A note on Witsenhausen′s lemma

Chih-Chieh Chen[†], Shi-Chun Tsai[*], and Ming-Chuan Yang[†]
Department of Computer Science,
National Chiao Tung University, Hsinchu, Taiwan
[*] sctsai@cs.nctu.edu.tw, [†‡] {ccchen, mcyangcs}@nctu.edu.tw

Abstract

In this note, we give a simpler and more intuitive proof of Witsenhausen′s lemma. For an addressing of a graph G, it is required that the distance of any two vertices in G is equal to the distance of their addresses. Witsenhausen′s lemma states that the minimum length of an addressing of G is at least the maximum of the number of positive and negative eigenvalues of the distance matrix of G.

1 INTRODUCTION

The well-known Graham-Pollak Theorem[5, 10] shows that any partition set of the edges of K_n consists at least $n-1$ complete bipartite graphs. Graham and Pollak proved it in their seminal paper as a corollary of Witsenhausen′s lemma [5] that is a consequence of some properties of quadratic forms and the Sylvesters Law of Inertia. The inertia of a square matrix is the ordered triple of the number of positive, zero, and negative eigenvalues. Due to wide applications, generalizations and extensions of the inertia of the distance matrix corresponding to a graph [1, 2, 8], it still draws attention of researchers. In fact, there have been more than five different proofs, without applying Witsenhausen′s inequality, since Graham and Pollak had published their paper [4, 7, 9, 11, 12]. Our aim in this note is to give an elementary and more intuitive proof of Witsenhausen′s inequality.

We review some background as follows. For a network of computers it is desirable to be able to send a message from the source to the destination without the destination knowing that a message is on its way [10]. We can model the network as a graph G and assign an address for each vertex. The address is from $\{0, 1\}^k$. Sometimes we need an extra symbol '*' to make it possible. The distance of two vertices in the graph is equal to the Hamming distance of the addresses. Thus, we consider addresses from $\{0, 1, *\}^k$. The distance between two addresses is defined to be the number of places where one has a 0 and the other a 1. For an addressing of a graph G, we require that the distance of any two vertices in G is equal to the distance of their addresses. Denote by $N(G)$ the minimum value of N for which there exists an addressing of G with length N.

2 The New Proofs

Theorem 1. *(Witsenhausen′s inequality [5]) Let n^+, respectively n^-, be the number of positive, respectively negative, eigenvalues of the distance matrix (d_{ij}) of the graph G. Then $N(G) \geq \max\{n^+, n^-\}$.*

We aim at giving a simpler and more intuitive proof of the above Theorem. We first prove the following lemma, which yields a simpler proof.

Theorem 2. [1] *Let A and B be two symmetric (or Hermitian) matrices. Then $n^+(A+B) \leq n^+(A) + n^+(B)$. It is also true for n^-.*

To prove Theorem 2, we use a known result for the eigenvalues of Hermitian matrices.

Lemma 3. *[6] If A is Hermitian and $x^*Ax > 0$ for all non-zero vectors x in a k-dimensional subspace, then A has at least k positive eigenvalues, i.e. $n^+(A) \geq k$.*

2.1 Proof of Theorem 2

Proof. For convenience, let $k = n^+(A+B), k_a = n^+(A)$ and $k_b = n^+(B)$. Let $u_1, \ldots, u_k$ be the orthonormal eigenvectors corresponding to the positive eigenvalues of $A+B$. It is clear that for any real vector x with $x^*(A+B)x > 0$ we have

[1] This theorem is a special case of Thm 2.8.1 in [3].

$x^*Ax > 0$ or $x^*Bx > 0$. Thus, $u_i^*Au_i > 0$ or $u_i^*Bu_i > 0$ for $i = 1, \ldots, k$.

If $k > k_a + k_b$, then $u_i^*Au_i > 0$ holds for more than k_a u_i's or $u_i^*Bu_i > 0$ holds for more than k_b u_i's. In either case, the satisfying u_i's form a subspace. While by Lemma 3, it implies $n^+(A) > k_a$ or $n^+(B) > k_b$. This is impossible! Therefore, we have $k \leq k_a + k_b$.

□

2.2 Proof of Theorem 1

To illustrate the idea, we consider the following example. Let A be the distance matrix of a graph as follows, where $V(G) = \{1, 2, 3, 4, 5\}$ and $A(i, j)$ is the distance between vertex i and vertex j.

$$A = \begin{pmatrix} 0 & 1 & 2 & 2 & 3 \\ 1 & 0 & 1 & 1 & 2 \\ 2 & 1 & 0 & 1 & 1 \\ 2 & 1 & 1 & 0 & 1 \\ 3 & 2 & 1 & 1 & 0 \end{pmatrix}$$

Let the following be a possible labeling, where the variable x_i relates to the address of the vertex i. For each column, there is a corresponding quadratic form. In this example we have: $(x_1 + x_2)(x_4 + x_5)$, $x_1(x_2 + x_3 + x_4 + x_5)$, $(x_1 + x_4)(x_3 + x_5)$, $x_2(x_3 + x_5)$ and x_3x_5. Summing up the quadratic forms, we have the form $\sum_{(i,j)} d_{i,j}x_ix_j$, where $d_{i,j}$ is the distance between vertex i and vertex j.

	1	2	3	4	5
x_1	1	1	1	$*$	$*$
x_2	1	0	$*$	1	$*$
x_3	$*$	0	0	0	1
x_4	0	0	1	$*$	$*$
x_5	0	0	0	0	0

Let $x = (x_1, \ldots, x_5)^t$ be a vector. Then each quadratic form can be represented as $x^tBx/2$ with some 0-1 symmetric matrix B of rank 2 and trace 0. Such matrix has two non-zero eigenvalues. In general, if x_ix_j appears in a quadratic form, then put '1' at the entries $B(i, j)$ and $B(j, i)$. So B is clearly symmetric with trace 0 and rank 2.

Proof. Let A be the distance matrix of G and suppose we can label the graph with $\{0, 1, *\}^N$ and preserve the distance, where N is the length of the address. Then there will be N quadratic forms, each relates to a 0-1 symmetric matrix of rank 2 and trace 0. The sum of these N matricies is simply A. I.e., there is a sequence of N matricies, $B_1, \ldots, B_N$ with $A = \sum_{i=1}^N B_i$. Since each B_i has rank 2 and trace 0, B_i has exactly one positive eigenvalue and one negative eigenvalue, i.e. $n^+(B_i) = n^-(B_i) = 1$. Initially, let A be the zero matrix, which implies $n^+(A) = n^-(A) = 0$. Then add the B_i's to A one by one. By Theorem 2, each time we add B_i to A, $n^+(A)$ and $n^-(A)$ each increases at most by 1. Thus it is clear there should be at least $\max\{n^+(A), n^-(A)\}$ additions, i.e. $N \geq \max\{n^+(A), n^-(A)\}$. This completes the proof.

□

3 Acknowledgements

We thank the anonymous reviewers for their comments. This work was supported in parts by the Ministry of Science and Technology of Taiwan under contracts MOST 104-2221-E-009-046 and MOST 104-2622-8-009-001.

References

[1] Aalipour, G., Abiad, A., Berikkyzy, Z., Cummings, J., De Silva, J., Gao, W., Heysse, K., Hogben, L., Kenter, F. H., Lin, J. C.-H., et al. On the distance spectra of graphs. *Linear Algebra and its Applications 497* (2016), 66–87.

[2] Alon, N., Bohman, T., and Huang, H. More on the bipartite decomposition of random graphs. *Journal of Graph Theory 84*, 1 (2017), 45–52.

[3] Brouwer, A. E., and Haemers, W. H. *Spectra of graphs.* Springer Science & Business Media, 2011.

[4] Cioabă, S. M., and Tait, M. Variations on a theme of graham and pollak. *Discrete Mathematics 313*, 5 (2013), 665–676.

[5] Graham, R. L., and Pollak, H. O. On the addressing problem for loop switching. *Bell System Technical Journal 50*, 8 (1971), 2495–2519.

[6] Horn, R., and Johnson, C. *Matrix analysis.* Cambridge University Press, 1990.

[7] Peck, G. A new proof of a theorem of graham and pollak. *Discrete Mathematics 49*, 3 (1984), 327 – 328.

[8] Sawa, M. On a symmetric representation of hermitian matrices and its applications to graph theory. *Journal of Combinatorial Theory, Series B 116* (2016), 484–503.

[9] Tverberg, H. On the decomposition of kn into complete bipartite graphs. *Journal of Graph Theory 6*, 4 (1982), 493–494.

[10] van Lint, J. H., and Wilson, R. M. *A course in combinatorics*. Cambridge University Press, 2001.

[11] Vishwanathan, S. A polynomial space proof of the graham–pollak theorem. *Journal of Combinatorial Theory, Series A 115*, 4 (2008), 674–676.

[12] Vishwanathan, S. A counting proof of the graham–pollak theorem. *Discrete Mathematics 313*, 6 (2013), 765–766.