of variables in (8.4).

We only have to check positive semidefiniteness of $M_{k,D}(z)$ for one code D in each H-orbit of $\mathcal{C}_k$, as for each $g \in H$, the matrix $M_{k,g(D)}(z)$ can be obtained by simultaneously permuting rows and columns of $M_{k,D}(z)$.

We sketch how to reduce these matrices in size. For $D \in \mathcal{C}_k$, let H_D be the subgroup of H consisting of all $g \in H$ with $g(D) = D$. Then the action of H on $\mathcal{C}_k$ induces an action of H_D on $\mathcal{C}_k(D)$. The simultaneous action of H_D on the rows and columns of $M_{k,D}(z)$ leaves $M_{k,D}(z)$ invariant. Therefore, there exists a block-diagonalization (as explained in Section 1.2) given by $M_{k,D}(z) \mapsto U^* M_{k,D}(z) U$ of $M_{k,D}(z)$, for a matrix U depending on H_D but not depending on z, such that the order of $U^* M_{k,D}(z) U$ is polynomial in n and such that $M_{k,D}(z)$ is positive semidefinite if and only if each of the blocks of $U^* M_{k,D}(z) U$ is positive semidefinite. In our case the matrix U can be taken to be real; so $U^* = U^{\mathsf{T}}$. The entries in each block of $U^{\mathsf{T}} M_{k,D}(z) U$ are linear functions in the variables $z(\omega)$ (with coefficients bounded polynomially in n). Hence, we have reduced the size of the matrices involved in our semidefinite program to polynomial size.

The reductions of the optimization problem will be described in detail in Section 8.2. Table 8.1 contains the new upper bounds. All improvements have been found using multiple precision versions of SDPA [61].

8.2 Reduction of the optimization problem

In this section we give the reduction of optimization problem (8.4) for computing the bound $B_3^L(q,n,d)$, using the representation theory from Section 2.4 and Chapter 3. First we consider block diagonalizing $M_{3,D}(z)$ for $D \in \mathcal{C}_3$ with $|D| = 1$. Subsequently we consider the case $D = \emptyset$. Note that for the cases $|D| = 2$ and $|D| = 3$ the matrix $M_{3,D}(z) = (z(D))$ has order 1×1, so it is its own block diagonalization. Hence, in those cases, $M_{3,D}(z)$ is positive semidefinite if and only if $z(D) \geq 0$.

8.2.1 The case $|D| = 1$

The Lee isometry group $H = D_q^n \rtimes S_n$ acts transitively on $\mathbb{Z}_q^n$, so we may assume that $D = \{\mathbf{0}\}$, where $\mathbf{0} = 0 \ldots 0$ is the all-zero word. The rows and columns of $M_{3,D}(z)$ are indexed by sets of the form $\{\mathbf{0}, \alpha\}$ for $\alpha \in \mathbb{Z}_q^n$. Then the subgroup H_D of H that leaves D invariant is equal to $S_2^n \rtimes S_n$, as the zero word must remain fixed (so we cannot apply a rotation of the alphabet in any coordinate position). Here the non-identity element of $G := S_2$ acts on $Z := \mathbb{Z}_q$, where we consider $0, \ldots, q-1$ as vertices of a regular q-gon, as a *reflection* switching vertices i and $q-i$ (for $i = 1, \ldots, \lfloor \frac{q-1}{2} \rfloor$). So vertex 0 is fixed if q is odd, and vertices 0 and $q/2$ are fixed if q is even. For $i = 0, \ldots, q-1$, let e_i be the ith unit vector of $\mathbb{C}^{\mathbb{Z}_q}$ (taken as column vector).

Proposition 8.2.1. *A representative matrix set for the reflection action of $G = S_2$ on $\mathbb{C}^Z = \mathbb{C}^{\mathbb{Z}_q}$ is*

$$\boldsymbol{B} := \{B_1, B_2\}, \text{ with } \quad B_1 := \left[e_0, (e_i + e_{q-i})_{i=1}^{\lfloor \frac{q}{2} \rfloor}\right], \quad B_2 := \left[(e_i - e_{q-i})_{i=1}^{\lfloor \frac{q-1}{2} \rfloor}\right]. \tag{8.5}$$

Proof. For $j = 1, \ldots, \lfloor q/2 \rfloor + 1$, define $W_{1,j}$ to be the 1-dimensional vector space spanned by the jth column $w_{1,j}$ of B_1. Moreover, for $j = 1, \ldots, \lfloor (q-1)/2 \rfloor$, define $W_{2,j}$ to be the 1-dimensional vector space spanned by the jth column $w_{2,j}$ of B_2. Note that each $W_{i,j}$ is S_2-stable and that $W_{i,j}$ and $W_{i',j'}$ are orthogonal whenever $(i,j) \neq (i',j')$ (with respect to the inner product $u, v \mapsto v^*u$). Observe that, for j, j' and l, l' the maps $W_{1,j} \to W_{1,j'}$ and $W_{2,l} \to W_{2,l'}$ defined by $w_{1,j} \mapsto w_{1,j'}$ and $w_{2,l} \mapsto w_{2,l'}$, respectively, are S_2-equivariant. Note that the number of $W_{1,j}$ we have defined is $\lfloor q/2 \rfloor + 1$, the number of $W_{2,j}$ is $\lfloor (q-1)/2 \rfloor$, and

$$(\lfloor q/2 \rfloor + 1)^2 + \lfloor (q-1)/2 \rfloor^2 = \begin{cases} \frac{1}{2}q^2 + 2 & \text{if } q \text{ is even,} \\ (q^2+1)/2 & \text{if } q \text{ is odd,} \end{cases}$$

which is equal to $|(\mathbb{Z}_q \times \mathbb{Z}_q)/S_2| = \dim(\mathbb{C}^{\mathbb{Z}_q} \otimes \mathbb{C}^{\mathbb{Z}_q})^{S_2}$. (If q is even, the points $(0,0)$, $(q/2,0)$, $(0,q/2)$ and $(q/2,q/2)$ in $\mathbb{Z}_q \times \mathbb{Z}_q$ are fixed by the nonidentity element in S_2. If q is odd, only the point $(0,0)$ in $\mathbb{Z}_q \times \mathbb{Z}_q$ is fixed by the nonidentity element in S_2.) It follows that the $W_{1,j}$ and $W_{2,j}$ form a *decomposition* of $\mathbb{C}^{\mathbb{Z}_q}$ into *irreducible representations* (as any further representation, or decomposition, or equivalence among the $W_{i,j}$ would yield that the sum of the squares of the multiplicities of the irreducible representations is strictly larger than $\dim(\mathbb{C}^{\mathbb{Z}_q} \otimes \mathbb{C}^{\mathbb{Z}_q})^{S_2}$, which contradicts the fact that Φ in (2.16) is bijective). So the matrix set $\boldsymbol{B}$ from (8.5) is indeed representative for the action of S_2 on $\mathbb{C}^{\mathbb{Z}_q}$. □

Note that the representative set is real. Set $k := 2$, $\boldsymbol{m} =: (m_1, m_2) := (\lfloor q/2 \rfloor + 1, \lfloor (q-1)/2 \rfloor)$. Now Proposition 3.1.1 (with $V := \mathbb{C}^Z$, where $Z = \mathbb{Z}_q$, and $G = S_2$) gives a representative set for the action of $S_2^n \rtimes S_n$ on $\mathbb{Z}_q^n$: it is the set

$$\left\{ \; [\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}} \mid \boldsymbol{\tau} \in \boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}] \quad \middle| \; \boldsymbol{n} \in \boldsymbol{N}, \boldsymbol{\lambda} \vdash \boldsymbol{n} \right\}$$

where $\boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}$ and $\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}$ are defined in (3.1) and (3.2) respectively. For convenience of the reader, we restate the main definitions of Chapter 3 and the main facts about representative sets applied to the context of this section — see Figure 8.1.

Computations for $|D| = 1$

Let $D = \{\mathbf{0}\} \in \mathcal{C}_3$ and let Ω_3 denote the set of all $D_q^n \rtimes S_n$-orbits of codes in $\mathcal{C}_3$. For each $\omega \in \Omega_3$, we define the $\mathcal{C}_3(D) \times \mathcal{C}_3(D)$ matrix N_ω with entries in $\{0,1\}$ by

$$(N_\omega)_{\{\mathbf{0},\alpha\},\{\mathbf{0},\beta\}} := \begin{cases} 1 & \text{if } \{\mathbf{0}, \alpha, \beta\} \in \omega, \\ 0 & \text{otherwise,} \end{cases} \tag{8.6}$$

for $\alpha, \beta \in \mathbb{Z}_q^n$. Given $\boldsymbol{n} = (n_1, n_2) \in \boldsymbol{N}$, for each $\boldsymbol{\lambda} \vdash \boldsymbol{n}$ we write $U_{\boldsymbol{\lambda}}$ for the matrix in (3.3) that corresponds with $\boldsymbol{\lambda}$. For each $z : \Omega_3 \to \mathbb{R}$ we obtain with (2.17) that

$$\Phi(M_{3,D}(z)) = \Phi\left(\sum_{\omega \in \Omega_3} z(\omega) N_\omega\right) = \bigoplus_{\boldsymbol{n} \in \boldsymbol{N}} \bigoplus_{\boldsymbol{\lambda} \vdash \boldsymbol{n}} \sum_{\omega \in \Omega_3} z(\omega) U_{\boldsymbol{\lambda}}^{\mathsf{T}} N_\omega U_{\boldsymbol{\lambda}}. \tag{8.7}$$

The number of $\boldsymbol{n} \in \boldsymbol{N}$, $\boldsymbol{\lambda} \vdash \boldsymbol{n}$, and the numbers $|\boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}|$ and $|\Omega_3|$ are all bounded by a polynomial in n. This implies that the number of blocks in (8.7), the size of each block

FACTS.

$G := S_2$.
$Z := \mathbb{Z}_q$.
The non-identity element of S_2 switches i and $q-i$ (for $i = 1, \ldots, \lfloor \frac{q-1}{2} \rfloor$).

$k := 2$, $\boldsymbol{m} =: (m_1, m_2) := (\lfloor q/2 \rfloor + 1, \lfloor (q-1)/2 \rfloor)$.

A representative set for the action of G on Z is $\boldsymbol{B} = \{B_1, B_2\}$ from (8.5).
A representative set for the action of $G^n \rtimes S_n$ on Z^n follows from Prop. 3.1.1.

$\Lambda := (\mathbb{Z}_q \times \mathbb{Z}_q)/S_2$.
$a_P := \sum_{(x,y) \in P} x \otimes y$ for $P \in \Lambda$.
$A := \{a_P \,|\, P \in \Lambda\}$, a basis of $W := (\mathbb{C}\mathbb{Z}_q \otimes \mathbb{C}\mathbb{Z}_q)^{S_2}$.
$K_{\omega'} := \sum_{(P_1, \ldots, P_n) \in \omega'} a_{P_1} \otimes \cdots \otimes a_{P_n}$ for $\omega' \in \Lambda^n/S_n$.

Figure 8.1: The main definitions of Chapter 3 and the main facts about representative sets applied to the context of Section 8.2.1.

and the number of variables occurring in all blocks are polynomially bounded in n. We now show how to compute the entries of the matrix $U_{\boldsymbol{\lambda}}^{\mathsf{T}} N_\omega U_{\boldsymbol{\lambda}}$, for all $\omega \in \Omega_3$, $\boldsymbol{n} \in \boldsymbol{N}$, $\boldsymbol{\lambda} \vdash \boldsymbol{n}$, in polynomial time. That is, we show how to compute the coefficients $\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}} N_\omega \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}$, for $\boldsymbol{\tau}, \boldsymbol{\sigma} \in \boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}$, in the blocks $\sum_{\omega \in \Omega_3} z(\omega) U_{\boldsymbol{\lambda}}^{\mathsf{T}} N_\omega U_{\boldsymbol{\lambda}}$ in polynomial time.

Recall that $\Lambda = (\mathbb{Z}_q \times \mathbb{Z}_q)/S_2$. By (3.7) there is a natural bijection between Λ^n/S_n and the set of H-orbits on $(\mathbb{Z}_q \times \mathbb{Z}_q)^n$. Since naturally $(\mathbb{Z}_q^n)^2 \cong (\mathbb{Z}_q \times \mathbb{Z}_q)^n$, there is a natural bijection between Λ^n/S_n and the set of H-orbits on $(\mathbb{Z}_q^n)^2$. The function $(\mathbb{Z}_q^n)^2 \to \mathcal{C}_3$ with $(\alpha, \beta) \mapsto \{\boldsymbol{0}, \alpha, \beta\}$ then gives a surjective function $r : \Lambda^n/S_n \to \Omega_3 \setminus \{\{\emptyset\}\}$.

Then (cf. Lemma 4.3.1) for each $\omega \in \Omega_3$,

$$N_\omega = \sum_{\substack{\omega' \in \Lambda^n/S_n \\ r(\omega') = \omega}} K_{\omega'}.$$

Hence, it suffices to compute $\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}} K_{\omega'} \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}$ for each $\omega' \in \Lambda^n/S_n$.

By Proposition 3.2.1, we have $\sum_{\omega' \in \Lambda^n/S_n} \left(\boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}} K_{\omega'} \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}} \right) \mu(\omega') = \prod_{i=1}^{2} p_{\tau_i, \sigma_i}(F_i)$, where the matrices $F_i \in (W^*)^{m_i \times m_i}$ are defined in (3.13) and the polynomial p_{τ_i,σ_i} is defined in (3.14). So it suffices to calculate the matrices F_i, that is, to express each $(F_i)_{j,h} = (B_i(j) \otimes B_i(h))|_W$ as linear function into the dual basis A^* of A. So we must calculate the numbers $(B_i(j) \otimes B_i(h))(a_P)$ for all $i = 1, 2$, $j, h = 1, \ldots, m_i$, and $P \in \Lambda$ — see Appendix 1 (Section 8.5.1 below).

Now one computes the entry $\sum_{\omega \in \Omega_3} z(\omega) \boldsymbol{u}_{\boldsymbol{\tau},\boldsymbol{B}}^{\mathsf{T}} N_\omega \boldsymbol{u}_{\boldsymbol{\sigma},\boldsymbol{B}}$ by first expressing $\prod_{i=1}^{2} p_{\tau_i,\sigma_i}(F_i)$ as a linear combination of degree n monomials expressed in the dual basis A^* of A and subsequently replacing each monomial $\mu(\omega')$ in $\prod_{i=1}^{2} p_{\tau_i,\sigma_i}(F_i)$ with the variable $z(r(\omega'))$.

8.2.2 The case $D = \emptyset$

Let $D = \emptyset$. The rows and columns of $M_{3,\emptyset}(z)$ (which is equal to $M_{2,\emptyset}(z)$) are indexed by words in $\mathbb{Z}_q^n$ together with the empty set, and H_D is equal to $D_q^n \rtimes S_n$. Here $G := D_q$ acts on $Z := \mathbb{Z}_q$. To compute the block diagonalization of $M_{2,\emptyset}(z)$, one can use the Delsarte formulas in the Lee scheme [4, 5]. Here we give the reduction in terms of representative sets.

Let $\zeta = e^{2\pi i/q}$ be a primitive qth root of unity. For each $j = 0, \ldots, \lfloor q/2 \rfloor$, define the vectors $a_j := (1, \zeta^j, \zeta^{2j}, \ldots, \zeta^{(q-1)j})^\mathsf{T}$, $b_j := (1, \zeta^{-j}, \zeta^{-2j}, \ldots, \zeta^{-(q-1)j})^\mathsf{T} \in \mathbb{C}^{\mathbb{Z}_q}$ and set $V_j := \operatorname{span}\{a_j, b_j\}$. Furthermore, put

$$c_j := \frac{\sqrt{\dim V_j}}{2}(a_j + b_j) = \sqrt{\dim V_j}(1, \cos(2j\pi/q), \ldots, \cos(2(q-1)j\pi/q))^\mathsf{T} \in \mathbb{R}^{\mathbb{Z}_q} \subseteq \mathbb{C}^{\mathbb{Z}_q}.$$

Proposition 8.2.2. *A representative set for the action of $G = D_q$ on $\mathbb{C}^Z = \mathbb{C}^{\mathbb{Z}_q}$ is given by*

$$\boldsymbol{B} := \left\{B_1, \ldots, B_{\lfloor \frac{q}{2} \rfloor + 1}\right\}, \text{ where } B_j := c_{j-1}, \text{ for } j = 1, \ldots, \lfloor q/2 \rfloor + 1. \tag{8.8}$$

Proof. Observe that each V_j is D_q-stable and that $c_j \in V_j$. Moreover, V_l and V_j are orthogonal (with respect to the inner product $u, v \mapsto v^* u$) if $l \neq j$. To see this, note that $x := \zeta^{\pm j \pm l}$ is a qth root of unity unequal to 1 if $j \neq l \in \{0, \ldots, \lfloor q/2 \rfloor\}$, so $1 + x + x^2 + \ldots + x^{q-1} = 0$. This implies that $a_j^* a_l = b_j^* a_l = a_j^* b_l = b_j^* b_l = 0$, so V_l and V_j are orthogonal. Note that $\sum_{j=0}^{\lfloor q/2 \rfloor} 1^2 = \lfloor q/2 \rfloor + 1$, which is the number of distinct V_j, is equal to the dimension of $(\mathbb{C}^{\mathbb{Z}_q} \otimes \mathbb{C}^{\mathbb{Z}_q})^{D_q}$. So the V_j form an orthogonal *decomposition* of $\mathbb{C}^{\mathbb{Z}_q}$ into *irreducible* representations (as any further representation, or decomposition, or equivalence among the V_j would yield that the sum of the squares of the multiplicities of the irreducible representations is strictly larger than $\lfloor q/2 \rfloor + 1$, which contradicts the fact that Φ in (2.16) is bijective). As B_{j+1} is an element of V_j for $j = 0, \ldots, \lfloor q/2 \rfloor$, this implies that $\boldsymbol{B}$ from (8.8) is a representative matrix set. □

Note that the representative set is real, and that each B_i is a $q \times 1$ matrix. For convenience of the reader, we restate the main definitions of Chapter 3 and the main facts about representative sets applied to the context of this section — see Figure 8.2.

Let $\boldsymbol{N}$ be the collection of all k-tuples $(n_1, \ldots, n_k)$ of nonnegative integers adding up to n (here $k = \lfloor q/2 \rfloor + 1$). For each $\boldsymbol{n} \in \boldsymbol{N}$, there is only one $\boldsymbol{\lambda} \vdash \boldsymbol{n}$ with height$(\lambda_i) \leq m_i = 1$ for all $i = 1, \ldots, k$. Moreover, for this $\boldsymbol{\lambda}$, the set $\boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}} = T_{\lambda_1,1} \times \ldots \times T_{\lambda_k,1}$ from (3.1) has only one element $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_k)$. Here each τ_i is a Young tableau of height 1 which only contains ones (for $i = 1, \ldots, k$). Write $\boldsymbol{\tau}_{\boldsymbol{n}}$ for this element $\boldsymbol{\tau}$. Then, for each $\boldsymbol{n} \in \boldsymbol{N}$, the element $\boldsymbol{u}_{\boldsymbol{\tau}_{\boldsymbol{n}},\boldsymbol{B}}$ from (3.2) is equal to

$$\boldsymbol{u}_{\boldsymbol{\tau}_{\boldsymbol{n}},\boldsymbol{B}} = B_1^{\otimes n_1} \otimes B_2^{\otimes n_2} \otimes \ldots \otimes B_k^{\otimes n_k}. \tag{8.9}$$

So a representative set for the action of $D_q^n \rtimes S_n$ on Z^n is, cf. Proposition 3.1.1,

$$\{\boldsymbol{u}_{\boldsymbol{\tau}_{\boldsymbol{n}},\boldsymbol{B}} \mid \boldsymbol{n} \in \boldsymbol{N}\}. \tag{8.10}$$

Observe that $D_q^n \rtimes S_n$ acts trivially on $\emptyset$. The $D_q^n \rtimes S_n$-isotypical component of $\mathbb{C}^{\mathbb{Z}_q^n}$ consisting of the $D_q^n \rtimes S_n$-invariant elements corresponds to the matrix in the representative set indexed by $\boldsymbol{n} = (n, 0, \ldots, 0)$. Hence we add a new unit base vector $e_\emptyset$ to this matrix (as a column) in order to obtain a representative set for the action of $D_q^n \rtimes S_n$ on $\mathbb{C}^{\mathbb{Z}_q^n \cup \{\emptyset\}} = \mathbb{C}^{\mathcal{C}_3(\emptyset)}$.

FACTS.

$G := D_q$.
$Z := \mathbb{Z}_q$.

$k := \lfloor \frac{q}{2} \rfloor + 1$, $\boldsymbol{m} := (m_1, \ldots, m_k) := (1, \ldots, 1)$.

A representative set for the action of G on Z is $\boldsymbol{B}$ from Prop. 8.8.
A representative set for the action of $G^n \rtimes S_n$ on Z^n follows from Prop. 3.1.1.

$\Lambda := (\mathbb{Z}_q \times \mathbb{Z}_q)/D_q$.
$a_P := \sum_{(x,y) \in P} x \otimes y$ for $P \in \Lambda$.
$A := \{a_P \,|\, P \in \Lambda\}$, a basis of $W := (\mathbb{C}\mathbb{Z}_q \otimes \mathbb{C}\mathbb{Z}_q)^{D_q}$.
$K_{\omega'} := \sum_{(P_1,\ldots,P_n)\in\omega'} a_{P_1} \otimes \cdots \otimes a_{P_n}$ for $\omega' \in \Lambda^n/S_n$.

Figure 8.2: The main definitions of Chapter 3 and the main facts about representative sets applied to the context of Section 8.2.2.

Computations for $D = \emptyset$

In this section we explain how to compute the coefficients in the block diagonalization of $M_{2,\emptyset}(z)$. First we give a reduction of $M_{2,\emptyset}(z)$ without the row and column indexed the empty code. Later we explain how the empty code is added.

For each $\omega \in \Omega_2$, we define the $\mathbb{Z}_q^n \times \mathbb{Z}_q^n$ matrix $\widetilde{N}_\omega$ with entries in $\{0,1\}$ by $(\widetilde{N}_\omega)_{\alpha,\beta} = 1$ if $\{\alpha,\beta\} \in \omega$ and $(\widetilde{N}_\omega)_{\alpha,\beta} = 0$ otherwise, for $\alpha, \beta \in \mathbb{Z}_q^n$. For each $z : \Omega_2 \to \mathbb{R}$ we obtain with (3.3) and (2.17) that $\Phi\left(\sum_{\omega\in\Omega_2} z(\omega)\widetilde{N}_\omega\right) = \bigoplus_{\boldsymbol{n}\in\boldsymbol{N}} \sum_{\omega\in\Omega_2} z(\omega)\boldsymbol{u}_{\boldsymbol{\tau_n},\boldsymbol{B}}^{\mathsf{T}}\widetilde{N}_\omega \boldsymbol{u}_{\boldsymbol{\tau_n},\boldsymbol{B}}$. This shows that $\Phi\left(\sum_{\omega\in\Omega_2} z(\omega)\widetilde{N}_\omega\right)$ is a diagonal matrix. Note that $|\Omega_2|$ and $|\boldsymbol{N}|$ are polynomially bounded in n. Now we show how to compute $\boldsymbol{u}_{\boldsymbol{\tau_n},\boldsymbol{B}}^{\mathsf{T}}\widetilde{N}_\omega \boldsymbol{u}_{\boldsymbol{\tau_n},\boldsymbol{B}}$, for $\boldsymbol{n} \in \boldsymbol{N}$, in polynomial time.

By (3.7), there is a natural bijection between Λ^n/S_n and the set of H-orbits on $(\mathbb{Z}_q \times \mathbb{Z}_q)^n$. Since naturally $(\mathbb{Z}_q^n)^2 \cong (\mathbb{Z}_q \times \mathbb{Z}_q)^n$, there is a natural bijection between Λ^n/S_n and $(\mathbb{Z}_q^n)^2/H$. The function $(\mathbb{Z}_q^n)^2 \to \mathcal{C}_2$ that maps (α,β) to $\{\alpha,\beta\}$ then induces a surjective function $\widetilde{r} : \Lambda^n/S_n \to \Omega_2 \setminus \{\{\emptyset\}\}$. Then (cf. Lemma 4.3.1) for each $\omega \in \Omega_2$,

$$\widetilde{N}_\omega = \sum_{\substack{\omega' \in \Lambda^n/S_n \\ \widetilde{r}(\omega')=\omega}} K_{\omega'}.$$

So it remains to compute $\boldsymbol{u}_{\boldsymbol{\tau_n},\boldsymbol{B}}^{\mathsf{T}} K_{\omega'} \boldsymbol{u}_{\boldsymbol{\tau_n},\boldsymbol{B}}$ for each $\omega' \in \Lambda^n/S_n$. By Proposition 3.2.1 we find that $\sum_{\omega'\in\Lambda^n/S_n} \left(\boldsymbol{u}_{\boldsymbol{\tau_n},\boldsymbol{B}}^{\mathsf{T}} K_{\omega'} \boldsymbol{u}_{\boldsymbol{\tau_n},\boldsymbol{B}}\right)\mu(\omega') = \prod_{i=1}^k p_{(\boldsymbol{\tau_n})_i,(\boldsymbol{\tau_n})_i}(F_i)$, where $p_{(\boldsymbol{\tau_n})_i,(\boldsymbol{\tau_n})_i}$ is defined in (3.14) and F_i is an 1×1 matrix in $(W^*)^{1\times 1}$ with $(F_i)_{1,1} := (B_i \otimes B_i)|_W = \sum_{P\in\Lambda}(B_i \otimes B_i)(a_P)a_P^* \in W^*$, for $i = 1,\ldots,k$. We compute the formulas $(F_i)_{1,1}$ in Appendix 1 (Section 8.5.1) below.

Now one computes the entry $\sum_{\omega\in\Omega_2} z(\omega)\boldsymbol{u}_{\boldsymbol{\tau_n},\boldsymbol{B}}^{\mathsf{T}}\widetilde{N}_\omega \boldsymbol{u}_{\boldsymbol{\tau_n},\boldsymbol{B}}$ by first expressing the polynomial $\prod_{i=1}^k p_{(\boldsymbol{\tau_n})_i,(\boldsymbol{\tau_n})_i}(F_i)$ as a linear combination of degree n monomials expressed in the dual basis A^* of A and subsequently replacing each monomial $\mu(\omega')$ in $\prod_{i=1}^k((F_i)_{1,1})^{n_i}$ with the variable $z(\widetilde{r}(\omega'))$.

To add the empty code, we add an extra row and column corresponding to the vector $e_\emptyset$ to the matrix in the representative set indexed by $\boldsymbol{n} = (n, 0, \dots, 0)$, cf. Section 8.2.2. We compute the remaining entries:

$$e_\emptyset^\mathsf{T} M_{2,\emptyset}(z) e_\emptyset = M_{2,\emptyset}(z)_{\emptyset,\emptyset} = x(\emptyset) = 1$$

by definition, see (8.4). Since $\boldsymbol{u}_{\boldsymbol{\tau_n},\boldsymbol{B}} = B_1^{\otimes n}$ is the all-ones vector, we have $e_\emptyset^\mathsf{T} M_\emptyset(z) \boldsymbol{u}_{\boldsymbol{\tau_n},\boldsymbol{B}} = q^n z(\omega_0)$, where $\omega_0 \in \Omega_2$ is the (unique) $D_q^n \rtimes S_n$-orbit of a code of size 1.

8.3 The unique code achieving $A_5^L(7,9) = 15$

An interesting case is $A_5^L(7,9)$. The SDP-bound $B_3^L(5,7,9)$, the linear programming bound (cf. [5]) and the bound from [74] all give $A_5^L(7,9) \leq 15$ as upper bound, but it was not known whether a $(7,9)_5^L$-code of size 15 exists. Here any code $C \subseteq \mathbb{Z}_q^n$ with $d_{\text{min}}^L(C) \geq d$ is called an *$(n,d)_q^L$-code* and similarly, any code $C \subseteq \mathbb{Z}_q^n$ with $d_{\text{min}}^H(C) \geq d$ is an *$(n,d)_q^H$-code*. We first derive some conditions that any $(7,9)_5^L$-code of size 15 satisfies.

8.3.1 Conditions on an $A_5^L(7,9) = 15$-code and Kirkman schoolgirls

Let C be an $(n,d)_q^L$ code of size M. By estimating $\sum_{\{u,v\}\subseteq C} d^L(u,v)$ one obtains:

$$\binom{M}{2} d \leq \sum_{\{u,v\}\subseteq C} d^L(u,v) = \sum_{i=1}^n \sum_{\{u,v\}\subseteq C} d^L(u_i,v_i) \leq n P_q(M), \tag{8.11}$$

where

$$P_q(M) := \max \left\{ \sum_{\{i,j\}\subseteq\{1,\dots,M\}} d^L(u_i,u_j) \;\middle|\; (u_1,\dots,u_M) \in \mathbb{Z}_q^M \right\}. \tag{8.12}$$

Wyner and Graham [95] proved that if q is odd, then $P_q(M) \leq M^2(q^2-1)/(8q)$ and moreover that if q divides M and the $(q-1)\times(q-1)$ matrix $(d_L(0,i) + d_L(0,j) - d_L(i,j))_{i,j=1,\dots,q-1}$ is positive definite, then the maximum in (8.12) is achieved only by vectors $(u_1,\dots,u_M)$ in which each symbol in $\mathbb{Z}_q$ appears exactly M/q times.

For the case $(n,d)_q^L = (7,9)_5^L$ and $M = 15$, we find that $P_5(15) = 135$, that the maximum in (8.12) is only achieved by vectors in which each symbol in $\mathbb{Z}_5$ appears exactly 3 times (as the matrix from the previous paragraph is positive definite in this case), and that the rightmost term in (8.11) is equal to the leftmost term in (8.11). This implies that if C is a $(7,9)_5^L$ code of size 15, then

(i) each symbol in $\mathbb{Z}_5$ appears exactly 3 times in each column of C (interpreting C as a matrix with the words as rows), and

(ii) any two distinct words in C have Lee distance exactly $d = 9$, i.e., C is *equidistant* with Lee distance 9.

So a $(7,9)_5^L$-code C of size 15 is equivalent to an arrangement of 15 girls 7 days in succession into triples, where the triples are placed at the corners of a pentagon, such that the total Lee distance between any two girls over the 7 days is 9. This problem is similar to, but different from, *Kirkman's school girl problem*, which asks for an arrangement of 15 girls 7 days in a row into triples such that no two girls appear in the same triple twice. Such an arrangement is equivalent to a $(7,6)_5^H$-code of size 15 (see [83] and Chapter 5 of this thesis), and there are 7 nonisomorphic arrangements possible [29].

Consider the following $\mathbb{Z}_7 \times \mathbb{Z}_7$ matrix with entries in $\mathbb{Z}_5$:

$$\widetilde{M} := \begin{pmatrix} 0&1&1&3&1&3&3\\ 1&1&3&1&3&3&0\\ 1&3&1&3&3&0&1\\ 3&1&3&3&0&1&1\\ 1&3&3&0&1&1&3\\ 3&3&0&1&1&3&1\\ 3&0&1&1&3&1&3 \end{pmatrix}, \quad \text{so } \widetilde{M}_{i,j} = \begin{cases} 0, & \text{if } i+j \equiv 0 \pmod 7,\\ 1, & \text{if } i+j \text{ is a nonzero square mod } 7,\\ 3, & \text{if } i+j \text{ is not a square mod } 7.^{1} \end{cases} \tag{8.13}$$

We will see that every $(7,9)_5^L$-code C of size 15 is equivalent to the code $\widetilde{M} \cup -\widetilde{M} \cup \{\mathbf{0}\}$, where the matrix $\widetilde{M}$ is interpreted as a $(7,9)_5^L$-code of size 7 (i.e., the rows are the codewords). Note that this code has minimum Hamming distance 5, so it follows that there is no $(7,9)_5^L$-code of size 15 which is also a $(7,6)_5^H$-code, i.e., there is no arrangement of 15 girls 7 days in succession into triples which is a solution simultaneously to both problems given above.

8.3.2 Information from semidefinite programming

Since $B_3^L(5,7,9) \approx 15.000..$, we hoped to obtain information from the semidefinite programming output about a $(7,9)_5^L$-code of size 15 in a way analogous to Chapter 7: we hoped to find a list of orbits $\omega \in \Omega_3^d$ that are forbidden in a $(7,9)_5^L$-code of size 15. However, the output of $B_3^L(5,7,9) = 15$ does not appear to give more information than we already have. Only orbits that contain Lee distances $\neq 9$ are forbidden by this output in a $(7,9)_5^L$-code of size 15. So the code is equidistant, but this follows already from the above considerations with (8.11). In the next section, we give a larger semidefinite program that yields more information about $(7,9)_5^L$ codes of size 15. The new information is described in Section 8.3.2, where we also briefly describe the procedure from Section 7.2.1.

A quadruple SDP-bound

We consider the following bound, which is a bound in between $B_{k-1}^L(q,n,d)$ and $B_k^L(q,n,d)$ (cf. [70]):

$$\begin{aligned} b_k^L(q,n,d) := \max\{\textstyle\sum_{v\in\mathbb{Z}_q^n} x(\{v\}) \mid x : \mathcal{C}_k \to \mathbb{R},\ x(\emptyset) = 1, x(S) = 0 \text{ if } d_{\text{min}}^L(S) < d,\\ M_{k-1,D}(x|_{\mathcal{C}_{k-1}}) \succeq 0 \text{ for each } D \in \mathcal{C}_{k-1} \text{ with } |D| < 2,\\ M_{k,D}(x) \succeq 0 \text{ for each } D \in \mathcal{C}_k \text{ with } |D| \geq 2\}. \end{aligned} \tag{8.14}$$

[1] Note that the $\{0,1\}$-matrix of order 7×7 which has 1's precisely in the positions where $\widetilde{M}$ is 1 and the $\{0,1\}$-matrix of order 7×7 which has 1's precisely where $\widetilde{M}$ is 3, both are incidence matrices of Fano planes [13] (with disjoint support).

We consider the bound $b_4^L(q,n,d)$. In the definition, it can be assumed that $x : \mathcal{C}_4 \to \mathbb{R}_{\geq 0}$. The reductions for the cases $D = \emptyset$ and $|D| = 1$ can be found in Section 8.2. In Appendix 8.5.2 we describe in detail how to block diagonalize $M_{4,D}(z)$ if $|D| = 2$. The matrices $M_{4,D}(z)$ for $|D| \in \{3,4\}$ are 1×1 matrices, hence they form their own block diagonalization.

Six orbits

The semidefinite program for computing $b_4^L(5,7,9)$ is very large, even after symmetry reductions. It contains 292, 483 variables after reductions, i.e., $D_5^7 \rtimes S_7$-orbits of nonempty codes in $\mathcal{C}_4$ with minimum Lee distance at least 9. Since any $(7,9)_5^L$-code of size 15 is equidistant with Lee distance 9, we add to $b_4^L(5,7,9)$ the constraint that $y(\omega) = 0$ if ω is an orbit of a code in which some pair of words has Lee distance unequal to 9. Write $b_4^L(5,7,9)_{\text{eq}}$ for the resulting semidefinite program. It contains only 1, 632 variables.

The program for computing $b_4^L(5,7,9)_{\text{eq}}$ contains constraints $z(\omega) \geq 0$ for every $\omega \in \Omega_4^d \setminus \{\{\emptyset\}\}$ that corresponds to an equidistant code with Lee distance 9, and we write (X_ω) for the 1×1 block corresponding to $(z(\omega))$ in the dual semidefinite program. Then $X_\omega > 0$ in any solution to the dual program implies that $z(\omega) = 0$ in all primal solutions to the semidefinite program, as explained in Chapter 7, which implies that no code of size 15 can contain a subcode D with $D \in \omega$. (Suppose otherwise; then one constructs a feasible solution to $b_4^L(5,7,9)_{\text{eq}}$ by putting $x(S) = 1$ for $S \in \mathcal{C}_k$ with $S \subseteq C$ and $x(S) = 0$ else, and hence by averaging over $H = D_5^7 \rtimes S_7$ we find a feasible H-invariant solution with $z(\omega) \geq 1/|H| > 0$, a contradiction.) If $X_\omega > 0$ in any dual solution, we call ω a *forbidden* orbit.

We used the solver SDPA-GMP [61, 96] to conclude which orbits are forbidden. The semidefinite programming solver does not produce exact solutions, but approximations up to a certain precision. All matrices in our approximate solution to the dual program were verified to be positive semidefinite (even strictly positive definite). This allows us to use equations (7.14)-(7.17) in Chapter 7 to verify with certainty which orbits are forbidden. (To use (7.17), we need a specific lower bound on $z(\omega)$ for non-forbidden orbits ω; in this case the lower bound of $1/|H| > 10^{-11}$ from the previous paragraph suffices.)

There are only six non-forbidden orbits in Ω_4 of equidistant codes with Lee distance 9 of cardinality 4 for which there is one coordinate in which three of the codewords have the same symbol, say α, and the last codeword has a symbol at Lee distance 1 from α. Here we list one representative N_i from each of these six orbits:

$$\begin{aligned}
N_1 &:= \{0000000, 0012222, 0230234, 1123414\},\\
N_2 &:= \{0000000, 0012222, 0230234, 1124413\},\\
N_3 &:= \{0000000, 0012222, 0230234, 1232002\},\\
N_4 &:= \{0000000, 0012222, 0230234, 1303424\},\\
N_5 &:= \{0000000, 0012222, 0230234, 1424341\},\\
N_6 &:= \{0000000, 0111222, 0222444, 1033023\}.
\end{aligned}$$

So any $(7,9)_5^L$-code of size 15 is equivalent to a $(7,9)_5^L$-code containing one of the N_i as a subcode.

8.3.3 Uniqueness of $A_5^L(7,9)=15$

We now descibe how one can obtain all possible $(7,9)_5^L$-codes of size 15 that contain N_i, for $i=1,\ldots,6$. For each $i=1,\ldots,6$, we do the following.

Let R_i be the set of all words in $\mathbb{Z}_5^7$ that have Lee distance 9 to all words in N_i. Let $R_{j,i}$, for each $j\in\{2,3,4\}$, be the collection of all triples of codewords in R_i with the property that each word starts with symbol j and that the triple is equidistant with Lee distance 9. Also, let $R_{1,i}$ be the collection of all pairs of codewords in R_i that start with symbol 1 and have Lee distance 9. Now observe that each $(7,9)_5^L$-code C of size 15 that contains N_i is a union of N_i and exactly one element in $R_{j,i}$ for each $j=1,\ldots,4$ (here note that each element in $R_{j,i}$ is a set consisting of 3 words if $j\in\{2,3,4\}$, and consisting of 2 words if $j=1$), as C is equidistant with Lee distance 9 and each symbol occurs exactly 3 times at the first (more generally: at any) position. The computer finds

$$\max_{i=1,\ldots,6}\left\{\prod_{j=1}^4|R_{j,i}|\right\}=528,384,$$

so a computer quickly enumerates all possible four-tuples $(T_1,T_2,T_3,T_4)\in R_{1,i}\times R_{2,i}\times R_{3,i}\times R_{4,i}$ and verifies whether $N_i\cup(\cup_{j=1}^4T_j)$ indeed has minimum Lee distance 9. In this way one obtains all possible $(7,9)_5^L$-codes C of size 15 that contain N_i. It is found that for each of N_1, N_4, N_5 there is only one $(7,9)_5^L$-code of size 15 containing N_i ($i=1,4,5$), while for each of N_2, N_3 and N_6, there are exactly two $(7,9)_5^L$-codes of size 15 containing N_i ($i=2,3,6$).

It remains to classify the 9 obtained codes. To do this, the graph isomorphism program `nauty` [60] is used. For each $(7,9)_5^L$-code C of size 15, a graph with $5\cdot7+15$ vertices is created: one vertex for each codeword $u\in C$ and five vertices $0_k,1_k,2_k,3_k,4_k$ for each coordinate position $k=1,\ldots,7$. Each code word u has neighbor a_k if $u_i=a$ ($i=1,\ldots,15$). Also, there are edges $\{0_k,1_k\},\{1_k,2_k\},\{2_k,3_k\},\{3_k,4_k\},\{4_k,0_k\}$ ($k=1,\ldots,7$).

The codewords have degree 7 and the coordinate positions have degree $2+3=5$ (as each symbol occurs exactly 3 times at each coordinate position). An automorphism of this graph permutes the codewords and permutes the coordinate positions. So two $(7,9)_5^L$-codes C of size 15 are equivalent if and only if the corresponding graphs are equivalent. In this way we find that all nine codes are equivalent, so the $(7,9)_5^L$-code of size 15 is unique. One of the two extensions of N_6 is for example

$$\begin{aligned}C:=\{&0000000,0111222,0222444,1033023,1303302,1330230,2142141,2214114,\\&2421411,3013330,3130303,3301033,4244421,4424142,4442214\}.\end{aligned}$$

The reader may check that it is equivalent to the code $\widetilde{M}\cup-\widetilde{M}\cup\{\mathbf{0}\}$, with $\widetilde{M}$ as in (8.13).

8.4 The unique code achieving $A_6^L(4,6)=18$

Let C be any $(4,6)_6^L$-code of cardinality 18. The solution of $B_2^L(6,4,6)\approx18.000..$ shows, by considering the forbidden orbits from the semidefinite programming output in a similar way as in the previous section, that any pair of codewords in C is contained in the same $D_6^4\rtimes S_4$-orbit as one of the following codes:

$$M_1:=\{0000,0222\},\quad M_2:=\{0000,1113\},\quad M_3:=\{0000,3333\}. \tag{8.15}$$

Assume that $\mathbf{0} \in C$. By (8.15), each word in C contains only symbols in $\{0, 2, 4\}$ or only symbols in $\{1, 3, 5\}$. As $A_3^L(4, 3) = 9$, there are at most 9 words containing only symbols $\{0, 2, 4\}$ in C and there are at most 9 words containing only symbols $\{1, 3, 5\}$ in C. As $|C| = 18$, the code C contains precisely 9 words with only symbols in $\{0, 2, 4\}$ and precisely 9 words with only symbols in $\{1, 3, 5\}$. It is well known that the $(4, 3)_3^H = (4, 3)_3^L$-code of size 9 is unique up to equivalence [64]. It is (up to equivalence) the code

$$B := \{0000, 0111, 0222, 1012, 1120, 1201, 2021, 2102, 2210\}.$$

As D_6 contains a subgroup that acts as $D_3 = S_3$ on $\{0, 2, 4\}$, we may assume that $C' := 2B \pmod 6$ is a subcode of C. Now we enumerate all 33 words $v \in \mathbb{Z}_6^4$ such that $\{\mathbf{0}, v\}$ is in the same $D_6^4 \rtimes S_4$-orbit as M_2 or M_3. There are only 9 of those words with Lee distance ≥ 6 to all words in C'. So these are the only 9 words that could be contained in a $(4, 6)_6^L$-code of size 18 together with all words from C'. Let us call the code formed by these 9 words C''. So

$$\begin{aligned} C' &= \{0000, 0222, 0444, 2024, 2240, 2402, 4042, 4204, 4420\}, \\ C'' &= \{1153, 1315, 1531, 3111, 3555, 5135, 5351, 5513, 3333\} = 3333 + C'. \end{aligned}$$

It is not hard to verify that $C' \cup C''$ has minimum Lee distance 6. So $C' \cup C''$ is a $(4, 6)_6^L$-code of cardinality 18, and it is the only such code (up to Lee equivalence).

8.5 Appendices

8.5.1 Appendix 1: The formulas $(F_i)_{j,h}$

Formulas for Section 8.2.1. Let all notation be as in Section 8.2.1 and Figure 8.1. For the computations in Section 8.2.1, we calculate the linear expressions

$$(F_i)_{j,h} = (B_i(j) \otimes B_i(h))|_W = \sum_{P \in \Lambda} (B_i(j) \otimes B_i(h))(a_P) a_P^* \in W^*,$$

for $i = 1, 2$ and $j, h = 1, \ldots, m_i$. This is routine, but we display the expressions. We denote an equivalence class P in $\Lambda = (\mathbb{Z}_q \times \mathbb{Z}_q)/S_2$ by its lexicographically smallest element. We find

$$\begin{aligned} (F_1)_{1,1} &= 1a_{00}^*, \\ (F_1)_{1,j+1} &= 2a_{0j}^*, \text{ for } j = 1, \ldots, \lfloor q/2 \rfloor \\ (F_1)_{j+1,1} &= 2a_{j0}^*, \text{ for } j = 1, \ldots, \lfloor q/2 \rfloor \\ (F_1)_{j+1,h+1} &= 2a_{jh}^* + 2a_{j(q-h)}^*, \text{ for } j, h \in \{1, \ldots, \lfloor q/2 \rfloor\}, \\ (F_2)_{j,h} &= 2a_{jh}^* - 2a_{j(q-h)}^*, \text{ for } j, h \in \{1, \ldots, \lfloor (q-1)/2 \rfloor\}. \end{aligned} \tag{8.16}$$

Formulas for Section 8.2.2. Now, let all notation be as in Section 8.2.2 and Figure 8.2. For the computations in Section 8.2.2, we calculate the linear expressions

$$(F_i)_{1,1} = (B_i \otimes B_i)|_W = \sum_{P \in \Lambda} (B_i \otimes B_i)(a_P) a_P^* \in W^*,$$

for $i = 1, \ldots, k$, where $k = \lfloor q/2 \rfloor + 1$. We denote an equivalence class P in $\Lambda = (\mathbb{Z}_q \times \mathbb{Z}_q)/D_q$ by its lexicographically smallest element. We find for even q, for $i \in \{1, \ldots, k\}$,

$$(F_i)_{1,1} = q \left(a^*_{00} + (-1)^{(i-1)} a^*_{0(q/2)} + 2 \sum_{j=1}^{\lfloor q/2 \rfloor - 1} \cos(2\pi j(i-1)/q) a^*_{0j} \right), \tag{8.17}$$

and for odd q, for $i \in \{1, \ldots, k\}$,

$$(F_i)_{1,1} = q \left(a^*_{00} + 2 \sum_{j=1}^{(q-1)/2} \cos(2\pi j(i-1)/q) a^*_{0j} \right). \tag{8.18}$$

Note that the formulas in (8.17) and (8.18) contain irrational numbers for $q \notin \{2, 3, 4, 6\}$. In the symmetry reduction of $M_{2,\emptyset}(z)$, it is possible to obtain matrix blocks which only contain integers: one may use the representative set for the reflection action S_2 on $\mathbb{C}^{\mathbb{Z}_q}$ instead of the representative set of the action of D_q on $\mathbb{C}^{\mathbb{Z}_q}$ to reduce the matrix $M_{2,\emptyset}(z)$. This results in much larger matrix blocks, but they only contain integers. We leave the details to the reader, see [71].

8.5.2 Appendix 2: Block diagonalizing $M_{4,D}(z)$ if $|D| = 2$

Here we sketch how to block diagonalize $M_{4,D}(z)$ if $|D| = 2$, for computing $b^L_4(q, n, d)$. We only consider the case $q = 5$, but the reductions can be easily generalized to higher q. (However, although the semidefinite programs are of polynomial size, they get very large in practice.) We can assume that $D = \{\mathbf{0}, v_1\}$ with

$$\begin{aligned} \mathbf{0} &= 0 \ldots 0\, 0 \ldots 0\ 0 \ldots 0 \\ v_1 &= \underbrace{0 \ldots 0}_{j_1} \underbrace{1 \ldots 1}_{j_2} \underbrace{2 \ldots 2}_{j_3}, \end{aligned} \tag{8.19}$$

where $j_2 + 2j_3 \geq d$. The rows and the columns of $M_{4,D}(y)$ are parametrized by codes $C \supseteq D$ of size at most 3.

Let H'_D be the group of distance-preserving permutations of $\mathcal{C}_4$ that fix $\mathbf{0}$ and v_1. So

$$H'_D \cong (S_2^{j_1} \rtimes S_{j_1}) \times S_{j_2} \times S_{j_3}. \tag{8.20}$$

We first describe a representative set for the action of H'_D on $\mathbb{C}^{\mathbb{Z}_5^n}$. We use the notation of Section 3.3. Fix $s = 3$. For $i = 1, \ldots, 3$, set $Z_i := \mathbb{Z}_5$. Set $G_1 = S_2$ and $G_i := \{1\}$ (the trivial group) for $i \in \{2, 3\}$. Furthermore, set $k_1 := 2$, $k_2 := 1$, $k_3 := 1$. Set $B_1^{(1)} := B_1$ from (8.5) and $B_2^{(1)} := B_2$ from (8.5), and set $\boldsymbol{B^{(1)}} := \{B_1^{(1)}, B_2^{(1)}\}$. Finally, let, for $i = 2, 3$, $B_1^{(i)} := [e_0, e_1, e_2, e_3, e_4]$ be the matrix with as columns the standard basis vectors in $\mathbb{C}^{\mathbb{Z}_5}$, i.e., the 5×5 identity matrix, and set $\boldsymbol{B^{(i)}} := \{B_1^{(i)}\}$. For convenience of the reader, we restate the main definitions of Section 3.3 and the main facts about representative sets applied to the context of this section — see Figure 8.3.

With Proposition 3.1.1, we obtain representative sets for the separate actions of of $G_i^{j_i} \rtimes S_{j_i}$ on $\mathbb{C}^{\mathbb{Z}_5^{j_i}}$, for each $i = 1, 2, 3$. Subsequently, with (2.18) we obtain a representative set for the action of H'_D on $(\mathbb{C}^{\mathbb{Z}_5^{j_1}}) \otimes \ldots \otimes (\mathbb{C}^{\mathbb{Z}_5^{j_3}}) \cong \mathbb{C}^{\mathbb{Z}_5^n}$.

FACTS.

$s = 3$, (j_1, j_2, j_3) are fixed with $j_1 + j_2 + j_3 = n$ and $j_2 + 2j_3 \geq d$.

$G_1 := S_2$, $G_i := \{1\}$, the trivial group, for $i = 2, 3$.
$Z_i := \mathbb{Z}_5$, for $i = 1, 2, 3$.

$k_1 := 2$, $k_2 := 1$, $k_3 := 1$.
$\boldsymbol{m}^{(1)} := (3, 2)$, $\boldsymbol{m}^{(2)} := (5)$, $\boldsymbol{m}^{(3)} := (5)$.

A representative set for the action of G_i on Z_i is $\boldsymbol{B}^{(i)}$ from Sect. 8.5.2.
A representative set for the action of H'_D on $(\mathbb{C}^{Z_1})^{\otimes j_1} \otimes \ldots \otimes (\mathbb{C}^{Z_3})^{\otimes j_3}$ follows from (3.3) and (2.18).

$\Lambda_i := (Z_i \times Z_i)/G_i$.
$a_P := \sum_{(x,y)\in P} x \otimes y$ for $P \in \Lambda_i$.
$A_i := \{a_P \,|\, P \in \Lambda_i\}$, a basis of $W_i := (\mathbb{C}Z_i \otimes \mathbb{C}Z_i)^{G_i}$.
$K^{(i)}_{\omega_i} := \sum_{(P_1,\ldots,P_{j_i})\in\omega_i} a_{P_1} \otimes \cdots \otimes a_{P_{j_i}}$ for $\omega_i \in \Lambda_i^{j_i}/S_{j_i}$.

Figure 8.3: The main definitions of Section 3.3 and the main facts about representative sets applied to the context of Section 8.5.2.

Sketch of the computations for $|D| = 2$

Fix $D = \{\mathbf{0}, v_1\} \in \mathcal{C}_4$. Let $\Omega_4(D)$ denote the set of all $D_5^n \rtimes S_n$-orbits of codes in $\mathcal{C}_4$ containing $D = \{\mathbf{0}, v_1\}$. For each $\omega \in \Omega_4(D)$, we define the $\mathbb{Z}_5^n \times \mathbb{Z}_5^n$ matrix N'_ω with entries in $\{0, 1\}$ by

$$(N'_\omega)_{\alpha,\beta} := \begin{cases} 1 & \text{if } \{\mathbf{0}, v_1, \alpha, \beta\} \in \omega, \\ 0 & \text{otherwise.} \end{cases} \tag{8.21}$$

Then, for each $z : \Omega_4(D) \to \mathbb{R}$, one has $M_{4,D}(z) \succeq 0$ if and only if $\sum_{\omega\in\Omega_4(D)} z(\omega)N'_\omega \succeq 0$. (The implication"$\Longrightarrow$" follows from the fact that $L^{\mathsf{T}} M_{4,D}(z)L = \sum_{\omega\in\Omega_4(D)} z(\omega)N'_\omega$, where L is the $\mathcal{C}_4(D) \times \mathbb{Z}_5^n$ matrix with $0, 1$ entries satisfying $L_{C,\alpha} = 1$ if and only if $C = \{\mathbf{0}, v_1, \alpha\}$, for $C \in \mathcal{C}_4(D)$ and $\alpha \in \mathbb{Z}_5^n$.)

As in Sect. 3.3, let $R = Z_1^{j_1} \times \ldots \times Z_3^{j_3}$, so $R = \mathbb{Z}_5^{j_1} \times \mathbb{Z}_5^{j_2} \times \mathbb{Z}_5^{j_3} \cong \mathbb{Z}_5^n$. Then the function

$$\begin{gathered} R^2 = \left(\mathbb{Z}_5^{j_1} \times \mathbb{Z}_5^{j_2} \times \mathbb{Z}_5^{j_3}\right)^2 \to \mathcal{C}_4, \\ ((\alpha^1, \alpha^2, \alpha^3), (\beta^1, \beta^2, \beta^3)) \mapsto \{\mathbf{0}, v_1, \alpha^1\alpha^2\alpha^3, \beta^1\beta^2\beta^3\}, \end{gathered} \tag{8.22}$$

induces a surjective function $r' : R^2/H'_D \to \Omega_4(D)$. For any $\omega' \in R^2/H'_D$, the matrix $K_{\omega'}$ is defined in (3.20). If $\omega \in \Omega_4(D)$, then in view of Lemma 4.3.1 we obtain

$$N'_\omega = \sum_{\substack{\omega'\in R^2/H'_D \\ r'(\omega')=\omega}} K_{\omega'}. \tag{8.23}$$

With the help of the representative set of the action of H'_D on $\mathbb{C}^{\mathbb{Z}_5^n}$, equation (2.17) gives a symmetry reduction of $\sum_{\omega\in\Omega_4(D)} z(\omega)N'_\omega$ to size polynomially bounded in n. The computation of the matrix entries in the reduced matrix can also be done in polynomial time, using (8.23), (3.21), (2.19) and Proposition 3.2.1. See also Section 6.2.1 about the computations for the case $|D| = 2$ for constant weight codes, which is a highly similar case.

8.5.3 Appendix 3: An overview of the program

In this section we give a high-level overview of the program for generating semidefinite programs to compute $B_3^L(q,n,d)$ (or $B_3^{L_\infty}(q,n,d)$ from Section 9.5 below). See Figure 8.4 for an outline of the method. Here we write ω_0 for the unique $D_q^n \rtimes S_n$-orbit corresponding to a code of size 1.[2]

[2] The programs we used to generate input for the SDP-solver can be found at `https://drive.google.com/open?id=1-XRbfc4TYhoySC33GRWfvNEMOZEltg6X`. (also accessible via the author's website).

```
Input:  Natural numbers $q, n$
Output: Semidefinite program to compute $B_3^L(q,n,1)$

print Maximize $q^n z(\omega_0)$
print Subject to:
//Start with $|D| = 1$. The definitions are as in Sect. 8.2.1.
foreach $\boldsymbol{n} = (n_1, n_2) \in \boldsymbol{N}$
//Recall: $\boldsymbol{m} = (m_1, m_2) = (\lfloor q/2 \rfloor + 1, \lfloor (q-1)/2 \rfloor)$.
    foreach $\boldsymbol{\lambda} = (\lambda_1, \lambda_2) \vdash \boldsymbol{n}$ with height$(\lambda_1) \leq m_1$, height$(\lambda_2) \leq m_2$
        start a new block $M_{\boldsymbol{\lambda}}$
        foreach $\boldsymbol{\tau} \in \boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}$ from (3.1)
            foreach $\boldsymbol{\sigma} \in \boldsymbol{T}_{\boldsymbol{\lambda},\boldsymbol{m}}$ from (3.1)
                compute $\prod_{i=1}^{2} p_{\tau_i,\sigma_i}(F_i)$ (cf. the definitions in (3.14) and (3.13))
                replace each degree $n$ monomial $\mu$ in variables $a_P^*$ by a variable $z(r(\mu))$
                $(M_{\boldsymbol{\lambda}})_{\boldsymbol{\tau},\boldsymbol{\sigma}}$ := the resulting linear polynomial in variables $z(\omega)$
            end
        end
        print $M_{\boldsymbol{\lambda}} \succeq 0$
    end
end
//Now $D = \emptyset$. The definitions are as in Sect. 8.2.2.
foreach $\boldsymbol{n} \in \boldsymbol{N}$
    start a new $(1 \times 1)$ block $M_{\boldsymbol{n}}$
    compute $\prod_{i=1}^{k} p_{(\boldsymbol{\tau_n})_i,(\boldsymbol{\tau_n})_i}(F_i)$ (cf. the definitions in (3.14) and Sect. 8.2.2)
    replace each degree $n$ monomial $\mu$ in variables $a_P^*$ by a variable $z(\widetilde{r}(\mu))$
    $(M_{\boldsymbol{n}})$ := (the resulting linear polynomial in variables $z(\omega)$)
    if $\boldsymbol{n} = (n, 0, \ldots, 0)$ //Add a row and a column corresponding to $\emptyset$.
        add a row and column to $M_{\boldsymbol{n}}$ indexed by $\emptyset$
        put $(M_{\boldsymbol{n}})_{\emptyset,\emptyset} := 1$ and $(M_{\boldsymbol{n}})_{\boldsymbol{\tau_n},\emptyset} = (M_{\boldsymbol{n}})_{\emptyset,\boldsymbol{\tau_n}} := q^n z(\omega_0)$
    end
    print $M_{\boldsymbol{n}} \succeq 0$
end
//Now nonnegativity of all variables.
foreach $\omega \in \Omega_3$
    print $z(\omega) \geq 0$
end
```

Figure 8.4: Algorithm to generate semidefinite programs for computing $B_3^L(q,n,1)$. To compute $B_3^L(q,n,d)$ (or $B_3^{L_\infty}(q,n,d)$ from Sect. 9.5 below), one must set all variables $z(\omega)$ with $\omega \in \Omega_3$ an orbit corresponding to a code of minimum Lee (respectively, Lee$_\infty$) distance $< d$ to zero. If rows and columns of matrix blocks consist solely of zeros after the replacement, one can remove these rows and columns.

Chapter 9

The Shannon capacity of circular graphs

We may have knowledge of the past but cannot control it;
we may control the future but have no knowledge of it.
— Claude Shannon (1916–2001)

In this chapter we consider the Shannon capacity $\Theta(C_{d,q})$ of circular graphs $C_{d,q}$. The circular graph $C_{d,q}$ is the graph with vertex set $\mathbb{Z}_q$ (the cyclic group of order q) in which two distinct vertices are adjacent if and only if their distance (mod q) is strictly less than d. The value of $\Theta(C_{d,q})$ can be seen to only depend on the quotient q/d.

We show that the function $q/d \mapsto \Theta(C_{d,q})$ is continuous at *integer* points $q/d \geq 3$. We also prove that the independent set achieving $\alpha(C_{5,14}^{\boxtimes 3}) = 14$, one of the independent sets used in our proof, is unique up to Lee equivalence. Furthermore, we adapt the SDP bound of Chapter 8 to an upper bound on $\alpha(C_{d,q}^{\boxtimes n})$ based on triples of codewords. Finally, we give a new lower bound of $367^{1/5}$ on the Shannon capacity of the 7-cycle. This chapter is based on joint work with Lex Schrijver, part of which can be found in [72].

9.1 Introduction

Let $G = (V, E)$ and $H = (V', E')$ be graphs. Recall that the *strong product* $G \boxtimes H$ is the graph with vertex set $V \times V'$ in which two distinct vertices (u, u') and (v, v') are adjacent if ($u = v$ or $uv \in E$) and ($u' = v'$ or $u'v' \in E'$) (cf. Sect. 1.5). For $n \in \mathbb{N}$, write

$$G^{\boxtimes n} := \underbrace{G \boxtimes G \boxtimes \ldots \boxtimes G}_{n \text{ times}}.$$

So two distinct vertices $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$ of $G^{\boxtimes n}$ are adjacent if and only if for each $i \in \{1, \ldots, n\}$ one has either $u_i = v_i$ or $u_i v_i \in E$. Recall that an *independent set* in G is a subset U of V such that $e \not\subseteq U$ for all $e \in E$, and that $\alpha(G)$ denotes the *independent set number* of G: the maximum cardinality of an independent set in G. If U and U' are independent sets in G and H, respectively, then $U \times U'$ is independent in $G \boxtimes H$. So $\alpha(G \boxtimes H) \geq \alpha(G)\alpha(H)$.

The *Shannon capacity* of G is defined as

$$\Theta(G) := \sup_{n \in \mathbb{N}} \sqrt[n]{\alpha(G^{\boxtimes n})}. \tag{9.1}$$

As $\alpha(G^{\boxtimes(n_1+n_2)}) \geq \alpha(G^{\boxtimes n_1})\alpha(G^{\boxtimes n_2})$ for any two positive integers n_1 and n_2, Fekete's lemma (cf. [34], see also [80, Corollary 2.2a]) implies that $\Theta(G) = \lim_{n\to\infty} \sqrt[n]{\alpha(G^{\boxtimes n})}$.

The Shannon capacity was introduced by Shannon [86] and is an important and widely studied parameter in information theory (see e.g., [3, 18, 43, 53, 98]). It is the effective size of an alphabet in an information channel represented by the graph G. The input is a set of letters $V(G) = \{0, \dots, q-1\}$ and two letters are 'confusable' when transmitted over the channel if and only if there is an edge between them in G. Then $\alpha(G)$ is the maximum size of a set of pairwise non-confusable single letters. Moreover, $\alpha(G^{\boxtimes n})$ is the maximum size of a set of pairwise non-confusable n-letter words. (Here two n-letter words u, v are confusable if and only if u_i and v_i are confusable for all $1 \leq i \leq n$.) Taking n-th roots and letting n go to infinity, we find the effective size of the alphabet in the information channel: $\Theta(G)$.

A classical upper bound on Θ is Lovász's ϑ-function [53]. For any graph G, the number $\vartheta(G)$ is defined as

$$\vartheta(G) := \max\left\{\textstyle\sum_{u,v\in V} X_{u,v} \;\middle|\; X \in \mathbb{R}^{V\times V},\ \operatorname{tr}(X) = 1,\ X_{u,v} = 0 \text{ if } uv \in E,\ X \succeq 0\right\}. \tag{9.2}$$

The Shannon capacity of C_5, the cycle on 5 vertices, was already discussed by Shannon in 1956 [86], who showed $\sqrt{5} \leq \Theta(C_5) \leq 5/2$. The easy lower bound of $\sqrt{5}$ is obtained from the independent set $\{(0,0),(1,2),(2,4),(3,1),(4,3)\}$ in $C_5^{\boxtimes 2}$. More than twenty years later, Lovász [53] determined that $\Theta(C_5) = \sqrt{5}$ by proving an upper bound matching this lower bound: he showed $\Theta(C_5) \leq \vartheta(C_5) = \sqrt{5}$. More generally, for odd q,

$$\Theta(C_q) \leq \vartheta(C_q) = \frac{q\cos(\pi/q)}{1+\cos(\pi/q)}. \tag{9.3}$$

For q even it is not hard to see that $\Theta(C_q) = q/2$.

The Shannon capacity of C_7 is still unknown and its determination is a notorious open problem in extremal combinatorics [18, 39]. Many lower bounds have been given by explicit independent sets in some fixed power of C_7 [10, 56, 93], while the best known upper bound is $\Theta(C_7) \leq \vartheta(C_7) < 3.3177$. We give an independent set of size 367 in $C_7^{\boxtimes 5}$, which yields $\Theta(C_7) \geq 367^{1/5} > 3.2578$. The best previously known lower bound on $\Theta(C_7)$ is $\Theta(C_7) \geq 350^{1/5} > 3.2271$, found by Mathew and Östergård [56]. They proved that $\alpha(C_7^{\boxtimes 5}) \geq 350$ using stochastic search methods that utilize the symmetry of the problem. We obtain our new lower bound on $\alpha(C_7^{\boxtimes 5})$ and on $\Theta(C_7)$ by considering circular graphs.

For positive integers q, d with $q \geq 2d$, recall that the *circular graph* $C_{d,q}$ is the graph with vertex set $\mathbb{Z}_q$ (the cyclic group of order q) in which two distinct vertices are adjacent if and only if their distance (mod q) is strictly less than d. So $C_{2,q} = C_q$. The circular graphs have the property that $\alpha(C_{d,q}^{\boxtimes n})$ (for fixed n), $\vartheta(C_{d,q})$ and $\Theta(C_{d,q})$ only depend on the fraction q/d. Moreover, the three mentioned quantities are nondecreasing functions in q/d (see Section 9.2 for details). Lovász's sandwich theorem [53] (see also [48]) implies that

$$\Theta(C_{d,q}) \leq \vartheta(C_{d,q}) \leq q/d \qquad \text{for all } q, d \in \mathbb{N} \text{ with } q \geq 2d. \tag{9.4}$$

Here q/d is equal to the 'fractional clique cover number' of $C_{d,q}$, which is an upper bound on $\vartheta(C_{d,q})$ cf. [53] (see Section 9.2). Currently, the only known values of $\Theta(C_{d,q})$ for $q \geq 2d$ are for q/d integer and $q/d = 5/2$.

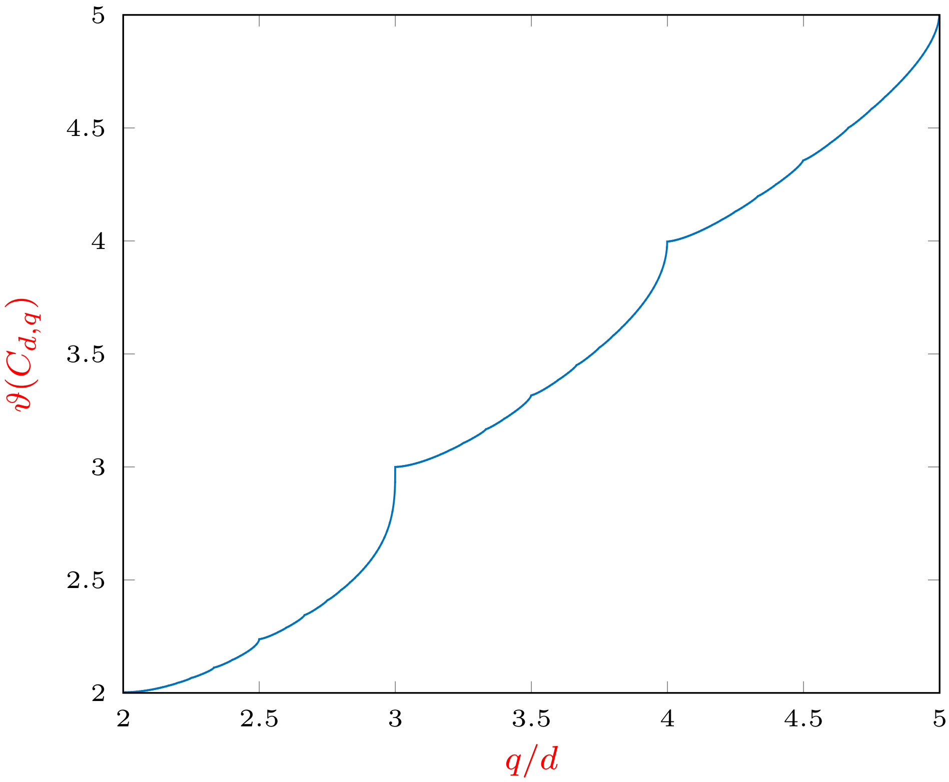


Figure 9.1: A graph of the function $q/d \mapsto \vartheta(C_{d,q})$.

The main result of this chapter is that the function $q/d \mapsto \Theta(C_{d,q})$ is continuous at *integers* $q/d = r \geq 3$, which implies that also $q/d \mapsto \vartheta(C_{d,q})$ is continuous at these points (by (9.4) and by the fact that $\Theta(C_{d,q}) = q/d$ if q/d is integer). Right-continuity of the two mentioned functions at integers $q/d = r \geq 2$ follows immediately from (9.4) in combination with the fact that $\Theta(C_{d,q}) = r$ if $q/d = r$ is an integer and the fact that $q/d \mapsto \Theta(C_{d,q})$ is a nondecreasing function in q/d. In order to prove left-continuity at integers $q/d = r \geq 3$, we show the following.

Theorem (Theorem 9.3.1)**.** *For each $r, n \in \mathbb{N}$ with $r \geq 3$,*

$$\max_{\frac{q}{d}<r} \alpha(C_{d,q}^{\boxtimes n}) = \frac{1 + r^n(r-2)}{r-1}.$$

The theorem will be used to prove that $\lim_{\frac{q}{d}\uparrow r} \Theta(C_{d,q}) = r$. As $\Theta(C_{d,q}) = r$ if $q/d = r$, it follows that $q/d \mapsto \Theta(C_{d,q})$ is left-continuous at r (and hence also $q/d \mapsto \vartheta(C_{d,q})$, by (9.4)). Continuity of $q/d \mapsto \Theta(C_{d,q})$ at *non*-integer points q/d seems hard to prove and even continuity of $q/d \mapsto \vartheta(C_{d,q})$ at these points is not yet known, although the latter function *looks* continuous (cf. Figure 9.1). We also prove that the independent set achieving $\alpha(C_{5,14}^{\boxtimes 3}) = 14$, one of the independent sets used in our proof of Theorem 9.3.1, is unique up to Lee equivalence.

In Section 9.5, we show how to adapt the bound $B_3^L(q,n,d)$ from Chapter 8 to an upper bound $B_3^{L\infty}(q,n,d)$ on $\alpha(C_{d,q}^{\boxtimes n})$. The new bound does not seem to improve significantly over the bound obtained from Lovász theta-function, except for very small n.

Finally, we give the mentioned independent set of size 367 in $C_7^{\boxtimes 5}$, demonstrating the new lower bound on $\Theta(C_7)$. It is obtained by adapting an independent set of size 382 in $C_{108,382}^{\boxtimes 5}$ which we found by computer, inspired by the construction used to prove Theorem 9.3.1.

9.2 Preliminaries on the Shannon capacity and circular graphs

In this section we give the preliminaries on the Shannon capacity and on circular graphs used throughout this chapter.

Graph homomorphisms and circular graphs. A homomorphism from a graph $G_1 = (V_1, E_1)$ to a graph $G_2 = (V_2, E_2)$ is a function $f : V_1 \to V_2$ such that if $ij \in E_1$ then $f(i)f(j) \in E_2$ (in particular, $f(i) \neq f(j)$). If there exists a homomorphism $f : G_1 \to G_2$ we write $G_1 \to G_2$. For any graph G, we write $\overline{G}$ for the complement of G. If $\overline{G} \to \overline{H}$, then $\alpha(G^{\boxtimes n}) \leq \alpha(H^{\boxtimes n})$ (for any n) and $\Theta(G) \leq \Theta(H)$. The circular graphs have the property that $\overline{C_{d',q'}} \to \overline{C_{d,q}}$ if and only if $q'/d' \leq q/d$ [19]. (The "if"-part follows from the following three facts, which are not hard to prove. Let $q, d \in \mathbb{N}$ with $q \geq 2d$, and let $t \in \mathbb{N}$. Then $\overline{C_{td,tq}} \to \overline{C_{d,q}}$, $\overline{C_{d,q}} \to \overline{C_{td,tq}}$ and $\overline{C_{d,q}} \to \overline{C_{d,q+1}}$.)

So if $q'/d' \leq q/d$, then $\alpha(C_{d',q'}^{\boxtimes n}) \leq \alpha(C_{d,q}^{\boxtimes n})$ (for any n) and $\Theta(C_{d',q'}) \leq \Theta(C_{d,q})$. Moreover, $\alpha(C_{d,q}^{\boxtimes n})$ and $\Theta(C_{d,q})$ only depend on the fraction q/d (fixing n).

Zuiddam's dual characterization of Θ. Let $\mathcal{G}$ denote the set of all finite, simple[1] graphs. Let Δ be the set of all functions $f : \mathcal{G} \to \mathbb{R}_{\geq 0}$ satisfying for all $G, H \in \mathcal{G}$:

(i) $f(G \sqcup H) = f(G) + f(H)$,
(ii) $f(G \boxtimes H) = f(G)f(H)$,
(iii) If $\overline{G} \to \overline{H}$, then $f(G) \leq f(H)$,
(iv) $f(K_1) = 1$.

Here $G \sqcup H$ is the graph with vertex set $V(G) \sqcup V(H)$ and edge set $E(G) \sqcup E(H)$, where $\sqcup$ denotes disjoint union. Note that Δ is compact in the Tychonoff product space $\mathbb{R}^{\mathcal{G}}$, since (i) – (iv) are closed conditions and $0 \leq f(G) \leq |V(G)|$ for all $G \in \mathcal{G}$, $f \in \Delta$.

If $f \in \Delta$ and $G \in \mathcal{G}$, then $\Theta(G) \leq f(G)$. This is not hard to see, by (iv) and (i) we have $\alpha(G) = f(\overline{K_{\alpha(G)}})$, so (iii) gives $\alpha(G) = f(\overline{K_{\alpha(G)}}) \leq f(G)$ (using that $K_{\alpha(G)} \to \overline{G}$), and (ii) then gives $\Theta(G) \leq f(G)$. Jeroen Zuiddam [98] proved that for any graph G,

$$\Theta(G) = \min_{f \in \Delta} f(G). \tag{9.5}$$

Zuiddam derived his theorem from Strassen's semiring theorem [89], using that $(\mathcal{G}, \sqcup, \boxtimes)$ is a commutative semiring with unit K_1 and with the empty graph as zero element. It is known that $\Theta \notin \Delta$, see Haemers [43]: there exists a $G \in \mathcal{G}$ (*the Schläfli graph*) satisfying $\Theta(G \boxtimes \overline{G}) \geq 27 > 3 \cdot 7 \geq \Theta(G)\Theta(\overline{G})$.

[1] A graph is *simple* if it has no loops or parallel edges.

One function contained in Δ is Lovász ϑ-function [53], which is defined in (9.2). There is a closed form formula for $\vartheta(C_{d,q})$, proved by Bachoc, Pêcher and Thiéry [8]:

$$\vartheta(C_{d,q}) = \frac{q}{d} \sum_{i=0}^{d-1} \prod_{j=1}^{d-1} \frac{\cos\left(\frac{2i\pi}{d}\right) - \cos\left(\lfloor \frac{qj}{d} \rfloor \frac{2\pi}{q}\right)}{1 - \cos\left(\lfloor \frac{qj}{d} \rfloor \frac{2\pi}{q}\right)}, \tag{9.6}$$

Another element of Δ is the fractional clique cover number, which was already observed to be an upper bound on Θ by Shannon [86]. Let $G \in \mathcal{G}$, and write $\mathcal{K}(G)$ for the collection of all *cliques* in G (a *clique* is a set of vertices, every two of which are adjacent). Then the fractional clique cover number $\overline{\chi}^*(G)$ admits the following definition:

$$\overline{\chi}^*(G) := \min \left\{ \textstyle\sum_{K \in \mathcal{K}(G)} y(K) \;\middle|\; y : \mathcal{K}(G) \to \mathbb{R}_{\geq 0},\ \forall\, v \in V : \textstyle\sum_{K \ni v} y(K) \geq 1 \right\}. \tag{9.7}$$

It is known that $\overline{\chi}^*(G) \in \Delta$ (see [80]). It is also known (cf. [58], see also [80, Theorem 67.17]) that

$$\overline{\chi}^*(G) = \inf_{n \in \mathbb{N}} \sqrt[n]{\overline{\chi}(G^{\boxtimes n})} = \lim_{n \to \infty} \sqrt[n]{\overline{\chi}(G^{\boxtimes n})}. \tag{9.8}$$

Here $\overline{\chi}(G)$ denotes the minimum number of cliques in G needed to cover the vertex set of G, the *clique cover number* of G. It is equal to $\min\{r \in \mathbb{N} : \overline{G} \to K_r\}$. If $f \in \Delta$, we have by (iv), (i), (iii) that $f(G) \leq \overline{\chi}(G)$, and (ii) and (9.8) then give $f(G) \leq \overline{\chi}^*(G)$. So

$$\overline{\chi}^*(G) = \max_{f \in \Delta} f(G). \tag{9.9}$$

Since the circular graph $C_{d,q}$ is vertex-transitive[2] and every vertex is contained in a clique of size d (but no vertex is contained in a larger clique), one can see that $\overline{\chi}^*(C_{d,q}) = q/d$. So if $f \in \Delta$, then

$$\begin{aligned} &\Theta(C_{d,q}) \leq f(C_{d,q}) \leq \overline{\chi}^*(G) = q/d \qquad \text{for all } q, d \in \mathbb{N} \text{ with } q \geq 2d, \\ &\text{with equality throughout if } q/d \text{ is an integer.} \end{aligned} \tag{9.10}$$

Note that (9.4) is a special case of (9.10).

Other known elements of Δ, which we do not discuss in detail here (see [98, 97]), are the *fractional orthogonal rank* (also called *projective rank*) [30] and the *fractional Haemers bound* [14, 27]. The latter parameter can be defined for any field $\mathbb{F}$, and a separation result of Bukh and Cox [27] shows that different fields $\mathbb{F}$ yield different parameters. So Δ contains infinitely many elements.

The Lee$_\infty$ distance. By definition there is an edge between two distinct vertices x, y of $C_{d,q}^{\boxtimes n}$ if and only if there is an $1 \leq i \leq n$ such that $x_i - y_i \pmod q$ is either strictly smaller than d or strictly larger than $q - d$. For distinct u, v in $\mathbb{Z}_q^n$, define their *Lee*$_\infty$ *distance* to be the maximum over the distances of u_i and $v_i \pmod q$, where i ranges from 1 to n. The *minimum Lee*$_\infty$ *distance* $d_{\text{min}}^{L_\infty}(D)$ of a set $D \subseteq \mathbb{Z}_q^n$ is the minimum distance between any

[2] A graph $G = (V, E)$ is *vertex-transitive* if for all $u, v \in V$ there exists an automorphism $g : V \to V$ of G such that $g(u) = v$.

pair of distinct elements of D. If $|D| \leq 1$, set $d_{\min}^{L_\infty}(D) = \infty$. Then $d_{\min}^{L_\infty} \geq k$ if and only if D is independent in $C_{d,q}^{\boxtimes n}$. So

$$A_q^{L_\infty}(n,d) := \alpha(C_{d,q}^{\boxtimes n}) = \max\{|C| \mid C \subseteq \mathbb{Z}_q^n,\ d_{\min}^{L_\infty}(C) \geq d\}. \tag{9.11}$$

It is well known that $\alpha(C_{d,q}^{\boxtimes n})$ is equal to the number of n-dimensional hypercubes of side d that can be packed in a discrete n-dimensional torus of width q [10].

9.3 Continuity of $q/d \mapsto \Theta(C_{d,q})$ at $q/d \in \mathbb{N}$

Let $C(\Delta, \infty)$ denote the Banach algebra of continuous functions $\Delta \to \mathbb{R}$, equipped with the $\|.\|_\infty$-norm. Then the evaluation map

$$\begin{aligned} \text{ev} : \mathcal{G} &\to C(\Delta, \infty) \\ G &\mapsto (f \mapsto f(G)) \end{aligned} \tag{9.12}$$

embeds $\mathcal{G}$ into $C(\Delta, \infty)$. A natural question to ask is whether the image of ev is closed. Since if not, the closure contains new ‘graph like’ objects not being graphs.

Natural candidates to investigate this question are the circular graphs $C_{d,q}$. By property (iii) of the functions in Δ, and by the fact that $\overline{C_{d',q'}} \to \overline{C_{d,q}}$ if and only if $q'/d' \leq q/d$, the image $\text{ev}(C_{d,q})$ only depends on the quotient q/d. The fractional clique cover number $\overline{\chi}^*(G)$ of any $G \in \mathcal{G}$ is a rational number, since it is the solution of a linear program with all input data rational [82]. Suppose that $q/d \mapsto \text{ev}(C_{d,q})$ is a continuous function in each $r \in \mathbb{Q}$ with $r \geq 2$. If $2 < s \in \mathbb{R} \setminus \mathbb{Q}$ with $q/d \to s$, then the limit of $(\text{ev}(C_{d,q}))$ is not the image $\text{ev}(G)$ of any $G \in \mathcal{G}$, as there is no $G \in \mathcal{G}$ with $\overline{\chi}^*(G) = s$. So in this case the image of ev is not closed.

So we aimed at proving continuity of $q/d \mapsto \text{ev}(C_{d,q})$ in each $r \in \mathbb{Q}$ with $r \geq 2$. However, we could not prove this. But for *integer* points $r \geq 3$, the function $q/d \mapsto \text{ev}(C_{d,q})$ is continuous at $q/d = r$. Right-continuity at integers $q/d = r \geq 2$ follows from (9.10) and the fact that $q/d \mapsto f(C_{d,q})$ is a nondecreasing function in q/d for each $f \in \Delta$. To prove left-continuity of $q/d \mapsto \text{ev}(C_{d,q})$ at integers $q/d = r \geq 3$, it suffices (again by (9.10)) to prove that $q/d \mapsto \Theta(C_{d,q})$ is left-continuous at these points.

Let $r \geq 3$ be an integer. We prove that if q/d tends to r from below, then $\Theta(C_{d,q})$ tends to r by proving the following:

Theorem 9.3.1. *For each $r, n \in \mathbb{N}$ with $r \geq 3$,*

$$\max_{\frac{q}{d} < r} \alpha(C_{d,q}^{\boxtimes n}) = \frac{1 + r^n(r-2)}{r-1}. \tag{9.13}$$

The theorem implies that

$$\sup_{\frac{q}{d}<r} \Theta(C_{d,q}) = \sup_{\frac{q}{d}<r} \sup_{n \in \mathbb{N}} \sqrt[n]{\alpha(C_{d,q}^{\boxtimes n})} = \sup_{n \in \mathbb{N}} \sup_{\frac{q}{d}<r} \sqrt[n]{\alpha(C_{d,q}^{\boxtimes n})} = \lim_{n \to \infty} \left(\frac{1 + r^n(r-2)}{r-1} \right)^{1/n} = r,$$

so the function $q/d \mapsto \Theta(C_{d,q})$ is left-continuous at r (using the fact that the function $q/d \mapsto \Theta(C_{d,q})$ is nondecreasing). Right-continuity of this function at integers ≥ 2 follows immediately from (9.10) and the fact that $q/d \mapsto \Theta(C_{d,q})$ is a nondecreasing function in q/d.

9.3.1 Proof of Theorem 9.3.1

In this section we prove Theorem 9.3.1. Throughout this section, fix an integer $r \geq 3$. Furthermore, we define for $n \in \mathbb{Z}_{\geq 0}$, the number

$$q_n := \frac{1 + r^n(r-2)}{r-1}. \tag{9.14}$$

First we prove:

Proposition 9.3.2. *For all $n \in \mathbb{N}$: $\max_{\frac{q}{d}<r} \alpha(C_{d,q}^{\boxtimes n}) \leq q_n$.*

Proof. Choose $q, d \in \mathbb{N}$ with $q \geq 2d$ and $q/d < r$. For each $n \in \mathbb{N}$, define $\alpha_n := \alpha(C_{d,q}^{\boxtimes n})$, and set $\alpha_0 := 1$. Let $A \subseteq \mathbb{Z}_q^n$ such that A is independent in $C_{d,q}^{\boxtimes n}$ with $|A| = \alpha_n$. We interprete A as an $\alpha_n \times n$ matrix with the words (elements of $\mathbb{Z}_q^n$) as rows. For $i \in \mathbb{Z}_q$, let c_i be the number of times symbol i occurs in column 1. Then $\sum_{i=t+1}^{t+d} c_i \leq \alpha_{n-1}$ for any $t \in \mathbb{Z}_q$, where we take indices of c mod q. So

$$d\alpha_n = d\sum_{i=0}^{q-1} c_i = \sum_{t=0}^{q-1} \sum_{i=t+1}^{t+d} c_i \leq q\alpha_{n-1}. \tag{9.15}$$

This implies that $\alpha_n \leq \lfloor q\alpha_{n-1}/d \rfloor \leq r\alpha_{n-1} - 1$. By induction we conclude

$$\alpha_n \leq r\alpha_{n-1} - 1 \leq rq_{n-1} - 1 = q_n.$$ □

To prove Theorem 9.3.1, it remains to show that for all $n \in \mathbb{N}$,

$$\max_{\frac{q}{d}<r} \alpha(C_{d,q}^{\boxtimes n}) \geq q_n. \tag{9.16}$$

Note that

$$\frac{q_n}{q_{n-1}} = \frac{1 + r^n(r-2)}{1 + r^{n-1}(r-2)} = r\left(\frac{1 + r^n(r-2)}{r + r^n(r-2)}\right) < r.$$

So in order to prove (9.16), it suffices to give an explicit independent set of size q_n in $C_{q_{n-1},q_n}^{\boxtimes n}$. In this chapter we use the notation $[a, b] := \{a, a+1, \ldots, b\}$ for any two integers a, b.

Theorem 9.3.3. *The set $S := \{t \cdot (1, r, \ldots, r^{n-1}) \,|\, t \in \mathbb{Z}_{q_n}\} \subseteq \mathbb{Z}_{q_n}^n$ is independent in $C_{q_{n-1},q_n}^{\boxtimes n}$.*

Proof. Note that $x, y \in S$ implies that also $x - y \in S$. So in order to prove the theorem, it suffices to prove that for all nonzero $x = t \cdot (1, r, \ldots, r^{n-1}) \in S$ there exists $i \in [1, n]$ such that $x_i \in [q_{n-1}, q_n - q_{n-1}] = [q_{n-1}, (r-1)q_{n-1} - 1]$. So we must prove:

$$\begin{aligned} &\text{for all } t \in [1, q_n - 1] \text{ there exists } i \in [0, n-1] \text{ such that} \\ &tr^i \pmod{q_n} \in [q_{n-1}, (r-1)q_{n-1} - 1]. \end{aligned} \tag{9.17}$$

In order to prove (9.17) we first prove:

Proposition 9.3.4. *Let $k \in [1, n]$, $j \in [0, (q_{n-k} - 1)/(r-2)]$. If $t \in [q_{k-1} + j(r-2)r^k, (r-1)q_{k-1} - 1 + j(r-2)r^k]$, then*

$$(r-1)jq_n \in [A(t), B(t)] := [tr^{n-k} - (r-1)q_{n-1} + 1, tr^{n-k} - q_{n-1}].$$

In particular, $tr^{n-k} \pmod{q_n} \in [q_{n-1}, (r-1)q_{n-1} - 1]$.

Proof. Let $t_1 = q_{k-1} + j(r-2)r^k$ and $t_2 = (r-1)q_{k-1} - 1 + j(r-2)r^k$. So $t_1 \leq t \leq t_2$. Note that

$$\begin{aligned} B(t) \geq B(t_1) &= (q_{k-1} + j(r-2)r^k)r^{n-k} - q_{n-1} = \frac{r^{n-k}-1}{r-1} + j(r-2)r^n \\ &\geq j + j(r-2)r^n = (r-1)jq_n, \end{aligned}$$

as $j \leq (q_{n-k}-1)/(r-2) = (r^{n-k}-1)/(r-1)$. Furthermore,

$$\begin{aligned} A(t) \leq A(t_2) &= ((r-1)q_{k-1} - 1 + j(r-2)r^k)r^{n-k} - (r-1)q_{n-1} + 1 \\ &= j(r-2)r^n \leq j + j(r-2)r^n = (r-1)jq_n. \end{aligned}$$

Hence $(r-1)jq_n \in [A(t), B(t)]$. □

We now continue the proof of (9.17), hence of Theorem 9.3.3. Let $t \in [1, q_n - 1]$. To finish the proof of (9.17), we show that

$$\begin{aligned} &\text{there exists } k \in [1,n] \text{ and } j \in [0, (q_{n-k}-1)/(r-2)] \\ &\text{such that } t \in [q_{k-1} + j(r-2)r^k, (r-1)q_{k-1} - 1 + j(r-2)r^k]. \end{aligned} \tag{9.18}$$

Assuming (9.18), Proposition 9.3.4 implies that $tr^{n-k} \pmod{q_n} \in [q_{n-1}, (r-1)q_{n-1} - 1]$, hence (9.17) is satisfied with $i = n - k$, as desired. So it remains to prove (9.18) for each $t \in [1, q_n - 1]$. To do that, we must show:

$$\bigcup_{k\in[1,n]} \bigcup_{j\in[0,(q_{n-k}-1)/(r-2)]} [q_{k-1} + j(r-2)r^k, (r-1)q_{k-1} - 1 + j(r-2)r^k] \supseteq [1, q_n - 1]. \tag{9.19}$$

We use induction on n. If $n = 0$ then the assertion is clear. Assume that (9.19) holds for $n-1$ instead of n, i.e.,

$$\bigcup_{k\in[1,n-1]} \bigcup_{j\in[0,(q_{n-1-k}-1)/(r-2)]} [q_{k-1} + j(r-2)r^k, (r-1)q_{k-1} - 1 + j(r-2)r^k] \supseteq [1, q_{n-1} - 1]. \tag{9.20}$$

Then adding $(r-2)r^{n-1}$ to both sides in (9.20) gives

$$\begin{aligned} &\bigcup_{k\in[1,n-1]} \bigcup_{j\in[0,(q_{n-1-k}-1)/(r-2)]} [q_{k-1} + j(r-2)r^k + (r-2)r^{n-1}, \\ &\qquad\qquad (r-1)q_{k-1} - 1 + j(r-2)r^k + (r-2)r^{n-1}] \\ &\supseteq [(r-2)r^{n-1} + 1, (r-2)r^{n-1} + q_{n-1} - 1] = [(r-1)q_{n-1}, q_n - 1]. \end{aligned} \tag{9.21}$$

Note that $j(r-2)r^k + (r-2)r^{n-1} = (j + r^{n-k-1})(r-2)r^k$. Moreover, for $j \in [0, (q_{n-1-k} - 1)/(r-2)]$ one has

$$j + r^{n-k-1} \leq (q_{n-1-k} - 1)/(r-2) + r^{n-k-1} = (q_{n-k} - 1)/(r-2).$$

So (9.21) becomes (by replacing $j + r^{n-k-1}$ with j)

$$\bigcup_{k\in[1,n-1]} \bigcup_{j\in[r^{n-k-1},(q_{n-k}-1)/(r-2)]} [q_{k-1} + j(r-2)r^k, (r-1)q_{k-1} - 1 + j(r-2)r^k] \supseteq [(r-1)q_{n-1}, q_n - 1], \tag{9.22}$$

so $[(r-1)q_{n-1}, q_n - 1]$ is contained in the left hand side of (9.19).

Also, $[q_{n-1}, (r-1)q_{n-1} - 1]$ is contained in the left hand side of (9.19) (for $k = n$ and $j = 0$). Hence

$$[1, q_{n-1} - 1] \cup [q_{n-1}, (r-1)q_{n-1} - 1] \cup [(r-1)q_{n-1}, q_n - 1] = [1, q_n - 1]$$

is contained in the left hand side of (9.19), which concludes the proof of (9.19), hence of (9.18), hence of (9.17), hence of Theorem 9.3.3. □

Theorem 9.3.3 implies the lower bound $\Theta(C_{q_{n-1},q_n}) \geq \sqrt[n]{q_n}$.

Theorem 9.3.1 is now proved, since it follows from Theorem 9.3.3 together with Proposition 9.3.2.

9.3.2 Further remarks

The structure of the explicit independent set in Theorem 9.3.3 gives rise to the following natural question.

$$\text{Given } q, n, r \in \mathbb{N}, \text{ what is } d(q,n,r) := d_{\min}^{L_\infty}(\{t \cdot (1, r, \dots, r^{n-1}) \mid t \in \mathbb{Z}_q\})? \tag{9.23}$$

Here $\{t \cdot (1, r, \dots, r^{n-1}) \mid t \in \mathbb{Z}_q\}$ is considered as subset of $\mathbb{Z}_q^n$. So

$$\alpha(C_{d(q,n,r),q}^{\boxtimes n}) \geq q. \tag{9.24}$$

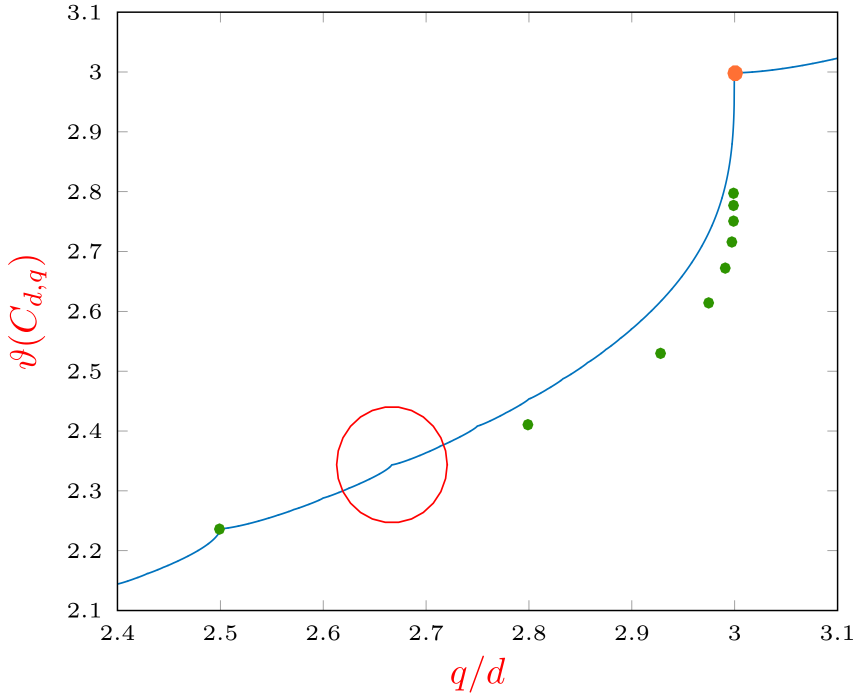


Figure 9.2: A graph of the function $q/d \mapsto \vartheta(C_{d,q})$ for $2.4 \leq q/d \leq 3.1$. The function seems nondifferentiable at $q/d = 5/2$ and $q/d = 3$, and also at $q/d = 8/3$ (marked with a red circle). The green points are points in the sequence $(q_n/q_{n-1}, \sqrt[n]{q_n})$ where q_n is defined as in (9.14) with $r = 3$. Note that $\sqrt[n]{q_n}$ is our lower bound on $\Theta(C_{q_{n-1},q_n})$. The sequence of green points converges to the orange point (3,3) as $n \to \infty$.

Question (9.23) seems not easy to solve in general, although for concrete cases of q, n, r the number $d(q, n, r)$ is easy to compute by computer. Note that Theorem 9.3.3 is equivalent to the statement that $d(q_n, n, r) \geq q_{n-1}$ for $n \in \mathbb{N}$ and $r \geq 3$ the fixed integer used to define q_n. In Section 9.6 we will see, motivated by Question (9.23), that the set $\{t \cdot (1, 7, \dots, 7^4) \mid t \in \mathbb{Z}_{382}\} \subseteq \mathbb{Z}_{382}^5$ is independent in $C_{108,382}^{\boxtimes 5}$. So $d(382, 5, 7) \geq 108$. We will modify this independent set to obtain a new lower bound on $\Theta(C_7)$.

Consider the graph of the function $q/d \mapsto \vartheta(C_{d,q})$ in Figure 9.1. It is continuous at integers ≥ 3, as $q/d \mapsto \mathrm{ev}(C_{d,q})$ is continuous at these points. From the figure, the function $q/d \mapsto \vartheta(C_{d,q})$ seems continuous at *all* rational numbers ≥ 2, but this is not known. However, it seems not differentiable at some points, for example at points of the form $q/2$ with q integer. If we zoom in further (as in Figure 9.2), we see new points appear where the function seems nondifferentiable (see the point $(8/3, \vartheta(C_{8,3}))$ marked with a red circle). In fact, we suspect (and numerical experiments seem to support this) that the function $q/d \mapsto \vartheta(C_{d,q})$ has left derivative $+\infty$ and right derivative 0 at *every* point $q/d \in \mathbb{Q}$ with $q/d > 2$.

9.4 Uniqueness of $\alpha(C_{5,14}^{\boxtimes 3}) = 14$

Fix an integer $r \geq 3$ and let the integer q_n be defined as in (9.14), for each $n \in \mathbb{N}$. By Proposition 9.3.2 and Theorem 9.3.3 we know that $\alpha(C_{q_{n-1},q_n}^{\boxtimes n}) = q_n$. The question arises whether there is a *unique* independent set of cardinality q_n in $C_{q_{n-1},q_n}^{\boxtimes n}$ up to Lee equivalence. We do not have a general answer, but in this section we present some partial results. First we note the following.

Proposition 9.4.1. *If $B \subseteq \mathbb{Z}_{q_n}^n$ is independent in $C_{q_{n-1},q_n}^{\boxtimes n}$ with $|B| = q_n$, then each symbol in $\mathbb{Z}_{q_n}$ appears exactly once in each column of B (interpreted as a $q_n \times n$ matrix with the words as rows).*

Proof. Fix a column, and let c_j denote the number of times symbol $j \in \mathbb{Z}_{q_n}$ occurs in this column. Then $\sum_{j=0}^{q_n-1} c_j = q_n$. Note that $r > q_n/q_{n-1}$, which implies with Proposition 9.3.2 that $\alpha(C_{q_{n-1},q_n}^{\boxtimes(n-1)}) \leq q_{n-1}$. This implies $\sum_{j=t+1}^{t+q_{n-1}} c_j \leq q_{n-1}$ for each $t \in \mathbb{Z}_{q_n}$, where we take indices of c mod q_n. As $\sum_{t=0}^{q_n-1} \sum_{j=t+1}^{t+q_{n-1}} c_j = q_n \cdot q_{n-1}$, we have $\sum_{j=t+1}^{t+q_{n-1}} c_j = q_{n-1}$ for each $t \in \mathbb{Z}_{q_n}$. This implies, using the equations $\sum_{j=t+1}^{t+q_{n-1}} c_j = q_{n-1}$ for t and $t+1$ that $c_t = c_{t+q_{n-1}}$ for any $t \in \mathbb{Z}_{q_n}$. As q_{n-1} and q_n are coprime, this means that $c_0 = c_1 = \ldots = c_{q_n-1}$. Together with $\sum_{j=0}^{q_n-1} c_j = q_n$, this proves the proposition. □

Let us now fix $r := 3$. Then $q_n = (3^n + 1)/2$, cf. (9.14). For $n = 1, 2$ it is an easy exercise to prove that there exists a *unique* independent set of size q_n in $C_{q_{n-1},q_n}^{\boxtimes n}$ up to Lee equivalence. We will prove that also the case $n = 3$ holds true.

Proposition 9.4.2. *Up to Lee equivalence there is a unique independent set of size 14 in $C_{5,14}^{\boxtimes 3}$.*

Proof. By Theorem 9.3.3, an independent set of size 14 in $C_{5,14}^{\boxtimes 3}$ is given by

$$A := \{t \cdot (1, 3, 9) \mid t \in \mathbb{Z}_{14}\} \subseteq \mathbb{Z}_{14}^3. \tag{9.25}$$

Let B be any independent set of size 14 in $C_{5,14}^{\boxtimes 3}$. We prove that B is Lee equivalent to A. Without loss of generality, we assume that B contains $\mathbf{0}$, the zero word. Proposition 9.4.1 implies the following.

$$\text{Each symbol in } \mathbb{Z}_{14} \text{ appears in each column of } B \text{ exactly once.} \tag{9.26}$$

For $i \in \mathbb{Z}_{14}$, and $k \in \{1, 2, 3\}$ let $f_k(i)$ be the symbol in column k in the row containing i in column 1, where by assumption $f_k(0) = 0$. (So f_1 is the identity function $\mathbb{Z}_{14} \to \mathbb{Z}_{14}$ and f_2, f_3 are bijective functions $Z_{14} \to \mathbb{Z}_{14}$ by (9.26).) Define the graphs

$$G_k := (\mathbb{Z}_{14}, \{\{i, j\} \mid |f_k(i) - f_k(j)|_{14} \geq 5\}), \quad (k \in \{1, 2, 3\}).$$

Note that $G_1 = \overline{C_{5,14}}$ and that G_2 and G_3 are isomorphic to $\overline{C_{5,14}}$, so each G_k contains no triangles. The edge $\{0, 1\}$ is not present in G_1, so it is present in at least one of G_2 and G_3. Assume it is in G_2. Then, for $u \neq v \in \mathbb{Z}_{14}$,

$$\begin{aligned} u - v \in \{\pm 1, \pm 4\} \pmod{14} \quad &\Longrightarrow \quad \{u, v\} \in E(G_2) \text{ and} \\ u - v \in \{\pm 2, \pm 3\} \pmod{14} \quad &\Longrightarrow \quad \{u, v\} \in E(G_3). \end{aligned} \tag{9.27}$$

We now prove (9.27). Define, for $t \in \mathbb{Z}_{14}$, $V_t := \{t, t+1, \ldots, t+4\} \subseteq \mathbb{Z}_{14}$ and set $E_{k,t} := E(G_k[V_t])$, the edge set of the subgraph of G_k induced by V_t (for $k \in \{2, 3\}$).[3] Note that for each t, the graph $(V_t, E_{2,t} \cup E_{3,t})$ is the complete graph on V_t. As both $G_2[V_t]$ and $G_3[V_t]$ contain no triangles, each of them cannot be bipartite (otherwise the complement, hence the other from the two would contain a triangle). So each $G_k[V_t]$ is a 5-cycle (any non-bipartite graph on 5 vertices without triangles is a 5-cycle), and as $(V_t, E_{2,t} \cup E_{3,t})$ is the complete graph, $G_2[V_t]$ and $G_3[V_t]$ are complementary 5-cycles.

Moreover, if $\{t, t+1\} \in E(G_2)$, then also $\{t+1, t+5\} \in E(G_2)$ and $\{t+5, t+6\} \in E(G_2)$. To see this, assume that $\{t, t+1\} \in E(G_2)$ and note that $G_2[V_t]$ and $G_2[V_{t+1}]$ are five-cycles. So $t+5$ has the same neighbors as t in G_2, hence $\{t+1, t+5\} \in E(G_2)$. Also, $G_2[V_{t+1}]$ and $G_2[V_{t+2}]$ are five-cycles. Hence $t+6$ has the same neighbors as $t+1$ in G_2, so $\{t+5, t+6\} \in E(G_2)$. As $\{0, 1\} \in E(G_2)$ we find by applying this observation repeatedly, using that 5 and 14 are coprime, that G_2 contains edges $\{t, t+1\}$ and $\{t, t+4\}$ for all $t \in \mathbb{Z}_{14}$. This proves the first part of (9.27). The second part follows from the observation that $G_2[V_t]$ and $G_3[V_t]$ are complementary 5-cycles for each $t \in \mathbb{Z}_{14}$. As vertex t has neighbors $t+1$ and $t+4$ in $G_2[V_t]$, it has neighbors $t+2$ and $t+3$ in $G_3[V_t]$. So G_3 contains edges $\{t, t+2\}$ and $\{t, t+3\}$ for each $t \in \mathbb{Z}_{14}$. This proves (9.27).

Next, we prove that for $u \neq v \in \mathbb{Z}_{14}$,

$$\begin{aligned} \{u, v\} \in E(G_2) \quad &\Longleftrightarrow \quad u - v \in \{\pm 1, \pm 4, 7\} \pmod{14} \text{ and} \\ \{u, v\} \in E(G_3) \quad &\Longleftrightarrow \quad u - v \in \{\pm 2, \pm 3, 7\} \pmod{14}. \end{aligned} \tag{9.28}$$

Consider a vertex u in G_2. Then u has neighbors $u \pm 1$ and $u \pm 4$. As $G_2 \cong \overline{C_{5,14}}$, a 5-regular graph, vertex u must have a fifth neighbor v. This neighbor cannot be $u+2$, for otherwise $(u, u+1, u+2, u)$ would be a triangle. This neighbor cannot be $u+3$, for otherwise $(u, u+3, u+4, u)$ would be a triangle. This neighbor cannot be $u+5$, for otherwise $(u, u+5, u+1, u)$ would be a triangle. This neighbor cannot be $u+6$, for

[3] If $G = (V, E)$ is a graph and $U \subseteq V$, we write $G[U] := (U, \{e \in E \mid e \subseteq U\})$ for the *subgraph of G induced by U*.

otherwise $(u, u+6, u+10, u)$ would be a triangle. By symmetry, this neighbor also not be $u-3$, $u-4$, $u-5$ or $u-6$. So the fifth neighbor must be $u+7$. This proves (9.28) for G_2.

Similarly, consider a vertex u in G_3. Then u has neighbors $u \pm 2$ and $u \pm 3$. As $G_3 \cong \overline{C_{5,14}}$, a 5-regular graph, vertex u must have a fifth neighbor v. This neighbor cannot be $u+1$, for otherwise $(u, u+1, u-2, u)$ would be a triangle. This neighbor cannot be $u+4$, for otherwise $(u, u+2, u+4, u)$ would be a triangle. This neighbor cannot be $u+5$, for otherwise $(u, u+5, u+3, u)$ would be a triangle. This neighbor cannot be $u+6$, for otherwise $(u, u+6, u+3, u)$ would be a triangle. By symmetry, this neighbor also not be $u-1$, $u-4$, $u-5$ or $u-6$. So the fifth neighbor must be $u+7$. This proves (9.28) for G_3.

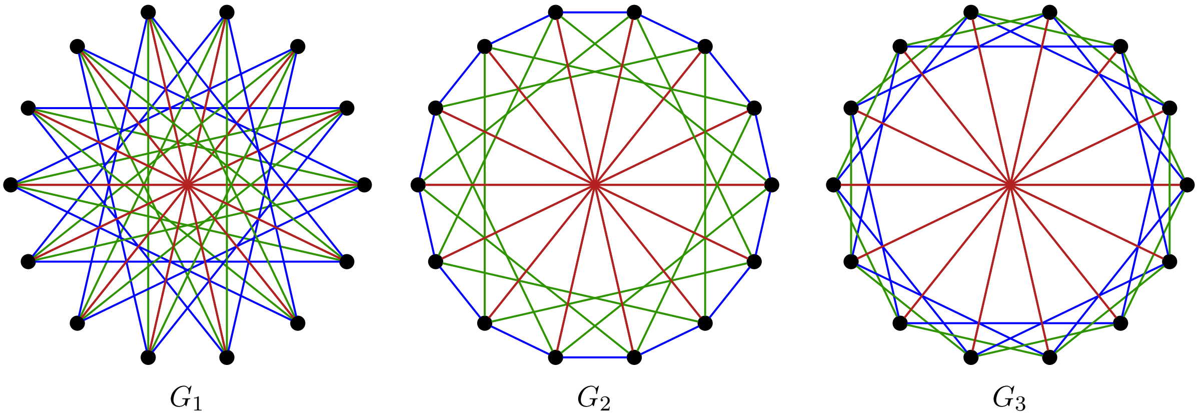


Figure 9.3: The graphs G_1, G_2, G_3. They all have vertex set $\mathbb{Z}_{14}$, depicted in cyclic clockwise order in this figure.

Note that

$$\begin{aligned} &(0,4,8,12,2,6,10,0) \text{ is an induced 7-cycle in } G_2 \text{ and} \\ &(0,2,4,6,8,10,12,0) \text{ is an induced 7-cycle in } G_3. \end{aligned} \tag{9.29}$$

This follows from (9.28), as $\{0,2,4,8,10,12,14\}$ contains no pairs $\{u,v\}$ with $u - v \in \{\pm 1, \pm 3, 7\} \pmod{14}$, as all its elements are $0 \pmod 2$.

$$\text{The only induced 7-cycle containing 0 in } \overline{C_{5,14}} \text{ is } (0,6,12,4,10,2,8,0). \tag{9.30}$$

This is easily verified by computer, by checking $\binom{13}{6}$ possibilities. (It is also not hard to verify by hand. Vertex 0 has neighbors $N := \{5,6,7,8,9\}$ in $\overline{C_{5,14}}$. Set $R := \mathbb{Z}_{14} \backslash (N \cup \{0\})$. An induced 7-cycle containing 0 in $\overline{C_{5,14}}$, starting at 0, first traverses N, then four vertices in R, then traverses N again and then returns to 0. The four vertices in R on the induced 7-cycle form an induced path of length 3 (in edges) in the induced subgraph $\overline{C_{5,14}}[R]$, the subgraph of $\overline{C_{5,14}}$ induced by R. This graph is bipartite with 8 vertices and 10 edges. By hand the reader may verify that there are 15 induced paths of length 3 in this graph, but of these paths only the path $(2,10,4,12)$ can be extended to an induced 7-cycle containing 0 in $\overline{C_{5,14}}$, and this extension is unique.)

It remains to determine the numbers $f_k(i)$, for $k \in \{2,3\}$ and $i \in \mathbb{Z}_{14}$. Note that f_k is a graph isomorphism $G_k \to \overline{C_{5,14}}$. So induced 7-cycles must go to induced 7-cycles.

Combining (9.29) and (9.30) we find (using that a 7-cycle can be traversed in two ways) that f_2 either satisfies $f_2(4t) = 6t$ for all $t \in \mathbb{Z}_{14}$, or $f_2(4t) = 8t$ for all $t \in \mathbb{Z}_{14}$. Substituting t by $4t$ we find mod 14 (as $4 \cdot 4t = 2t$) that either $f_2(2t) = 10t = -4t$ for all $t \in \mathbb{Z}_{14}$, or $f_2(2t) = 4t$ for all $t \in \mathbb{Z}_{14}$. If we replace f_2 by $-f_2$ and change the symbols in the second column of B accordingly, we obtain an independent set which is Lee equivalent to B. So we may assume that $f_2(2t) = 4t$ (otherwise we replace f_2 by $-f_2$).

t	0	2	4	6	8	10	12
$f_2(t)$	0	4	8	12	2	6	10

Table 9.1: The values of f_2.

Note that $\{s, s+1\} \in E(G_2)$ for each $s \in \mathbb{Z}_{14}$, so $\{f_2(s), f_2(s+1)\} \in E(\overline{C_{5,14}})$. So $f_2(2t) = 4t$ and $f_2(2t+2) = 4t+4$ have $f_2(2t+1)$ as common neighbor in $\overline{C_{5,14}}$ ($t \in \mathbb{Z}_{14}$). As the only common neighbor of $4t$ and $4t+4$ in $\overline{C_{5,14}}$ is $4t+9$, we have $f_2(2t+1) = 4t+9$ for each t. Together with $f_2(2t) = 4t$ this gives $f_2(t) = 9t$ for all $t \in \mathbb{Z}_{14}$.

Now we determine f_3. Combining (9.29) and (9.30) we find that f_3 either satisfies $f_3(2t) = 6t$ for all $t \in \mathbb{Z}_{14}$, or $f_2(2t) = 8t = -6t$ for all $t \in \mathbb{Z}_{14}$. Without loss of generality we may assume that $f_3(2t) = 6t$ for all $t \in \mathbb{Z}_{14}$ (otherwise we replace f_3 by $-f_3$). Note that $\{s, s+3\} \in E(G_3)$ for each $s \in \mathbb{Z}_{14}$, so $\{f_3(s), f_3(s+3)\} \in E(\overline{C_{5,14}})$. So $f_3(2t) = 6t$ and $f_3(2t+6) = 6t+4$ have $f_3(2t+3)$ as common neighbor in $\overline{C_{5,14}}$ ($t \in \mathbb{Z}_{14}$). As the only common neighbor of $6t$ and $6t+4$ in $\overline{C_{5,14}}$ is $6t+9$, we have $f_3(2t+3) = 6t+9$, hence $f_3(2t+1) = 6t+3$. Together with $f_3(2t) = 6t$ this gives $f_3(t) = 3t$ for all $t \in \mathbb{Z}_{14}$. Hence we have determined f_3.

So $f_1(t) = t$, $f_2(t) = 9t$ and $f_3(t) = 3t$ for all $t \in \mathbb{Z}_{14}$. We conclude that B is Lee equivalent to A. □

9.5 Semidefinite programming bounds on $\alpha(C_{d,q}^{\boxtimes n})$

We describe how the semidefinite programming bound $B_3^L(q,n,d)$ from (8.4) can be adapted to an upper bound $B_3^{L_\infty}(q,n,d)$ on $\alpha(C_{d,q}^{\boxtimes n})$, which either improves or is equal to the bound obtained from Lovász's ϑ-function. Since $\vartheta \in \Delta$ (see Section 9.2), it satisfies for all $n \in \mathbb{N}$,

$$\alpha(C_{d,q}^{\boxtimes n}) \leq \vartheta(C_{d,q}^{\boxtimes n}) = \vartheta(C_{d,q})^n. \tag{9.31}$$

This implies that $\Theta(C_{d,q}) \leq \vartheta(C_{d,q})$.

However, the new bound $B_3^L(q,n,d)$ is not multiplicative over the strong product, so it does not need to give an upper bound on $\Theta(C_{d,q})$. Define, for $k \geq 2$,

$$\begin{aligned} B_k^{L_\infty}(q,n,d) := \max\{\textstyle\sum_{v \in \mathbb{Z}_q^n} x(\{v\}) \mid x : \mathcal{C}_k \to \mathbb{R},\ x(\emptyset) = 1,\ x(S) = 0 \text{ if } d_{\min}^{L_\infty}(S) < d, \\ M_{k,D}(x) \succeq 0 \text{ for each } D \text{ in } \mathcal{C}_k\}. \end{aligned} \tag{9.32}$$

Here $\mathcal{C}_k$ again is the collection of codes $C \subseteq \mathbb{Z}_q^n$ with $|C| \leq k$, and the matrix $M_{k,D}(x)$ is defined in Section 8.1.1, for $x : \mathcal{C}_k \to \mathbb{R}$ and $D \in \mathcal{C}_k$.

So $B_k^{L_\infty}(q,n,d)$ is obtained from the bound $B_k^L(q,n,d)$ in (8.4) by replacing in the definition $d_{\min}^L(S)$ by $d_{\min}^{L_\infty}(S)$. It is not hard to see that $\alpha(C_{d,q}^{\boxtimes n}) \leq B_k^{L_\infty}(q,n,d)$, by a proof analogous to that of Proposition 8.1.1. For comparison, $\vartheta(C_{d,q}^{\boxtimes n})$ is equal to the bound obtained from $B_2^{L_\infty}(q,n,d)$ by removing the constraints that $M_{2,D}(x)$ is positive semidefinite for subsets $D \in \mathcal{C}_2$ with $D \neq \emptyset$. Moreover, $B_2^{L_\infty}(q,n,d)$ is equal to the Delsarte bound, which is equal to the bound $\vartheta'(C_{d,q}^{\boxtimes n})$, with ϑ' as in [79].

n	1	2	3	4	5
$B_2^{L_\infty}(5,n,2)$	2.236	5.000	11.180	25.000	55.902
$B_3^{L_\infty}(5,n,2)$	2.000	5.000	10.915	25.000	55.902
$B_2^{L_\infty}(7,n,2)$	3.318	11.007	36.517	121.152	401.943
$B_3^{L_\infty}(7,n,2)$	3.000	10.260	35.128	119.537	401.908
$B_2^{L_\infty}(7,n,3)$	2.110	4.452	9.393	19.818	41.814
$B_3^{L_\infty}(7,n,3)$	2.000	4.139	8.957	19.494	41.782
#Vars in $B_3^{L_\infty}(5,n,2)$	2	9	48	214	799
#Vars in $B_3^{L_\infty}(7,n,2)$	3	43	423	3161	19023
#Vars in $B_3^{L_\infty}(7,n,3)$	2	12	137	1316	9745

Table 9.2: Bounds on $\alpha(C_5^{\boxtimes n})$, $\alpha(C_7^{\boxtimes n})$ and $\alpha(C_{3,7}^{\boxtimes n})$, rounded to three decimal places. It holds that $B_2^{L_\infty}(5,n,2) = \sqrt{5}^n$.

To compute $B_3^{L_\infty}(q,n,d)$, the reductions from Section 8.2 can be used — see also Section 8.5.3 for an overview of the program. The new bound $B_3^{L_\infty}(q,n,d)$ does not seem to improve significantly over the bound obtained from Lovász's ϑ-function, except for very small n. See Table 9.2 for some results for $q \in \{5,7\}$ and $1 \leq n \leq 5$. For these cases, $B_3^{L_\infty}(q,n,d)$ does not give new upper bounds on $\alpha(C_{d,q}^{\boxtimes n})$, as the values $\alpha(C_5^{\boxtimes 3}) = 10$, $\alpha(C_7^{\boxtimes 2}) = 10$, $\alpha(C_7^{\boxtimes 3}) = 33$ (cf. [10]), $\alpha(C_{3,7}^{\boxtimes 3}) = 8$ (cf. [45]) are already known and $\alpha(C_7^{\boxtimes 4}) \leq \lfloor (7/2)\alpha(C_7^{\boxtimes 3}) \rfloor = 115$. For the cases in Table 9.2, the bound $B_2^{L_\infty}(q,n,d)$ is equal to $\vartheta(C_{d,q})^n$.

The number of variables "#Vars" in $B_3^{L_\infty}(q,n,d)$, which is the number of $D_q^n \rtimes S_n$-orbits of nonempty codes of size ≤ 3 and minimum Lee$_\infty$ distance at least d, is also given in Table 9.2 for the cases considered.

9.6 New lower bound on the Shannon capacity of C_7

As noted in Section 9.1, the Shannon capacity of C_7 is still unknown and its determination is a notorious open problem in extremal combinatorics [18, 39]. Many lower bounds have been given by explicit independent sets in some fixed strong product power of C_7 [10, 56, 93], while the best known upper bound is $\Theta(C_7) \leq \vartheta(C_7) < 3.3177$. Here we give an independent set of size 367 in $C_7^{\boxtimes 5}$, which yields $\Theta(C_7) \geq 367^{1/5} > 3.2578$. The best previously known lower bound on $\Theta(C_7)$ is $\Theta(C_7) \geq 350^{1/5} > 3.2271$, found by Mathew and Östergård [56]. They proved that $\alpha(C_7^{\boxtimes 5}) \geq 350$ using stochastic search methods that utilize the symmetry of the problem. In [10], a construction is given of an independent set of size $7^3 = 343$ in $C_7^{\boxtimes 5}$. The best known lower bound on $\alpha(C_7^{\boxtimes 4})$ is 108, by Vesel and Žerovnik [93]. See Table 9.3 for the currently best known bounds on $\alpha(C_7^{\boxtimes n})$ for small n.

For comparison, $\alpha(C_7^{\boxtimes 3})^{1/3} = 33^{1/3} \approx 3.2075$, $\alpha(C_7^{\boxtimes 4})^{1/4} \geq 108^{1/4} \approx 3.2237$ and the previously best known lower bound on $\alpha(C_7^{\boxtimes 5})^{1/5}$ is $350^{1/5} \approx 3.2271$. Now we know that $\alpha(C_7^{\boxtimes 5}) \geq 367 > 3.2578^5$.

d	1	2	3	4	5
$\alpha(C_7^{\boxtimes n})$	3	10^a	33^d	108^e–115^b	367^f–401^c

Table 9.3: Bounds on $\alpha(C_7^{\boxtimes n})$. Key:
[a] $\alpha(C_q^{\boxtimes 2}) = \lfloor (q^2-q)/4 \rfloor$ [10, Theorem 2]
[b] $\alpha(C_q^{\boxtimes n}) \leq \alpha(C_q^{\boxtimes (n-1)})q/2$ [10, Lemma 2]
[c] $\alpha(G^{\boxtimes n}) \leq \vartheta(G)^n$ by Lovász [53]
[d] Baumert et al. [10]
[e] Vesel and Žerovnik [93]
[f] this chapter, see the Appendix for the explicit independent set.

An independent set in $C_{d,q}^{\boxtimes n}$ gives an independent set in $C_{\lceil 2q/d \rceil}^{\boxtimes n}$, since $\overline{C_{d,q}} \to \overline{C_{2,\lceil 2q/d \rceil}}$. Explicitly, consider the elements of $\mathbb{Z}_q$ as integers between 0 and $q-1$ and replace each element i by $\lfloor 2i/d \rfloor$, and consider the outcome as an element of $\mathbb{Z}_{\lceil 2q/d \rceil}$. This gives indeed a homomorphism $\overline{C_{d,q}} \to \overline{C_{2,\lceil 2q/d \rceil}}$ as the image of any two elements with distance at least d has distance at least 2.

In Section 9.6.1 we give an explicit description of an independent set S of size 382 in the graph $C_{108,382}^{\boxtimes 5}$. It is of the form $\{t \cdot (1, r, \ldots, r^{n-1}) \mid t \in \mathbb{Z}_q\}$, as in (9.23). As $382/108 > 7/2$ this does not directly give an independent set in $C_{2,7}^{\boxtimes 5}$. However, in Section 9.6.2 we describe how one can obtain an independent set of size 367 in $C_7^{\boxtimes 5}$ from S, by adapting S, removing vertices and adding new ones. This independent set is given explicitly in the Appendix.

9.6.1 Independent set of size 382 in $C_{108,382}^{\boxtimes 5}$

Proposition 9.6.1. *The set* $S := \{t \cdot (1, 7, 7^2, 7^3, 7^4) \mid t \in \mathbb{Z}_{382}\} \subseteq \mathbb{Z}_{382}^5$ *is independent in* $C_{108,382}^{\boxtimes 5}$.

Proof. If $x, y \in S$ then also $x - y \in S$. So it suffices to check that for all nonzero $x \in S$:[4]

$$\exists\ i \in [1,5] \text{ such that } x_i \in [108, 274]. \tag{9.33}$$

Let $x = t \cdot (1, 7, 7^2, 7^3, 7^4) \in S$ be arbitrary, with $0 \neq t \in \mathbb{Z}_{382}$. For $t \in [108, 274]$ clearly (9.33) holds with $i = 1$ (as then $x_i = t \in [108, 274]$). Also we have $[275, 381] = -[1, 107]$, so it suffices to verify (9.33) for $t \in [1, 107]$. Note that for $t \in [16, 39]$ one has $108 \leq 7t \leq 274$, so (9.33) is satisfied with $i = 2$. Also note that $69 \cdot 7 \equiv 101 \pmod{382}$. So for $t \in [70, 93]$ one has $7t \equiv 101 + 7(t - 69) \pmod{382} \in [108, 274]$, i.e., (9.33) is satisfied with $i = 2$. For the remaining $t \in [1, 107]$, please take a glance at Table 9.4. In each row, in each of the three subtables, there is at least one entry in $[108, 274]$. This completes the proof. □

We found the above independent set by computer, when looking for answers to (9.23) (with $q \geq 350$ and $n = 5$ such that $q/d(q, n, r)$ is close to $7/2$).

[4] Recall that we write $[a, b] := \{a, a+1, \ldots, b\}$ for any two integers a, b.

1	7	49	343	109	45	315	295	155	321	65	73	129	139	209
2	14	98	304	218	46	322	344	116	48	66	80	178	100	318
3	21	147	265	327	47	329	11	77	157	67	87	227	61	45
4	28	196	226	54	48	336	60	38	266	68	94	276	22	154
5	35	245	187	163	49	343	109	381	375	69	101	325	365	263
6	42	294	148	272	50	350	158	342	102					
7	49	343	109	381	51	357	207	303	211	94	276	22	154	314
8	56	10	70	108	52	364	256	264	320	95	283	71	115	41
9	63	59	31	217	53	371	305	225	47	96	290	120	76	150
10	70	108	374	326	54	378	354	186	156	97	297	169	37	259
11	77	157	335	53	55	3	21	147	265	98	304	218	380	368
12	84	206	296	162	56	10	70	108	374	99	311	267	341	95
13	91	255	257	271	57	17	119	69	101	100	318	316	302	204
14	98	304	218	380	58	24	168	30	210	101	325	365	263	313
15	105	353	179	107	59	31	217	373	319	102	332	32	224	40
					60	38	266	334	46	103	339	81	185	149
40	280	50	350	158	61	45	315	295	155	104	346	130	146	258
41	287	99	311	267	62	52	364	256	264	105	353	179	107	367
42	294	148	272	376	63	59	31	217	373	106	360	228	68	94
43	301	197	233	103	64	66	80	178	100	107	367	277	29	203
44	308	246	194	212										

Table 9.4: Part of the verification that S is independent in $C_{108,382}^{\boxtimes 5}$.

9.6.2 Description of the method

Here we describe how to use the independent set from Proposition 9.6.1 to find an independent set of size 367 in $C_7^{\boxtimes 5}$. The procedure is as follows.

(i) Start with the independent set S in $C_{108,382}^{\boxtimes 5}$ from Proposition 9.6.1.

(ii) Add the word $(40, 123, 40, 123, 40) \bmod 382$ to each word in S.

(iii) Replace each letter i, which we now consider to be an integer between 0 and 381 and not anymore an element in $\mathbb{Z}_{382}$, in each word from S by $\lfloor i/54.5 \rfloor$. Now we have a set of words S' with only symbols in $[0, 6]$ in it, which we consider as elements of $\mathbb{Z}_7$.

(iv) Remove each word $u \in S'$ for which there is a $v \in S'$ such that $uv \in E(C_7^{\boxtimes 5})$ from S', i.e., we remove u if there is a $v \in S'$ with $v \neq u$ such that $u_i - v_i \in \{0, 1, 6\}$ for all $i \in [1, 5]$. We denote the set of words which are not removed from S' by this procedure by M. The computer finds $|M| = 327$. Note that M is independent in $C_7^{\boxtimes 5}$.

(v) Find the best possible extension of M to a larger independent set in $C_7^{\boxtimes 5}$. To do this, consider the subgraph G of $C_7^{\boxtimes 5}$ induced by the words x in $\mathbb{Z}_7^5$ with the property that $M \cup \{x\}$ is independent in $C_7^{\boxtimes 5}$. This graph is not large, in this case it has 71 vertices and 85 edges, so a computer finds a maximum size independent set I in G quickly. The computer finds $|I| = \alpha(G) = 40$, so we can add 40 words to M. Write $R := M \cup I$. Then $|R| = 327 + 40 = 367$ and R is independent in $C_7^{\boxtimes 5}$.

The maximum size independent set I in the graph G in (v) was found using Gurobi [42]. In steps (ii) and (iii), many possibilities for adding a constant word and for the division factor were tried, but no independent set of size 368 or larger was found. Also, the independent set R of size 367 did not seem to be easily extendable. A local search was performed, showing that there exists no triple of words from R such that if one removes these three words from R, four words can be added to obtain an independent set of size 368 in $C_7^{\boxtimes 5}$.

Remark 9.6.2. One other new bound on $\alpha(C_q^{\boxtimes n})$ was obtained (for $q \leq 15$ and $n \leq 5$) using independent sets of the form from (9.23). With $q = 4009$, $n = 5$ and $r = 27$, we found $d(q, n, r) = 729$. As $q/(d(q, n, r)) = 4009/729 < 11/2$, this directly yields the new lower bound $\alpha(C_{11}^{\boxtimes 5}) \geq 4009$. The previously best known lower bound is $\alpha(C_{11}^{\boxtimes 5}) \geq 3996$ from [45, 56]. However, the new lower bound on $\alpha(C_{11}^{\boxtimes 5})$ does not imply a new lower bound on $\Theta(C_{11})$. It is known that $\Theta(C_{11}) \geq \alpha(C_{11}^{\boxtimes 3})^{1/3} = 148^{1/3} > 5.2895$ (cf. [10]), which is larger than $4009^{1/5}$.

9.7 Appendix: Explicit code

The following 367 words form an independent set in $C_7^{\boxtimes 5}$, which proves the new bound $\Theta(C_7) \geq 367^{1/5} > 3.2578$. It is the set R from Section 9.6.2.

```
02020, 02112, 02204, 02306, 02461, 02553, 03645, 03040, 03032, 03124, 03226, 03311, 03403, 14144, 14231, 14323, 14415, 14510, 15602, 15064, 15166, 15251,
15343, 15430, 15522, 16614, 16016, 16101, 16263, 16355, 16450, 16542, 10636, 10021, 10113, 10205, 10300, 10462, 10554, 11656, 11041, 11033, 11125, 11220,
11312, 11404, 11506, 12661, 12053, 12145, 12240, 12232, 12324, 12426, 12511, 13603, 13065, 13160, 13252, 13344, 13446, 13431, 24010, 24102, 24264, 24366,
24451, 24543, 25630, 25022, 25114, 25216, 25301, 25463, 25555, 26650, 26042, 26034, 26136, 26221, 26313, 26405, 26500, 20662, 20054, 20156, 20241, 20233,
20325, 20420, 20512, 21604, 21006, 21161, 21253, 21345, 21440, 21432, 22626, 22011, 22103, 22265, 22360, 22452, 22544, 23631, 23023, 23115, 23210, 23302,
23464, 23566, 34130, 34222, 34314, 34416, 34501, 35663, 35055, 35150, 35242, 35234, 35336, 35421, 35513, 36605, 36000, 36162, 36254, 36356, 36441, 36433,
30620, 30012, 30104, 30206, 30361, 30453, 30545, 31632, 31024, 31126, 31211, 31303, 31465, 31560, 32652, 32044, 32131, 32223, 32315, 32410, 32502, 33664,
33066, 33151, 33243, 33235, 33330, 33422, 44616, 44001, 44163, 44255, 44350, 44442, 44434, 44536, 45621, 45013, 45105, 45200, 45362, 45454, 45556, 46633,
46025, 46120, 46212, 46304, 46406, 46561, 40653, 40045, 40132, 40224, 40326, 40411, 40503, 41665, 41060, 41152, 41244, 41331, 41423, 41515, 42610, 42002,
42164, 42266, 42351, 42443, 42435, 43622, 43014, 43116, 43201, 43363, 43455, 43550, 54634, 54036, 54121, 54213, 54305, 54400, 54562, 55654, 55056, 55141,
55133, 55225, 55320, 55412, 55504, 56606, 56061, 56153, 56245, 56332, 56424, 56526, 50611, 50003, 50165, 50260, 50352, 50444, 51623, 51015, 51110, 51202,
51364, 51551, 52643, 52635, 52030, 52122, 52214, 53655, 53134, 64332, 64424, 64526, 65611, 65003, 65260, 65352, 65444, 65546, 66623, 66110, 66202, 66364,
66466, 66551, 60643, 60645, 60030, 60122, 60214, 60316, 60401, 60563, 61050, 61142, 61134, 61236, 61321, 61413, 62600, 62062, 62154, 62256, 62341, 62333,
62520, 63612, 63004, 63106, 63261, 63353, 63445, 63540, 64532, 04026, 04111, 04203, 04460, 04552, 05644, 05031, 05123, 05310, 05402, 05564, 06666, 06051,
06143, 06230, 06322, 06414, 06516, 00601, 00063, 00155, 00250, 00342, 00334, 00436, 01613, 01100, 01262, 01354, 01456, 01541, 02625, 00521, 01005, 02533,
03565, 04052, 04365, 04624, 04660, 05046, 05225, 10534, 14246, 15435, 22524, 24615, 24651, 32046, 34035, 34043, 36525, 40040, 41246, 42530, 43514, 45641,
50531, 51456, 52400, 52563, 53050, 53142, 53320, 53412, 56340, 61505, 62425, 64154, 64340, 65105, 66025.
```

Summary

New methods in coding theory: error-correcting codes and the Shannon capacity

Error-correcting codes have been studied since 1948, when Claude Shannon published his influential paper *A Mathematical Theory of Communication* [85]. Fix three positive integers q, n, d and let $Q := \{0, \dots, q-1\}$ be our *alphabet*. We identify elements of Q^n with *words* of length n consisting of letters (elements) from Q. A *code of length* n is any subset of Q^n. For two words u, v, their *Hamming distance* is the number of i with $u_i \neq v_i$. The *minimum distance* of a code C is the minimum Hamming distance between any two distinct elements of C. The central question in coding theory is the following.

$$\text{What is the maximum size of a code } C \subseteq Q^n \text{ with minimum distance at least } d? \quad \text{(S.1)}$$

The maximum size in (S.1) is denoted by $A_q(n, d)$. A code C with minimum distance $d := 2e + 1$ (for some integer e) is called *e-error-correcting*. If a codeword from C is distorted in at most e positions, we can recover the original codeword by taking the codeword that is closest to the distorted codeword in Hamming distance. This principle is used in communication systems for the correction of transmission errors.

The numbers $A_q(n, d)$ are hard to compute in general. For many q, n, d, only upper and lower bounds are known. Explicit codes yield lower bounds on $A_q(n, d)$ and they can be used for error-correction as explained. A classical upper bound on $A_q(n, d)$ is Delsarte's linear programming upper bound [31], which bound can be interpreted as a semidefinite programming (SDP) bound based on pairs of codewords.

In this thesis we try to improve upper bounds on $A_q(n, d)$. We give an SDP bound based on quadruples of codewords, which a priori has size exponential in n. The optimization problem is highly symmetric: it can be assumed that the optimal solution is invariant under the group of distance preserving permutations of Q^n. This symmetry group is the wreath product $S_q^n \rtimes S_n$. By the symmetry of the problem, the SDP can be reduced to a size bounded by a polynomial in n.

In Chapter 3 we give a general method for symmetry reduction, based on representation theory. If G is a finite group acting on a finite set Z and $n \in \mathbb{N}$, we give a reduction of $Z^n \times Z^n$-matrices which are invariant under the simultaneous action of the group $G^n \rtimes S_n$ on their rows and columns. In the reduction, we assume that a reduction is known of $Z \times Z$-matrices which are invariant under the simultaneous action of G on their rows and columns.

In Chapter 4 we apply this general method to reduce the mentioned SDP based on quadruples of codewords for computing upper bounds on $A_q(n, d)$. With the method, we sharpen known upper bounds for five triples (q, n, d).

In Chapter 5, we explore other methods of finding upper bounds on $A_q(n, d)$, based on combinatorial divisibility arguments. The methods yield new upper bounds for four triples (q, n, d). Our most prominent result in this direction is the following bound, which gives in certain cases a strengthening of a bound implied by the Plotkin bound [67].

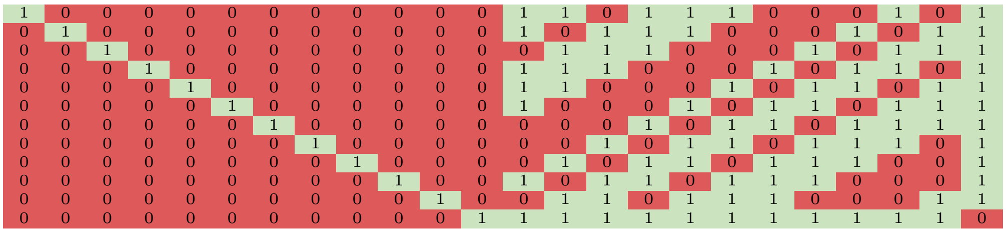
Theorem. *Suppose that q, n, d, m are positive integers with $q \geq 2$, such that $d = m(qd - (q-1)(n-1))$, and such that $n - d$ does not divide $m(n-1)$. If $r \in \{1, \ldots, q-1\}$ satisfies*

$$n(n-1-d)(r-1)r < (q-r+1)(qm(q+r-2)-2r),$$

then $A_q(n, d) < q^2m - r$.

In Chapter 6 we consider (binary) *constant weight* codes. Here the alphabet is $\{0, 1\}$. The *weight* of a word is the number of 1's it contains. For $n, d, w \in \mathbb{N}$, the number $A(n, d, w)$ denotes the maximum size of a code $C \subseteq \{0, 1\}^n$ with minimum distance at least d and in which every codeword has weight w. (Such a code is called a 'constant weight code' with weight w.) With SDP based on quadruples of codewords and a symmetry reduction with the method of Chapter 3, we find several new upper bounds on $A(n, d, w)$. Two upper bounds matching the known lower bounds are obtained, so that we know the value of $A(n, d, w)$ exactly: $A(22, 8, 10) = 616$ and $A(22, 8, 11) = 672$.

In Chapter 7, we prove with the SDP-output, using 'complementary slackness', that the optimal constant weight codes achieving $A(23, 8, 11) = 1288$, $A(22, 8, 10) = 616$ and $A(22, 8, 11) = 672$ are unique up to coordinate permutations. The mentioned unique constant weight codes can be obtained from the binary Golay code —a famous code with good error-correcting properties— by taking subcodes and deleting coordinates ('shortening').



1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	1	0	0	0	1	0	1
0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0	0	0	1	0	1	1
0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	0	1	1	1
0	0	0	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	0	1	1	0	1
0	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	1	0	1	1	0	1	1
0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0	1	1	1
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	1	1	0	1	1	1	1
0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1	0	1	1	1	0	1
0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	0	1	1	1	0	0	1
0	0	0	0	0	0	0	0	0	1	0	0	1	0	1	1	0	1	1	1	0	0	0	1
0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	1	1	0	0	0	1	1
0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0

Figure S.1: A generator matrix of the extended binary Golay code (i.e., the 2^{12} codewords are sums mod 2 of the rows of this matrix). The extended binary Golay code was used for error-correction in the *Voyager* missions to Jupiter and Saturn [94].

For unrestricted (non-constant weight) binary codes, the bound $A_2(20, 8) \leq 256$ was obtained by Gijswijt, Mittelmann and Schrijver [37], implying that the quadruply shortened extended binary Golay code of size 256 is optimal. Two unrestricted codes $C, D \subseteq \{0, 1\}^n$ are equivalent if there is a $g \in S_2^n \rtimes S_n$ such that $g \cdot C = D$. Up to equivalence the optimal binary codes attaining $A_2(24 - i, 8) = 2^{12-i}$ for $i = 0, 1, 2, 3$ are unique, namely they are the i times shortened extended binary Golay codes [20]. We show that there exist several nonequivalent optimal codes achieving $A_2(20, 8) = 256$. We classify such codes under the additional condition that all distances are divisible by 4, and find 15 such codes. We also show that there exist such codes with not all distances divisible by 4.

In Chapter 8 we consider *Lee codes*. Fix three integers $q, n, d \in \mathbb{N}$ and define $Q := \mathbb{Z}_q$ (the cyclic group of order q). For two words $u, v \in Q^n$, their *Lee distance* is $\sum_{i=1}^n \min\{|u_i - v_i|, q - |u_i - v_i|\}$. The *minimum Lee distance* of a code $C \subseteq Q^n$ is the minimum Lee distance between any two distinct elements of C. Let $A_q^L(n, d)$ denote the maximum size of a code $C \subseteq Q^n$ with minimum Lee distance at least d. We give an SDP upper bound based on triples of codewords and show that it can be computed efficiently, using the symmetry reduction method of Chapter 3. This finally yields new upper bounds on $A_q^L(n,d)$ for several triples (q,n,d).

Chapter 9 is about the Shannon capacity of circular graphs. For any graph $G = (V,E)$ and $n \in \mathbb{N}$, the *n-th strong product power* $G^{\boxtimes n}$ is the graph with vertex set V^n in which two distinct vertices $(u_1,\ldots,u_n)$ and $(v_1,\ldots,v_n)$ of $G^{\boxtimes n}$ are adjacent if and only if for each $i \in \{1,\ldots,n\}$ one has either $u_i = v_i$ or $u_iv_i \in E$. The *Shannon capacity* of G is defined as

$$\Theta(G) := \sup_{n\in\mathbb{N}} \sqrt[n]{\alpha(G^{\boxtimes n})},$$

where for any graph G, the maximum cardinality of an independent set in G (a set of vertices, no two of which are adjacent) is denoted by $\alpha(G)$. The circular graph $C_{d,q}$ is the graph with vertex set $\mathbb{Z}_q$, in which two distinct vertices are adjacent if and only if their distance (mod q) is strictly less than d. The value of $\alpha(C_{d,q}^{\boxtimes n})$ (for fixed n) and $\Theta(C_{d,q})$ can be seen to only depend on the quotient q/d. We show that the function $q/d \mapsto \Theta(C_{d,q})$ is continuous at *integer* points $q/d \geq 3$. It implies that also the function $q/d \mapsto \vartheta(C_{d,q})$, Lovász's upper bound on $\Theta(C_{d,q})$ [53], is continuous at these points — see Figure S.2.

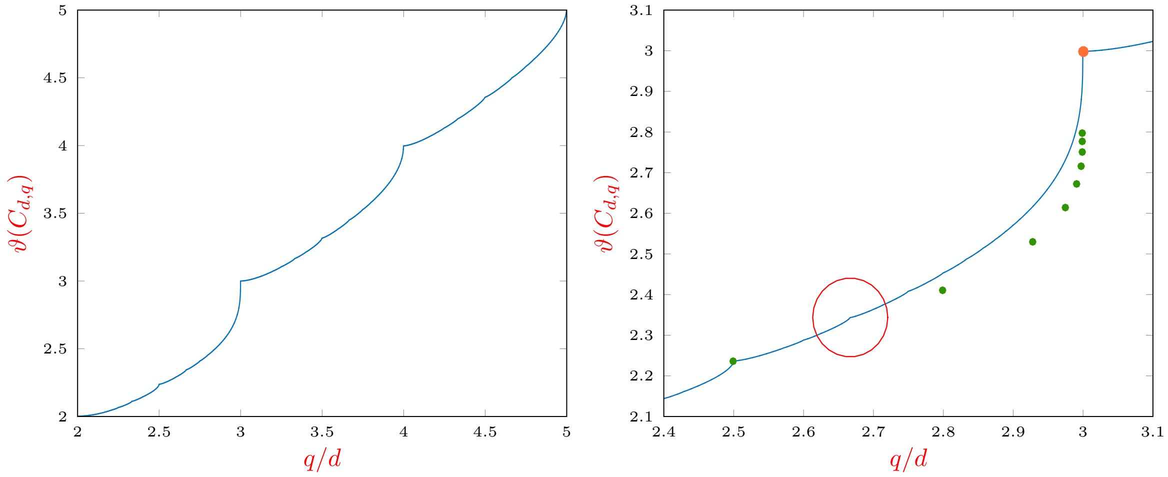


Figure S.2: Two graphs of the function $q/d \mapsto \vartheta(C_{d,q})$. The green points (converging to the orange point $(3,3)$) are some of our lower bounds on $\Theta(C_{d,q})$, which are used to prove left-continuity of $q/d \mapsto \Theta(C_{d,q})$ at integers ≥ 3.

Left-continuity we derive from the following result (proved using an explicit construction).

Theorem. *For each $r,n \in \mathbb{N}$ with $r \geq 3$, we have*

$$\max_{\frac{q}{d}<r} \alpha(C_{d,q}^{\boxtimes n}) = \frac{1+r^n(r-2)}{r-1}.$$

We also prove that the independent set achieving $\alpha(C_{5,14}^{\boxtimes 3}) = 14$, one of the independent sets used in our proof, is unique up to Lee equivalence. Here two sets $C, D \subseteq \mathbb{Z}_q^n$ are *Lee equivalent* if there is a $g \in D_q^n \rtimes S_n$ with $g \cdot C = D$, where D_q is the dihedral group of order $2q$. We adapt our SDP upper bound for Lee codes to compute upper bounds on $\alpha(C_{d,q}^{\boxtimes n})$. Finally, we give a new lower bound of $367^{1/5} > 3.2578$ on the Shannon capacity of the 7-cycle.

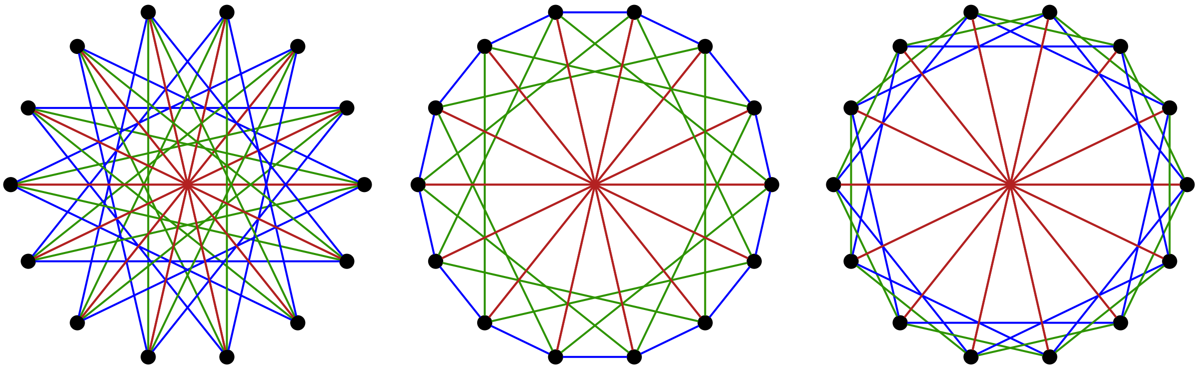


Figure S.3: Three graphs used in the proof to show that the independent set achieving $\alpha(C_{5,14}^{\boxtimes 3}) = 14$ is unique up to Lee equivalence.

An overarching theme: independent sets in graph products.

For any graph $G = (V, E)$, define the number

$$\alpha_d(G) := \max\{|U| \mid U \subseteq V,\ d_G(u,v) \geq d \text{ for all distinct } u,v \in U\}. \tag{S.2}$$

Here $d_G(u,v)$ denotes the smallest length (in edges) of a path between u and v in G. So $\alpha_2(G) = \alpha(G)$. Let K_q denote the complete graph on q vertices, and let C_q be the circuit on q vertices. Then

$$\begin{aligned} A_q(n,d) &= \alpha_d(K_q^{\square n}), \\ A_q^L(n,d) &= \alpha_d(C_q^{\square n}), \\ A_q^{L_\infty}(n,d) := \alpha(C_{d,q}^{\boxtimes n}) &= \alpha_d(C_q^{\boxtimes n}). \end{aligned}$$

Here $G^{\square n}$ denotes the *n-th Cartesian product power of* G: the graph with vertex set $V(G)^n$ in which two distinct vertices $(u_1,\dots,u_n)$ and $(v_1,\dots,v_n)$ are adjacent if and only if there is an $i \in \{1,\dots,n\}$ such that $u_iv_i \in E$, and $u_j = v_j$ for all $j \neq i$.

So the main objects studied in this thesis are of the form $\alpha_d(G^n)$, where $G \in \{C_q, K_q\}$, and where G^n denotes either $G^{\boxtimes n}$ or $G^{\square n}$. Moreover, we have $A(n,d,w) = \alpha_d(H)$, where H is the subgraph of $K_2^{\square n}$ induced by the vertices $(u_1,\dots,u_n)$ with $u_i = 1$ for exactly w indices $i \in \{1,\dots,n\}$ (where the vertices of K_2 are labeled with 0 and 1).

Samenvatting

Nieuwe methoden in coderingstheorie: foutencorrigerende codes en de Shannoncapaciteit

Foutencorrigerende codes worden al bestudeerd sinds 1948, toen Claude Shannon zijn invloedrijke artikel *A Mathematical Theory of Communication* publiceerde [85]. Laat q, n, d positieve gehele getallen zijn. De verzameling $Q := \{0, \ldots, q-1\}$ is ons *alfabet*. We identificeren elementen van Q^n met *woorden* van lengte n die bestaan uit letters uit Q. Een *code van lengte* n is een deelverzameling van Q^n. De *Hammingafstand* tussen twee woorden u, v is het aantal i met $u_i \neq v_i$. De *minimumafstand* van een code C is de kleinste Hammingafstand die voorkomt tussen twee verschillende elementen van C. We formuleren nu de centrale vraag uit de coderingstheorie.

$$\text{Wat is de maximale grootte van een code } C \text{ met minimumafstand ten minste } d? \tag{S.3}$$

De maximale grootte in (S.3) wordt aangegeven met $A_q(n, d)$. Een code C met minimumafstand $d := 2e + 1$ (voor een geheel getal e) heet *e-foutencorrigerend*. Als —bijvoorbeeld door storing— een codewoord uit C veranderd wordt in ten hoogste e posities, kunnen we het originele codewoord terugvinden door het codewoord te nemen dat het dichtst bij het veranderde woord in Hammingafstand zit. Dit principe wordt gebruikt voor het corrigeren van transmissiefouten in communicatiesystemen.

De getallen $A_q(n, d)$ zijn over het algemeen moeilijk te berekenen. Voor veel q, n, d zijn er alleen boven- en ondergrenzen op $A_q(n, d)$ bekend. Expliciete codes geven ondergrenzen op $A_q(n, d)$ en kunnen gebruikt worden voor foutencorrectie. Een klassieke bovengrens op $A_q(n, d)$ is Delsartes lineairprogrammeergrens [31]. Deze grens kan beschreven worden als een semidefiniet programma (SDP) gebaseerd op paren van codewoorden.

In dit proefschrift proberen we bovengrenzen op $A_q(n, d)$ te verbeteren. We geven een SDP gebaseerd op viertallen van codewoorden. Het optimalisatieprobleem is zeer symmetrisch: we kunnen aannemen dat de optimale oplossing invariant is onder de groepswerking van de groep van afstandsbewarende permutaties van Q^n: het kransproduct $S_q^n \rtimes S_n$. Vanwege de symmetrie van het probleem, kan het SDP gereduceerd worden tot een grootte polynomiaal begrensd door n.

In Hoofdstuk 3 geven we een algemene methode voor symmetriereductie, gebaseerd op representatietheorie. Stel dat G een eindige groep is die werkt op een eindige verzameling Z en laat $n \in \mathbb{N}$. We geven een reductie van $Z^n \times Z^n$ matrices die invariant zijn onder de simultane werking van de groep $G^n \rtimes S_n$ op de rijen en kolommen. In de reductie gaan we uit van een reductie van $Z \times Z$ matrices die invariant zijn onder de simultane werking van G op de rijen en kolommen.

In Hoofdstuk 4 passen we deze algemene methode toe om de grootte te reduceren van het genoemde SDP gebaseerd op viertallen van codewoorden voor het berekenen van bovengrenzen op $A_q(n,d)$. Met deze methode verbeteren we bekende bovengrenzen voor vijf drietallen (q,n,d).

In Hoofdstuk 5 verkennen we andere methoden om bovengrenzen op $A_q(n,d)$ te vinden, gebaseerd op combinatorische deelbaarheidsargumenten. De methoden geven nieuwe bovengrenzen voor vier drietallen (q,n,d). Ons meest prominente resultaat in deze richting is de volgende grens, die in sommige gevallen een verscherping oplevert van een grens die geïmpliceerd wordt door de Plotkingrens [67].

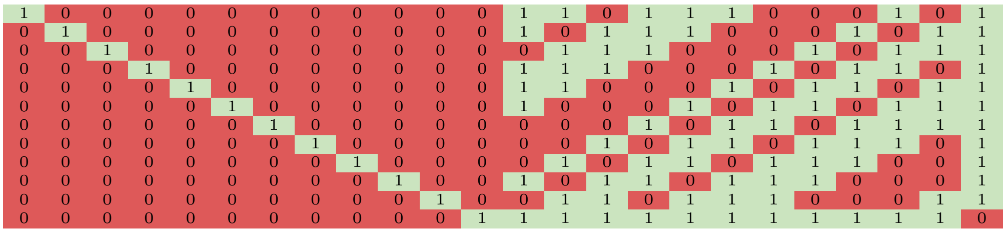
Stelling. *Stel dat q,n,d,m positieve gehele getallen zijn met $q \geq 2$, dat $d = m(qd-(q-1)(n-1))$, en dat $n-d$ geen deler is van $m(n-1)$. Als $r \in \{1,\ldots,q-1\}$ voldoet aan*

$$n(n-1-d)(r-1)r < (q-r+1)(qm(q+r-2)-2r),$$

dan geldt $A_q(n,d) < q^2m - r$.

In Hoofdstuk 6 bekijken we (binaire) *constant-gewicht-codes*. Hier is het alfabet $\{0,1\}$. Het *gewicht* van een woord is het aantal 1'en dat het bevat. Voor $n,d,w \in \mathbb{N}$, noteren we met $A(n,d,w)$ de maximale grootte van een code $C \subseteq \{0,1\}^n$ met minimumafstand ten minste d en waarin ieder codewoord gewicht w heeft. (Een dergelijke code heet een 'constant-gewicht-code' met gewicht w.) Met een SDP gebaseerd op viertallen van codewoorden en een symmetriereductie met de methode van Hoofdstuk 3, vinden we een groot aantal nieuwe bovengrenzen op $A(n,d,w)$. Twee van onze bovengrenzen zijn gelijk aan de best bekende ondergrenzen zodat we $A(n,d,w)$ precies kennen: $A(22,8,10) = 616$ en $A(22,8,11) = 672$.

In Hoofdstuk 7 bewijzen we met hulp van de duale oplossingen van de SDP-uitvoer dat de optimale constant-gewicht-codes die de waarden $A(23,8,11) = 1288$, $A(22,8,10) = 616$ en $A(22,8,11) = 672$ aantonen uniek zijn, op coördinaatpermutaties na. De genoemde unieke constant-gewicht-codes kunnen uit de binaire Golay-code —een beroemde code met goede foutencorrigerende eigenschappen— gehaald worden, door deelcodes te nemen en coördinaten weg te gooien.



1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	1	0	0	0	1	0	1
0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0	0	0	1	0	1	1
0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	0	1	1	1
0	0	0	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	0	1	1	0	1
0	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	1	0	1	1	0	1	1
0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0	1	1	1
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	1	1	0	1	1	1	1
0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1	0	1	1	1	0	1
0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	0	1	1	1	0	0	1
0	0	0	0	0	0	0	0	0	1	0	0	1	0	1	1	0	1	1	1	0	0	0	1
0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	1	1	0	0	0	1	1
0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0

Figuur S.4: Een voortbrengersmatrix van de uitgebreide binaire Golay-code (dit betekent dat de 2^{12} codewoorden sommen mod 2 van de rijen van deze matrix zijn). Deze code werd gebruikt om transmissiefouten te corrigeren in de *Voyager*-missies naar Jupiter and Saturnus [94].

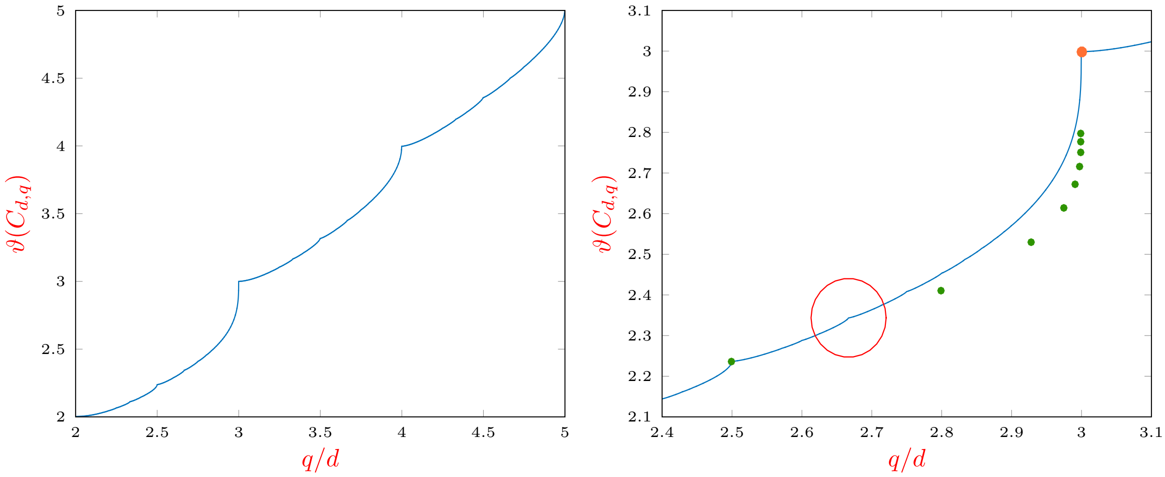
Voor 'gewone' (niet-constant-gewicht-) codes hebben Gijswijt, Mittelmann en Schrijver met SDP aangetoond dat $A_2(20,8) \leq 256$ [37]. Dit impliceert dat de vier keer verkorte uitgebreide binaire Golay-code van grootte 256 optimaal is. Twee niet-constant-gewicht-codes $C, D \subseteq \{0,1\}$ zijn *equivalent* als er een $g \in S_2^n \rtimes S_n$ is met $g \cdot C = D$. Op equivalentie na zijn de optimale codes die $A_2(24-i,8) = 2^{12-i}$ bereiken, voor $i = 0,1,2,3$, uniek [20]. Dit zijn de i-keer verkorte uitgebreide binaire Golay-codes. Wij bewijzen dat er verschillende niet-equivalente codes zijn die $A_2(20,8) = 256$ bereiken. We classificeren zulke codes met de extra eis dat alle afstanden deelbaar zijn door 4: we vinden 15 verschillende codes. We bewijzen ook dat er zulke codes bestaan met niet alle afstanden deelbaar door 4.

In Hoofdstuk 8 bekijken we *Lee-codes*. Laat $q, n, d \in \mathbb{N}$ en definieer $Q := \{0, \dots, q-1\}$. De *Lee-afstand* tussen twee woorden u, v is $\sum_{i=1}^{n} \min\{|u_i - v_i|, q - |u_i - v_i|\}$. De *minimum-Lee-afstand* van een code C is de kleinste Lee-afstand die voorkomt tussen twee verschillende elementen van C. We schrijven $A_q^L(n,d)$ voor de maximale grootte van een code $C \subseteq Q^n$ met minimum-Lee-afstand ten minste d. We geven een SDP-bovengrens gebaseerd op drietallen van codewoorden en laten zien dat deze efficiënt berekend kan worden, door middel van symmetriereducties met de methode van Hoofdstuk 3. Dit geeft nieuwe bovengrenzen op $A_q^L(n,d)$ voor veel drietallen (q,n,d).

Hoofdstuk 9 gaat over de Shannoncapaciteit van circulaire grafen. Zij $G = (V, E)$ een graaf en $n \in \mathbb{N}$. De *n-de sterkproductmacht* $G^{\boxtimes n}$ is de graaf met puntenverzameling V^n, en twee verschillende punten $(u_1, \dots, u_n)$ en $(v_1, \dots, v_n)$ van $G^{\boxtimes n}$ zijn verbonden dan en slechts dan als voor iedere $i \in \{1, \dots, n\}$ geldt dat ofwel $u_i = v_i$ ofwel $u_i v_i \in E$. De *Shannoncapaciteit* van G is gedefinieerd als

$$\Theta(G) := \sup_{n \in \mathbb{N}} \sqrt[n]{\alpha(G^{\boxtimes n})},$$

waar voor iedere graaf G de maximale grootte van een onafhankelijke verzameling in G (een verzameling punten waarvan geen twee punten verbonden zijn door een lijn) genoteerd wordt met $\alpha(G)$. De *circulaire graaf* $C_{d,q}$ is de graaf met puntenverzameling $\mathbb{Z}_q$ waarin twee verschillende punten verbonden zijn dan en slechts dan als hun afstand (mod q) strikt kleiner is dan d. Het is in te zien dat de waarde van $\alpha(C_{d,q}^n)$ (voor vaste n) en $\Theta(C_{d,q})$ alleen van de breuk q/d afhangt. We bewijzen dat de functie $q/d \mapsto \Theta(C_{d,q})$ continu is in *gehele getallen* $q/d \geq 3$. Dit impliceert dat ook de functie $q/d \mapsto \vartheta(C_{d,q})$, Lovász' bovengrens op $\Theta(C_{d,q})$ [53], continu is in deze punten — zie Figuur S.5.



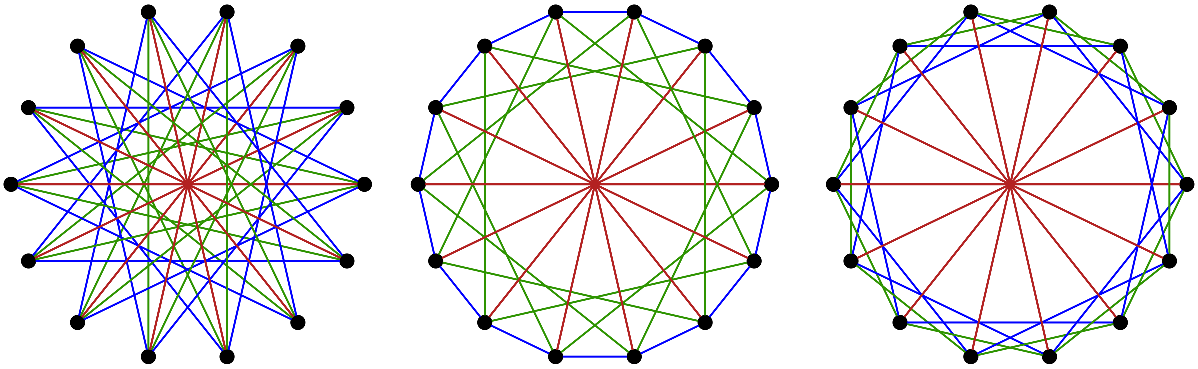
Figuur S.5: Twee grafieken van de functie $q/d \mapsto \vartheta(C_{d,q})$. De groene punten (die naar het oranje punt $(3,3)$ toebewegen) zijn een paar van onze ondergrenzen op $\Theta(C_{d,q})$ uit het bewijs van de linkscontinuïteit van $q/d \mapsto \Theta(C_{d,q})$.

Linkscontinuïteit van $q/d \mapsto \Theta(C_{d,q})$ leiden we af uit het volgende (bewezen met een expliciete constructie).

Stelling. *Voor iedere $r, n \in \mathbb{N}$ met $r \geq 3$ geldt dat*

$$\max_{\frac{q}{d}<r} \alpha(C_{d,q}^{\boxtimes n}) = \frac{1 + r^n(r-2)}{r-1}.$$

We bewijzen ook dat de onafhankelijke verzameling die $\alpha(C_{5,14}^{\boxtimes 3}) = 14$ aantoont, een van de onafhankelijke verzamelingen gebruikt in ons bewijs, uniek is op Lee-equivalentie na. Hier zijn twee verzamelingen $C, D \subseteq \mathbb{Z}_q^n$ *Lee-equivalent* als er een $g \in D_q^n \rtimes S_n$ is met $g \cdot C = D$, waar D_q de dihedrale groep van orde $2q$ is. We passen onze SDP-bovengrens voor Lee-codes aan om bovengrenzen op $\alpha(C_{d,q}^{\boxtimes n})$ te berekenen. Tot slot geven we een nieuwe ondergrens van $367^{1/5} > 3.2578$ op de Shannoncapaciteit van de 7-cykel.



Figuur S.6: Drie grafen die we gebruiken om te bewijzen dat de onafhankelijke verzameling die $\alpha(C_{5,14}^{\boxtimes 3}) = 14$ aantoont, uniek is (op Lee-equivalentie na).

Een overkoepelend thema: onafhankelijke verzamelingen in graafproducten.

Voor iedere graaf $G = (V, E)$ en $d \in \mathbb{N}$, definieren we het getal

$$\alpha_d(G) := \max\{|U| \mid U \subseteq V,\ d_G(u, v) \geq d \text{ voor alle } u \neq v \in U\}. \tag{S.4}$$

Hier schrijven we $d_G(u, v)$ voor de kleinste lengte (in lijnen) van een pad tussen u en v in G. Dus $\alpha_2(G) = \alpha(G)$. We schrijven K_q respectievelijk C_q voor de complete graaf respectievelijk het circuit op q punten. Dan geldt

$$\begin{aligned} A_q(n, d) &= \alpha_d(K_q^{\square n}), \\ A_q^L(n, d) &= \alpha_d(C_q^{\square n}), \\ A_q^{L_\infty}(n, d) := \alpha(C_{d,q}^{\boxtimes n}) &= \alpha_d(C_q^{\boxtimes n}). \end{aligned}$$

Hierin is $G^{\square n}$ de *n-de Cartesisch-product-macht van G*: dit is de graaf met puntenverzameling $V(G)^n$, waarin twee verschillende punten $(u_1, \ldots, u_n)$ en $(v_1, \ldots, v_n)$ verbonden zijn dan en slechts dan als er een $i \in \{1, \ldots, n\}$ is zo dat $u_i v_i \in E$, en $u_j = v_j$ voor alle $j \neq i$.

De objecten die we in dit proefschrift bestuderen hebben dus de vorm $\alpha_d(G^n)$, waar $G \in \{C_q, K_q\}$, en waar G^n ofwel $G^{\boxtimes n}$ of $G^{\square n}$ betekent. Verder is $A(n, d, w) = \alpha_d(H)$, met H de deelgraaf van $K_2^{\square n}$ geïnduceerd door de punten $(u_1, \ldots, u_n)$ met $u_i = 1$ voor precies w indices $i \in \{1, \ldots, n\}$ (hier zijn de punten van K_2 genummerd met 0 and 1).

Bibliography

[1] E. Agrell, A. Wardy, K. Zeger, Upper bounds for constant weight codes, *IEEE Transactions on Information Theory* **46** (2000), 2373–2395.

[2] A. Al-Kenani, The code of the symmetric net with $m = 4$ and $\mu = 2$, *Open Journal of Discrete Mathematics* **2** (1) (2012), 1–4.

[3] N. Alon, The Shannon capacity of a union, *Combinatorica* **18** (1998), 301–310.

[4] J. Astola, The Lee-scheme and bounds for Lee-codes, *Cybernetics and Systems* **13** (1982), 331–343.

[5] H. Astola, I. Tabus, Bounds on the size of Lee-codes, *8th International Symposium on Image and Signal Processing and Analysis (ISPA 2013)*, September 2013, Trieste (Italy), 471–476.

[6] H. Astola, I. Tabus, Sharpening the linear programming bound for linear Lee-codes, Electronics Letters **51** (2015), 492–494.

[7] C. Bachoc, D.C. Gijswijt, A. Schrijver, F. Vallentin, Invariant semidefinite programs, In *Handbook of Semidefinite, Conic and Polynomial Optimization: Theory, Algorithms, Software and Applications*, edited by M.F. Anjos and J.B. Lasserre, Springer, Chapter 9 (2011), 219–269.

[8] C. Bachoc, A. Pêcher, A. Thiéry, On the theta number of powers of cycle graphs, *Combinatorica* **33** (2013), 297–317.

[9] L.A. Bassalygo, S.M. Dodunekov, T. Helleseth, V.A. Zinoviev, The Grey-Rankin bound for nonbinary codes, *Problems of Information Transmission* **42** (2006), 197–203.

[10] L. Baumert, R. McEliece, E. Rodemich, H. Rumsey, R. Stanley, H. Taylor, A combinatorial packing problem, *Computers in Algebra and Number Theory*, American Mathematical Society, Providence, RI, 1971, 97–108.

[11] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York (1968).

[12] M.R. Best, A.E. Brouwer, F.J. MacWilliams, A.M. Odlyzko, and N.J.A. Sloane, Bounds for binary codes of length less than 25, *IEEE Transactions on Information Theory* **24** (1978), 81–93.

[13] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, second edition, 1986.

[14] A. Blasiak, *A Graph-Theoretic Approach to Network Coding*, PhD thesis, Cornell University, 2013.

[15] G. Bogdanova, A.E. Brouwer, S.N. Kapralov, P.R.J. Östergård, Error-correcting codes over an alphabet of four elements, *Designs, Codes and Cryptography* **23** (2001), 333–342.

[16] G. Bogdanova, P.R.J. Östergård, Bounds on codes over an alphabet of five elements, *Discrete Mathematics* **240** (2001), 13–19.

[17] G.T. Bogdanova, V.A. Zinoviev, T.J. Todorov, On the construction of q-ary equidistant codes, *Problems of Information Transmission* **43** (2007), 13–36.

[18] T. Bohman, A limit theorem for the Shannon capacities of odd cycles I, *Proceedings of the American Mathematical Society* **131** (2003), 3559–3569.

[19] J.A. Bondy, P. Hell, A note on the star chromatic number, *Journal of Graph Theory* **14** (1990), 479–482.

[20] A.E. Brouwer, Block designs, in: *Handbook of Combinatorics*, R. Graham, M. Grötschel, L. Lovász, eds., Elsevier, 1995, 693–745.

[21] A.E. Brouwer, Tables with bounds on $A(n,d)$, `http://www.win.tue.nl/~aeb/codes/binary-1.html`.

[22] A.E. Brouwer, Tables with bounds on $A(n,d,w)$, `http://www.win.tue.nl/~aeb/codes/Andw.html`.

[23] A.E. Brouwer, Tables with bounds on $A_q(n,d)$, `http://www.win.tue.nl/~aeb/`.

[24] A.E. Brouwer, S.C. Polak, Computer programs used for [25], `https://github.com/codeuniqueness/code_uniqueness`.

[25] A.E. Brouwer, S.C. Polak, Uniqueness of codes using semidefinite programming, *Designs, Codes and Cryptography* **87** (2019), 1881–1895.

[26] A.E. Brouwer, J.B. Shearer, N.J.A. Sloane, W.D. Smith, A new table of constant weight codes, *IEEE Transactions on Information Theory* **36** (1990), 1334–1380.

[27] B. Bukh, C. Cox, On a fractional version of Haemers' bound, `arXiv` 1802.00476 (2018).

[28] A.R. Calderbank, P.J. Cameron, W.M. Kantor, J.J. Seidel, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Transactions on Information Theory* **40** (1994), 301–319.

[29] F.N. Cole, Kirkman parades, *Bulletin of the American Mathematical Society* **28** (1922), 435–437.

[30] T. Cubitt, L. Mančinska, D.E. Roberson, S. Severini, D. Stahlke, A. Winter, Bounds on entanglement assisted source-channel coding via the Lovász theta number and its variants, *IEEE Transactions on Information Theory* **60** (2014), 7330–7344.

[31] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Research Reports Supplements* **10** (1973).

[32] P. Delsarte, J.M. Goethals, Unrestricted codes with the Golay parameters are unique, *Discrete Mathematics* **12** (1975), 211–224.

[33] S.M. Dodunekov, S.B. Encheva, Uniqueness of some linear subcodes of the extended binary Golay code, *Problems of Information Transmission* **29** (1993), 45-–51.

[34] M. Fekete, Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten, *Mathematische Zeitschrift* **17** (1923), 228–249.

[35] D.C. Gijswijt, Block diagonalization for algebras associated with block codes, `arXiv` 0910.4515 (2009).

[36] D.C. Gijswijt, *Matrix Algebras and Semidefinite Programming Techniques for Codes*, PhD thesis, University of Amsterdam, 2005.

[37] D.C. Gijswijt, H.D. Mittelmann, A. Schrijver, Semidefinite code bounds based on quadruple distances, *IEEE Transactions on Information Theory* **58** (2012), 2697–2705.

[38] D.C. Gijswijt, A. Schrijver, H. Tanaka, New upper bounds for nonbinary codes based on the Terwilliger algebra and semidefinite programming, *Journal of Combinatorial Theory, Series A* **113** (2006), 1719–1731.

[39] C.D. Godsil, Problems in algebraic combinatorics, *The Electronic Journal of Combinatorics* **2** (1995), #F1.

[40] M.J.E. Golay, Notes on digital coding, *Proceedings of the IRE* **37** (1949), 657.

[41] M. Grötschel, L. Lovász, A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, Vol. 2, Springer, 2012.

[42] Gurobi Optimization, LLC, *Gurobi Optimizer Reference Manual*, 2018, `http://www.gurobi.com`.

[43] W.H. Haemers, On some problems of Lovász concerning the Shannon capacity of a graph, *IEEE Transactions on Information Theory* **25** (1979), 231–232.

[44] R.W. Hamming, Error detecting and error correcting codes, *The Bell System Technical Journal* **29** (1950), 147–160.

[45] M. Jurkiewicz, M. Kubale, K. Turowski, Some lower bounds on the Shannon capacity, *Journal of Applied Computer Science* **22** (2014), 31–42.

[46] P. Kaski, P.R.J. Östergård, *Classification Algorithms for Codes and Designs*, Springer, Berlin, 2006.

[47] H.K. Kim, P.T. Toan, Improved semidefinite programming bound on sizes of codes, *IEEE Transactions on Information Theory* **59** (2013), 7337–7345.

[48] D.E. Knuth, The sandwich theorem, *The Electronic Journal of Combinatorics* **1** (1994), #A1.

[49] C.Y. Lee, Some properties of nonbinary error-correcting codes, *IRE Transactions on Information Theory* **4** (1958), 77–82.

[50] J.H. van Lint, *Introduction to Coding Theory*, Springer, Third edition, 1998.

[51] B.M. Litjens, Semidefinite bounds for mixed binary/ternary codes, *Discrete Mathematics* **341** (2018), 1740–1748.

[52] B.M. Litjens, S.C. Polak, A. Schrijver, Semidefinite bounds for nonbinary codes based on quadruples, *Designs, Codes and Cryptography* **84** (2017), 87–100.

[53] L. Lovász, On the Shannon capacity of a graph, *IEEE Transactions on Information Theory* **25** (1973), 1–7.

[54] C. Mackenzie, J. Seberry, Maximal q-ary codes and Plotkin's bound, *Ars Combinatoria* **26B** (1988), 37–50.

[55] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, 1983.

[56] K.A. Mathew, P.R.J. Östergård, New lower bounds for the Shannon capacity of odd cycles, *Designs, Codes and Cryptography* **84** (2017), 13–22.

[57] V. Mavron, V.D. Tonchev, On symmetric nets and generalized Hadamard matrices, *Journal of Geometry* **67** (2000), 180–187.

[58] R.J. McEliece, E.C. Posner, Hide and seek, data storage, and entropy, *The Annals of Mathematical Statistics* **42** (1971), 1706–1716.

[59] R.J. McEliece, E.R. Rodemich, H.C. Rumsey, Jr, The Lovász bound and some generalizations, *Journal of Combinatorics, Information and System Sciences* **3** (1978), 134–152.

[60] B.D. McKay, A. Piperno, Practical graph isomorphism, II, *Journal of Symbolic Computation* **60** (2013), 94–112.

[61] M. Nakata, A numerical evaluation of highly accurate multiple-precision arithmetic version of semidefinite programming solver: SDPA-GMP, -QD and -DD, *Proceedings of 2010 IEEE Multi-Conference on Systems and Control*, 2010, 29–34.

[62] Y. Nesterov, A. Nemirovskii, *Interior-point Polynomial Algorithms in Convex Programming*, Vol. 13, SIAM, Philadelphia, 1994.

[63] P.R.J. Östergård, Classification of binary constant weight codes, *IEEE Transactions on Information Theory* **56** (2010), 3779–3785.

[64] P.R.J. Östergård, Classification of binary/ternary one-error-correcting codes, *Discrete Mathematics* **223** (2000), 253–262.

[65] V. Pless, A classification of self-orthogonal codes over GF(2), *Discrete Mathematics* **3** (1972), 209–246.

[66] V. Pless, N.J.A. Sloane, On the classification and enumeration of self-dual codes, *Journal of Combinatorial Theory, Series A* **18** (1975), 313–335.

[67] M. Plotkin, Binary codes with specified minimum distance, *IRE Transactions on Information Theory* **6** (1960), 445–450.

[68] M. Plotkin, *Binary Codes with Specified Minimum Distance*, MSc thesis, Moore School of Electrical Engineering, University of Pennsylvania, 1952.

[69] S.C. Polak, New nonbinary code bounds based on divisibility arguments, *Designs, Codes and Cryptography* **86** (2018), 861–874.

[70] S.C. Polak, Semidefinite programming bounds for constant weight codes, *IEEE Transactions on Information Theory* **65** (2019), 28–38.

[71] S.C. Polak, Semidefinite programming bounds for Lee codes, *Discrete Mathematics* **342** (2019), 2579–2589.

[72] S.C. Polak, A. Schrijver, New lower bound on the Shannon capacity of C_7, *Information Processing Letters* **143** (2019), 37–40.

[73] C. Procesi, *Lie Groups: An Approach through Invariants and Representations*, Springer, New York, 2006.

[74] J. Quistorff, New upper bounds on Lee codes, *Discrete Applied Mathematics* **154** (2006), 1510–1521.

[75] J. Quistorff, Some remarks on the Plotkin bound, *The Electronic Journal of Combinatorics* **10** (2003), #N6.

[76] G. Regts, *Upper Bounds for Ternary Constant Weight Codes from Semidefinite Programming and Representation Theory*, MSc thesis, University of Amsterdam, 2009.

[77] B.E. Sagan, *The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions*, Graduate Texts in Mathematics, Vol. 203, Springer, New York, 2001.

[78] C. Sarami, On classification of generalized Hadamard matrices, *Proceedings of the 2007 International Conference on Foundations of Computer Science (FCS.07)*, Las Vegas.

[79] A. Schrijver, A comparison of the Delsarte and Lovász bounds, *IEEE Transactions on Information Theory* **25** (1979), 425–429.

[80] A. Schrijver, *Combinatorial Optimization: Polyhedra and Efficiency*, Vol. 24, Springer, Heidelberg, 2003.

[81] A. Schrijver, New code upper bounds from the Terwilliger algebra and semidefinite programming, *IEEE Transactions on Information Theory* **51** (2005), 2859–2866.

[82] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley, Chichester, 1986.

[83] N.V. Semakov, V.A. Zinoviev, Equidistant q-ary codes with maximal distance and resolvable balanced incomplete block designs, *Problems of Information Transmission* **4** (1968), 1–7.

[84] N.V. Semakov, V.A. Zinoviev, G.V. Zaitzev, Class of maximal equidistant codes, *Problems of Information Transmission* **5** (1969), 65–68.

[85] C.E. Shannon, A mathematical theory of communication, *Bell System Technical Journal* **27** (1948), 379–423, 623–656.

[86] C.E. Shannon, The zero-error capacity of a noisy channel, *IRE Transactions on Information Theory* **2** (1956), 8–19.

[87] D.H. Smith, L.A. Hughes, S. Perkins, A new table of constant weight codes of length greater than 28, *The Electronic Journal of Combinatorics* **13** (2006), #A2.

[88] S.L. Snover, *The Uniqueness of the Nordstrom-Robinson and Golay Binary Codes*, PhD thesis, Michigan State University, East Lansing, Michigan, 1973.

[89] V. Strassen, The asymptotic spectrum of tensors, *Journal für die reine und angewandte Mathematik* **382** (1988), 102–152.

[90] P.T. Toan, H.K. Kim, J. Kim, Improved linear programming bound on sizes of doubly constant weight codes, *Finite Fields and their Applications* **54** (2018), 230–252.

[91] M.J. Todd, Semidefinite optimization, *Acta Numerica* **10** (2001), 515–560.

[92] R.J.M. Vaessens, E.H.L. Aarts, J.H. van Lint, Genetic algorithms in coding theory — a table for $A_3(n,d)$, *Discrete Applied Mathematics* **45** (1993), 71–87.

[93] A. Vesel, J. Žerovnik, Improved lower bound on the Shannon capacity of C_7, *Information Processing Letters* **81** (2002), 277–282.

[94] S. Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice Hall, Upper Saddle River, NJ, 1995.

[95] A.D. Wyner, R.L. Graham, An upper bound on minimum distance for a k-ary code, *Information and Control* **13** (1968), 46–52.

[96] M. Yamashita, K. Fujisawa, M. Fukuda, K. Kobayashi, K. Nakta, M. Nakata, Latest developments in the SDPA Family for solving large-scale SDPs, In *Handbook on Semidefinite, Cone and Polynomial Optimization: Theory, Algorithms, Software and Applications*, edited by Miguel F. Anjos and Jean B. Lasserre, Springer, Chapter 24 (2011), 687–714.

[97] J. Zuiddam, *Algebraic Complexity, Asymptotic Spectra and Entanglement Polytopes*, PhD thesis, University of Amsterdam, 2018.

[98] J. Zuiddam, The asymptotic spectrum of graphs and the Shannon capacity, `arXiv` 1807.00169 (2018).

Index

List of symbols

$\mathbf{0}$	all-zeros word,	4
$\mathbf{1}$	all-ones word,	67
A	basis $\{a_P \mid P \in \Lambda\}$ of W,	29
A^*	basis $\{a_P^* \mid P \in \Lambda\}$ of W^*, i.e., dual basis of A,	30
A^*	conjugate transpose of matrix A,	18
$A(n,d)$	maximum size of a code $C \subseteq \mathbb{F}_2^n$ with $d_{\min}(C) \geq d$,	2
$A(n,d,w)$	maximum size of a constant weight w code $C \subseteq \mathbb{F}_2^n$ with $d_{\min}(C) \geq d$,	4
$\langle A, B\rangle$	trace inner product of matrices A and B,	18
$[a,b]$	the set $\{a, a+1, \ldots, b\}$,	117
A_i	basis $\{a_P \mid P \in \Lambda_i\}$ of W_i,	32
A_i	number of words of weight i in code (only in Prop. 7.5.1),	88
$(a_i)_{i=0}^n$	distance distribution,	20
$A_k(n,d)$	upper bound on $A(n,d)$ (only in Chapter 7),	80
$A_k(n,d,w)$	upper bound on $A(n,d,w)$,	64
$\alpha(G)$	independent set number of graph G,	2, 17
$\alpha_d(G)$	$\max\{\lvert U\rvert \mid U \subseteq V(G),\ d_G(u,v) \geq d$ for all distinct $u, v \in U\}$,	13
α_n	number defined and used in the proof of Prop. 9.3.2,	117
a_P	basis element of W,	29
$A_q(n,d)$	maximum size of a code $C \subseteq [q]^n$ with $d_{\min}(C) \geq d$,	2
$A_q^L(n,d)$	maximum size of a code $C \subseteq \mathbb{Z}_q^n$ with $d_{\min}^L(C) \geq d$,	5
$A_q^{L_\infty}(n,d)$	maximum size of a code $C \subseteq \mathbb{Z}_q^n$ with $d_{\min}^{L_\infty}(C) \geq d$, i.e., $\alpha(C_{d,q}^{\boxtimes n})$,	11
A^T	transpose of matrix A,	18
$\boldsymbol{B}$	representative set $\boldsymbol{B} = \{B_1, \ldots, B_k\}$ for the action of G on V,	27
B	quadruply shortened extended binary Golay code (only in Sect. 7.5.1),	87
b_ω	constant in semidefinite programs (7.3) and (7.4),	81
$B_k(n,d)$	upper bound on $A(n,d)$,	75
$B_k(n,d,w)$	upper bound on $A(n,d,w)$,	65
$B_k^{L_\infty}(q,n,d)$	upper bound on $\alpha(C_{d,q}^{\boxtimes n}) = A_q^{L_\infty}(n,d)$,	123
$B_k^L(q,n,d)$	upper bound on $A_q^L(n,d)$,	95
$b_k^L(q,n,d)$	upper bound on $A_q^L(n,d)$,	102
$B_q(n,d)$	upper bound on $A_q(n,d)$,	3, 39
$B(u)$	ball around codeword u,	20
$\langle C\rangle$	$\mathbb{F}_2$-linear span of code $C \subseteq \mathbb{F}_2^n$,	83
$c_{\alpha,j}$	number of times symbol α appears in column j of C,	50
$C(\Delta,\infty)$	Banach algebra of continuous functions $\Delta \to \mathbb{R}$ with the $\lVert . \rVert_\infty$-norm,	116

$G \boxtimes H$	strong product of graphs G and H,	13
$G^{\boxtimes n}$	n-th strong product power of graph G,	9
$\overline{\chi}^*(G)$	fractional clique cover number of graph G,	115
$G^n \rtimes S_n$	wreath product of group G and S_n,	6
$G(q, n, d)$	graph with independent set number $A_q(n, d)$,	2
$G \,\Box\, H$	Cartesian product of graphs G and H,	12
$G^{\Box n}$	n-th Cartesian product power of graph G,	12
$G[U]$	subgraph of graph G induced by $U \subseteq V(G)$,	121
$h(q, n, d, M)$	leftmost term minus rightmost term in (5.4),	51
H_D	subgroup of H that leaves D invariant,	96
H'_D	subgroup of H that leaves each element of D invariant,	66
I_n	$n \times n$ identity matrix,	18
J_n	$n \times n$ all-ones matrix,	18
K^Z	vector space consisting of all functions $Z \to K$,	18
$\mathcal{K}(G)$	the collection of all cliques in G,	115
κ	count function,	33
KG	group algebra of G over K,	18
K_ω	adjacency matrix of ω,	29, 32
$K^{(i)}_{\omega_i}$	adjacency matrix of ω_i,	32
K_q	complete graph on q vertices,	13
$K_t(x)$	Krawtchouk polynomial,	2
KZ	free vector space of Z over K,	17
L	$(\mathcal{C}_2 \setminus \{\emptyset\}) \times ([q]^n)^2$ matrix,	43
Λ	$(Z \times Z)/G$,	29
Λ_i	$(Z_i \times Z_i)/G_i$,	31
λ^*	dual partition of λ,	33
$\lambda \vdash n$	λ is a partition of n,	26
$\boldsymbol{\lambda} \vdash \boldsymbol{n}$	k partitions $\lambda_i \vdash n_i$,	27
L_t	subspace of $\mathbb{C}^{\mathcal{C}_2}$,	44
$L^{(2)}_{w_1,w_2,d_1}$	subspace of $\mathbb{C}^{(\mathbb{F}_2^n)^2}$,	72
L_{w,d_1,d_2}	subspace of $\mathbb{C}^{\mathbb{F}_2^n}$,	69
$[m]$	set $\{1, \ldots, m\}$,	17
$\boldsymbol{m}$	k-tuple of integers $(m_1, \ldots, m_k)$,	27
$\widetilde{M}$	$\mathbb{Z}_7 \times \mathbb{Z}_7$ matrix with entries in $\mathbb{Z}_5$,	9
$M(x)$	variable matrix,	3, 39
$M(z)$	matrix in in $(\mathbb{C}^{Z^n \times Z^n})^H$,	29
$M(z)$	reduced variable matrix,	40
M_{23}	Mathieu group,	20
M_{24}	Mathieu group,	20
$M_{k,D}(x)$	variable matrix,	64, 80, 95
$M_{k,D}(z)$	reduced variable matrix,	66, 80, 96
$\mu(\omega)$	monomial $a^*_{P_1} \cdots a^*_{P_n} \in \mathcal{O}_n(W)$,	30
(M, z)	feasible (or optimum) solution to (7.3),	81

N	matrix $(e_0 - e_1)\mathbf{1}^\mathsf{T}$,	42
N	subset of $\mathbb{F}_2^n$,	64, 75, 80
$\mathbb{N}$	set of positive integers,	17
$\boldsymbol{N}$	collection of k-tuples $(n_1, \ldots, n_k)$ of nonnegative integers with sum n,	27
N_ω	$([q]^n \times [q]^n) \times ([q]^n \times [q]^n)$ matrix,	45
N_ω	$\mathbb{F}_2^n \times \mathbb{F}_2^n$ matrix,	70
N_ω	$\mathcal{C}_3(D) \times \mathcal{C}_3(D)$ matrix,	97
$\widetilde{N}_\omega$	$\mathbb{Z}_q^n \times \mathbb{Z}_q^n$ matrix,	100
N'_ω	$\mathbb{Z}_5^n \times \mathbb{Z}_5^n$ matrix,	107
N'_ω	$\mathcal{C}_2 \times \mathcal{C}_2$ matrix,	41
$N_\omega^{(1)}$	$\mathbb{F}_2^n \times \mathbb{F}_2^n$ matrix,	73
$N_\omega^{(2)}$	$(\mathbb{F}_2^n \times \mathbb{F}_2^n) \times (\mathbb{F}_2^n \times \mathbb{F}_2^n)$ matrix,	73
$\mathcal{O}(V)$	coordinate ring of V,	18
$\mathcal{O}_n(V)$	set of homogeneous polynomials of degree n on V,	18
ω_i	H-orbit of two words at distance i,	35
ω_0	orbit of a code of size 1,	74, 108
$\omega_\emptyset$	the orbit $\{\emptyset\}$,	47
Ω_k	set of H-orbits on $\mathcal{C}_k$,	6, 40, 66, 95
Ω_k^d	collection of H-orbits of codes of minimum distance at least d,	47, 80
ω_t	S_n-orbit of a pair of constant weight code words at distance $2t$,	74
ω_t	$S_q^n \rtimes S_n$-orbit of a pair of code words at distance t,	47
$P_\lambda(X)$	polynomial defined in (3.27),	34
$p_{\tau,\sigma}$	polynomial corresponding to semistandard Young tableaux,	30
Q	alphabet,	1
$[q]$	alphabet $\{0, \ldots, q-1\}$,	17
q_n	number defined in (9.14),	117
R	The set $Z_1^{j_1} \times \ldots \times Z_s^{j_s}$ (in Sect. 3.3),	31
r	surjective function,	45, 70, 98
$\widetilde{r}$	surjective function,	100
r'	surjective function,	74, 107
$r(s,j)$	$\#$ symbols s in row j of τ,	33
$\mathbb{R}_{\geq 0}$	set of nonnegative real numbers,	17
R_λ	row stabilizer of λ,	26
$R^{Y \times Z}$	set of $Y \times Z$ matrices with entries in R,	18
S^c	the code $S + \mathbf{1}$,	67
σ	nonidentity element in S_2 (in Sect. 4.2.3),	43
S_n	symmetric group on n elements,	5
$\mathrm{Sym}_t(X)$	vector space $(X^{\otimes t})^{S_t}$,	28
S_Z	group of bijections of Z to itself,	22
$\tau \sim \tau'$	$\tau' = \tau r$ for some $r \in R_\lambda$,	26
$\boldsymbol{\tau_n}$	unique element of $\boldsymbol{T_{\lambda,m}}$ with $\boldsymbol{m} = (1, \ldots, 1)$,	99
$\vartheta'(G)$	upper bound on $\alpha(G)$,	2
$\Theta(G)$	Shannon capacity of graph G,	9

$\vartheta(G)$	Lovász's theta number of graph G,	10, 112
$T^{(1)}_{\lambda,2}$	subset of $T_{\lambda,2}$,	72
$T^{(2)}_{\lambda,4}$	subset of $T_{\lambda,4}$,	72
$T_{\lambda,m}$	collection of semistandard λ-tableaux with entries in $[m]$,	26
$\boldsymbol{T_{\lambda,m}}$	product of T_{λ_i,m_i},	28
$\boldsymbol{T'_{\lambda,m}}$	subset of $\boldsymbol{T_{\lambda,m}}$,	44, 69
$\boldsymbol{T''_{\lambda,m}}$	subset of $\boldsymbol{T'_{\lambda,m}}$,	45
$u \cap v$	word in $\mathbb{F}_2^n$ that has 1 at position i if and only if $u_i = v_i = 1$,	82
$u(s,j)$	# symbols s in row j of σ,	33
$U_{\boldsymbol{\lambda}}$	matrix in representative set that corresponds with $\boldsymbol{\lambda}$,	29
$u_{\tau,B}$	element of ordered $\lvert T_{\lambda,m}\rvert$-tuple in representative set in (2.21),	26
$\boldsymbol{u_{\tau,B}}$	element of ordered tuple in representative set in (3.3),	28
$V(G)$	vertex set of graph G,	17
V^*	dual vector space of V,	18
W	$(\mathbb{C}Z \otimes \mathbb{C}Z)^G$,	29
$\widehat{w}$	element of $\mathcal{O}_n(W)$ associated to $w = (w_1^* \otimes \cdots \otimes w_n^*) \in (W^*)^{\otimes n}$,	30
W_i	$(\mathbb{C}Z_i \otimes \mathbb{C}Z_i)^{G_i}$,	31
$\mathrm{wt}(v)$	weight of word v,	4, 19
$X \succeq 0$	matrix X is positive semidefinite,	2
X	feasible (or optimum) solution to (7.4),	81
X	the set of irregular pairs in C (only in Chapter 5),	52
(X_ω)	1×1 block in X corresponding to the 1×1 block $(z(\omega))$ in M,	81
$Y(\lambda)$	Young shape of λ,	26
$z(\omega)$	variable of reduced program,	30, 40, 66, 96
$\overline{z}$	complex conjugate of $z \in \mathbb{C}$,	18
Z^G	subset of Z of G-invariant elements,	22
$\mathbb{Z}_{\geq 0}$	set of nonnegative integers,	17
$\mathbb{Z}_q$	group of integers modulo q,	17