AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **94(2)** (2026), Pages 300–304

A new upper bound for codes with a single Hamming distance

Gábor Hegedüs

Óbuda University
Bécsi út 96/B, Budapest, H-1037
Hungary
hegedus.gabor@uni-obuda.hu

Abstract

In this short note we give a new upper bound for the size of a set family with a single Hamming distance. Our proof is an application of the linear algebra bound method.

1 Introduction

Throughout the paper n denotes a positive integer and $[n]$ stands for the set $\{1, 2, \ldots, n\}$. We denote the family of all subsets of $[n]$ by $2^{[n]}$.

Let $\mathcal{F} \subseteq 2^{[n]}$ be a family of subsets and $F, G \in \mathcal{F}$ be two distinct elements of $\mathcal{F}$. Let $d_H(F, G)$ denote the Hamming distance of the sets F and G, i.e., $d_H(F, G) := |F \Delta G|$, where $F \Delta G$ is the usual symmetric difference.

Let $q > 1$ be an integer. Let $\{0, 1, \ldots, q-1\}^n$ denote the set of length n vectors with entries from $\{0, 1, \ldots, q-1\}$. Let $\mathcal{H} \subseteq \{0, 1, \ldots, q-1\}^n$ and let $\mathbf{h}_1, \mathbf{h}_2 \in \mathcal{H}$ be two elements of the vector system $\mathcal{H}$. Let $d_H(\mathbf{h}_1, \mathbf{h}_2)$ stand for the Hamming distance between the vectors $\mathbf{h}_1, \mathbf{h}_2 \in \mathcal{H}$:

$$d_H(\mathbf{h}_1, \mathbf{h}_2) := |\{i \in [n] : \ (\mathbf{h}_1)_i \neq (\mathbf{h}_2)_i\}|.$$

Delsarte proved the following remarkable upper bound for the size of the vectors systems with s distinct Hamming distances in [3], [4]. Babai, Snevily and Wilson gave a different proof of this upper bound in [2], which used the polynomial method.

Theorem 1.1 *Let $0 < s \leq n$ and $q > 1$ be positive integers. Let $L = \{\ell_1, \ldots, \ell_s\} \subseteq [n]$ be a set of s positive integers. Let $\mathcal{H} \subseteq \{0, 1, \ldots, q-1\}^n$ and suppose that $d_H(\mathbf{h}_1, \mathbf{h}_2) \in L$ for each distinct $\mathbf{h}_1, \mathbf{h}_2 \in \mathcal{H}$. Then*

$$|\mathcal{H}| \leq \sum_{i=0}^{s} \binom{n}{i} (q-1)^i.$$

ISSN: 2202-3518

In the special case $q = 2$ we get the following statement.

Corollary 1.2 *Let $0 < s \leq n$ be positive integers. Let $L = \{\ell_1, \dots, \ell_s\} \subseteq [n]$ be a set of s positive integers. Let $\mathcal{F} \subseteq 2^{[n]}$ be a set system such that $d_H(F, G) \in L$ for each distinct $F, G \in \mathcal{F}$. Then*

$$|\mathcal{F}| \leq \sum_{j=0}^{s} \binom{n}{j}.$$

Our main result, Theorem 1.3, is inspired by the nonuniform version of Fisher's inequality (see [8], [6]).

Theorem 1.3 *Let $\mathcal{F} = \{F_1, \dots, F_m\}$ be a family of subsets of $[n]$ such that there exists a positive integer λ with $d_H(F_i, F_j) = \lambda$ for each $i \neq j$. Then $m = |\mathcal{F}| \leq n$, if $\lambda \neq \frac{n+1}{2}$.*

Our proof gives no information about the case $\lambda = \frac{n+1}{2}$.

The proof of this theorem is given below. To the best of the author's knowledge, this result is completely new, but Ferdinand Ihringer pointed out that a weaker version of Theorem 1.3, with $\lambda \leq n/2$ rather than $\lambda \neq (n+1)/2$, follows from [6] Corollary 3.2, which is the following reformulation of Godsil's old result [5], Theorem 3.5.

Theorem 1.4 *Let $(X, \mathcal{R})$ be an association scheme with $d + 1$ classes. Let $P = (P_{kj}) \in \mathbb{C}^{d+1,d+1}$ and $Q = (Q_{kj}) \in \mathbb{C}^{d+1,d+1}$ denote the eigenmatrices of the association scheme and let f_k denote the multiplicities of the eigenvalues P_{kj}. Let R_i be a relation of the association scheme $(X, \mathcal{R})$. Let Y be a subset of X of maximum size under the condition that all elements of Y are pairwise in relation R_0 or R_i. Let $j \in [d]$. if $Q_{0j} \neq Q_{ij}$, then $|Y| \leq 1 + f_j$, and if in addition $Q_{ij} \neq -1$, then $|Y| \leq f_j$.*

Here we should apply Theorem 1.4 to the Hamming scheme, where the eigenvalues of the Hamming graph are $P_{i1} = Q_{i1} = n - 2i$ for each i and the multiplicities of the eigenvalues are $f_i = \binom{n}{i}$.

It is easy to verify that our upper bound is sharp when $n = 4k$ and there exists a Hadamard matrix of order $4k$.

Let $n = 4k$ and if it exists, then let H denote a Hadamard matrix of order $4k$. Denote by $\mathbf{h}(i)$ the i^{th} row of the matrix H. Let $\mathbf{k}(i) \in \{0, 1\}^n$ denote the corresponding (0-1) vector, i.e., $\mathbf{k}(i)_t = 0$ if and only if $\mathbf{h}(i)_t = -1$.

Consider the set system $\mathcal{F}$, which corresponds to the set of characteristic vectors $\{\mathbf{k}(i) : 1 \leq i \leq n\}$. Then clearly $d_H(F, G) = \frac{n}{2}$ for each distinct $F, G \in \mathcal{F}$ and $|\mathcal{F}| = n$ (see e.g. [7] Theorem 15.7).

In Section 2 we prove first Theorem 1.3, then we give a different proof for the special case of Theorem 1.3, when $\lambda \leq \frac{n}{2}$. In Section 3 we present a conjecture, which gives a possible generalization of our main result for $q > 2$.

2 Proofs

The proof of our main inequality is based on the linear algebra bound method and the following result on the determinant of a special matrix.

Proposition 2.1 *Let J_m be the $m \times m$ all one matrix and let I_m denote the $m \times m$ identity matrix. Let $\theta, \gamma \in \mathbb{R}$ be fixed real numbers. Then*

$$\det(\theta J_m + \gamma I_m) = (\gamma + m\theta)\gamma^{m-1}.$$

Proposition 2.1 was proved in [1] Exercise 4.1.3.

Proof of Theorem 1.3:

Let M denote the $m \times n$ $(-1, 1)$ *signed incidence matrix* of the set system $\mathcal{F}$, i.e., define $M(i, j)$ as

$$M(i,j) = \begin{cases} 1 & \text{if } j \in F_i \\ -1 & \text{otherwise.} \end{cases}$$

Let $\mathbf{v}_i$ denote the $(-1, 1)$ *signed* characteristic vector of the set F_i, i.e,

$$(\mathbf{v}_i)_j = \begin{cases} 1 & \text{if } j \in F_i \\ -1 & \text{otherwise.} \end{cases}$$

Define $N := M \cdot M^T$. Then $N(i, j) = \langle \mathbf{v}_i, \mathbf{v}_j \rangle$. If $i \neq j$, then this equals the number of positions at which $\mathbf{v}_i$ and $\mathbf{v}_j$ agree minus the number of positions at which they disagree. By definition they disagree at λ positions so this is $(n-\lambda)-\lambda = n-2\lambda$. If $i = j$ we clearly have $N(i, j) = n$. Hence $N = (n - 2\lambda)J_m + 2\lambda I_m$.

It follows from Proposition 2.1, with the choices $\theta := n - 2\lambda$, $\gamma := 2\lambda$, that

$$\det(N) = \det((n - 2\lambda)J_m + 2\lambda I_m) = (2\lambda + m(n - 2\lambda))(2\lambda)^{m-1}.$$

Hence $\det(N) \neq 0$ precisely if $2\lambda + m(n - 2\lambda) \neq 0$. Clearly if $\det(N) \neq 0$, then

$$m = \text{rank}(M \cdot M^T) = \text{rank}(M) \leq n,$$

and we have proved our result.

On the other hand, it follows from Corollary 1.2 that $m \leq n + 1$. Our aim is to prove that $m \leq n$. We prove this in an indirect way. Suppose that $m = n + 1$. Then $\det(N) = 0$, and hence it follows from $2\lambda + m(n - 2\lambda) = 0$ that $\lambda = \frac{n+1}{2}$, a contradiction. □

Remark. If $\lambda \leq \frac{n}{2}$, then it is easy to verify that the matrix N is positive definite.

Finally we give a different proof of Theorem 1.3 in the special case $\lambda \leq \frac{n}{2}$.

Let $\mathbf{v}_i$ denote the $(-1, 1)$ *signed* characteristic vector of the set F_i.

It is enough to prove that $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{R}^n$ are linearly independent vectors over $\mathbb{R}$.

We prove an indirect way. Assume that there exists such linear relation

$$\sum_{i=1}^{m} \mu_i \mathbf{v}_i = \mathbf{0},$$

where not all coefficients μ_i are zero.

It follows from the condition $d_H(F_i, F_j) = \lambda$ for each $i \neq j$ that $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = n - 2\lambda$ if $i \neq j$ and clearly $\langle \mathbf{v}_i, \mathbf{v}_i \rangle = n$ for each i.

Consider the expression

$$A := \langle \sum_{i=1}^{m} \mu_i \mathbf{v}_i, \sum_{j=1}^{m} \mu_j \mathbf{v}_j \rangle = 0.$$

Clearly then

$$\begin{aligned} A &= \sum_{i=1}^{m} \mu_i^2 \langle \mathbf{v}_i, \mathbf{v}_i \rangle + \sum_{1 \leq i \neq j \leq m} \mu_i \mu_j \langle \mathbf{v}_i, \mathbf{v}_j \rangle \\ &\geq \sum_{i=1}^{m} \mu_i^2 \cdot n + \sum_{1 \leq i \neq j \leq m} \mu_i \mu_j \cdot (n - 2\lambda). \end{aligned}$$

But

$$\begin{aligned} \sum_{i=1}^{m} \mu_i^2 \cdot n + \sum_{1 \leq i \neq j \leq m} \mu_i \mu_j \cdot (n - 2\lambda) &= 2\lambda \sum_{i=1}^{m} \mu_i^2 + \sum_{i=1}^{m} \mu_i^2 \cdot (n - 2\lambda) \\ &\quad + \sum_{1 \leq i \neq j \leq m} \mu_i \mu_j \cdot (n - 2\lambda) \\ &= 2\lambda \sum_{i=1}^{m} \mu_i^2 + (n - 2\lambda) \cdot (\sum_{i=1}^{m} \mu_i)^2 \end{aligned}$$

and

$$2\lambda \sum_{i=1}^{m} \mu_i^2 + (n - 2\lambda) \cdot (\sum_{i=1}^{m} \mu_i)^2 > 0,$$

because $\lambda > 0$, $n - 2\lambda \geq 0$ and there exists an index i such that the coefficient μ_i is nonzero by the indirect condition. Consequently $A > 0$, a contradiction. □

3 Concluding remarks

We conjecture the following generalization of Theorem 1.3.

Conjecture 1 *Let $\mathcal{V} = \{\mathbf{v}_1, \dots, \mathbf{v}_m\} \subseteq \{0, 1, \dots, q-1\}^n$ be a vector system such that there exists a positive integer $\lambda > 0$ with $d_H(\mathbf{v}_i, \mathbf{v}_j) = \lambda$ for each $i \neq j$. Suppose that $\lambda \neq \frac{(q-1)(n+1)}{q}$. Then $m = |\mathcal{V}| \leq n(q-1)$.*

It would be very interesting to characterize the extremal configurations in Theorem 1.3, i.e. the set systems $\mathcal{F} = \{F_1, \dots, F_m\}$ and the $\lambda > 0$ positive integers such that $d_H(F_i, F_j) = \lambda$ for each $i \neq j$ and $|\mathcal{F}| = n$. Finally it would be desirable to determine if Theorem 1.3 remains valid in the case $n \geq 5$ and $\lambda = \frac{n+1}{2}$.

Acknowledgments

I am grateful to Ferdinand Ihringer for his useful remarks.

References

[1] L. Babai and P. Frankl, Linear algebra methods in combinatorics, manuscript, September 1992.

[2] L. Babai, H. Snevily and R. M. Wilson, A new proof of several inequalities on codes and sets, *J. Combin. Theory, Ser. A* **71**(1) (1995), 146–153.

[3] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Rep. Suppl.* **10** (1973), 1–97.

[4] P. Delsarte, The association schemes of coding theory, In: *Combinatorics: Proc. NATO Advanced Study Institute*, Nijenrode Castle, Breukelen, Springer Netherlands (1975), 143–161.

[5] C. D. Godsil, Graphs, groups and polytopes, In: *Combinatorial Mathematics* (Proc. Int. Conf. Combinatorial Theory, Australian Nat. Univ., Canberra, 1977), *Lecture Notes in Math.* vol. 686, Springer, Berlin, 1977, 157–164.

[6] J. R. Isbell, An inequality for incidence matrices, *Proc. Amer. Math. Soc.* **10**(2) (1959), 216–218.

[7] S. Jukna, Extremal combinatorics: with applications in computer science, (Vol. 571), Berlin, Springer, 2011.

[8] K. N. Majumdar, On some theorems in combinatorics relating to incomplete block designs, *Annals Math. Stat.* **24**(3) (1953), 377–389.

(Received 1 Apr 2025; revised 7 Jan 2026)