STRENGTHENED SEMIDEFINITE BOUNDS FOR CODES

MONIQUE LAURENT

Abstract. We give a hierarchy of semidefinite upper bounds for the maximum size $A(n, d)$ of a binary code of word length n and minimum distance at least d. At any fixed stage in the hierarchy, the bound can be computed (to an arbitrary precision) in time polynomial in n; this is based on a result of Schrijver [12] about the regular $*$-representation for matrix $*$-algebras. The Delsarte bound for $A(n, d)$ is the first bound in the hierarchy, and the new bound of Schrijver [11] is located between the first and second bounds in the hierarchy. While computing the second bound involves a semidefinite program with $O(n^7)$ variables and thus seems out of reach for interesting values of n, Schrijver's bound can be computed via a semidefinite program of size $O(n^3)$, a result which uses the explicit block-diagonalization of the Terwiliger algebra. We propose two strengthenings of Schrijver's bound with the same computational complexity.

1. Introduction

We consider the problem of computing the parameter $A(n, d)$, defined as the maximum size of a binary code of word length n and minimum distance at least d. With $\mathcal{P}$ denoting the collection of all subsets of $\{1, \ldots, n\}$, we can identify code words in $\{0, 1\}^n$ with their supports; so a code C is a subset of $\mathcal{P}$ and the Hamming distance of $I, J \in \mathcal{P}$ is equal to $|I\Delta J|$. The minimum distance of a code C is the minimum Hamming distance of distinct elements of C. If we define the graph $\mathcal{G}(n, d)$ with node set $\mathcal{P}$, two nodes $I, J \in \mathcal{P}$ being adjacent if $|I\Delta J| \in \{1, \ldots, d-1\}$, then a code with minimum distance d corresponds to a stable set in the graph $\mathcal{G}(n, d)$. Therefore, the parameter $A(n, d)$ is equal to the stability number of the graph $\mathcal{G}(n, d)$, i.e., the maximum cardinality of a stable set in $\mathcal{G}(n, d)$.

Schrijver [11] introduced recently an upper bound for $A(n, d)$ which refines the classical bound of Delsarte [1]. While Delsarte bound is based on diagonalizing the (commutative) Bose-Mesner algebra of the Hamming scheme and can be computed via linear programming, Schrijver's bound is based on block-diagonalizing the (non-commutative) Terwiliger algebra of the Hamming scheme and can be computed via semidefinite programming. In both cases the bounds can be formulated as the optimum of a (linear or semidefinite) program of size polynomial in n (size $O(n)$ for Delsarte bound and size $O(n^3)$ for Schrijver's bound).

Finding tight upper bounds for the stability number $\alpha(\mathcal{G})$ of a graph $\mathcal{G} = (V, E)$ has been the subject of extensive research. Lovász [7] introduced the theta number $\vartheta(\mathcal{G})$,

---

Date: January 24, 2005.
1991 *Mathematics Subject Classification.* Primary 90C27, 90C22, 05E20, 94B65.
Key words and phrases. stability number, binary code, semidefinite bound, Terwiliger algebra.
Supported by the Netherlands Organisation for Scientific Research grant NWO 639.032.203.

which can be computed via the semidefinite program:

$$\vartheta(\mathcal{G}) := \max \sum_{i\in V} X_{ii} \quad \text{s.t.} \quad \begin{array}{l} X = (X_{ij})_{i,j\in V\cup\{0\}} \succeq 0,\ X_{00} = 1, \\ X_{0i} = X_{ii}\ (i \in V),\ X_{ij} = 0\ (ij \in E). \end{array} \tag{1}$$

The theta number can be computed (with arbitrary precision) in time polynomial in the number of nodes of the graph. Moreover, $\vartheta(\mathcal{G}) = \alpha(\mathcal{G})$ when $\mathcal{G}$ is a perfect graph (see [3]). Schrijver [10] introduced the strenghtening $\vartheta'(\mathcal{G})$ of $\vartheta(\mathcal{G})$ obtained by adding the nonnegativity constraint $X \geq 0$ to the program (1) and proved that $\vartheta'(\mathcal{G}(n,d))$ coincides with Delsarte bound.

Various methods have been proposed in the litterature for constructing tighter semidefinite upper bounds for the stability number of a graph, in particular, by Lovász and Schrijver [8] and more recently by Lasserre [4, 5]. In both cases a hierarchy of upper bounds for $\alpha(\mathcal{G})$ is obtained with the property that the bound reached at the $\alpha(\mathcal{G})$-th iteration coincides in fact with $\alpha(\mathcal{G})$. It turns out that Lasserre's hierarchy refines the hierarchy of Lovász and Schrijver (see [6]).

For $k \geq 1$, denote by $\ell^{(k)}(\mathcal{G})$ the bound in Lasserre's hierarchy at the k-th iteration; see Section 3.1 for the precise definition. It is known that, for *fixed* k, one can compute (with arbitrary precision) the parameter $\ell^{(k)}(\mathcal{G})$ in time polynomial in the number of nodes of the graph $\mathcal{G}$. However, for the coding problem, the graph $\mathcal{G}(n,d)$ has 2^n nodes and such complexity is prohibitive for large n. A first contribution of this paper (see Section 3.2) is to show that, for fixed k, the bound $\ell^{(k)}(\mathcal{G}(n,d))$ can be computed (with arbitrary precision) in time polynomial in n. This result is based on a result of Schrijver [12], recalled in Section 2.1, about reducing the size of invariant semidefinite programs using the regular $*$-representation for the algebra of invariant matrices under action of a group.

The first bound $\ell^{(1)}(\mathcal{G})$ in the hierarchy is equal to the theta number $\vartheta(\mathcal{G})$; its strengthening obtained by adding nonnegativity is equal to $\vartheta'(\mathcal{G})$ which, for the graph $\mathcal{G} = \mathcal{G}(n,d)$, coincides with the bound of Delsarte for the parameter $A(n,d)$. It turns out that the bound of Schrijver [11] for $A(n,d)$ lies between $\ell^{(1)}_+(\mathcal{G})$ and $\ell^{(2)}_+(\mathcal{G})$, the strengthenings of $\ell^{(1)}(\mathcal{G})$ and $\ell^{(2)}(\mathcal{G})$ obtained by adding certain bounds on the variables. While Schrijver's bound can be computed via a semidefinite program of size $O(n^3)$ and thus computed in practice for reasonable values of n, a practical computation of $\ell^{(2)}_+(\mathcal{G}(n,d))$ seems out of reach for interesting values of n since one would have to solve a semidefinite program with $O(n^7)$ variables.

In Section 3.3, we introduce two bounds $\ell_+(\mathcal{G}(n,d))$ and $\tilde{\ell}(\mathcal{G}(n,d))$ satisfying

$$\ell^{(2)}_+(\mathcal{G}(n,d)) \leq \tilde{\ell}(\mathcal{G}(n,d)) \leq \ell_+(\mathcal{G}(n,d)) \leq \ell^{(1)}_+(\mathcal{G}(n,d));$$

they are at least as good as Schrijver's bound, and their computation still relies on solving a semidefinite program of size $O(n^3)$. This complexity result follows from the fact that the new bounds, analogously to Schrijver's bound, require the positive semidefiniteness of certain matrices lying in the Terwiliger algebra (or a variation of it) whose dimension is $O(n^3)$ and for which the explicit block-diagonalization has been given by Schrijver [11].

2. Algebraic preliminaries

2.1. Preliminaries on invariant matrices. Let G be a finite group acting on a finite set $\mathcal{X}$; that is, we have a homomorphism $h : G \to Sym(\mathcal{X})$, where $Sym(\mathcal{X})$ is the group of permutations of $\mathcal{X}$. For $\sigma \in G$, $h(\sigma)$ is a permutation of $\mathcal{X}$ and M_σ is the associated $\mathcal{X} \times \mathcal{X}$ permutation matrix with

$$(M_\sigma)_{x,y} = \begin{cases} 1 & \text{if } h(\sigma)(x) = y, \\ 0 & \text{otherwise.} \end{cases}$$

The set:

$$\mathcal{A} := \{\sum_{\sigma \in G} \lambda_\sigma M_\sigma \mid \lambda_\sigma \in \mathbb{R}\ (\sigma \in G)\}$$

is a *matrix $*$-algebra*; that is, $\mathcal{A}$ is closed under addition, scalar and matrix multiplication, and conjugation. Its *commutant*:

$$\mathcal{A}^G := \{N \in \mathbb{C}^{\mathcal{X} \times \mathcal{X}} \mid NM = MN\ \forall M \in \mathcal{A}\}$$

is again a matrix $*$-algebra. The commutant algebra $\mathcal{A}^G$ consists precisely of the $\mathcal{X} \times \mathcal{X}$ matrices N that are *invariant under the action of* G, i.e., satisfy $\sigma(N) = N$ for all $\sigma \in G$, where

$$\sigma(N) := (N_{\sigma(x),\sigma(y)})_{x,y \in \mathcal{X}}.$$

Let $\mathcal{O}_1, \ldots, \mathcal{O}_N$ denote the orbits of the set $\mathcal{X} \times \mathcal{X}$ under the action of the group G and, for $i = 1, \ldots, N$, let $\tilde{D}_i$ be the $\mathcal{X} \times \mathcal{X}$ matrix:

$$(\tilde{D}_i)_{x,y} = \begin{cases} 1 & \text{if } (x, y) \in \mathcal{O}_i \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

Then, $\tilde{D}_1, \ldots, \tilde{D}_N$ form a basis of the commutant $\mathcal{A}^G$ (as vector space) and $\tilde{D}_1 + \ldots + \tilde{D}_N = J$ (the all-ones matrix). We normalize the $\tilde{D}_i$ to

$$D_i := \frac{\tilde{D}_i}{\sqrt{\langle \tilde{D}_i, \tilde{D}_i \rangle}} \tag{3}$$

for $i = 1, \ldots, N$. (For two $N \times N$ matrices A, B, $\langle A, B \rangle := Tr(A^T B) = \sum_{i,j=1}^N A_{ij} B_{ij}$.) Then, $\langle D_i, D_j \rangle = 1$ if $i = j$ and 0 otherwise. The *multiplication parameters* γ_{ij}^k are defined by

$$D_i D_j = \sum_{k=1}^N \gamma_{ij}^k D_k \tag{4}$$

for all $i, j = 1, \ldots, N$. Define the $N \times N$ matrices $L_1, \ldots, L_N$ by

$$(L_k)_{i,j} := \gamma_{i,k}^j \quad \text{for } k, i, j = 1, \ldots, N. \tag{5}$$

Schrijver [12] shows:

Theorem 1. *The mapping $D_k \mapsto L_k$ is a $*$-isomorphism, known as the* regular $*$-representation *of $\mathcal{A}^G$. In particular, given real scalars $x_1, \ldots, x_N$,*

$$\sum_{i=1}^{N} x_i D_i \succeq 0 \Longleftrightarrow \sum_{i=1}^{N} x_i L_i \succeq 0. \tag{6}$$

This result has important algorithmic applications, as it permits to give more compact formulations for invariant semidefinite programs. Consider a semidefinite program:

$$\min \ \langle C, Y\rangle \ \text{ s.t. } \langle A_\ell, Y\rangle \leq b_\ell \ (\ell = 1, \ldots, m), \ Y \succeq 0 \tag{7}$$

in the $\mathcal{X} \times \mathcal{X}$ matrix variable Y. Assume that the program (7) is *invariant under action of the group G*; that is, C is invariant under action of G and, for every matrix Y feasible for (7) and $\sigma \in G$, the matrix $\sigma(Y)$ is again feasible for Y. (This holds, e.g., if the class of constraints is invariant under action of G, i.e., if for each $\ell \in \{1, \ldots, m\}$ and $\sigma \in G$, there exists $\ell' \in \{1, \ldots, m\}$ such that $\sigma(A_\ell) = A_{\ell'}$ and $b_\ell = b_{\ell'}$.) Then, if Y is feasible for (7) then the matrix $Y_0 := \frac{1}{|G|}\sum_{\sigma \in G} \sigma(Y)$ too is feasible for (7), with the same objective value as Y. Therefore, in (7), one can assume without loss of generality that Y is invariant, i.e., of the form $Y = \sum_{i=1}^{N} x_i D_i$ with $x_1, \ldots, x_N \in \mathbb{R}$. Then the objective function reads $\langle C, Y\rangle = \sum_{i=1}^{N} c_i x_i$, after setting $C = \sum_{i=1}^{N} c_i D_i$ and the constraints in (7) become linear constraints in x. As a direct application of Theorem 1, we find:

Corollary 2. *Consider the program (7) in the $\mathcal{X} \times \mathcal{X}$ matrix variable Y. If (7) is invariant under the action of the group G, then it can be equivalently reformulated as*

$$\min \ \sum_{i=1}^{N} c_i x_i \quad s.t. \ a_\ell^T x \leq b_\ell \ (\ell = 1, \ldots, m), \ \sum_{i=1}^{N} x_i L_i \succeq 0 \tag{8}$$

which involves $N \times N$ matrices and N variables. Here, N is the dimension of the algebra $\mathcal{A}^G$ (the set of $\mathcal{X} \times \mathcal{X}$ invariant matrices under the action of the group G), typically much smaller than $|\mathcal{X}|$.

To use computationally this result, one needs the matrices $L_1, \ldots, L_N$, which involves computing the cardinality of the orbits of $\mathcal{X} \times \mathcal{X}$ and the multiplication parameters $\gamma_{i,j}^k$ in (4). Schrijver [12] applies this technique for computing tighter bounds for the crossing number of a complete bipartite graph. We apply it in Section 3.2 for reducing the size of the semidefinite programs permitting to compute the hierarchy of semidefinite bounds for the parameter $A(n, d)$.

Example 3. Let $\mathcal{X} := \mathcal{P}$, the collection of all subsets of the set $V = \{1, \ldots, n\}$, and $G := Sym(V)$, the group of permutations of V. Each $\pi \in G$ induces a permutation of $\mathcal{X}$, again denoted by π, by letting $\pi(I) := \{\pi(i) \mid i \in I\}$ for $I \in \mathcal{P}$. Two pairs $(I, J), (I', J')$ $(I, J, I', J' \in \mathcal{P})$ lie in the same orbit [i.e., $I' = \pi(I)$, $J' = \pi(J)$ for some $\pi \in G$] if and only if $|I| = |I'|$, $|J| = |J'|$ and $|I \cap J| = |I' \cap J'|$. Therefore, the commutant algebra $\mathcal{A}^G$ is generated by the matrices $M_{i,j}^t$ $(i, j, t \in \mathbb{Z}_+)$, where

$$(M_{i,j}^t)_{I,J} := \begin{cases} 1 & \text{if } |I| = i, |J| = j, |I \cap J| = t, \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

for $I, J \in \mathcal{P}$; $\mathcal{A}^G =: \mathcal{A}_n$ is known as the *Terwiliger algebra* of the Hamming scheme (Terwiliger [13]).

Example 4. Let $\mathcal{X} := \mathcal{P}$ and $G := Aut(\mathcal{P})$, the automorphism group of $\mathcal{P}$, consisting of the permutations $\sigma \in Sym(\mathcal{P})$ preserving the symmetric difference, i.e., such that $|\sigma(I)\Delta\sigma(J)| = |I\Delta J|$ for all $I, J \in \mathcal{P}$. Thus, $G = \{\pi s_A \mid A \subseteq V, \pi \in Sym(V)\}$, $|G| = 2^n n!$; for a set $A \subseteq V$, s_A is the permutation of $\mathcal{P}$ mapping any $I \in \mathcal{P}$ to $s_A(I) := A\Delta I$. Two pairs $(I, J), (I', J')$ $(I, J, I', J' \in \mathcal{P})$ lie in the same orbit [i.e., $I' = \sigma(I)$, $J' = \sigma(J)$ for some $\sigma \in G$] if and only if $|I\Delta J| = |I'\Delta J'|$. Therefore, the algebra $\mathcal{A}^G$ is generated by the matrices M_k $(k = 0, 1, \ldots, n)$ where

$$(M_k)_{I,J} := \begin{cases} 1 & \text{if } |I\Delta J| = k, \\ 0 & \text{otherwise} \end{cases} \tag{10}$$

for $I, J \in \mathcal{P}$; $\mathcal{A}^G =: \mathcal{B}_n$ is known as the *Bose Mesner algebra* of the Hamming scheme. The Bose-Mesner algebra is a subalgebra of the Terwiliger algebra, as $M_k = \sum_{i,j=0}^{n} M_{i,j}^{(i+j-k)/2}$ for $k = 0, 1, \ldots, n$.

In fact, it is known from invariant theory and $C*$-algebra theory that the algebra $\mathcal{A}^G$ can be block-diagonalized. Therefore, there exists a semidefinite program equivalent to the invariant program (7), where the matrix Y is replaced by a block-diagonal matrix with possibly repeated blocks; see, e.g., Gaterman and Parrilo [2]. Such program is typically more compact than the program (8). However, finding explicitely the block-diagonalization is a nontrivial task in general. An advantage of the above mentioned reduction method, based on the regular $*$-representation, is that it involves the matrices L_i which are explicitely defined in terms of the matrices D_i generating the algebra. Nevertheless, Schrijver [11] was able to determine explicitely the block-diagonalization for the Terwiliger algebra; we recall this result in the next section as we will need it for the computation of our stronger bounds for the coding problem.

2.2. Block-diagonalization of the Terwiliger algebra.

While the Bose-Mesner algebra $\mathcal{B}_n$ is a commutative algebra and thus can be diagonalized (see [1]), the Terwiliger algebra $\mathcal{A}_n$ is a non-commutative algebra. Its dimension is $\dim \mathcal{A}_n = \binom{n+3}{3}$, which is the number of triples (i, j, t) for which $M_{i,j}^t \neq 0$. As $\mathcal{A}_n$ is a matrix $*$-algebra containing the identity, there exists a unitary $\mathcal{P} \times \mathcal{P}$ complex matrix U (i.e., $U^*U = I$) and positive integers m and $p_0, q_0, \ldots, p_m, q_m$ such that the set $U^*\mathcal{A}_n U := \{U^*MU \mid M \in \mathcal{A}_n\}$ is equal to the collection of block-diagonal matrices

$$\begin{pmatrix} C_0 & 0 & \ldots & 0 \\ 0 & C_1 & \ldots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \ldots & C_m \end{pmatrix}$$

where each C_k $(k = 0, 1, \ldots, m)$ is a block-diagonal matrix with q_k identical blocks B_k of order p_k:

$$C_k = \begin{pmatrix} B_k & 0 & \ldots & 0 \\ 0 & B_k & \ldots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \ldots & B_k \end{pmatrix};$$

thus $2^n = \sum_{k=0}^m p_k q_k$ and $\sum_{k=0}^m p_k^2 = \dim \mathcal{A}_n$. By deleting copies of identical blocks, it follows that $\mathcal{A}_n$ is isomorphic to the algebra

$$\bigoplus_{k=0}^{m} \mathbb{C}^{p_k \times p_k} = \{ \begin{pmatrix} B_0 & 0 & \ldots & 0 \\ 0 & B_1 & \ldots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \ldots & B_m \end{pmatrix} \mid B_k \in \mathbb{C}^{p_k \times p_k} \text{ for } k = 0, 1, \ldots, m\}. \tag{11}$$

An important fact for our purpose is that this isomorphism preserves positive semidefiniteness. The existence of a unitary matrix U with the above properties is standard $C*$-algebra theory. Schrijver [11] has constructed explicitely this matrix U and the image of a matrix $M \in \mathcal{A}_n$ in the algebra (11). We recall some details from [11] needed for our treatment.

It turns out that U is real valued, $m = \lfloor \frac{n}{2} \rfloor$ and, for $k = 0, 1, \ldots, \lfloor \frac{n}{2} \rfloor$, the block B_k has order $p_k = n - 2k + 1$ and multiplicity $q_k = \binom{n}{k} - \binom{n}{k-1}$. In particular, the block B_0 has order $n + 1$ and multilplicity 1. For $k = 1, \ldots, \lfloor \frac{n}{2} \rfloor$, define

$$L_k := \{b \in \mathbb{R}^{\mathcal{P}} \mid M^{k-1}_{k-1,k} b = 0 \text{ and } b_I = 0 \text{ if } |I| \neq k\}.$$

Let $\mathcal{B}_k$ be a basis of L_k. Then $|\mathcal{B}_k| = \binom{n}{k} - \binom{n}{k-1}$ and $\sum_{I \in \mathcal{P}} b_I = 0$ for $b \in L_k$. Set $\mathcal{B}_0 := \{b_0\}$ where $b_0 := (1, 0, \ldots, 0)^T \in \mathbb{R}^{\mathcal{P}}$ (the nonzero entry being indexed by $\emptyset \in \mathcal{P}$) and define

$$\mathcal{Q} := \{(k, b, i) \mid k \in \{0, \ldots, \lfloor \frac{n}{2} \rfloor\}, b \in \mathcal{B}_k, i \in \{k, k+1, \ldots, n-k\}\}.$$

Then $|\mathcal{Q}| = 2^n = |\mathcal{P}|$. For $(k, i, b) \in \mathcal{Q}$, define the vector

$$u_{k,i,b} := \binom{n-2k}{i-k}^{-\frac{1}{2}} M^k_{i,k} b \in \mathbb{R}^{\mathcal{P}}.$$

Finally let U be the $\mathcal{P} \times \mathcal{Q}$ matrix whose columns are the vectors $u_{k,i,b}$ for $(k, i, b) \in \mathcal{Q}$. It can be shown that U is orthogonal, i.e., $U^T U = I$. Moreover, for $M = \sum_{i,j,t=0}^n x^t_{i,j} M^t_{i,j} \in \mathcal{A}_n$, the matrix $U^T M U$ is a block-diagonal matrix determined by the partition of $\mathcal{Q}$ into the classes $\mathcal{Q}_{k,b} := \{(k, i, b) \mid k \le i \le n - k\}$ (for $k = 0, \ldots, \lfloor \frac{n}{2} \rfloor$, $b \in \mathcal{B}_k$). For a given integer $k = 0, \ldots, \lfloor \frac{n}{2} \rfloor$, the blocks corresponding to the classes $\mathcal{Q}_{k,b}$ (for $b \in \mathcal{B}_k$) are all identical to the following matrix:

$$B_k(x) := \left(\sum_t \binom{n-2k}{i-k}^{-\frac{1}{2}} \binom{n-2k}{j-k}^{-\frac{1}{2}} \beta^t_{i,j,k} x^t_{i,j} \right)_{i,j=k}^{n-k}, \tag{12}$$

after setting

$$\beta^t_{i,j,k} := \sum_{u=0}^{n} (-1)^{t-u} \binom{u}{t} \binom{n-2k}{n-k-u} \binom{n-k-u}{i-u} \binom{n-k-u}{j-u} \tag{13}$$

for $i, j, k, t \in \{0, \ldots, n\}$. As $\mathcal{A}_n$ is isomorphic to the algebra (11),

$$\sum_{i,j,t=0}^{n} x^t_{i,j} M^t_{i,j} \succeq 0 \Longleftrightarrow B_k(x) \succeq 0 \text{ for } k = 0, 1, \ldots, \lfloor \frac{n}{2} \rfloor. \tag{14}$$

This is a key tool used in [11] and the present paper, which allows reducing semidefinite programs involving matrices in the Terwiliger algebra to semidefinite programs of size $O(n^3)$. We will deal in this note with matrices of the form

$$\tilde{M} = \begin{pmatrix} d & c^T \\ c & M \end{pmatrix}, \text{ where } M = \sum_{i,j,t=0}^{n} x^t_{i,j} M^t_{i,j},\ d \in \mathbb{R},\ c = \sum_{i=0}^{n} c_i \chi^{\binom{\mathcal{P}}{i}}, \tag{15}$$

and $\chi^{\binom{\mathcal{P}}{i}} \in \{0,1\}^{\mathcal{P}}$ whose I-th entry is 1 if and only if $|I| = i$ (for $I \in \mathcal{P}$).

Lemma 5. *The matrix $\tilde{M}$ from (15) is positive semidefinite if and only if $B_k(x) \succeq 0$ for $k = 1, \ldots, \lfloor \frac{n}{2} \rfloor$, and*

$$\tilde{B}_0(x) := \begin{pmatrix} d & \tilde{c}^T \\ \tilde{c} & B_0(x) \end{pmatrix} \succeq 0, \textit{ where } \tilde{c} := (c_i \binom{n}{i}^{\frac{1}{2}})_{i=0}^{n}.$$

Proof. We have:

$$\tilde{U}^T \tilde{M} \tilde{U} := \begin{pmatrix} 1 & 0 \\ 0 & U^T \end{pmatrix} \tilde{M} \begin{pmatrix} 1 & 0 \\ 0 & U \end{pmatrix} = \begin{pmatrix} d & c^T U \\ U^T c & U^T M U \end{pmatrix}.$$

It suffices now to verify that $(c^T U)_{k,i,b} = c^T u_{k,i,b} = 0$ for $(k, i, b) \in \mathcal{Q}$ with $k \geq 1$, and that $(c^T U)_{0,i,b_0} = c_i \binom{n}{i}^{\frac{1}{2}}$ for $i = 0, \ldots, n$. This is direct verification using the above definitions. Therefore, $\tilde{U}^T \tilde{M} \tilde{U}$ is block-diagonal, with blocks $\tilde{B}_0(x)$ (with multiplicity 1) and $B_k(x)$ (with multiplicity q_k) for $k = 1, \ldots, \lfloor \frac{n}{2} \rfloor$. The lemma now follows. ∎

3. Semidefinite bounds for the stability number of a graph

3.1. **Lasserre's construction.** Let $\mathcal{G} = (V, E)$ be a graph. A *stable set* in $\mathcal{G}$ is a set $S \subseteq V$ containing no edge and the *stability number* $\alpha(\mathcal{G})$ of $\mathcal{G}$ is the maximum cardinality of a stable set in $\mathcal{G}$. Set $V_k := \{I \subseteq V \mid |I| \leq k\}$ for an integer k. Given a stable set S in $\mathcal{G}$, define $x = (x_I)_{I \in V_k} \in \{0,1\}^{V_k}$ and $y = (y_I)_{I \in V_{2k}} \in \{0,1\}^{V_{2k}}$ with $x_I = 1$ (resp., $y_I = 1$) if and only if $I \subseteq S$, for $I \in V_k$ (resp., for $I \in V_{2k}$). Then y and the matrix $Y := xx^T$ satisfy:

$$Y \succeq 0 \tag{16}$$

$$Y_{I,J} = y_{I \cup J} \quad (\text{for } I, J \in V_k) \tag{17}$$

$$Y_{I,J} = y_{I \cup J} = 0 \text{ if } I \cup J \text{ contains an edge} \quad (\text{for } I, J \in V_k) \tag{18}$$

$$Y_{\emptyset,\emptyset} = y_\emptyset = 1 \tag{19}$$

$$0 \le y_I \le y_J \ \text{ if } J \subseteq I \text{ (for } I, J \in V_{2k}). \tag{20}$$

We refer to (18) as the *edge condition* and to (17) as the *moment condition*. A matrix Y satisfying (17) is known as a moment matrix and is denoted as $Y = M_k(y)$ (see [4, 5, 6]). Under the assumption (16), the edge condition (18) is, in fact, equivalent to $y_{ij} = 0$ (for $ij \in E$). (Here and below, we set $y_{ij} := y_{\{i\},\{j\}}$, $y_i := y_{\{i\}}$, etc.) Under (16), (20) holds for $I \in V_k$; indeed, the principal submatrix of $M_k(y)$ indexed by $\{I, J\}$ has the form $\begin{pmatrix} y_I & y_I \\ y_I & y_J \end{pmatrix}$, whose positive semidefiniteness implies $0 \le y_J \le y_I$. On the other hand, $M_1(y) \succeq 0$ implies $y_{ij} \le \max(y_i, y_j)$; $M_2(y) \succeq 0$ implies that y_{ijk} is at most the largest two values among y_{ij}, y_{ik}, y_{jk}, etc.

Consider the semidefinite program:

$$\ell^{(k)}(\mathcal{G}) := \max \sum_{i \in V} y_i \ \text{ s.t. } M_k(y) \succeq 0,\ y_\emptyset = 1,\ y_{ij} = 0 \ (ij \in E). \tag{21}$$

Then, $\alpha(\mathcal{G}) \le \ell^{(k)}(\mathcal{G})$, with equality if $k \ge \alpha(\mathcal{G})$ ([5, 6]). Define $\ell_+^{(k)}(\mathcal{G})$ as the parameter obtained by adding to (21) the constraints (20); thus, $\alpha(\mathcal{G}) \le \ell_+^{(k)}(\mathcal{G}) \le \ell^{(k)}(\mathcal{G})$.

For $k = 1$, $\ell^{(1)}(\mathcal{G}) = \vartheta(\mathcal{G})$, the Lovász' theta number, and the stronger bound obtained by adding nonnegativity to (21) is $\vartheta'(\mathcal{G})$, the strengthening of $\vartheta(\mathcal{G})$ introduced by McEliece, Rodemich and Rumsey [9] and Schrijver [10]. The bound $\ell^{(2)}(\mathcal{G})$ is at least as good as the parameter obtained by optimizing over $N_+(\text{TH}(\mathcal{G}))$, the convex relaxation of the stable set polytope of $\mathcal{G}$ obtained by applying the Lovász-Schrijver N_+-operator to the theta body $\text{TH}(\mathcal{G})$ ([6]; see (25)). For $k = 2$, the program (21) has size $O(|V|^4)$. We now formulate a bound $\ell(\mathcal{G})$, which is weaker than $\ell^{(2)}(\mathcal{G})$, but still at least as good as the bound obtained from $N_+(\text{TH}(\mathcal{G}))$, although its computation is more economical since it can be expressed via a semidefinite program of size $O(|V|^3)$.

Namely, for each $\ell \in V$, consider the principal submatrix $Y_\ell(y)$ of $M_2(y)$ indexed by the set $V_2(\ell) := V_1 \cup \{\{\ell, i\} \mid i \in V\}$; thus the matrices $Y_\ell(y)$ involves only variables y_I for $I \in V_3$. Define

$$\ell(\mathcal{G}) := \max \sum_{i \in V} y_i \ \text{ s.t. } y_\emptyset = 1,\ y_{ij} = 0 \ (ij \in E),\ Y_\ell(y) \succeq 0 \ (\ell \in V) \tag{22}$$

and $\ell_+(\mathcal{G})$ as the parameter obtained by adding to (22) the constraints: $0 \le y_{ijk} \le y_{ij}$ for distinct $i, j, k \in V$ (coming from (20)). Obviously, $\ell^{(2)}(\mathcal{G}) \le \ell(\mathcal{G}) \le \ell^{(1)}(\mathcal{G})$; analogously for the ℓ_+ parameters. We will see in Section 3.3 that, for the graph $\mathcal{G} = \mathcal{G}(n, d)$, the matrices involved in (22) lie in (a variation of) the Terwiliger algebra, which allows reformulating the parameters $\ell(\mathcal{G}(n, d))$, $\ell_+(\mathcal{G}(n, d))$ via semidefinite programs of size $O(n^3)$.

From the moment condition (17), the matrix $Y_\ell(y)$ has the block structure:

$$Y_\ell(y) = \begin{pmatrix} 1 & a^T & b_\ell^T \\ a & A & B_\ell \\ b_\ell & B_\ell & B_\ell \end{pmatrix}, \tag{23}$$

where $A := (y_{ij})_{i,j\in V}$, $B_\ell := (y_{\{i,j,\ell\}})_{i,j\in V}$ are symmetric $V\times V$ matrices, and $a := (y_i)_{\in V}$, $b_\ell := (y_{i\ell})_{i\in V}$. As b_ℓ coincides with the ℓ-th column of A and of B_ℓ, by applying some column/row manipulation to $Y_\ell(y)$, one deduces that

$$Y_\ell(y) \succeq 0 \Longleftrightarrow B_\ell \succeq 0 \text{ and } \tilde{C}_\ell := \begin{pmatrix} 1-y_\ell & a^T - b_\ell^T \\ a - b_\ell & A - B_\ell \end{pmatrix} \succeq 0, \tag{24}$$

which permits to reduce the size of the matrices involved in program (22). Setting

$$\mathrm{TH}(\mathcal{G}) = \{x \in \mathbb{R}^{V_1} \mid \exists y \in \mathbb{R}^{V_2} \text{ s.t. } M_1(y) \succeq 0,\ y_{ij} = 0\ (ij \in E),\ x_I = y_I\ (I \in V_1)\},$$

$$N_+(\mathrm{TH}(\mathcal{G})) = \{x \in \mathbb{R}^V \mid \exists y \in \mathbb{R}^{V_2} \text{ s.t. } \begin{array}{l} M_1(y) \succeq 0,\ y_\emptyset = 1,\ x_i = y_i\ (i \in V), \\ (y_{I\cup\{\ell\}})_{I\in V_1}, (y_I - y_{I\cup\{\ell\}})_{I\in V_1} \in \mathrm{TH}(\mathcal{G})\} \end{array}$$

one can verify that

$$\ell(\mathcal{G}) \le \max_{x\in N_+(\mathrm{TH}(\mathcal{G}))} \sum_{i\in V} x_i. \tag{25}$$

To see it, let y be feasible for (22); then $x := (y_i)_{i\in V} \in N_+(\mathrm{TH}(\mathcal{G}))$. Indeed, the vector $(y_{I\cup\{\ell\}})_{I\in V_1}$ is equal to the first column of the principal submatrix of $Y_\ell(y)$ indexed by $\{\ell\} \cup \{\{\ell, i\} \mid i \in V\}$, and $(y_I - y_{I\cup\{\ell\}})_{I\in V_1}$ is the first column of the matrix $\tilde{C}_\ell$ in (24).

3.2. **The semidefinite bounds $\ell^{(k)}(\mathcal{G})$ for the coding problem.** Let G be a group of automorphisms of the graph $\mathcal{G} = (V, E)$, i.e., $G \subseteq Sym(V)$ and each $\sigma \in G$ preserves edges ($ij \in E \Longrightarrow \sigma(i)\sigma(j) \in E$). Then G acts on the set V_k indexing matrices in the program (21).

LEMMA 6. *Let G be a group of automorphisms of $\mathcal{G}$. Then the program (21) is invariant under the action of G.*

Proof. Set $Y = M_k(y)$. The objective function is of the form $\sum_{i\in V} y_i = \sum_{i\in V} Y_{i,i} = \langle C, Y\rangle$, where C is invariant under action of G, since the set $\{(\{i\},\{i\}) \mid i \in V\}$ is a union of orbits of $V_k \times V_k$ (a single orbit if G is vertex-transitive). The constraint $y_\emptyset = Y_{\emptyset,\emptyset} = 1$ is of the form $\langle A, Y\rangle = 1$ where A is invariant, since the set $\{(\emptyset, \emptyset)\}$ is an orbit. The class of edge constraints (18) is invariant under action of G: If $I\cup J$ contains an edge ij and $\sigma \in G$, then $\sigma(I)\cup\sigma(J)$ contains the edge $\sigma(i)\sigma(j)$ and thus the equation: $y_{\sigma(I)\sigma(J)} = Y_{\sigma(I),\sigma(J)} = 0$ is again an edge constraint. Similarly, the class of moment constraints (17) is also invariant under action of G. ∎

By Corollary 2, the parameter $\ell^{(k)}(\mathcal{G})$ can therefore be formulated as the optimum of a semidefinite program in N variables involving $N \times N$ matrices, where N is the number of orbits of the set $V_k \times V_k$ under the action of the group G. We now apply this technique to the graph $\mathcal{G} = \mathcal{G}(n, d)$ and the group $G = Aut(\mathcal{P})$, the group of automorphisms of $\mathcal{P}$. Recall that $\mathcal{G}(n, d)$ has node set $\mathcal{P}$, the collection of subsets of $\{1, \ldots, n\}$, with an edge (I, J) if $|I\Delta J| \in \{1, \ldots, d-1\}$ for $I, J \in \mathcal{P}$. Thus G acts on the set $\mathcal{X}_k := \{\mathcal{A} \subseteq \mathcal{P} \mid |\mathcal{A}| \le k\}$ indexing the matrix variable in program (21). We show:

Theorem 7. *For any fixed k, one can compute (to an arbitrary precision) the parameter $\ell^{(k)}(\mathcal{G}(n,d))$ from (21) in time polynomial in n. The same holds for the parameter $\ell_+^{(k)}(\mathcal{G})$ obtained by adding the constraints (20) to (21).*

Proof. Let k be fixed and let N_k denote the number of orbits of the set $\mathcal{X}_k \times \mathcal{X}_k$ under the action of the group G. As mentioned above, the parameter $\ell^{(k)}(\mathcal{G}(n,d))$ can be expressed via a semidefinite program of the form (8), involving $N_k \times N_k$ matrices and N_k variables. Hence, to show Theorem 7, it suffices to verify that N_k is bounded by a polynomial in n and that the new program equivalent to (21) can be constructed in time polynomial in n. To begin with, it is useful to have a way to identify the orbits of the set $\mathcal{X}_k \times \mathcal{X}_k$.

Consider $(\mathcal{A},\mathcal{B}) \in \mathcal{X}_k \times \mathcal{X}_k$ with $r := |\mathcal{A}|$ and $s := |\mathcal{B}|$. If $r = s = 0$ then $\mathcal{A} = \mathcal{B} = \emptyset$, the empty subset of $\mathcal{P}$, and the orbit of $(\emptyset,\emptyset)$ just consists of the pair $(\emptyset,\emptyset)$. We can now assume that $r+s \geq 1$. Let $\vec{\mathcal{A}} = (A_1,\ldots,A_r)$ be an ordering of the elements of $\mathcal{A}$; similarly, $\vec{\mathcal{B}} = (B_1,\ldots,B_s)$ is an ordering of the elements of $\mathcal{B}$. Then one can define the $(r+s)\times n$ *incidence tableau* of $(\vec{\mathcal{A}},\vec{\mathcal{B}})$, whose rows are the incidence vectors $\chi^{A_1},\ldots,\chi^{A_r},\chi^{B_1},\ldots,\chi^{B_s}$ (in that order) of the sets $A_1,\ldots,A_r,B_1,\ldots,B_s$. Define the function $\varphi_{\vec{\mathcal{A}},\vec{\mathcal{B}}} : 2^r \times 2^s \longrightarrow \mathbb{Z}_+$ where, for $(u,v) \in 2^r \times 2^s$, $\varphi_{\vec{\mathcal{A}},\vec{\mathcal{B}}}(u,v)$ is the multiplicity of (u,v) as a column of the incidence tableau of $(\vec{\mathcal{A}},\vec{\mathcal{B}})$. Here and below, we set $2^r := \{0,1\}^r$, $2^s := \{0,1\}^s$. Thus $\varphi_{\vec{\mathcal{A}},\vec{\mathcal{B}}}$ belongs to the set $\Phi_{r,s}$ consisting of the functions $\phi : 2^r \times 2^s \longrightarrow \{0,1,\ldots,n\}$ satisfying: $\sum_{u\in 2^r, v\in 2^s} \phi(u,v) = n$ and, for all $i \neq j \in \{1,\ldots,r\}$ (resp., $i \neq j \in \{1,\ldots,s\}$), there exists $(u,v) \in 2^r \times 2^s$ for which $\phi(u,v) \geq 1$ and $u_i \neq u_j$ (resp., $v_i \neq v_j$).

Let $\vec{\mathcal{A}'}$ (resp., $\vec{\mathcal{B}'}$) be another ordered sequence of r (resp., of s) distinct elements of $\mathcal{P}$ and $\phi = \phi_{\vec{\mathcal{A}},\vec{\mathcal{B}}}$, $\phi' = \varphi_{\vec{\mathcal{A}'},\vec{\mathcal{B}'}}$. Then, $\vec{\mathcal{A}'} = (\sigma(A_1),\ldots,\sigma(A_r))$ and $\vec{\mathcal{B}'} = (\sigma(B_1),\ldots,\sigma(B_s))$ for some $\sigma \in G$ if and only if $\phi(u,v) + \phi(\mathbf{1}-u,\mathbf{1}-v) = \phi'(u,v) + \phi'(\mathbf{1}-u,\mathbf{1}-v)$ for all $(u,v) \in 2^r \times 2^s$. Moreover, $\vec{\mathcal{A}'} = (A_{\alpha(1)},\ldots,A_{\alpha(r)})$ and $\vec{\mathcal{B}'} = (B_{\beta(1)},\ldots,B_{\beta(s)})$ for some permutations $\alpha \in Sym(r)$, $\beta \in Sym(s)$ if and only if $\phi'(u,v) = \phi(\alpha(u),\beta(v))$ for all $(u,v) \in 2^r \times 2^s$, setting $\alpha(u) := (u_{\alpha(1)},\ldots,u_{\alpha(r)})$, $\beta(v) := (v_{\beta(1)},\ldots,v_{\beta(s)})$. For two elements $\phi,\phi' \in \Phi_{r,s}$, write $\phi \sim \phi'$ if

$$\phi'(u,v) + \phi'(\mathbf{1}-u,\mathbf{1}-v) = \phi(\alpha(u),\beta(v)) + \phi(\mathbf{1}-\alpha(u),\mathbf{1}-\beta(v))) \ \forall (u,v) \in 2^r \times 2^s$$

for some $\alpha \in Sym(r)$, $\beta \in Sym(s)$. This defines an equivalence relation on $\Phi_{r,s}$.

Then two pairs $(\mathcal{A},\mathcal{B}),(\mathcal{A}',\mathcal{B}')$ belong to the same orbit of $\mathcal{X}_k \times \mathcal{X}_k$ under action of G if and only if $|\mathcal{A}| = |\mathcal{A}'| =: r$, $|\mathcal{B}| = |\mathcal{B}'| =: s$ and $\varphi_{\vec{\mathcal{A}},\vec{\mathcal{B}}} \sim \varphi_{\vec{\mathcal{A}'},\vec{\mathcal{B}'}}$ for some respective orderings $\vec{\mathcal{A}}$, $\vec{\mathcal{B}}$, $\vec{\mathcal{A}'}$, $\vec{\mathcal{B}'}$ of $\mathcal{A}$, $\mathcal{B}$, $\mathcal{A}'$, $\mathcal{B}'$. Thus each orbit of $\mathcal{X}_k \times \mathcal{X}_k$ correspond to an equivalence class of $\cup_{r,s\leq k}\Phi_{r,s}$. Hence the number N_k of orbits of $\mathcal{X}_k \times \mathcal{X}_k$ is at most $1 + \sum_{\substack{0\leq r,s\leq k\\ r+s\geq 1}} (n+1)^{2^{r+s-1}-1}$, giving:

$$N_k \leq O(n^{2^{2k-1}-1}). \tag{26}$$

We now verify that the matrices L_i $(i = 1,\ldots,N_k)$ (as defined in (5)) can be constructed in time polynomial in n.

For this one first needs to be able to compute the cardinality of the orbits of $\mathcal{X}_k \times \mathcal{X}_k$ in polynomial time. Given $\phi_0 \in \Phi_{r,s}$ $(0 \leq r,s \leq k, r+s \geq 1)$, one has to count the number L_{ϕ_0} of pairs $(\mathcal{A},\mathcal{B}) \in \binom{\mathcal{P}}{r} \times \binom{\mathcal{P}}{s}$ for which $\varphi_{\vec{\mathcal{A}},\vec{\mathcal{B}}} \sim \phi_0$ for some orderings $\vec{\mathcal{A}}$, $\vec{\mathcal{B}}$ of $\mathcal{A}$, $\mathcal{B}$. Given $\phi \sim \phi_0$, there are $\ell_\phi := n!/\prod_{\substack{u\in 2^r\\ v\in 2^s}} \phi(u,v)!$ pairs $(\vec{\mathcal{A}},\vec{\mathcal{B}})$ for which $\varphi_{\vec{\mathcal{A}},\vec{\mathcal{B}}} = \phi_0$. Therefore, $L_{\phi_0} = \frac{1}{r!s!}\sum_{\phi\sim\phi_0} \ell_\phi$, which can be computed in time polynomial in n since one can enumerate the equivalence class of ϕ_0 in time polynomial in n.

Next we verify that one can compute in time polynomial in n the multiplication parameters $\gamma^k_{i,j}$ from (4), used for defining the matrices L_i in (5). For this, given $(\mathcal{A},\mathcal{B}) \in \binom{\mathcal{P}}{r}\times\binom{\mathcal{P}}{s}$ with respective orderings $\vec{\mathcal{A}}$, $\vec{\mathcal{B}}$, an integer $0 \le t \le k$, and $\phi_0 \in \Phi_{r,t}$, $\psi_0 \in \Phi_{s,t}$, one has to count the number L_{ϕ_0,ψ_0} of elements $\mathcal{C} \in \binom{\mathcal{P}}{t}$ for which $\varphi_{\vec{\mathcal{A}},\vec{\mathcal{C}}} \sim \phi_0$ and $\varphi_{\vec{\mathcal{B}},\vec{\mathcal{C}}} \sim \psi_0$ for some ordering $\vec{\mathcal{C}}$ of $\mathcal{C}$. Set $\xi := \varphi_{\vec{\mathcal{A}},\vec{\mathcal{B}}}$. Given $\phi \sim \phi_0$ and $\psi \sim \psi_0$, we first count the number $\ell_{\phi,\psi}$ of ordered sequences $\vec{\mathcal{C}}$ of t elements of $\mathcal{P}$ for which $\varphi_{\vec{\mathcal{A}},\vec{\mathcal{C}}} = \phi$ and $\varphi_{\vec{\mathcal{B}},\vec{\mathcal{C}}} = \psi$. For this let $x(u,v,w)$ denote the multiplicity of $(u,v,w) \in 2^r \times 2^s \times 2^t$ as column of the incidence tableau of $(\vec{\mathcal{A}},\vec{\mathcal{B}},\vec{\mathcal{C}})$. The first $r+s$ rows of the tableau are given and one needs to determine its last t rows. Then, $x(u,v,w) \in \{0,1,\ldots,n\}$ satisfy the system

$$
\begin{array}{lll}
\sum_{v\in 2^s} x(u,v,w) = \phi(u,w) & \forall u \in 2^r, w \in 2^t \\
\sum_{u\in 2^r} x(u,v,w) = \psi(v,w) & \forall v \in 2^s, w \in 2^t \\
\sum_{w\in 2^t} x(u,v,w) = \xi(u,v) & \forall u \in 2^r, v \in 2^s.
\end{array}
\tag{27}
$$

As the system (27) has polynomially many variables and equations, its set S of solutions can be found by complete enumeration and $|S| \le (n+1)^{2^{r+s+t}}$. Therefore, $\ell_{\phi,\psi} = \sum_{x\in S}\sum_{u\in 2^r, v\in 2^s} \frac{\xi(u,v)!}{\prod_{w\in 2^t} x(u,v,w)!}$, the number of possible ways to assign the vectors $w \in 2^t$ as columns of the lower $t\times n$ part of the tableau. Now, $L_{\phi_0,\psi_0} = \frac{1}{t!}\sum_{\substack{\phi\sim\phi_0\\ \psi\sim\psi_0}} \ell_{\phi,\psi}$ can be computed in time polynomial in n since one can enumerate the equivalence classes of ϕ_0 and ψ_0.

Remains only to construct the linear constraints corresponding to the moment constraints (17) and the edge constraints (18). Label the orbits of $\mathcal{X}_k \times \mathcal{X}_k$ as $\mathcal{O}_1,\ldots,\mathcal{O}_{N_k}$ and determine a pair $(\mathcal{A}_i,\mathcal{B}_i)$ belonging to each orbit $\mathcal{O}_i$. Then the moment constraints read: $x_i = x_j$ if $\mathcal{A}_i \cup \mathcal{B}_i = \sigma(\mathcal{A}_j \cup \mathcal{B}_j)$ for some $\sigma \in G$ (which can be tested in time polynomial in n), and the edge constraints read: $x_i = 0$ if $\mathcal{A}_i \cup \mathcal{B}_i$ contains a pair (I,J) with $|I\Delta J| \in \{1,\ldots,d-1\}$.

The bounds (20) become: $x_i \ge 0$ $(i = 1,\ldots,N_k)$ and $x_i \le x_j$ if $\mathcal{A}_i \cup \mathcal{B}_i \supseteq \sigma(\mathcal{A}_j \cup \mathcal{B}_j)$ for some $\sigma \in G$ (which can be tested in time polynomial in n).

Therefore, the parameter $\ell^{(k)}(\mathcal{G}(n,d))$ (or $\ell^{(k)}_+(\mathcal{G}(n,d))$) can be computed as the optimum value of a semidefinite program of the form (8) involving $N_k \times N_k$ matrices, with N_k variables and $O(N_k^2)$ linear constriants. As $N_k = O(n^{2^{2k-1}-1})$, it can be computed in time polynomial in n (to any precision), which concludes the proof of Theorem 7. ∎

The result from Theorem 7 is mainly of theoretical value for $k \ge 2$. Indeed, for $k = 2$, $N_k = O(n^7)$ and thus the semidefinite program defining $\ell^{(2)}(\mathcal{G}(n,d))$ is already too large to be solved in practice for interesting values of n by the currently available semidefinite software.

3.3. **Refining Schrijver's bound.** We begin with observing that, when a graph $\mathcal{G}$ has a vertex-transitive group of automorphims then, in the program (22), it suffices to require the condition $Y_\ell(y) \succeq 0$ for *one* choice of $\ell \in V$.

LEMMA 8. *Let G be a group of automorphisms of the graph $\mathcal{G} = (V, E)$. The program (22) is invariant under action of G. If G is vertex-transitive then, in (22), it suffices to require the constraint $Y_\ell(y) \succeq 0$ for one choice of $\ell \in V$ (instead of for all $\ell \in V$).*

Proof. The first part of the proof is analogous to the proof of Lemma 6. Here, we use the fact that, for $\ell \in V$, $\sigma \in G$, $Y_\ell(\sigma(y)) = \sigma(Y_{\sigma(\ell)}(y))$. Hence, if y is invariant under action of G, then $Y_\ell(y) \succeq 0$ for some $\ell \in V$ implies that $Y_\ell(y) \succeq 0$ for all $\ell \in V$. ∎

3.3.1. *A compact semidefinite formulation for the bound $\ell(\mathcal{G}(n,d))$.* Let $\mathcal{G} = \mathcal{G}(n,d)$ and $G = Aut(\mathcal{P})$ (which is indeed vertex-transitive). Applying Lemma 8, one can reformulate the parameter $\ell(\mathcal{G}(n,d))$ as

$$\begin{array}{rll} \ell(\mathcal{G}(n,d)) = & \max & \sum_{I\in\mathcal{P}} y_{\{I\}} \\ & \text{s.t.} & Y(y) \succeq 0,\ y_\emptyset = 1, \\ & & y_{\{I,J\}} = 0 \text{ if } |I\Delta J| \in \{1,\ldots,d-1\} \\ & & y_{\mathcal{A}} = y_{\sigma(\mathcal{A})} \text{ for } \sigma \in G, \mathcal{A} \in \mathcal{X}_2, \text{ or } A \in \mathcal{X}_3 \text{ with } \emptyset \in \mathcal{A}, \end{array}$$

where $Y(y)$ is the matrix indexed by $\mathcal{X} := \{\emptyset\} \cup \{\{I\} \mid I \in \mathcal{P}\} \cup \{\{\emptyset, I\} \mid I \in \mathcal{P}\}$ with $Y(y)_{\mathcal{A},\mathcal{B}} = y_{\mathcal{A}\cup\mathcal{B}}$ for $\mathcal{A},\mathcal{B} \in \mathcal{X}$. By (23),

$$Y(y) = \begin{pmatrix} 1 & a^T & b^T \\ a & A & B \\ b & B & B \end{pmatrix} \tag{28}$$

with $A = (y_{\{I,J\}})_{I,J\in\mathcal{P}}$, $B = (y_{\{\emptyset,I,J\}})_{I,J\in\mathcal{P}}$, $a = (y_{\{I\}})_{I\in\mathcal{P}}$, and $b = (y_{\{\emptyset,I\}})_{I\in\mathcal{P}}$. As y is invariant under action of G, it follows that $A_{I,J} = A_{I',J'}$ if $I' = \sigma(I)$, $J' = \sigma(J)$ for some $\sigma \in G$, i.e., if $|I\Delta J| = |I'\Delta J'|$. That is, the matrix A belongs to the Bose-Mesner algebra $\mathcal{B}_n$; say,

$$A = \sum_{k=0}^{n} x_k M_k \quad \text{for some real scalars } x_0, \ldots, x_n \tag{29}$$

where the matrices M_k are as in (10). Moreover, $B_{I,J} = B_{I',J'}$ if $I' = \sigma(I)$, $J' = \sigma(J)$, $\emptyset = \sigma(\emptyset)$ for some $\sigma \in G$, i.e., if $|I'| = |I|$, $|J'| = |J|$ and $|I \cap J| = |I' \cap J'|$. That is, the matrix B belongs to the Terwiliger algebra $\mathcal{A}_n$; say,

$$B = \sum_{i,j,t\geq 0} x_{i,j}^t M_{i,j}^t \quad \text{for some real scalars } x_{i,j}^t \tag{30}$$

where the matrices $M_{i,j}^t$ are as in (9) and $x_{i,j}^t = x_{j,i}^t$ for all i,j,t. The variables x_k and $x_{i,j}^t$ are related by

$$x_k = x_{0,k}^0 \quad \text{for } k = 0, 1, \ldots, n. \tag{31}$$

(since $x_k = A_{\emptyset,I} = B_{\emptyset,I} = x^k_{0,k}$ for $|I| = k$). Moreover,

$$x^t_{i,j} = x^{t'}_{i',j'} \text{ if } (i', j', i'+j'-2t') \text{ is a permutation of } (i, j, i+j-2t). \tag{32}$$

Equivalently, $x^t_{i,j} = x^{i-t}_{i+j-2t,i} = x^{j-t}_{i+j-2t,j}$. (Indeed, let $I, J \in \mathcal{P}$ with $i = |I|$, $j = |J|$, $t = |I \cap J|$. As $\sigma := s_J$ maps $\mathcal{A} := \{\emptyset, I, J\}$ to $\{\emptyset, J, I\Delta J\}$ and $y_{\sigma(\mathcal{A})} = y_{\mathcal{A}}$, then $x^t_{i,j} = y_{\{\emptyset,I,J\}} = y_{\{\emptyset,J,I\Delta J\}} = x^{j-t}_{j,i+j-2t}$.) The edge inequalities become:

$$x^t_{i,j} = 0 \text{ if } \{i, j, i+j-2t\} \cap \{1, \ldots, d-1\} \neq \emptyset, \tag{33}$$

and the bounds (20) read:

$$0 \leq x^t_{i,j} \leq x^0_{i,0} \text{ for } i, j, t = 0, \ldots, n. \tag{34}$$

From (24), we know that $Y(y) \succeq 0$ if and only if

$$B = \sum_{i,j,t=0}^{n} x^t_{i,j} M^t_{i,j} \succeq 0 \text{ and } \tilde{C} := \begin{pmatrix} 1 - x^0_{0,0} & c^T \\ c & C \end{pmatrix} \succeq 0,$$

where

$$C := A - B = \sum_{i,j,t=0}^{n} (x^0_{0,i+j-2t} - x^t_{i,j}) M^t_{i,j} \text{ and } c := a - b = \sum_{i=0}^{n} (x^0_{0,0} - x^0_{0,i}) \chi^{\binom{\mathcal{P}}{i}}.$$

Thus $\tilde{C}$ is of the form (15). For $k = 0, 1, \ldots, \lfloor \frac{n}{2} \rfloor$, define the matrices:

$$A_k(x) := \left(\sum_t \binom{n-2t}{i-k}^{-\frac{1}{2}} \binom{n-2t}{j-k}^{-\frac{1}{2}} \beta^t_{i,j,k} x^0_{0,i+j-2t} \right)_{i,j=k}^{n-k} \tag{35}$$

and $B_k(x)$ as in (12), where $\beta^t_{i,j,k}$ are as in (13). It follows from Lemma 5 that the positive semidefiniteness of $Y(y)$ is equivalent to

$$\begin{array}{ll} \text{(i)} & B_k(x) \succeq 0 \text{ for } k = 0, 1, \ldots, \lfloor \frac{n}{2} \rfloor \\ \text{(ii)} & A_k(x) - B_k(x) \succeq 0 \text{ for } k = 0, 1, \ldots, \lfloor \frac{n}{2} \rfloor \\ \text{(iii)} & \begin{pmatrix} 1 - x^0_{0,0} & \tilde{c}^T \\ \tilde{c} & A_0(x) - B_0(x) \end{pmatrix} \succeq 0, \text{ setting } \tilde{c} := (\binom{n}{i}^{\frac{1}{2}} (x^0_{0,0} - x^0_{0,i}))_{i=0}^n. \end{array} \tag{36}$$

(Of course, (36)(iii) implies (ii) for $k = 0$.) Summarizing, we have shown:

$$\ell(\mathcal{G}(n,d)) = \max\ 2^n x^0_{0,0} \text{ s.t. } \begin{array}{l} x^t_{i,j}\ (i, j, t = 0, \ldots, n) \text{ satisfy} \\ (32), (33), (36)(i)-(iii). \end{array} \tag{37}$$

Similarly,

$$\ell_+(\mathcal{G}(n,d)) = \max\ 2^n x^0_{0,0} \text{ s.t. } \begin{array}{l} x^t_{i,j}\ (i, j, t = 0, \ldots, n) \text{ satisfy} \\ (32), (33), (34), (36)(i)-(iii). \end{array} \tag{38}$$

Hence both parameters can be computed via a semidefinite program of size $O(n^3)$.

3.3.2. *Comparison with Schrijver's bound.* Schrijver [11] introduced the following upper bound for the stability number $A(n,d)$ of the graph $\mathcal{G}(n,d)$:

$$\begin{aligned} \max \quad & \sum_{i=0}^{n} \binom{n}{i} x_{0,i}^0 \\ \text{s.t.} \quad & x_{i,j}^t \ (i,j,t=0,\ldots,n) \ \text{ satisfy } (32),(33),(34),(36)(i)-(ii), \text{ and } x_{0,0}^0 = 1. \end{aligned} \tag{39}$$

As noted in [11], Schrijver's bound is at least as good as the Delsarte bound, which coincides with $\vartheta'(\mathcal{G}(n,d)) = \ell_+^{(1)}(\mathcal{G}(n,d))$. We now show:

LEMMA 9. *The bound $\ell_+(\mathcal{G}(n,d))$ is at least as good as Schrijver's bound from (39).*

Proof. Let $(x_{i,j}^t)_{i,j,t=0}^n$ be feasible for the program (38). Define $y_{i,j}^t := x_{i,j}^t / x_{0,0}^0$ for all $i,j,t = 0,\ldots,n$. Then the variables $y_{i,j}^t$ satisfy (32), (33), (34), (36) (i)-(ii), and $y_{0,0}^0 = 1$. Remains to verify that $2^n x_{0,0}^0 \leq \sum_{i=0}^n \binom{n}{i} y_{0,i}^0$, i.e., $2^n (x_{0,0}^0)^2 \leq \sum_{i=0}^n \binom{n}{i} x_{0,i}^0$. For this, recall that the conditions (36) (i)-(iii) are equivalent to the positive semidefiniteness of the matrix in (28). In particular, they imply

$$\begin{pmatrix} 1 & a^T \\ a & A \end{pmatrix} \succeq 0, \quad \text{i.e., } A - aa^T \succeq 0,$$

where A is as in (29), $a^T = (x_{0,0}^0, \ldots, x_{0,0}^0)$, $x_k = x_{0,k}^0$ for $k = 0,\ldots,n$. As $A - (x_{0,0}^0)^2 J \succeq 0$, $\langle J, A\rangle \geq (x_{0,0}^0)^2 \langle J, J\rangle = (x_{0,0}^0 2^n)^2$. But $\langle J, A\rangle = \sum_{k=0}^n x_k \langle J, M_k\rangle = \sum_{k=0}^n x_k 2^n \binom{n}{k}$, which gives $\sum_{k=0}^n x_{0,k}^0 \binom{n}{k} \geq 2^n (x_{0,0}^0)^2$. ∎

3.3.3. *Refining the bound $\ell_+(\mathcal{G}(n,d))$.* It is possible to define a new bound $\tilde{\ell}(\mathcal{G}(n,d))$, stronger than the bound $\ell_+(\mathcal{G}(n,d))$, whose computation still involves a semidefinite program of size $O(n^3)$. Namely, let us now consider as matrix variable the principal submatrix $Y(y)$ of $M_2(y)$ indexed by the set

$$\tilde{\mathcal{X}} := \{\emptyset\} \cup \{\{I\} \mid I \in \mathcal{P}\} \cup \{\{\emptyset, I\} \mid I \in \mathcal{P}\} \cup \{\{I, V\} \mid I \in \mathcal{P}\}.$$

Then, $Y(y)$ has the block structure:

$$Y(y) = \begin{pmatrix} 1 & a^T & b^T & c^T \\ a & A & B & C \\ b & B & B & D \\ c & C & D & C \end{pmatrix} \tag{40}$$

where $A = (y_{\{I,J\}})_{I,J\in\mathcal{P}}$, $B = (y_{\{\emptyset,I,J\}})_{I,J\in\mathcal{P}}$, $C = (y_{\{I,J,V\}})_{I,J\in\mathcal{P}}$, $D = (y_{\{\emptyset,I,J,V\}})_{I,J\in\mathcal{P}}$, $a = (y_{\{I\}})_{I\in\mathcal{P}}$, $b = (y_{\{\emptyset,I\}})_{I\in\mathcal{P}}$, and $c = (y_{\{I,V\}})_{I\in\mathcal{P}}$. The matrices A, B are given by (29), (30). The matrix C is a permutation of B; namely,

$$C = \sum_{i,j,t=0}^{n} x_{n-i,n-j}^{n+t-i-j} M_{i,j}^t.$$

The matrix D too belongs to the Terwiliger algebra:

$$D = \sum_{i,j,t=0}^{n} z_{i,j}^t M_{i,j}^t \text{ for some real scalars } z_{i,j}^t$$

satisfying $z_{i,j}^t = z_{j,i}^t$; indeed, $D_{I,J} = D_{I',J'}$ if there exists $\sigma \in G$ such that $\sigma(\emptyset) = \emptyset$, $\sigma(I) = I'$, $\sigma(J) = J'$ (then $\sigma(V) = V$), i.e., if $|I| = |I'|$, $|J| = |J'|$, $|I \cap J| = |I' \cap J'|$. We have the following relations for the variables $x_{i,j}^t$, $z_{i,j}^t$:

$$z_{i,j}^t = z_{n-i,n-j}^{n+t-i-j} \text{ for all } i,j,t = 0,\ldots,n \tag{41}$$

since $D_{I,J} = y_{\{\emptyset,V,I,J\}} = y_{\{\emptyset,V,V\Delta I,V\Delta J\}} = D_{V\Delta I,V\Delta J}$, and

$$z_{i,i}^i = z_{0,i}^0 = z_{n,i}^i = x_{i,n}^i \text{ for } i = 0,\ldots,n \tag{42}$$

since $y_{\{\emptyset,V,I\}} = D_{I,I} = D_{\emptyset,I} = D_{V,I} = B_{V,I}$. The edge condition for the z-variables reads:

$$z_{i,j}^t = 0 \text{ if } \{i,j,n-i,n-j,i+j-2t\} \cap \{1,\ldots,d-1\} \neq 0 \text{ for } i,j,t = 0,\ldots,n. \tag{43}$$

The bounds (20) imply:

$$0 \leq z_{i,j}^t \leq x_{i,j}^t,\ z_{i,j}^t \leq z_{i,i}^i \text{ for } i,j,t = 0,\ldots,n. \tag{44}$$

As each non-border block of the matrix $Y(y)$ in (40) belongs to the Terwiliger algebra, one can block-diagonalize $Y(y)$. Indeed, each non-border block in the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & U^T & 0 & 0 \\ 0 & 0 & U^T & 0 \\ 0 & 0 & 0 & U^T \end{pmatrix} Y(y) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & U & 0 & 0 \\ 0 & 0 & U & 0 \\ 0 & 0 & 0 & U \end{pmatrix} = \begin{pmatrix} 1 & a^TU & b^TU & c^TU \\ Ua & U^TAU & U^TBU & U^TCU \\ Ub & U^TBU & U^TBU & U^TDU \\ Uc & U^TCU & U^TDU & U^TCU \end{pmatrix}$$

is block-diagonal with respect to the same partition, with $\lfloor \frac{n}{2} \rfloor + 1$ distinct blocks labeled by $k = 0,1,\ldots,\lfloor \frac{n}{2} \rfloor$. It follows from Lemma 5 that $a^TU = (\tilde{a}^T, 0, \ldots, 0)$, $b^TU = (\tilde{b}^T, 0, \ldots, 0)$, $c^TU = (\tilde{c}^T, 0, \ldots, 0)$, where $\tilde{a} = x_{0,0}^0 \sum_{i=0}^n \binom{n}{i}^{\frac{1}{2}} \chi^{\binom{\mathcal{P}}{i}}$, $\tilde{b} = \sum_{i=0}^n x_{0,i}^0 \binom{n}{i}^{\frac{1}{2}} \chi^{\binom{\mathcal{P}}{i}}$ and $\tilde{c} = \sum_{i=0}^n x_{0,n-i}^0 \binom{n}{i}^{\frac{1}{2}} \chi^{\binom{\mathcal{P}}{i}}$ are indexed by the positions corresponding to the 0-th block. Therefore, $Y(y) \succeq 0$ if and only if

$$\begin{pmatrix} 1 & \tilde{a}^T & \tilde{b}^T & \tilde{c}^T \\ \tilde{a} & A_0 & B_0 & C_0 \\ \tilde{b} & B_0 & B_0 & D_0 \\ \tilde{c} & C_0 & D_0 & C_0 \end{pmatrix} \succeq 0, \quad \begin{pmatrix} A_k & B_k & C_k \\ B_k & B_k & D_k \\ C_k & D_k & C_k \end{pmatrix} \succeq 0 \text{ for } k = 1,\ldots,\lfloor \frac{n}{2} \rfloor \tag{45}$$

where $A_k = A_k(x)$ is as in (35), $B_k = B_k(x)$ is as in (12) and

$$C_k = \left(\sum_t \binom{n-2t}{i-k}^{-\frac{1}{2}} \binom{n-2t}{j-k}^{-\frac{1}{2}} \beta_{i,j,k}^t x_{n-i,n-j}^{n+t-i-j} \right)_{i,j=k}^{n-k},$$

$$D_k = \left(\sum_t \binom{n-2t}{i-k}^{-\frac{1}{2}} \binom{n-2t}{j-k}^{-\frac{1}{2}} \beta_{i,j,k}^t z_{i,j}^t \right)_{i,j=k}^{n-k}.$$

One can now define the bound

$$\tilde{\ell}(\mathcal{G}(n,d)) := \max 2^n x^0_{0,0} \text{ s.t. } x^t_{i,j},\ z^t_{i,j}\ (i,j,t=0,\ldots,n) \text{ satisfy } (32),(33),(34),(41),(42),(43),(44),(45). \tag{46}$$

Obviously, $A(n,d) \leq \tilde{\ell}(\mathcal{G}(n,d)) \leq \ell_+(\mathcal{G}(n,d))$, and the bound $\tilde{\ell}(\mathcal{G}(n,d))$ is again expressed via a semidefinite program of size $O(n^3)$.

3.3.4. *Some computational results.* The following trick from [11] can be used for further reduction of the number of variables. As is well known, if d is odd then $A(n,d) = A(n+1,d+1)$ and if d is even then $A(n,d)$ is attained by a code with all code words having even Hamming weights. Therefore, it suffices to compute $A(n,d)$ for d even. Then one can set certain variables to zero. Namely, for the variables $x^t_{i,j}$ present in the programs (37), (38), or (46), $x^t_{i,j} = 0$ if one of i or j is odd. Similarly, for the variables $z^t_{i,j}$ used in (46), $z^t_{i,j} = 0$ if one of n, i or j is odd. (Thus, in the case when n is odd, all variables $z^t_{i,j}$ are set to 0.)

We have tested the various bounds on several instances (n,d), in particular, on those where Schrijver's bound gave a improvement on the previously best known upper bound for $A(n,d)$. There are two instances: $(20,8)$ and $(25,6)$, for which we could find an upper bound for $A(n,d)$ (slightly) better than Schrijver's bound; namely, $\lfloor \ell_+(\mathcal{G}(25,6)) \rfloor$ and $\lfloor \tilde{\ell}(\mathcal{G}(20,8)) \rfloor$ improve the upper bound given by Schrijver by one. See the Table below (the values given there are the bounds rounded down to the nearest integer). For other instances (n,d), the bounds ℓ_+ and $\tilde{\ell}$ give an improvement over Schrijver's bound limited to some decimals, thus yielding no improved upper boud on $A(n,d)$.

(n,d)	Delsarte bound	Schrijver bound (39)	$\ell_+(\mathcal{G}(n,d))$ bound (38)	$\tilde{\ell}(\mathcal{G}(n,d))$ bound (46)
(20,8)	290	274	274	273
(25,6)	48148	47998	47997	-

References

[1] Delsarte, P. 1973. *An Algebraic Approach to the Association Schemes of Coding Theory.* [Philips Research Reports Supplements (1973) No. 10] Philips Research Laboratories, Eindhoven.

[2] Gaterman, K., P. Parrilo. 2004. Symmetry groups, semidefinite programs, and sums of squares. *Journal of Pure and Applied Algebra* **192** 95–128.

[3] Grötschel, M., Lovász, L., Schrijver A. *Geometric Algorithms and Combinatorial Optimization.* Springer-Verlag, Berlin, 1988.

[4] Lasserre, J.B. 2001a. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization* **11** 796–817.

[5] Lasserre, J.B. 2001b. An explicit exact SDP relaxation for nonlinear $0-1$ programs. In K. Aardal and A.M.H. Gerards, eds., *Lecture Notes in Computer Science* **2081** 293–303.

[6] Laurent, M. 2003. A comparison of the Sherali-Adams, Lovász-Schrijver and Lasserre relaxations for $0-1$ programming. *Mathematics of Operations Research* **28(3)** 470–496.

[7] Lovász, L. 1979. On the Shannon capacity of a graph. *IEEE Trans. Inform. Theory* **25** 1–7.

[8] Lovász, L., Schrijver, A. 1991. Cones of matrices and set-functions and $0-1$ optimization. *SIAM Journal on Optimization* **1** 166–190.

[9] R.J. McEliece, E.R. Rodemich, H.C. Rumsey. 1978. The Lovász' bound and some generalizations. *Journal of Combinatorics, Information & System Sciences* **3** 134–152.

[10] Schrijver A. 1979. A comparison of the Delsarte and Lovász bounds. *IEEE Trans. Inform. Theory* **25** 425–429.
[11] Schrijver A. 2004a. New code upper bounds from the Terwiliger algebra. Preprint.
[12] Schrijver A. 2004b. Reduction of symmetric semidefinite programs using the regular $*$-representation. Preprint.
[13] Terwiliger, P. 1992. The subconstituent algebra of an association scheme (Part I). *Journal of Applied Combinatorics* **1** 363–388.

CWI, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands
E-mail address: `monique@cwi.nl`