# Semidefinite programming bounds for Lee codes

Sven C. Polak[1]

*Korteweg–De Vries Institute for Mathematics, University of Amsterdam, Netherlands*

## ARTICLE INFO

## ABSTRACT

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 a semidefinite programming bound based on triples of codewords, which bound can be computed efficiently using symmetry reductions, resulting in several new upper bounds on $A_q^L(n, d)$.

The technique also yields an upper bound on the independent set number of the $n$th strong product power of the circular graph $C_{d,q}$, which number is related to the Shannon capacity of $C_{d,q}$. Here $C_{d,q}$ is the graph with vertex set $\mathbb{Z}_q$, in which two vertices are adjacent if and only if their distance (mod $q$) is strictly less than $d$. The new bound does not seem to improve significantly over the bound obtained from Lovász theta-function, except for very small $n$.

© 2019 Elsevier B.V. All rights reserved.

## 1. Introduction

Fix two integers $n, q \in \mathbb{N}$. Denote by $\mathbb{Z}_q$ the group of integers $0, 1, \ldots, q - 1 \pmod{q}$, which serves as alphabet. A *word* is an element $v \in \mathbb{Z}_q^n$ and a *code* is a subset $C \subseteq \mathbb{Z}_q^n$. For two words $u, v \in \mathbb{Z}_q^n$, their *Lee distance* is $d_L(u, v) := \sum_{i=1}^n \min\{|u_i - v_i|, q - |u_i - v_i|\}$. 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

$$A_q^L(n, d) := \max\{|C| \mid C \subseteq \mathbb{Z}_q^n, \; d_{\min}^L(C) \geq d\}. \tag{1}$$

The Lee distance was introduced by C.Y. Lee in 1958 [14]. If $q = 2$ or $q = 3$, the Lee distance coincides with the Hamming distance. For $q \geq 4$, the Lee distance does not only take into account the number of symbols that are different in two words (which is measured by the Hamming distance), but also to what extent these symbols are different. Because of this property, the Lee distance is used in certain communication systems for information transmission (so called 'phase modulated systems', see [7, Chapter 8]).

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 [20]. H. Astola and I. Tabus calculated several new upper bounds by linear programming [2], using an adaptation of the classical Delsarte bound based on pairs of codewords [9] (see also [1]).

For binary codes equipped with the Hamming distance, the Delsarte bound was generalized to a semidefinite programming bound based on triples of codewords by A. Schrijver [23], and later to a quadruple bound by Gijswijt, Mittelmann and Schrijver [11]. Also, nonbinary codes with the Hamming distance have been considered [12,16], codes

---

**Table 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 (3) below. The superscript $l$ refers to a bound obtained by Astola and Tabus using linear programming [2]. The superscript $b$ refers to a bound from Quistorff [20]. The superscript $*$ refers to an upper bound matching the known lower bound: $A_7^L(4, 5) = 49$ is achieved by a linear code [3].

| q | n | d | New upper bound | Best upper bound previously known | q | n | d | New upper bound | Best upper bound previously known |
|---|---|---|---|---|---|---|---|---|---|
| 5 | 4 | 3 | 62 | $64^l$ | 6 | 5 | 6 | 61 | $67^l$ |
| 5 | 4 | 4 | 27 | $30^l$ | 6 | 5 | 7 | 22 | $24^{bl}$ |
| 5 | 4 | 5 | 10 | $11^l$ | 6 | 6 | 6 | 273 | $293^l$ |
| 5 | 5 | 3 | 270 | $276^l$ | 6 | 6 | 7 | 79 | $85^l$ |
| 5 | 5 | 5 | 36 | $39^l$ | 6 | 6 | 8 | 48 | $52^l$ |
| 5 | 5 | 6 | 15 | $18^l$ | 6 | 6 | 9 | 16 | $17^l$ |
| 5 | 6 | 3 | 1170 | $1176^l$ | 7 | 3 | 4 | 21 | $24^{bl}$ |
| 5 | 6 | 4 | 494 | $520^b$ | 7 | 3 | 5 | 10 | $11^l$ |
| 5 | 6 | 5 | 149 | $155^l$ | 7 | 4 | 3 | 256 | $263^l$ |
| 5 | 6 | 6 | 60 | $63^l$ | 7 | 4 | 4 | 121 | $128^b$ |
| 5 | 6 | 7 | 25 | $28^l$ | 7 | 4 | 5 | **49*** | $50^l$ |
| 5 | 7 | 3 | 5180 | $5208^{bl}$ | 7 | 4 | 6 | 23 | $27^l$ |
| 5 | 7 | 4 | 2183 | $2232^b$ | 7 | 4 | 7 | 11 | $13^l$ |
| 5 | 7 | 5 | 590 | $608^l$ | 7 | 4 | 8 | 6 | $7^{bl}$ |
| 5 | 7 | 6 | 250 | $284^l$ | 7 | 5 | 3 | 1499 | $1512^l$ |
| 5 | 7 | 7 | 79 | $81^l$ | 7 | 5 | 4 | 686 | $720^b$ |
| 5 | 7 | 8 | 35 | $41^l$ | 7 | 5 | 5 | 240 | $249^l$ |
| 6 | 3 | 3 | 27 | $29^l$ | 7 | 5 | 6 | 116 | $130^l$ |
| 6 | 3 | 4 | 14 | $17^l$ | 7 | 5 | 7 | 49 | $54^l$ |
| 6 | 4 | 4 | 78 | $79^l$ | 7 | 5 | 8 | 25 | $28^l$ |
| 6 | 4 | 5 | 22 | $26^l$ | 7 | 5 | 9 | 13 | $14^l$ |
| 6 | 5 | 3 | 693 | $699^l$ | 7 | 6 | 10 | 26 | $31^l$ |
| 6 | 5 | 4 | 366 | $378^l$ | 7 | 6 | 11 | 13 | $14^b$ |
| 6 | 5 | 5 | 107 | $114^l$ | | | | | |

with mixed alphabets [15] and constant weight (binary) codes [19,23]. In [4], the authors mention the possibility of applying semidefinite programming to Lee codes and they state that to their best knowledge, such bounds for Lee codes using triples have not yet been studied.

In this paper, 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 only consider $q \geq 5$, since for $q = 4$, the problem of determining $A_4^L(n, d)$ is equivalent to determining the maximum size of a binary code of length $2n$ and minimum distance $d$ using the Gray map (see, for example, [8]). We find several new upper bounds on $A_q^L(n, d)$, see Table 1.

In Section 4, we show how to adapt the new bound to an upper bound $B_3^{L\infty}(q, n, d)$ on the independent set number of the $n$th strong product power of the circular graph $C_{d,q}$, which number is related to the Shannon capacity of $C_{d,q}$. The *circular graph* $C_{d,q}$ is the graph with vertex set $\mathbb{Z}_q$, in which two vertices are adjacent if and only if their distance (mod $q$) is strictly less than $d$. The new bound does not seem to improve significantly over the bound obtained from Lovász theta-function, except for very small $n$.

## 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 [11]. 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

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

Note that with this definition $|C \cup C'| \leq k$ for all $C, C' \subseteq \mathcal{C}_k(D)$. Also we define, for any function $x : \mathcal{C}_k \to \mathbb{R}$ and $D \in \mathcal{C}_k$, 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:

$$B_k^L(q, n, d) := \max\{\sum_{v \in \mathbb{Z}_q^n} x(\{v\}) \mid x : \mathcal{C}_k \to \mathbb{R}, \ x(\emptyset) = 1, \ x(S) = 0 \text{ if } d_{\min}^L(S) < d,$$

$$M_{k,D}(x) \text{ is positive semidefinite for each } D \text{ in } \mathcal{C}_k\}. \tag{3}$$

**Proposition 1.1.** *Fix $k \in \mathbb{N}$. For all $q, n, d \in \mathbb{N}$, 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 $d_{\min}^L(C) \geq d$ 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. Then $x$ satisfies the conditions in (3), where the last condition 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 many instances by Astola and Tabus in [2]. In this paper 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 [16].

### 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 (3) is $H$-invariant, i.e., $g \circ x = x$ for all $g \in H$. Indeed, if $x$ is any optimum solution for (3), then for each $g \in H$, the function $g \circ x$ is again an optimum solution, since the objective value of $g \circ x$ equals the objective value of $x$ and $g \circ x$ still satisfies all constraints in (3). Since the feasible region is convex, the optimum $x$ can be replaced by the average of $g \circ x$ over all $g \in H$. This gives an $H$-invariant optimum solution.

Let $\Omega_k$ be the set of $H$-orbits on $\mathcal{C}_k$. Then $|\Omega_k|$ is bounded by a polynomial in $n$, for fixed $q$. 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 (3).

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. This means that the matrices $M_{k,D}(z)$ are elements of $(\mathbb{C}^{\mathcal{C}_k(D) \times \mathcal{C}_k(D)})^{H_D}$, which is naturally isomorphic to the *centralizer algebra* of the action of $H_D$ on $\mathbb{C}^{\mathcal{C}_k(D)}$, i.e., the collection of $H_D$-equivariant endomorphisms $\mathbb{C}^{\mathcal{C}_k(D)} \to \mathbb{C}^{\mathcal{C}_k(D)}$. Therefore, there exists a block-diagonalization $M_{k,D}(z) \mapsto U^T M_{k,D}(z)U$ of $M_{k,D}(z)$, for a matrix $U$ depending on $H_D$ but not depending on $z$. Then $M_{k,D}(z)$ is positive semidefinite if and only if each of the blocks is positive semidefinite. There are several equal (or equivalent) blocks and after removing duplicate (or equivalent) blocks we obtain a matrix of order bounded polynomially in $n$, for fixed $q$, where the entries in each block 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.

The reductions of the optimization problem will be described in detail in Section 3. Table 1 contains the new upper bounds. All improvements have been found using multiple precision versions of SDPA [18].

## 2. Preliminaries on representation theory

In this section we give the definitions and notation from representation theory (mostly concerning the symmetric group) used throughout the paper, similarly to the notation used in [16]. Proofs are omitted, but for more information, the reader can consult Sagan [21]. The content of this section is the same as Section 2 of [16,19], so readers who are familiar with one of these papers can safely skip this section.

A *group action* of a group $G$ on a set $X$ is a group homomorphism $\phi : G \to S_X$, where $S_X$ is the group of bijections of $X$ to itself. If $G$ acts on $X$, we write $g \circ x := \phi(g)(x)$ for all $g \in G$ and $x \in X$ and we write $X^G$ for the set of elements of $X$ invariant under the action of $G$. If $X$ is a linear space, the elements of $S_X$ are assumed to be linear functions. The action of $G$ on a set $X$ induces an action of $G$ on the linear space $\mathbb{C}^X$, by $(g \circ f)(x) := f(g^{-1} \circ x)$, for $g \in G, f \in \mathbb{C}^X$ and $x \in X$.

If $m \in \mathbb{N}$ and $G$ is a finite group acting on $V = \mathbb{C}^m$, then $V$ is a *G-module*. 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 $g \circ \psi(v) = \psi(g \circ v)$ for all $g \in G, v \in V$. Moreover, a module $V$ is called *irreducible* if the only $G$-invariant submodules of $V$ are $\{0\}$ and $V$ itself.

Suppose that $G$ is a finite group acting *unitarily* on $V = \mathbb{C}^m$. This means that for each $g \in G$ there is a unitary matrix $U_g \in \mathbb{C}^{m \times m}$ such that $g \circ x = U_g x$ for all $x \in \mathbb{C}^m$. Consider the inner product $\langle x, y \rangle := x^* y$ for $x, y \in \mathbb{C}^m$, where $x^*$ denotes the conjugate transpose of $x \in \mathbb{C}^m$. Then $V$ can be decomposed as a direct sum of *G-isotypical components* $V_1, \ldots, V_k$. This means that $V_i$ and $V_j$ are orthogonal for distinct $i$ and $j$ (with respect to the mentioned inner product), and each $V_i$ is a direct sum $V_{i,1} \oplus \cdots \oplus V_{i,m_i}$ of irreducible and mutually isomorphic $G$-modules, such that $V_{i,j}$ and $V_{i',j'}$ are isomorphic if and only if $i = i'$.

For each $i \leq k$ and $j \leq m_i$ we choose a nonzero vector $u_{i,j} \in V_{i,j}$ with the property 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 $i \leq k$, we define $U_i$ to be the matrix $[u_{i,1}, \ldots, u_{i,m_i}]$ with columns $u_{i,j}$ ($j = 1, \ldots, m_i$). Any set of matrices $\{U_1, \ldots, U_k\}$ obtained in this way is called a *representative* set for the action of $G$ on $\mathbb{C}^m$. Then the map

$$\Phi : (\mathbb{C}^{m \times m})^G \to \bigoplus_{i=1}^k \mathbb{C}^{m_i \times m_i} \quad \text{with} \quad A \mapsto \bigoplus_{i=1}^k U_i^* A U_i \tag{4}$$

is bijective. So $\dim((\mathbb{C}^{m\times m})^G) = \sum_{i=1}^{k} m_i^2$, which can be considerably smaller than $m$. Another crucial property for our purposes is that any $A \in (\mathbb{C}^{m\times m})^G$ is positive semidefinite (i.e., self-adjoint with all eigenvalues nonnegative) if and only if the image $\Phi(A)$ is positive semidefinite, i.e., each of the matrices $U_i^* A U_i$ is positive semidefinite.

It turns out that all representative sets we define consist of real matrices. Then

$$\Phi(A) = \bigoplus_{i=1}^{k} U_i^T A U_i \text{ for } A \in (\mathbb{R}^{m\times m})^G, \quad \text{and } \Phi\left((\mathbb{R}^{m\times m})^G\right) = \bigoplus_{i=1}^{k} \mathbb{R}^{m_i \times m_i}. \tag{5}$$

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

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

$$\mathbb{C}^m = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{m_i} \mathbb{C}G \circ u_{i,j}, \tag{6}$$

where $\mathbb{C}G$ denotes the group algebra of $G$. It will also be convenient to consider the columns of $U_i$ as elements of the dual space $(\mathbb{C}^m)^*$ via the inner product mentioned above.

## 2.1. 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 will consider the natural action of $S_n$ on $V^{\otimes n}$ by permuting the indices. We describe a representative set for the action of $S_n$ on $V^{\otimes n}$ that will be used repeatedly in the reductions throughout this paper.

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

$$Y(\lambda) := \{(i, j) \in \mathbb{N}^2 \mid 1 \leq j \leq h, \ 1 \leq i \leq \lambda_j\}. \tag{7}$$

Fixing an index $j_0 \leq h$, the set of elements $(i, j_0)$ (for $1 \leq i \leq \lambda_j$) 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* $R_\lambda$ of $\lambda$ is the group of permutations $\pi$ of $Y(\lambda)$ with $\pi(Z) = Z$ for each row $Z$ of $Y(\lambda)$. Similarly, the *column stabilizer* $C_\lambda$ of $\lambda$ is the group of permutations $\pi$ of $Y(\lambda)$ with $\pi(Z) = Z$ for each column $Z$ of $Y(\lambda)$.

A *Young tableau* with shape $\lambda$ (also called a $\lambda$-*tableau*) is a function $\tau : Y(\lambda) \to \mathbb{N}$. A Young tableau with shape $\lambda$ 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 $\lambda$-tableaux with entries in $[m]$. Then $T_{\lambda,m} \neq \emptyset$ if and only if $m$ is at least the height of $\lambda$. We write $\tau \sim \tau'$ for $\lambda$-tableaux $\tau, \tau$ 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

$$u_{\tau,B} := \sum_{\tau' \sim \tau} \sum_{c \in C_\lambda} \text{sgn}(c) \bigotimes_{y \in Y(\lambda)} B\left(\tau'(c(y))\right). \tag{8}$$

Here the Young shape $Y(\lambda)$ is ordered by concatenating its rows. Then (cf. [21] and [16]) the set

$$\left\{ [u_{\tau,B} \mid \tau \in T_{\lambda,m}] \mid \lambda \vdash n \right\}, \tag{9}$$

consisting of matrices, is a representative set for the natural action of $S_n$ on $V^{\otimes n}$, for any ordering of the elements in $T_{\lambda,m}$.

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

Let $G$ be any group acting unitarily on $V := \mathbb{C}^m$. Suppose that a representative set for the action of $G$ on $\mathbb{C}^m$ is given. Here each $B_i$ is an $m \times m_i$ matrix, for given integers $k, m_1, \ldots, m_k$.

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 $\lambda_i$ is equal to a partition $(\lambda_{i,1}, \ldots, \lambda_{i,t})$ of $n_i$, for some $t$.)

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

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

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

$$v_{\boldsymbol{\tau}} := \bigotimes_{i=1}^{k} u_{\tau_i, B_i}. \tag{10}$$

Proposition 2 of [16] implies the following. (In Ref. [16], it is stated that $G = S_q$ and $V = \mathbb{R}^{q\times q}$, but with a straightforward adaptation one obtains the following result.)

**Proposition 2.1.** *The matrix set*

$$\{ \ [v_\tau \mid \tau \in W_\lambda] \ \mid \bm{n} \in \bm{N}, \lambda \vdash \bm{n}\} \tag{11}$$

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

Note that the representative set from (11) is real if we start with a real representative set $\{B_1, \ldots, B_k\}$ for the action of $G$ on $V$.

## 3. Reduction of the optimization problem

In this section we give the reduction of optimization problem (3) for computing $B_3^l(q, n, d)$, using the representation theory from the previous section. 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 $1 \times 1$, so it is its own block diagonalization. Hence, in those cases, $M_{3,D}(z)$ is positive semidefinite if and only if $z(D) \geq 0$.

*3.1. 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 $D = \{\bm{0}\}$, where $\bm{0} = 0 \ldots 0$ is the all-zero word. The rows and columns of $M_{3,D}(z)$ are indexed by sets of the form $\{\bm{0}, \alpha\}$ 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 $S_2$ acts on $\mathbb{Z}_q$, 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 $i$th unit vector of $\mathbb{C}^{\mathbb{Z}_q}$.

**Proposition 3.1.** *A representative matrix set for the reflection action of $S_2$ on $\mathbb{C}^{\mathbb{Z}_q}$ is*

$$\{B_1, B_2\}, \quad \text{with} \quad B_1 := \left[e_0, \left(e_i + e_{q-i}\right)_{i=1}^{\lfloor \frac{q}{2} \rfloor}\right], \quad B_2 := \left[\left(e_i - e_{q-i}\right)_{i=1}^{\lfloor \frac{q-1}{2} \rfloor}\right]. \tag{12}$$

**Proof.** For $j = 1, \ldots, \lfloor q/2 \rfloor + 1$, define $W_{1,j}$ to be the 1-dimensional vector space spanned by the $j$th 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 $j$th 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 $\Phi$ in (4) is bijective). So the matrix set (12) is indeed representative for the action of $S_2$ on $\mathbb{C}^{\mathbb{Z}_q}$. $\square$

Note that the representative set is real. Set $m_1 := \lfloor q/2 \rfloor + 1$ and $m_2 := \lfloor (q-1)/2 \rfloor$. Let $\bm{N}$ be the collection of all 2-tuples $(n_1, n_2)$ of nonnegative integers adding up to $n$. As before, for $\bm{n} = (n_1, n_2) \in \bm{N}$, let $\lambda \vdash \bm{n}$ mean that $\lambda = (\lambda_1, \lambda_2)$ with $\lambda_i \vdash n_i$ for $i = 1, 2$. (So each $\lambda_i$ is equal to a partition $(\lambda_{i,1}, \ldots, \lambda_{i,t})$ of $n_i$, for some $t$.)

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

$$W_\lambda := T_{\lambda_1, m_1} \times T_{\lambda_2, m_2}, \tag{13}$$

and for $\tau = (\tau_1, \tau_2) \in W_\lambda$ define

$$v_\tau := u_{\tau_1, B_1} \otimes u_{\tau_2, B_2}. \tag{14}$$

Then Proposition 2.1 implies that

$$\{ \ [v_\tau \mid \tau \in W_\lambda] \ \mid \bm{n} \in \bm{N}, \lambda \vdash \bm{n}\} \tag{15}$$

is representative for the action of $S_2^n \rtimes S_n$ on $(\mathbb{C}^{\mathbb{Z}_q})^{\otimes n} = \mathbb{C}^{\mathbb{Z}_q^n}$. Note that the representative set is real.

### 3.1.1. Computations for $|D| = 1$

Let $D = \{\mathbf{0}\} \in \mathcal{C}_3$ and let $\Omega_3$ 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 $N_\omega$ with entries in $\{0, 1\}$ by

$$(N_\omega)_{\{\mathbf{0},\alpha\},\{\mathbf{0},\beta\}} := \begin{cases} 1 & \text{if } \{\mathbf{0}, \alpha, \beta\} \in \omega, \\ 0 & \text{else.} \end{cases} \tag{16}$$

Given $\mathbf{n} = (n_1, n_2) \in \mathbf{N}$, for each $\lambda \vdash \mathbf{n}$ we write $U_\lambda$ for the matrix in (15) that corresponds with $\lambda$. For each $z : \Omega_3 \to \mathbb{R}$ we obtain with (5) that

$$\Phi(M_{3,D}(z)) = \Phi\left(\sum_{\omega \in \Omega_3} z(\omega)N_\omega\right) = \bigoplus_{\mathbf{n} \in \mathbf{N}} \bigoplus_{\lambda \vdash \mathbf{n}} \sum_{\omega \in \Omega_3} z(\omega)U_\lambda^T N_\omega U_\lambda. \tag{17}$$

The number of $\mathbf{n} \in \mathbf{N}$, $\lambda \vdash \mathbf{n}$, and the numbers $|W_\lambda|$ and $|\Omega_3|$ are all bounded by a polynomial in $n$. This implies that the number of blocks in (17), the size of each block 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 $U_\lambda^T N_\omega U_\lambda$, for all $\omega \in \Omega_3$, $\mathbf{n} \in \mathbf{N}$, $\lambda \vdash \mathbf{n}$, in polynomial time. That is, we show how to compute the coefficients $v_\tau^T N_\omega v_\sigma$, for $\tau, \sigma \in W_\lambda$, in the blocks $\sum_{\omega \in \Omega_3} z(\omega)U_\lambda^T N_\omega U_\lambda$ in polynomial time.

Let $\Pi$ be the set of those words that appear as lexicographically minimal element in a $D_q$-orbit of $\mathbb{Z}_q^3$. So there is a bijection between $\Pi$ and the set of orbits of the action of $D_q$ on $\mathbb{Z}_q^3$. For any word $v \in \mathbb{Z}_q^3$, write $\pi(v)$ for the element in $\Pi$ that is in the same $D_q$-orbit of $\mathbb{Z}_q^3$ as $v$. Note that

$$\Pi = \{00j \mid j = 0, \ldots, \lfloor q/2 \rfloor\} \cup \{0jh \mid j = 1, \ldots, \lfloor q/2 \rfloor, h = 0, \ldots, q-1\}. \tag{18}$$

For any element $P \in \Pi$, define

$$d_P := \sum_{\substack{i,j \in \mathbb{Z}_q: \\ \pi(0ij)=P}} e_i \otimes e_j. \tag{19}$$

Then the set $Z := \{d_P \mid P \in \Pi\}$ forms a basis for $(\mathbb{C}^{\mathbb{Z}_q} \otimes \mathbb{C}^{\mathbb{Z}_q})^{S_2}$, where we consider the reflection action of $S_2$ on $\mathbb{Z}_q$, 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 $i = 1, \ldots, \lfloor \frac{q-1}{2} \rfloor$). We write $Z^*$ for the dual basis.

Let $Q$ denote the set of monomials of degree $n$ on $(\mathbb{C}^{\mathbb{Z}_q} \otimes \mathbb{C}^{\mathbb{Z}_q})^{S_2}$. Then the function $(\mathbb{Z}_q^n)^3 \to \mathcal{C}_3$ that maps an ordered triple $(\alpha, \beta, \gamma)$ to the unordered triple $\{\alpha, \beta, \gamma\}$ induces a surjective function $r : Q \to \Omega_3 \setminus \{\{\emptyset\}\}$. For any $\mu \in Q$, define

$$K_\mu := \sum_{\substack{d_1,\ldots,d_n \in Z \\ d_1^* \cdots d_n^* = \mu}} \bigotimes_{j=1}^n d_j.$$

Then a routine calculation (as in Lemma 1 of [16]) implies that, for each $\omega \in \Omega_3$,

$$N_\omega = \sum_{\substack{\mu \in Q \\ r(\mu)=\omega}} K_\mu.$$

For any $\tau, \sigma \in W_\lambda$, define the following degree $n$ polynomial on $(\mathbb{C}^{\mathbb{Z}_q} \otimes \mathbb{C}^{\mathbb{Z}_q})^{S_2}$:

$$p_{\tau,\sigma} := \prod_{i=1}^2 \sum_{\substack{\tau_i' \sim \tau_i \\ \sigma_i' \sim \sigma_i}} \sum_{c_i,c_i' \in C_{\lambda_i}} \text{sgn}(c_i c_i') \prod_{y \in Y(\lambda_i)} B_i(\tau_i' c_i(y)) \otimes B_i(\sigma_i' c_i'(y)). \tag{20}$$

This polynomial can be computed (i.e., expressed as linear combination of monomials in $B_i(j) \otimes B_i(h)$) in time polynomially bounded in $n$, for fixed $q$ (cf. [10,16]). Then a straightforward calculation, highly similar to the one in Lemma 2 of [16], yields that

$$\sum_{\mu \in Q} (v_\tau^T K_\mu v_\sigma)\mu = p_{\tau,\sigma}. \tag{21}$$

So $\sum_{\mu \in Q} v_\tau^T K_\mu v_\sigma \mu$ can be computed by expressing the polynomial $p_{\tau,\sigma}$ as linear combination of monomials $\mu \in Q$, which are products of linear functions in $Z^*$. In order to express $p_{\tau,\sigma}$ as linear combination of monomials $\mu \in Q$ it remains to express each $B_i(j) \otimes B_i(h)$ as a linear function into the basis $Z^*$, that is, to calculate the numbers $(B_i(j) \otimes B_i(h))(d_P)$ for all $i = 1, 2$ and $j, h = 1, \ldots, m_i$, and $P \in \Pi$. We find

$$B_1(1) \otimes B_1(1) = 1 d_{000}^*,$$
$$B_1(1) \otimes B_1(j+1) = 2 d_{00j}^*, \text{ for } j = 1, \ldots, \lfloor q/2 \rfloor$$

$$B_1(j+1) \otimes B_1(1) = 2d^*_{0j0}, \quad \text{for } j = 1, \ldots, \lfloor q/2 \rfloor$$
$$B_1(j+1) \otimes B_1(h+1) = 2d^*_{0jh} + 2d^*_{0j(q-h)}, \quad \text{for } j, h \in \{1, \ldots, \lfloor q/2 \rfloor\},$$
$$B_2(j) \otimes B_2(h) = 2d^*_{0jh} - 2d^*_{0j(q-h)}, \quad \text{for } j, h \in \{1, \ldots, \lfloor (q-1)/2 \rfloor\}, \tag{22}$$

where the coefficient of $d^*_P$ is obtained by evaluating $(B_i(j) \otimes B_i(h))(d_P)$. Now one computes the entry $\sum_{\omega \in \Omega_3} z(\omega) v^T_\tau N_\omega v_\sigma$ by first expressing $p_{\tau,\sigma}$ as a linear combination of $\mu \in Q$ and subsequently replacing each $\mu \in Q$ in $\tilde{p}_{\tau,\sigma}$ with the variable $z(r(\mu))$.

### 3.2. The case $D = \emptyset$

Let $D = \emptyset$. The rows and columns of $M_{3,\emptyset}(z) = M_{2,\emptyset}(z)$ 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 $D_q$ acts on $\mathbb{C}^{\mathbb{Z}_q}$ by permuting the vertices $0, \ldots, q-1$ of a regular $q$-gon. To compute the block diagonalization of $M_{2,\emptyset}(z)$, one can use the Delsarte formulas in the Lee scheme [1,2]. Here we give the reduction in terms of representative sets.

Let $\zeta = e^{2\pi i/q}$ be a primitive $q$th root of unity. For each $j = 0, \ldots, \lfloor q/2 \rfloor$, define the vectors $a_j := (1, \zeta^j, \zeta^{2j}, \ldots, \zeta^{(q-1)j})^T$, $b_j := (1, \zeta^{-j}, \zeta^{-2j}, \ldots, \zeta^{-(q-1)j})^T \in \mathbb{C}^{\mathbb{Z}_q}$ and set $V_j := \text{span}\{a_j, b_j\}$. Furthermore, put

$$c_j := \frac{\sqrt{\dim V_j}}{2}(a_j + b_j) = \sqrt{\dim V_j}(1, \cos(2j\pi/q), \ldots, \cos(2(q-1)j\pi/q))^T \in \mathbb{R}^{\mathbb{Z}_q} \subseteq \mathbb{C}^{\mathbb{Z}_q}.$$

**Proposition 3.2.** *A representative set for the action of $D_q$ on $\mathbb{C}^{\mathbb{Z}_q}$ is given by*

$$\left\{ C_1, \ldots, C_{\lfloor \frac{q}{2} \rfloor + 1} \right\}, \quad \text{where } C_j := c_{j-1}, \text{ for } j = 1, \ldots, \lfloor \frac{q}{2} \rfloor + 1. \tag{23}$$

**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 if $l \neq j$ (with respect to the inner product $u, v \mapsto u^*v$). To see this, note that $x := \zeta^{\pm j \pm l}$ is a $q$th root of unity unequal to 1 if $j \neq l \in \{0, \ldots, \lfloor q/2 \rfloor\}$, so $1 + x + x^2 + \cdots + x^{q-1} = 0$. 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 $(\mathbb{C}^{\mathbb{Z}_q \times \mathbb{Z}_q})^{D_q}$. 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 $\Phi$ in (4) is bijective). As $C_{j+1}$ is an element of $V_j$ for $j = 0, \ldots, \lfloor q/2 \rfloor$, this implies that $\left\{ C_1, \ldots, C_{\lfloor \frac{q}{2} \rfloor + 1} \right\}$ is a representative matrix set. $\square$

Note that the representative set is real, and that each $C_i$ is a $q \times 1$-matrix. For simplicity of notation, set $s := \lfloor \frac{q}{2} \rfloor + 1$. Let $M$ be the collection of all $s$-tuples $(n_1, \ldots, n_s)$ of nonnegative integers adding up to $n$. For $\boldsymbol{n} \in M$, define $v_{\boldsymbol{n}} := C_1^{\otimes n_1} \otimes C_2^{\otimes n_2} \otimes \cdots \otimes C_s^{\otimes n_s}$. Section 2.2 gives the following.

**Proposition 3.3.** *The set*

$$\{ v_{\boldsymbol{n}} \mid \boldsymbol{n} \in M \} \tag{24}$$

*is representative for the action of $D_q^n \rtimes S_n$ on $(\mathbb{C}^{\mathbb{Z}_q})^{\otimes n} = \mathbb{C}^{\mathbb{Z}_q^n} = \mathbb{C}^{\mathcal{C}_3(\emptyset) \setminus \{\emptyset\}}$.*

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 $\epsilon_\emptyset$ to this matrix (as a column) in order to obtain a representative set for the action of $D_q^n \rtimes S_n$ on $\mathbb{C}^{\mathbb{Z}_q^n \cup \{\emptyset\}} = \mathbb{C}^{\mathcal{C}_3(\emptyset)}$.

#### 3.2.1. 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 $N'_\omega$ with entries in $\{0, 1\}$ by

$$(N'_\omega)_{\alpha,\beta} := \begin{cases} 1 & \text{if } \{\alpha, \beta\} \in \omega, \\ 0 & \text{else.} \end{cases} \tag{25}$$

For each $z : \Omega_2 \to \mathbb{R}$ we obtain with Eqs. (24) and (5) that $\Phi\left(\sum_{\omega \in \Omega_2} z(\omega)N'_\omega\right) = \bigoplus_{\boldsymbol{n} \in M} \sum_{\omega \in \Omega_2} z(\omega)v^T_{\boldsymbol{n}} N'_\omega v_{\boldsymbol{n}}$. This shows that $\Phi\left(\sum_{\omega \in \Omega_2} z(\omega)N'_\omega\right)$ is a diagonal matrix. Note that $|\Omega_2|$ and $|M|$ are polynomially bounded in $n$. Now we show how to compute $v^T_{\boldsymbol{n}} N'_\omega v_{\boldsymbol{n}}$, for $\boldsymbol{n} \in M$ in polynomial time.

Define $\Pi' = \{00j \mid j = 0, \ldots, \lfloor q/2 \rfloor\} \subseteq \Pi$. For any element $P \in \Pi'$, define

$$f_P := \sum_{\substack{i,j \in \mathbb{Z}_q: \\ \pi(iij)=P}} e_i \otimes e_j \tag{26}$$

Then the set $\tilde{Z} := \{f_P \mid P \in \Pi'\}$ forms a basis for $(\mathbb{C}^{\mathbb{Z}_q} \otimes \mathbb{C}^{\mathbb{Z}_q})^{D_q}$. Let $\tilde{Z}^*$ denote the dual basis. Let $Q'$ denote the set of monomials of degree $n$ on $(\mathbb{C}^{\mathbb{Z}_q} \otimes \mathbb{C}^{\mathbb{Z}_q})^{D_q}$. The function $(\mathbb{Z}_q^n)^2 \to \mathcal{C}_2$ that maps $(\alpha, \beta)$ to $\{\alpha, \beta\}$ induces a surjective function $r' : Q' \to \Omega_2 \setminus \{\{\emptyset\}\}$. For any $\boldsymbol{n} \in \boldsymbol{M}$, define the following degree $n$ polynomial on $(\mathbb{C}^{\mathbb{Z}_q} \otimes \mathbb{C}^{\mathbb{Z}_q})^{D_q}$:

$$p_{\boldsymbol{n}} := \prod_{i=1}^{s} (C_i \otimes C_i)^{n_i}. \tag{27}$$

For any $\mu \in Q'$, define

$$K'_\mu := \sum_{\substack{f_1,\ldots,f_n \in Z \\ f_1^* \cdots f_n^* = \mu}} \bigotimes_{j=1}^{n} f_j, \quad \text{so that (cf. Lemma 2 of [16])} \sum_{\mu \in Q'} v_{\boldsymbol{n}}^T K'_\mu v_{\boldsymbol{n}} \mu = p_{\boldsymbol{n}}.$$

So $\sum_{\mu \in Q'} v_{\boldsymbol{n}}^T K'_\mu v_{\boldsymbol{n}} \mu$ can be computed by expressing the polynomial $p_{\boldsymbol{n}}$ as linear combination of monomials $\mu \in Q'$, which are products of linear functions in $\tilde{Z}^*$. To this end, we express each $C_i \otimes C_i$ as linear function into the basis $\tilde{Z}^*$, i.e., we calculate the numbers $(C_i \otimes C_i)(f_P)$ for all $i = 1, \ldots, s$ and $P \in \Pi'$. We find

$$\text{for } q \text{ even: } C_i \otimes C_i = q \left( f_{000}^* + (-1)^i f_{00(q/2)}^* + 2 \sum_{j=1}^{q/2-1} \cos(2\pi ji/q) f_{00j}^* \right), \quad \text{for } i \in \{0, \ldots, q/2\},$$

$$\text{for } q \text{ odd: } C_i \otimes C_i = q \left( f_{000}^* + 2 \sum_{j=1}^{(q-1)/2} \cos(2\pi ji/q) f_{00j}^* \right), \quad \text{for } i \in \{0, \ldots, (q-1)/2\}. \tag{28}$$

Now, as $N'_\omega = \sum_{\substack{\mu \in Q' \\ r'(\mu)=\omega}} K'_\mu$ (for each $\omega \in \Omega_2$), one computes the entry $\sum_{\omega \in \Omega_2} z(\omega) v_{\boldsymbol{n}}^T N'_\omega v_{\boldsymbol{n}}$ by first expressing $p_{\boldsymbol{n}}$ as a linear combination of $\mu \in Q'$ and subsequently replacing each $\mu \in Q'$ in $p_{\boldsymbol{n}}$ with the variable $z(r'(\mu))$.

To add the empty code, we add an extra row and column corresponding to the vector $\epsilon_\emptyset$ to the matrix in the representative set indexed by $\boldsymbol{n} = (n, 0, \ldots, 0)$, as explained below Proposition (24). So the only matrix block affected by the empty code in the block diagonalization of $M_{2,\emptyset}(z)$ is

$$T := [\epsilon_\emptyset, v_{\boldsymbol{n}}]^T M_{2,\emptyset}(z)[\epsilon_\emptyset, v_{\boldsymbol{n}}], \tag{29}$$

which is a $2 \times 2$-matrix. Then $\epsilon_\emptyset^T M_{2,\emptyset}(z) \epsilon_\emptyset = M_{2,\emptyset}(z)_{\emptyset,\emptyset} = x(\emptyset) = 1$ by definition, see (3). Since $v_{\boldsymbol{n}} = C_1^{\otimes n}$ is the all-ones vector, we have $\epsilon_\emptyset^T M_\emptyset(z) v_{\boldsymbol{n}} = q^n z_{\omega_0}$, where $\omega_0 \in \Omega_2$ is the (unique) $D_q^n \rtimes S_n$-orbit of a code of size 1.

## 4. The strong product power of circular graphs

For any graph $G = (V, E)$, let $G^n$ 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 $u_i v_i \in E$. The *Shannon capacity* of $G$ is defined as

$$\Theta(G) := \sup_{d \in \mathbb{N}} \sqrt[d]{\alpha(G^d)}, \tag{30}$$

where $\alpha(G^d)$ denotes the maximum cardinality of an independent set in $G^d$, i.e., a set of vertices no two of which are adjacent [24].

For two integers $d, q$ 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 $C_{2,q} = C_q$, the circuit on $q$ vertices. A classical upper bound on $\alpha(C_{d,q}^n)$ is given by Lovász's $\vartheta$-function (see [17]): one has

$$\alpha(C_{d,q}^n) \leq \vartheta(C_{d,q}^n) = \vartheta(C_{d,q})^n. \tag{31}$$

Hence, Lovász's $\vartheta$-function gives an upper bound on the Shannon capacity of $C_{d,q}$. A closed formula for $\vartheta(C_{d,q})$ is given in [5]. We describe how the bound $B_3^l(q, n, d)$ can be adapted to an upper bound $B_3^{L_\infty}(q, n, d)$ on $\alpha(C_{d,q}^n)$, which either improves or is equal to the bound obtained from Lovász's $\vartheta$-function. However, the new bound is not multiplicative over the strong product, so it does not give an upper bound on $\Theta(C_{d,q})$.

For distinct $u, v$ in $\mathbb{Z}_q^n$, define their *Lee$_\infty$-distance* $d_{L_\infty}(u, v)$ to be the maximum over the distances of $u_i$ and $v_i$ (mod $q$), where $i$ ranges from 1 to $n$. The *minimum Lee$_\infty$-distance* $d_{\min}^{L_\infty}(D)$ of a set $D \subseteq \mathbb{Z}_q^n$ is the minimum Lee$_\infty$-distance between

**Table 2**
Bounds on $\alpha(C_5^n)$, $\alpha(C_7^n)$ and $\alpha(C_{3,7}^n)$, rounded to three decimal places. It holds that $B_2^{L\infty}(5,n,2) = \sqrt{5}^n$.

|  | 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 |

any pair of distinct elements of $D$. (If $|D| \le 1$, set $d_{\min}^{L\infty}(D) = \infty$.) Then $d_{\min}^{L\infty}(D) \ge d$ if and only if $D$ is independent in $C_{d,q}^n$. Define, for $k \ge 2$,

$$B_k^{L\infty}(q,n,d) := \max\{\sum_{v \in \mathbb{Z}_q^n} x(\{v\}) \mid x : \mathcal{C}_k \to \mathbb{R}, \ x(\emptyset) = 1, \ x(S) = 0 \text{ if } d_{\min}^{L\infty}(S) < d,$$

$$M_{k,D}(x) \text{ is positive semidefinite for each } D \text{ in } \mathcal{C}_k\}. \tag{32}$$

So $B_k^{L\infty}(q,n,d)$ is obtained from the bound $B_k^L(q,n,d)$ in (3) by replacing in the definition $d_{\min}^L(S)$ by $d_{\min}^{L\infty}(S)$. It is not hard to see that $\alpha(C_{d,q}^n) \le B_k^{L\infty}(q,n,d)$, by a proof analogous to that of Proposition 1.1. For comparison, $\vartheta(C_{d,q}^n)$ 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 $\vartheta'(C_{d,q}^n)$, with $\vartheta'$ as in [22].

To compute $B_3^{L\infty}(q,n,d)$, the reductions from Section 3 can be used. The new bound $B_3^{L\infty}(q,n,d)$ does not seem to improve significantly over the bound obtained from Lovász's $\vartheta$-function, except for very small $n$. See Table 2 for some results for $q \in \{5,7\}$ and $1 \le n \le 5$. For these cases, $B_3^{L\infty}(q,n,d)$ does not give new upper bounds on $\alpha(C_{d,q}^n)$, as the values $\alpha(C_5^2) = 10$, $\alpha(C_7^2) = 10$, $\alpha(C_7^3) = 33$ (cf. [6]), $\alpha(C_{3,7}^3) = 8$ (cf. [13]) are already known and $\alpha(C_7^4) \le \lfloor (7/2)\alpha(C_7^3) \rfloor = 115$. 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 $\le 3$ and minimum Lee$_\infty$-distance at least $d$, is also given in Table 2 for the considered cases.

## Acknowledgments

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Appendix A. Formulas with integers

Note that for $q \le 4$ or $q = 6$ all coefficients the formulas in Section 3.2.1 for the block diagonalization of $M_{3,\emptyset}(z)$ are rational (hence all constraints can be made integer). For other $q$ the formulas contain irrational numbers. To obtain a semidefinite program which only contains integers we used in the implementation for $q = 5$ and $q = 7$ not the representative set from (24) for the action of $D_q^n \rtimes S_n$ on $\mathbb{C}^{\mathbb{Z}_q^n}$ but the representative set from (15) for the action of $S_2^n \rtimes S_n$ on $\mathbb{C}^{\mathbb{Z}_q^n}$ to reduce the matrix $\sum_{\omega \in \Omega_2} z(\omega) N'_\omega$. Then (5) gives (where we write $\Psi$ for the map in (5) to distinguish it from the map $\Phi$ from Section 3.2.1)

$$\Psi\left(\sum_{\omega \in \Omega_2} z(\omega) N'_\omega\right) = \bigoplus_{n \in N} \bigoplus_{\lambda \vdash n} \sum_{\omega \in \Omega_2} z(\omega) U_\lambda^T N'_\omega U_\lambda, \tag{33}$$

where $U_\lambda$ denotes the matrix in (15) that corresponds with $\lambda \in W_\lambda$. By (21), we have $\sum_{\mu \in Q} v_\tau^T K_\mu v_\sigma \mu = p_{\tau,\sigma}$. From this, one obtains that $\sum_{\mu \in Q'} v_\tau^T K'_\mu v_\sigma \mu = p'_{\tau,\sigma}$, where $p'_{\tau,\sigma}$ is the polynomial obtained from $p_{\tau,\sigma}$ by replacing each

```
Input:   Natural numbers q, n
Output:  Semidefinite program to compute B₃ᴸ(q, n, 1) (= B₃ᴸ∞(q, n, 1)).

print Maximize qⁿz(ω₀)
print Subject to:
//Start with |D| = 1.
foreach n = (n₁, n₂) ∈ N
    foreach λ = (λ₁, λ₂) ⊢ n with height(λ₁) ≤ ⌊q/2⌋ + 1, height(λ₂) ≤ ⌊(q−1)/2⌋
        start a new block Mλ
        foreach τ ∈ Wλ from (13)
            foreach σ ∈ Wλ from (13)
                compute pτ,σ from (20) as linear combination in Bᵢ(j) ⊗ Bᵢ(h)
                replace each Bᵢ(j) ⊗ Bᵢ(h) by the linear expression in d*ₚ from (22)
                replace each degree n monomial μ in d*ₚ by a variable z(r(μ))
                (Mλ)τ,σ := the resulting linear polynomial in variables z(ω)
            end
        end
        print Mλ positive semidefinite.
    end
end
//Now D = ∅.
foreach n ∈ M
    start a new (1 × 1)-block Mₙ
    compute pₙ from (27) as linear combination in Cᵢ ⊗ Cᵢ
    replace each Cᵢ ⊗ Cᵢ by the linear expression in f*ₚ from (28)
    replace each degree n monomial μ in f*ₚ by a variable z(r'(μ))
    (Mₙ) := (the resulting linear polynomial in variables z(ω))
    if n = (n, 0, ..., 0)    //add a row and a column corresponding to ∅.
        add a row and column to Mₙ indexed by ∅
        put (Mₙ)∅,∅ := 1 and (Mₙ)ₙ,∅ = (Mₙ)∅,ₙ := qⁿz_ω₀
    end
    print Mₙ positive semidefinite.
end
//Now nonnegativity of all variables.
foreach ω ∈ Ω₃
    print z(ω) ≥ 0
end
```

**Fig. 1.** Algorithm to generate a semidefinite program for computing $B_3^L(q, n, 1)$. To compute $B_3^L(q, n, d)$ or $B_3^{L\infty}(q, n, d)$, 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 in matrix blocks $M_\lambda$ consist only of zeros after the replacement, it is useful to remove these rows and columns.

variable $d_{0ij}^* \in Z^*$ (with $0ij \in \Pi$) by the variable $f_{\pi(iij)}^* \in \widetilde{Z}^*$. Hence the following replacements must be done, using the formulas from (22):

$$
\begin{aligned}
B_1(1) \otimes B_1(1) = 1d_{000}^* &\mapsto 1f_{000}^*, \\
B_1(1) \otimes B_1(j+1) = 2d_{00j}^* &\mapsto 2f_{00j}^*, \text{ for } j = 1, \ldots, \lfloor q/2 \rfloor \\
B_1(j+1) \otimes B_1(1) = 2d_{0j0}^* &\mapsto 2f_{00j}^*, \text{ for } j = 1, \ldots, \lfloor q/2 \rfloor \\
B_1(j+1) \otimes B_1(h+1) = 2d_{0jh}^* + 2d_{0j(q-h)}^* &\mapsto 2f_{00t_1}^* + 2f_{00t_2}^*, \text{ for } j, h \in \{1, \ldots, \lfloor q/2 \rfloor\}, \\
B_2(j) \otimes B_2(h) = 2d_{0jh}^* - 2d_{0j(q-h)}^* &\mapsto 2f_{00t_1}^* - 2f_{00t_2}^*, \text{ for } j, h \in \{1, \ldots, \lfloor (q-1)/2 \rfloor\},
\end{aligned}
\tag{34}
$$

where in the above formulas we set $t_1 := j - h$ if $j \geq h$ and $t_1 := h - j$ else, and we set $t_2 := j + h$ if $j + h \leq \lfloor q/2 \rfloor$ and $t_2 := q - (j + h)$ else.

So one computes the entry $\sum_{\omega \in \Omega_2} z(\omega) v_\tau^T N_\omega' v_\sigma$ in the block $\sum_{\omega \in \Omega_2} z(\omega) U_\lambda^T N_\omega' U_\lambda$ by first expressing $p_{\tau,\sigma}'$ as a linear combination of $\mu \in Q'$ and subsequently replacing each $\mu \in Q'$ in $p_{\tau,\sigma}'$ with the variable $z(r'(\mu))$.

To add the empty code, one may add a new unit base vector $\epsilon_\emptyset$ to the matrix in the representative set (15) indexed by $n = ((n), ())$ and calculate the new entries $\epsilon_\emptyset^T M_{2,\emptyset}(z) v_\sigma$, for each $\sigma \in W_\lambda$. However, this is not necessary. As $\Psi\left(\sum_{\omega \in \Omega_2} z(\omega) N_\omega'\right)$ is positive semidefinite if and only if $\Phi\left(\sum_{\omega \in \Omega_2} z(\omega) N_\omega'\right)$ is positive semidefinite, and $M_{2,\emptyset}(z)$ is

positive semidefinite if and only if both $\Phi\left(\sum_{\omega\in\Omega_2} z(\omega)N'_\omega\right)$ and $T$ from (29) are positive semidefinite, we find that

$$M_{2,\emptyset}(z) \text{ is positive semidefinite} \iff \Psi\left(\sum_{\omega\in\Omega_2} z(\omega)N'_\omega\right) \text{ and } T \text{ are positive semidefinite.}$$

So the $2 \times 2$ matrix $T$ together with the matrix blocks in (33) form a block diagonalization of $M_{2,\emptyset}(z)$.

## Appendix B. 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 Fig. 1 for an outline of the method.

A few remarks regarding the implementation:

  (i) We write $\omega_0$ for the unique $D_q^n \rtimes S_n$-orbit corresponding to a code of size 1.
 (ii) To speed up the replacement of monomials in $d_P^*$ or $f_P^*$ by variables $z(\omega)$, it is useful to add a preprocessing step to determine in advance for each degree $n$ monomial $\mu = d_{P_1}^* \ldots d_{P_n}^*$ with all $P_i \in \Pi$ and $\mu' = f_{P_1}^* \ldots f_{P_n}^*$ with all $P_i \in \Pi'$ which orbit $r(\mu) \in \Omega_3$ or $r'(\mu') \in \Omega_2$ corresponds with it. If the orbit corresponds to a code of minimum Lee (or Lee$_\infty$) distance $< d$ to zero, we must set the corresponding variable to zero and can delete it from the program.
(iii) In case $D = \emptyset$, the matrix blocks contain irrational numbers for $q \notin \{2, 3, 4, 6\}$. In Appendix A it is explained how to obtain a semidefinite program which only contains integers. This is not displayed in the above pseudocode, but the adaptations are straightforward.
 In order to obtain the matrix blocks from (33) for $D = \emptyset$ one can simply repeat the steps in the above pseudocode for $|D| = 1$, but with the following adaptation: replace each $B_i(j) \otimes B_i(h)$ by the linear expression in $f_P^*$ from (34), and subsequently replace each monomial $\mu$ of degree $n$ in $f_P^*$ by a variable $z(r'(\mu))$.
 (iv) The programs we used to generate input for the SDP-solver can be found at the following location (also accessible via the author's website):
 https://drive.google.com/open?id=1-XRbfc4TYhoySC33GRWfvNEMOZEltg6X.

## References

[1] J. Astola, The Lee-scheme and bounds for Lee-codes, Cybernet. Systems Anal. 13 (1982) 331–343.
 [2] H. Astola, I. Tabus, Bounds on the size of Lee-codes, in: 8th International Symposium on Image and Signal Processing and Analysis, ISPA 2013, Trieste (Italy), 2013, pp. 471–476.
 [3] H. Astola, I. Tabus, Sharpening the linear programming bound for linear Lee-codes, Electron. Lett. 51 (6) (2015) 492–494.
 [4] C. Bachoc, D.C. Gijswijt, A. Schrijver, F. Vallentin, Invariant semidefinite programs, in: M.F. Anjos, J.B. Lasserre (Eds.), Handbook of Semidefinite, Conic and Polynomial Optimization: Theory, Algorithms, Software and Applications, Springer, 2011, pp. 219–269, Chapter 9.
 [5] C. Bachoc, A. Pêcher, A. Thiéry, On the theta number of powers of cycle graphs, Combinatorica 33 (2013) 297–317.
 [6] L. Baumert, R. McEliece, E. Rodemich, H. Rumsey, R. Stanley, H. Taylor, A combinatorial packing problem, in: Computers in Algebra and Number Theory, American Mathematical Society, Providence, RI, 1971, pp. 97–108.
 [7] E.R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.
 [8] 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 Trans. Inform. Theory 40 (1994) 301–319.
 [9] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Repts. Suppl. (10) (1973).
[10] D.C. Gijswijt, Block diagonalization for algebras associated with block codes, 2009, arXiv:0910.4515.
[11] D.C. Gijswijt, H.D. Mittelmann, A. Schrijver, Semidefinite code bounds based on quadruple distances, IEEE Trans. Inform. Theory 58 (5) (2012) 2697–2705.
[12] D.C. Gijswijt, A. Schrijver, H. Tanaka, New upper bounds for nonbinary codes based on the Terwilliger algebra and semidefinite programming, J. Combin. Theory Ser. A 113 (2006) 1719–1731.
[13] M. Jurkiewicz, M. Kubale, K. Turowski, Some lower bounds on the Shannon capacity, J. Appl. Comput. Sci. 22 (2014) 31–42.
[14] C.Y. Lee, Some properties of nonbinary error-correcting codes, IRE Trans. Inform. Theory 4 (1958) 77–82.
[15] B.M. Litjens, Semidefinite bounds for mixed binary/ternary codes, Discrete Math. 341 (6) (2018) 1740–1748.
[16] B.M. Litjens, S.C. Polak, A. Schrijver, Semidefinite bounds for nonbinary codes based on quadruples, Des. Codes Cryptogr. 84 (1) (2017) 87–100.
[17] L. Lovász, On the Shannon capacity of a graph, IEEE Trans. Inform. Theory 25 (1973) 1–7.
[18] M. Nakata, A numerical evaluation of highly accurate multiple-precision arithmetic version of semidefinite programming solver: SDPA-GMP, -QD and -DD, in: The proceedings of 2010 IEEE Multi-Conference on Systems and Control, 2010, pp. 29–34.
[19] S.C. Polak, Semidefinite programming bounds for constant weight codes, IEEE Trans. Inform. Theory 65 (2019) 28–38.
[20] J. Quistorff, New upper bounds on lee codes, Discrete Appl. Math. 154 (2006) 1510–1521.
[21] B.E. Sagan, The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions, in: Graduate Texts in Mathematics, vol. 203, Springer, New York, 2001.
[22] A. Schrijver, A comparison of the Delsarte and Lovász bounds, IEEE Trans. Inform. Theory 25 (4) (1979) 425–429.
[23] A. Schrijver, New code upper bounds from the Terwilliger algebra and semidefinite programming, IEEE Trans. Inform. Theory 51 (2005) 2859–2866.
[24] C.E. Shannon, The zero-error capacity of a noisy channel, IRE Trans. Inform. Theory 2 (1956) 8–19.