THE INDEPENDENCE NUMBER OF THE ORTHOGONALITY GRAPH IN DIMENSION 2^k

FERDINAND IHRINGER AND HAJIME TANAKA

Abstract. We determine the independence number of the orthogonality graph on 2^k-dimensional hypercubes. This answers a question by Galliard from 2001 which is motivated by a problem in quantum information theory. Our method is a modification of a rank argument due to Frankl who showed the analogous result for $4p^k$-dimensional hypercubes, where p is an odd prime.

1. Introduction

The *orthogonality graph* Ω_n has the elements of $\{-1,1\}^n$ as vertices, and two vertices are adjacent if they are orthogonal, in other words, if their Hamming distance is $n/2$. The graph Ω_n occurs naturally when comparing classical and quantum communication [3]. In particular, for $n = 2^k$ the cost of simulating a specific quantum entanglement on k qubits can be reduced to determining the chromatic number $\chi(\Omega_n)$ of Ω_n [2, 9]. The graph Ω_n is edgeless if n is odd, and is bipartite if $n \equiv 2 \pmod 4$. For $n \equiv 0 \pmod 4$, Frankl [7] and Galliard [9] constructed an independent set of Ω_n of size

$$a_n := 4 \sum_{i=0}^{n/4-1} \binom{n-1}{i},$$

and Galliard [9] asked in 2001 if this is the independence number $\alpha(\Omega_n)$ of Ω_n when $n = 2^k$, $k \geqslant 2$. Newman [15] and, according to [8, p. 275, Remark], Frankl conjectured that this holds whenever $n \equiv 0 \pmod 4$. See also [4]. Frankl [7] already showed the conjecture in 1986 for all $n = 4p^k$ for $k \geqslant 1$, where p is an odd prime. De Klerk and Pasechnik [13] proved the conjecture for $n = 16$, i.e., that $\alpha(\Omega_{16}) = 2304$, using Schrijver's semidefinite programming bound [16]. Furthermore, Frankl and Rödl [8] showed that $\alpha(\Omega_n) < 1.99^n$ if $n \equiv 0 \pmod 4$. In this note, we apply Frankl's method from [7] to show the following:

Theorem. *Let $n = 2^k$ for some $k \geqslant 2$. Then $\alpha(\Omega_n) = a_n$.*

Together with the discussion in [9, Section 5.5], that is using $\chi(\Omega_n) \geqslant 2^n/\alpha(\Omega_n)$, our result implies an explicit version of Theorem 4 in [2]. Finding such an explicit result is one motivation for Galliard's work. See also [10, 12].

The first author is supported by a postdoctoral fellowship of the Research Foundation — Flanders (FWO).

The second author is supported by JSPS KAKENHI Grant Number JP17K05156.

2. Proof of the Theorem

Let A_j be the 0-1-matrix indexed by the vertices of the hypercube $Q_n = \{-1,1\}^n$ with $(A_j)_{xy} = 1$ if x and y have Hamming distance j. The matrices A_j have $n+1$ common eigenspaces $V_0, V_1, \dots, V_n$, and in the usual ordering of the eigenspaces the eigenvalue of A_j with respect to V_i is given by the Krawtchouk polynomial (see [5, Theorem 4.2])

$$K_j(i) = K_j(i;n) := \sum_{h=0}^{j} (-1)^h \binom{i}{h}\binom{n-i}{j-h}.$$

It is known that the orthogonal projection matrix E_i onto V_i has the entry $(E_i)_{xy} = 2^{-n}K_i(j)$ if x and y are at Hamming distance j [5, Theorem 4.2], so that we have in particular $\operatorname{rank} E_i = \operatorname{trace} E_i = K_i(0) = \binom{n}{i}$. The $(n+1)$-dimensional matrix algebra spanned by $A_0 = I, A_1, \dots, A_n$ is called the *Bose–Mesner algebra* of Q_n.

Assume now that $n = 2^k$, $k \geqslant 3$. (The result is trivial if $k = 2$.) Let C be an independent set of Ω_{2^k}, and let $C^{\pm}_{\text{even}}, C^{\pm}_{\text{odd}} \subseteq \{-1,1\}^{2^k-1}$ be as in [7]: C^{+}_{even} is given by taking all the even-weight elements of C that end with $+1$, followed by truncating at the last coordinate, and the other three are analogous. Let C' be one of these four families. Then the Hamming distances in C' are even and unequal to 2^{k-1}, so they lie in the following set:

$$\{2s : s = 0, 1, \dots, 2^{k-1}-1,\ s \neq 2^{k-2}\}. \tag{1}$$

Below we work with the Bose–Mesner algebra $\mathscr{A}$ of Q_{2^k-1}. For every $M \in \mathscr{A}$, let $\overline{M}$ denote the principal submatrix corresponding to C'. Consider the polynomial

$$\varphi(\xi) = \binom{\xi/2 - 1}{2^{k-2}-1} \in \mathbb{R}[\xi],$$

and expand it in terms of the Krawtchouk polynomials $K_i(\xi) = K_i(\xi; 2^k - 1)$:

$$\varphi(\xi) = \sum_{i=0}^{2^{k-2}-1} c_i K_i(\xi). \tag{2}$$

Let

$$X = \sum_{j=0}^{2^k-1} \varphi(j) A_j \in \mathscr{A}.$$

On the one hand, observe that $\overline{X}$ has only integral entries in view of (1), and an easy application of Lucas' theorem (cf. [6]) shows moreover that $\overline{X} \equiv \overline{I} \pmod 2$. In particular, $\overline{X}$ is invertible. On the other hand, from (2) we have

$$X = 2^{2^k-1} \sum_{i=0}^{2^{k-2}-1} c_i E_i.$$

It follows that

$$|C'| = \operatorname{rank} \overline{X} \leqslant \operatorname{rank} X \leqslant \sum_{i=0}^{2^{k-2}-1} \operatorname{rank} E_i = \sum_{i=0}^{2^{k-2}-1} \binom{2^k-1}{i}.$$

As $|C| = |C^{+}_{\text{even}}| + |C^{-}_{\text{even}}| + |C^{+}_{\text{odd}}| + |C^{-}_{\text{odd}}|$, the theorem follows.

3. Future Work

Schrijver's semidefinite programming bound has been extended to hierarchies of upper bounds; see, e.g., [1, 14]. In view of [13], it is interesting to investigate if these bounds in turn prove the conjecture for other values of n. One of the referees pointed out to us that using next level in the hierarchy, see [11], yields the correct bound of $a_{24} = 178208$ for the case $n = 24$.

Problem. Prove the conjecture for $n = 40$, which is the first open case.

Acknowledgements. We thank the anonymous referee for solving the case $n = 24$.

References

[1] C. Bachoc, D. C. Gijswijt, A. Schrijver, and F. Vallentin, Invariant semidefinite programs, in: Handbook on semidefinite, conic and polynomial optimization (M. F. Anjos and J. B. Lasserre, eds.), Springer, New York, 2012, pp. 219–269; arXiv:1007.2905.

[2] G. Brassard, R. Cleve, and A. Tapp, Cost of exactly simulating quantum entanglement with classical communication, Phys. Rev. Lett. 83 (1999) 1874–1877; arXiv:quant-ph/9901035.

[3] H. Buhrman, R. Cleve, and A. Widgerson, Quantum vs. classical communication and computation, in: Proceedings of the 30th Annual ACM Symposium on the Theory of Computing, Dallas, TX, USA, 1998, pp. 63–68; arXiv:quant-ph/9802040.

[4] P. J. Cameron, Problems from CGCS Luminy, May 2007, European J. Combin. 31 (2010) 644–648.

[5] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl., No. 10, 1973.

[6] N. J. Fine, Binomial coefficients modulo a prime, Amer. Math. Monthly 54 (1947) 589–592.

[7] P. Frankl, Orthogonal vectors in the n-dimensional cube and codes with missing distances, Combinatorica 6 (1986) 279–285.

[8] P. Frankl and V. Rödl, Forbidden intersections, Trans. Amer. Math. Soc. 300 (1987) 259–286.

[9] V. Galliard, Classical pseudo-telepathy and colouring graphs, diploma thesis, ETH Zurich, 2001; available at `http://math.galliard.ch/Cryptography/Papers/PseudoTelepathy/SimulationOfEntanglement.pdf` .

[10] V. Galliard, A. Tapp, and S. Wolf, The impossibility of pseudo-telepathy without quantum entanglement, in: Proceedings 2003 IEEE International Symposium on Information Theory, Yokohama, Japan, 2003; arXiv:quant-ph/0211011.

[11] D. C. Gijswijt, H. D. Mittelmann, and A. Schrijver, Semidefinite code bounds based on quadruple distances, IEEE Trans. Inform. Theory 58 (2012) 2697–2705; arXiv:1005.4959.

[12] C. D. Godsil and M. W. Newman, Coloring an orthogonality graph, SIAM J. Discrete Math. 22 (2008) 683–692; arXiv:math/0509151.

[13] E. de Klerk and D. V. Pasechnik, A note on the stability number of an orthogonality graph, European J. Combin. 28 (2007) 1971–1979; arXiv:math/0505038.

[14] M. Laurent, Strengthened semidefinite programming bounds for codes, Math. Program. 109 (2007) 239–261.

[15] M. W. Newman, Independent sets and eigenspaces, thesis, University of Waterloo, 2004.

[16] A. Schrijver, New code upper bounds from the Terwilliger algebra and semidefinite programming, IEEE Trans. Inform. Theory 51 (2005) 2859–2866.

Department of Mathematics: Analysis, Logic and Discrete Mathematics, Ghent University, Belgium

Email address: `ferdinand.ihringer@ugent.be`

Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Japan

Email address: `htanaka@tohoku.ac.jp`