CentER Discussion Paper

No. 2005–66

A NOTE ON THE STABILITY NUMBER OF AN ORTHOGONALITY GRAPH

By Etienne de Klerk, Dimitrii Pasechnik

May 2005

ISSN 0924-7815

Tilburg University

A note on the stability number of an orthogonality graph

E. de Klerk* D.V. Pasechnik†

May 2, 2005

Abstract

We consider the orthogonality graph $\Omega(n)$ with 2^n vertices corresponding to the vectors $\{0,1\}^n$, two vertices adjacent if and only if the Hamming distance between them is $n/2$. We show that, for $n = 16$, the stability number of $\Omega(n)$ is $\alpha(\Omega(16)) = 2304$, thus proving a conjecture by Galliard [7]. The main tool we employ is a recent semidefinite programming relaxation for minimal distance binary codes due to Schrijver [16].

Moreover, we give a general condition for Delsarte bound on the (co)cliques in graphs of relations of association schemes to coincide with the ratio bound, and use it to show that for $\Omega(n)$ the latter two bounds are equal to $2^n/n$.

Keywords: Semidefinite programming, minimal distance codes, stability number, orthogonality graph, Hamming association scheme, Delsarte bound.

AMS subject classification: 90C22, 90C27, 05C69,05C15,

JEL code: C0, C61

1 Introduction

The graph $\Omega(n)$ and its properties

Let $\Omega(n)$ be the graph on 2^n vertices corresponding to the vectors $\{0,1\}^n$, such that two vertices are adjacent if and only if the Hamming distance between them is $n/2$. Note that $\Omega(n)$ is k-regular, where $k = \binom{n}{\frac{1}{2}n}$.

It is known that $\Omega(n)$ is bipartite if $n = 2 \bmod 4$, and empty if n is odd. We will therefore assume throughout that n is a factor of 4. The graph owns its

*Tilburg University. E-mail: e.deklerk@uvt.nl. Supported by the Netherlands Organisation for Scientific Research grant NWO 613.000.214 as well as the NSERC grant 283331 - 04. Part of this research was performed while on leave from the Department of Combinatorics and Optimization, University of Waterloo.

†Tilburg University. E-mail: d.v.pasechnik@uvt.nl. *Corresponding author.*

name to another description, in terms of ± 1-vectors. Then the orthogonality of vectors corresponds to the Hamming distance $n/2$.
Moreover, $\Omega(n)$ consists of two isomorphic components, one containing all the vertices of even Hamming weight and the other the vertices of odd Hamming weight. For a detailed discussion of the properties of $\Omega(n)$, see Godsil [9] and the PhD thesis of Newman [13].

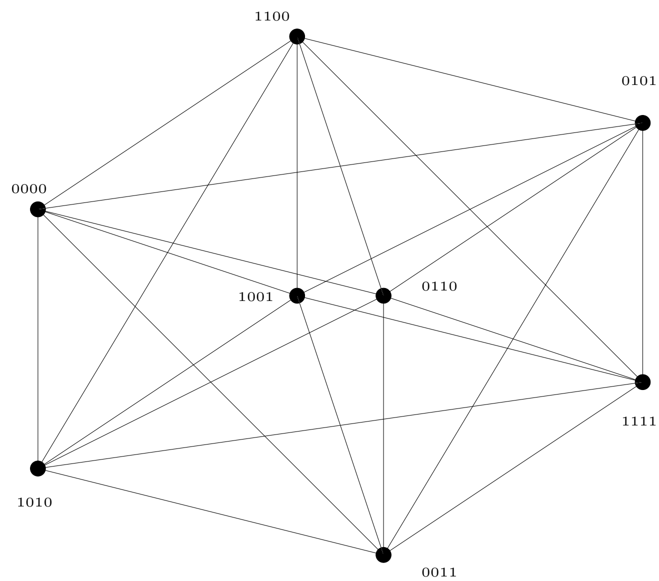

Figure 1: The connected component of $\Omega(4)$ corresponding to vertices of even Hamming weight.

In this note we study upper bounds on the stability number $\alpha(\Omega(n))$.
Galliard [7] pointed out the following way of constructing maximal stable sets in $\Omega(n)$. Consider the "odd component" of $\Omega(n)$ and take all vertices of Hamming weight $1, 3, \ldots, n/4-1$. Obviously, these vertices form a stable set of $\Omega(n)$ of size

$$\sum_{1 \le i \le n/8} \binom{n}{2i-1}. \tag{1}$$

We can double the size of this stable set by adding the bit-wise complements of the vertices in S, and double it again by taking the union with the corresponding stable set in the other (isomorphic) component.
Thus we find that

$$\alpha(\Omega(n)) \ge 4 \sum_{1 \le i \le n/8} \binom{n}{2i-1} := \underline{\alpha}(n).$$

For $n = 16$ this evaluates to $\alpha(\Omega(n)) \ge 2304$. Galliard et al [8] could show that $\alpha(\Omega(16)) \le 3912$. In this note we will show that, in fact, $\alpha(\Omega(16)) = 2304$. This was conjectured by Galliard [7], and Newman [13] has recently conjectured that the value (1) actually equals $\alpha(\Omega(n))$ whenever n is a multiple of 4.

A quantum information game

One motivation for studying the graph $\Omega(n)$ comes from quantum information theory. Consider the following game from [8].
Let $n \geq 1$ and $N = 2^n$. Two players, A and B, are asked the questions x_A and x_B, coded as N-bit strings satisfying

$$d_H(x_A, x_B) \in \left\{0, \frac{1}{2}N\right\}$$

where d_H denotes the Hamming distance. A and B win the game if they give answers y_A and y_B, coded as binary strings of length n such that

$$y_A = y_B \iff x_A = x_B.$$

A and B are not allowed any communication (except a priori deliberation).
It is known that A and B can always win the game if their n output bits are *maximally entangled quantum bits* [2] (see also [13]).
For classical bits, it was shown by Galliard et al [8] that the game cannot always be won if $n = 4$. The authors proved this by pointing out that whether or not the game can always be won is equivalent to the question

$$\chi(\Omega(n)) \leq N \equiv 2^n?$$

Indeed, if $\chi(\Omega(n)) \leq N$ then A and B may color $\Omega(n)$ a priori using N colors. The questions x_A and x_B may then be viewed as two vertices of $\Omega(n)$, and the A and B may answer their respective questions by giving the color of the vertices x_A and x_B respectively, coded as binary strings of length $\log_2 N = n$.
Galliard et al. [8] showed that $\chi(\Omega(16)) > 16$, i.e. that the game cannot be won for $n = 16$. They proved this by showing that $\alpha(\Omega(16)) \leq 3912$ which implies

$$\chi(\Omega(16)) \geq \left\lceil \frac{2^{16}}{\alpha(\Omega(16))} \right\rceil \geq \left\lceil \frac{2^{16}}{3912} \right\rceil = 17.$$

In this note we sharpen their bound by showing that $\alpha(\Omega(16)) = 2304$, which implies $\chi(\Omega(16)) \geq 21$.
Our main tool will be a semidefinite programming bound on $\alpha(\Omega(n))$ that is due to Schrijver [16], where it is formulated for minimal distance binary codes.

2 Upper bounds on $\alpha(\Omega(n))$

In this section we give a review of known upper bounds on $\alpha(\Omega(n))$ and their relationship.

2.1 The ratio bound

The following discussion is condensed from Godsil [9].

Theorem 1. Let $G = (V, E)$ be a k-regular graph with adjacency matrix $A(G)$, and let $\lambda_{\min}(A(G))$ denote the smallest eigenvalue of $A(G)$. Then

$$\alpha(G) \leq \frac{|V|}{1 - \frac{k}{\lambda_{\min}(A(G))}}. \tag{2}$$

This bound is called the *ratio bound*, and was first derived by Delsarte [4] for graphs in association schemes (see Sect. 2.2 for more on the latter).
Recall that $\Omega(n)$ is k-regular with $k = \binom{n}{\frac{1}{2}n}$. Ignoring multiplicities, the spectrum of $\Omega(n)$ is given by

$$\lambda_m = \frac{2^{\frac{1}{2}n}}{(\frac{1}{2}n)!}(m-1)(m-3)\cdots(m-n+1) \qquad (m = 1, \ldots, n). \tag{3}$$

The minimum is reached at $m = 2$, and we get

$$\lambda_{\min}(A(\Omega(n)) = \frac{2^{\frac{1}{2}n}}{(\frac{1}{2}n)!}(1)(-1)(-3)\cdots(-n+3) = -\frac{\binom{n}{\frac{1}{2}n}}{n-1}. \tag{4}$$

The ratio bound therefore becomes

$$\alpha(\Omega(n)) \leq \frac{2^n}{n}. \tag{5}$$

This is the best known upper bound on $\alpha(\Omega(n))$, but it is known that this bound is not tight: Frankl and Rödl [6] showed that there exists some $\epsilon > 0$ such that $\alpha(\Omega(n)) \leq (2-\epsilon)^n$. For specific (small) values of n one can improve on the bound (5), as we will show for $n \leq 32$.

2.2 The Delsarte bound and ϑ'

Here we are going to use more linear algebra that naturally arise around $\Omega(n)$. We recall the following definitions, cf. e.g. Bannai and Ito [1].

Association schemes. An association scheme $\mathcal{A}$ is a commutative subalgebra of the full $v \times v$-matrix algebra with a distinguished basis $(A_0 = I, A_1, \ldots, A_n)$ of 0-1 matrices. One often views A_j, $j \geq 1$, as the adjacency matrix of a graph on v vertices; A_j is often referred to as the j-th *relation* of $\mathcal{A}$. As the A_j's commute, they have $n+1$ common eigenspaces V_i. Then $\mathcal{A}$ is isomorphic, as an algebra, to the algebra of diagonal matrices diag $(P_{0,j}, \ldots, P_{n,j})$, where P_{ij} denotes the eigenvalue of A_j on V_i. The matrix $P = (P_{ij})$ is called *first eigenvalue matrix* of $\mathcal{A}$. The set of A_j's is closed under taking transpositions: for each $0 \leq j \leq n$ there exists j' so that $A_j = A_{j'}^T$. In particular, $P_{ij} = \overline{P_{ij'}}$. An association scheme with all A_j symmetric is called *symmetric*, and here we shall consider such schemes only. There is a matrix Q (called *second eigenvalue matrix*) satisfying $PQ = QP = vI$. In what follows it is assumed (as is customary in the literature) that the eigenspace V_0 corresponds to the eigenvector $(1, \ldots, 1)$; then the 0-th row of P consists of the degrees v_j of the graphs A_j. It is remarkable that the 0-th row of Q consists of dimensions of V_i.

Let ϑ' denote the Schrijver ϑ'-function [15]:

$$\vartheta'(G) = \max \{ \mathrm{Tr}\,(JX) \;:\; \mathrm{Tr}\,(AX) = 0,\ \mathrm{Tr}(X) = 1,\ X \succeq 0,\ X \geq 0 \}.$$

For any graph G one has $\alpha(G) \leq \vartheta'(G)$. Moreover, $\vartheta'(G)$ is smaller than or equal to the ratio bound (2) for regular graphs, as noted by Godsil [9, Sect. 3.7]. For graphs with adjacency matrices of the form $\sum_{j \in \mathcal{M}} A_j$, with $\mathcal{M} \subset \{1, \ldots, n\}$ and A_j's from the 0-1 basis of an association scheme $\mathcal{A}$, the bound ϑ' coincides, as was proved by Schrijver [15], with the following bound due to Delsarte [3, 4]

$$\max 1^T w \text{ subject to } w \geq 0,\ Q^T w \geq 0,\ w_0 = 1, w_j = 0 \text{ for } j \in \mathcal{M}, \tag{6}$$

where Q is the second eigenvalue matrix of $\mathcal{A}$.
The bound (6) is often stated for (and was originally developed for) bounding the maximal size of a q-ary code of length n and minimal distance d; then the association scheme $\mathcal{A}$ becomes the Hamming distance association scheme $H(n, q)$ and $\mathcal{M} = \{1, \ldots, d-1\}$. The relations of $H(n, q)$ can be viewed as graphs on the vertex set of n-strings on $\{0, \ldots, q-1\}$: the j-th graph of $H(n, q)$ is given by

$$(A_j)_{XY} = \begin{cases} 1 & \text{if } d_H(X, Y) = j \\ 0 & \text{otherwise} \end{cases}$$

For $H(n, q)$ the first and the second eigenvalue matrices P and Q coincide, and are given by $P_{ij} = K_i(j)$, where K_k is the *Krawtchouk polynomial*

$$K_k(x) := \sum_{j=0}^{n} (-1)^j (q-1)^{k-j} \binom{x}{j} \binom{n-x}{k-j}.$$

For $\Omega(n)$, the bound (6) is as above with $\mathcal{A} = H(n, 2)$ and $\mathcal{M} = \{\frac{n}{2}\}$. Newman [13] has shown computationally that $\vartheta'(\Omega(n)) = 2^n/n$ if $n \leq 64$, i.e. the ratio and ϑ' bounds coincide for $\Omega(n)$ if $n \leq 64$. We show that it is the case for all n, as an easy consequence of the following.

Proposition 1. Let $\mathcal{A}$ be an association scheme with the 0-1 basis $(A_0, \ldots, A_n)$ and eigenvalue matrices P and Q. Let A_r have the least eigenvalue $\tau = P_{\ell r}$ and assume

$$v_r P_{\ell i} \geq v_i \tau, \quad 0 \leq i \leq n.$$

Then the Delsarte bound (6), with $\mathcal{M} = \{r\}$, and the ratio bound (2) for A_r coincide.

Proof. Let P_j denote the j-th row of P.

As we already mentioned, the bound (2) for regular graphs always majorates (6). Thus it suffices to present a feasible vector for the LP in (6) that gives the objective value the same as (2).
We claim that

$$a = \frac{-\tau}{v_r - \tau} P_0 + \frac{v_r}{v_r - \tau} P_\ell$$

is such a vector. It is straighforward to check that $a_0 = 1$ and $a_r = 0$, as required. By the assumption of the proposition, $a \geq 0$. As $PQ = vI$, any nonnegative linear combination z of the rows of P satisfies $Q^T z \geq 0$. As a is such a combination, we obtain $Q^T a \geq 0$.
Finally, to compute $1^T a$, note that $1^T P_0 = v$ and $1^T P_\ell = 0$. □

Corollary 1. The bounds (6) and (2) coincide for $\Omega(n)$.

Proof. We apply Proposition 1 to $\mathcal{A} = H(n, 2)$ and $r = \frac{n}{2}$. Then the eigenvalues of $A_r = \Omega(n)$ given in (3) comprise the r-th column on P, in particular the least eigenvalue τ equals $P_{2,r}$, by (4) above. The assumption of the proposition translates into[1]

$$\binom{n}{\frac{n}{2}} K_i(2) - \binom{n}{i} K_{\frac{n}{2}}(2) = \frac{2^{\frac{n}{2}+2}(n-2)!(n-1)!!(\frac{n}{2} - i)^2}{i!(\frac{n}{2})!(n-i)!} \geq 0,$$

as claimed. □

2.3 Schrijver's improved SDP-based bound

Recently, Schrijver [16] has suggested a new SDP-based bound for minimal distance codes, that is at least as good as the ϑ' bound, and still of size polynomial in n. It is given as the optimal value of a semidefinite programming (SDP) problem.
In order to introduce this bound (as applied to $\alpha(\Omega(n))$) we require some notation.
For $i, j, t \in \{0, 1, \ldots, n\}$, and $X, Y \in \{0, 1\}^n$ define the matrices

$$\left(M_{i,j}^t\right)_{X,Y} = \begin{cases} 1 & \text{if } |X| = i,\ |Y| = j,\ d_H(X, Y) = n - t \\ 0 & \text{otherwise} \end{cases}$$

The upper bound is given as the optimal value of the following semidefinite program:

$$\bar{\alpha}(n) := \max \sum_{i=0}^{n} \binom{n}{i} x_{i,0}^0$$

subject to

$$\begin{aligned} x_{0,0}^0 &= 1 \\ 0 &\leq x_{i,j}^t \leq x_{i,0}^0 \text{ for all } i, j, t \in \{0, \ldots, n\} \\ x_{i,j}^t &= x_{i',j'}^{t'} \text{ if } \{i', j', i' + j' - 2t'\} \text{ is a permutation of } \{i, j, i + j - 2t\} \\ x_{i,j}^t &= 0 \text{ if } \{i, j, i + j - 2t\} \cap \{\tfrac{1}{2}n\} \neq \emptyset, \end{aligned}$$

[1] Here $m!! = m(m-2)(m-4)\ldots$, the *double factorial*.

as well as

$$\sum_{i,j,t} x_{i,j}^t M_{i,j}^t \succeq 0, \ \sum_{i,j,t} \left(x_{i+j-2t,0}^0 - x_{i,j}^t\right) M_{i,j}^t \succeq 0.$$

The matrices $M_{i,j}^t$ are of order 2^n and therefore too large to compute with in general. Schrijver pointed out that these matrices form a basis of the Terwilliger algebra of the Hamming scheme, and worked out the details for computing the irreducible block diagonalization of this (non-commutative) matrix algebra of dimension $O(n^3)$.

Thus, analogously to the ϑ'-case, the constraint $\sum_{i,j,t} x_{i,j}^t M_{i,j}^t \succeq 0$ is replaced by

$$\sum_{i,j,t} x_{i,j}^t Q^T M_{i,j}^t Q \succeq 0$$

where Q is an orthogonal matrix that gives the irreducible block diagonalization. For details the reader is referred to Schrijver [16]. Since SDP solvers can exploit block diagonal structure, this reduces the sizes of the matrices in question to the extent that computation is possible in the range $n \leq 32$.

2.4 Laurent's improvement

In Laurent [12] one finds a study placing the relaxation [16] into the framework of *moment sequences* of [10, 11]. This study also explains the relationship with known lift-and-project methods for obtaining hierarchies of upper bounds on $\alpha(G)$.

Moreover, Laurent [12] suggests a refinement of the Schrijver relaxation that takes the following form:

$$l_+(n) := \max 2^n x_{0,0}^0$$

subject to

$$\begin{aligned} 0 &\leq x_{i,j}^t \leq x_{i,0}^0 \text{ for all } i,j,t \in \{0,\ldots,n\} \\ x_{i,j}^t &= x_{i',j'}^{t'} \text{ if } \{i',j',i'+j'-2t'\} \text{ is a permutation of } \{i,j,i+j-2t\} \\ x_{i,j}^t &= 0 \text{ if } \{i,j,i+j-2t\} \cap \{\tfrac{1}{2}n\} \neq \emptyset, \end{aligned}$$

as well as

$$\sum_{i,j,t} x_{i,j}^t M_{i,j}^t \succeq 0$$

and

$$\begin{pmatrix} 1 - x_{0,0}^0 & c^T \\ c & \sum_{i,j,t} \left(x_{i+j-2t,0}^0 - x_{i,j}^t\right) M_{i,j}^t \end{pmatrix} \succeq 0,$$

where $c := \sum_{i=0}^n \left(x_{0,0}^0 - x_{0,i}^0\right) \chi_i$, and χ_i is defined by

$$(\chi_i)_X := \begin{cases} 1 & \text{if } |X| = i \\ 0 & \text{else.} \end{cases}$$

This SDP problem may be block-diagonalised as before to obtain an SDP of size $O(n^3)$.

3 Computational results

To summarize, the bounds we have mentioned satisfy:

$$\underline{\alpha}(n) \leq \alpha(\Omega(n)) \leq l^+(n) \leq \bar{\alpha}(n) \leq \vartheta'(\Omega(n)) = 2^n/n.$$

In Table 1 we show the numerical values for $\bar{\alpha}(n)$ and $l_+(n)$ that were obtained using the SDP solver SeDuMi by Sturm [17], with Matlab 7 on a Pentium IV machine with 1GB of memory. The Maltab routines that we have written to generate the corresponding SeDuMi input are available online [14].

n	$\underline{\alpha}(n)$	$l_+(n)$	$\bar{\alpha}(n)$	$\vartheta'(\Omega(n)) = \lfloor 2^n/n \rfloor$
16	2304	2304	2304	4096
20	20,144	20,166.62	20,166.98	52,428
24	178,208	183,373	184,194	699,050
28	406,336	1,883,009	1,848,580	9,586,980
32	14,288,896	21,103,609	21,723,404	134,217,728

Table 1: Lower and upper bounds on $\alpha(\Omega(n))$.

Note that the lower and upper bounds coincide for $n = 16$, proving that $\alpha(\Omega(16)) = 2304$. The best previously known upper bound, obtained by an *ad hoc* method, was $\alpha(\Omega(16)) \leq 3912$ [8].
The value $\bar{\alpha}(20) = 20,166.98$ implies that

$$\alpha(\Omega(20)) \in \{20144, 20148, 20152, 20156, 20160, 20164\}$$

since $\alpha(\Omega(n))$ is always a factor of 4. Another implication is that $n = 20$ is the smallest value of n where the upper bounds $\bar{\alpha}(n)$ and $l_+(n)$ are not tight.
It is worth noticing that the Schrijver and Laurent bounds ($\bar{\alpha}(n)$ and $l_+(n)$ respectively) give relatively big improvements over the Delsarte bound $\frac{2^n}{n}$. This is in contrast to the relatively small improvements that these bounds give for binary codes, cf. [16, 12]. We also note that these relaxations are numerically ill-conditioned for $n \geq 24$. This makes it difficult to solve the corresponding SDP problems to high accuracy. The recent study by De Klerk, Pasechnik, and Schrijver [5] suggests a different way to solve such SDP problems, leading to larger SDP instances, but which may avoid the numerical ill-conditioning caused by performing the irreducible block factorization.

Acknowledgements

The authors would like to thank Chris Godsil for communicating this problem to them and for fruitful comments, and Willem Haemers, Mike Newman and Lex Schrijver for useful discussions.

References

[1] E. Bannai, T. Ito. Algebraic Combinatorics I. Benjamin/Cummings Publishing Company, London 1984.

[2] G. Brassard, R. Cleve, and A. Tapp. The cost of exactly simulating quantum entanglement with classical communication. *Physical Review Letter*, 83(9):1874–1878, 1999.

[3] P. Delsarte, Bounds for unrestricted codes, by linear programming, Philips Res. Rep. 27, 272–289, 1972.

[4] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Research Repts Suppl. 10, 1–97, 1973.

[5] E. de Klerk, D.V. Pasechnik, and A. Schrijver. Reduction of symmetric semidefinite programs using the regular *-representation. Preprint, 2005. Available at `http://www.optimization-online.org`.

[6] P. Frankl and V. Rödl, Forbidden intersections, Trans. AMS 300, 259-286, 1987.

[7] V. Galliard. Classical pseudo telepathy and coloring graphs. Diploma thesis, ETH Zurich, 2001. Available at `http://math.galliard.ch/Cryptography/Papers/PseudoTelepathy/SimulationOfEntanglement.pdf`

[8] V. Galliard, A. Tapp and S. Wolf. The impossibility of pseudo-telepathy without quantum entanglement. Preprint, 2002.

[9] C. Godsil. Interesting graphs and their colourings. Lecture notes, University of Waterloo, ON, Canada, N2L 3G1. Available at `http://quoll.uwaterloo.ca`

[10] J. Lassere. Global optimization with polynomials and the problem of moments. *SIAM J.Optim.*, 11(3):796–817, 2001.

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

[12] M. Laurent. Strengthened semidefinite bounds for codes. Preprint, 2005. Available at `http://homepages.cwi.nl/~monique/`

[13] M. W. Newman. Independent Sets and Eigenspaces. PhD thesis, University of Waterloo, Waterloo, Canada, 2004. Available at: `http://www.math.uwaterloo.ca/~mwnewman/thesis.pdf`

[14] `http://stuwww.uvt.nl/~dpasech/code/matlab/`

[15] A. Schrijver. A comparison of the Delsarte and Lovász bounds. *IEEE Trans. Inform. Theory*, 25(4):425–429, 1979.

[16] A. Schrijver. New code upper bounds from the Terwilliger algebra. To appear in *IEEE Transactions on Information Theory*, 2004. Available at `http://homepages.cwi.nl/~lex/`

[17] J.F. Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization Methods and Software*, 11-12:625–653, 1999.