Europ. J. Combinatorics (1988) **9**, 175–181

Inequalities for Code Pairs

RUDOLF AHLSWEDE AND MICHAEL MÖRS

Our main discovery is the *inequality*:

If $A, B \subset \{1, \ldots, \alpha\}^m$; $m \in \mathbb{N}$; satisfies for the Hamming distance d

$$d(a, b) - d(a, b') + d(a', b') - d(a', b) \neq 1, 2$$
$$\text{for all } a, a' \in A \text{ and } b, b' \in B,$$

then $|A||B| \leqslant d^{*m}$, where

$$d^* = \begin{cases} \alpha & \text{for } \alpha = 2, 3, 4, \\ \left\lfloor \frac{\alpha}{2} \right\rfloor \left\lceil \frac{\alpha}{2} \right\rceil & \text{for } \alpha \geqslant 4, \end{cases}$$

and the bound is best.

It is much more general than its predecessors ([1], [2]) and has a perspicuous combinatorial proof.

1. INTRODUCTION

The pair (A, B); $A, B \subset \mathscr{X}^m$; where $\mathscr{X} = \{1, \ldots, \alpha\}$, is called an (m, δ)-pair (or δ-distance code pair of block length m), if for the Hamming distance d

$$d(a, b) = \delta, \qquad \text{for all } a \in A, b \in B. \tag{$\bar{\text{H}}$}$$

The discovery of [1] was

THEOREM 1. In the case $\alpha = 2$, *for every* (m, δ)*-pair* (A, B),

$$|A||B| \leqslant \begin{cases} 2^m, & \text{if } m \text{ is even}, \\ 2^{m-1}, & \text{if } m \text{ is odd}. \end{cases}$$

Equality occurs with $\delta = \lfloor \frac{m}{2} \rfloor$ for the sets in:

EXAMPLE 1.

$$A = \{01,10\}^\delta,\ B = \{11,00\}^\delta, \qquad m \text{ even},$$
$$A = \{01,10\}^\delta \times \{0\},\ B = \{11,00\}^\delta \times \{0\}, \qquad m \text{ odd}.$$

In trying to extend this inequality to cases for $\alpha \geqslant 3$ we found the inequality as stated in the abstract.

Whereas the original two proofs of Theorem [1] (by a 1-step and a 2-step induction on m) use frequency and complementation arguments, the simpler (and closely related) proofs of [2] and [3] are based on elementary algebra of the m-dimensional vector space over GF(2).

Since, for general α, $\mathscr{X}^m$ cannot be endowed with a complement-operation or vector space structure, a new argument was required. In problems concerning a cartesian product it is natural to proceed by induction in the number of factors. For a set $C \subset \mathscr{X}^m$, $m \geqslant 2$, and

0195-6698/88/020175+07 $02.00/0

$i \in \mathscr{X}$ we define

$$C_i = \{(c_2, \ldots, c_m) | (i, c_2, \ldots, c_m) \in C\}. \tag{1.1}$$

Our proofs are based on properties of the systems $\{(A_i, B_j) : 1 \leqslant i \leqslant \alpha;\ 1 \leqslant j \leqslant \alpha\}$. Of course having the induction hypothesis for a larger class of pairs helps in the induction. A first fruitful idea in this respect was to replace the property $(\bar{\mathrm{H}})$, that is the property of two-sided equal distances, by the weaker property of one-sided equal distances

$$d(a, b) = d(a, b'), \qquad \text{for every } a \in A \quad \text{and all } b, b' \in B. \tag{$\vec{\mathrm{H}}$}$$

A pair (A, B); $A, B \subset \mathscr{X}^m$; satisfying $(\vec{\mathrm{H}})$ is called one-sided equidistant code pair of block length m or in short an *m-pair.*

The proof of the inequality stated in the abstract (Theorem 1) is particularly simple for m-pairs and is extremely simple for the case $\alpha = 2$. Since from this case Theorem [1] easily follows (see Section 3), we have as a by-product a proof of this Theorem, which we consider to be simpler than all previous proofs ([1], [2], [3]). It was the analysis of the proof for m-pairs, which led for $\alpha = 2$ to the weaker 4-words property

$$d(a, b) - d(a, b') + d(a', b') - d(a', b) \neq 2, \tag{4-WWP}$$

and for $\alpha \geqslant 2$ to the 4-words property

$$d(a, b) - d(a, b') + d(a', b') - d(a', b) \neq 1, 2, \qquad \forall a, a' \in A, \forall b, b' \in B. \tag{4-WP}$$

One can readily verify that for $\alpha = 2$ the two conditions are equivalent and that they are *not* equivalent for $\alpha \geqslant 3$.

Also one can immediately see that for any α there are the following implications

$$(\bar{\mathrm{H}}) \Rightarrow (\vec{\mathrm{H}}) \Rightarrow (\text{4-WP}) \Rightarrow (\text{4-WWP}). \tag{1.2}$$

It is clear from the form of the bound α^{*m} in the main inequality (Theorem 1), where

$$\alpha^* = \begin{cases} \alpha, & \text{for } \alpha = 2, 3, 4 \\ \bar{\alpha} = \left\lfloor \dfrac{\alpha}{2} \right\rfloor \left\lceil \dfrac{\alpha}{2} \right\rceil, & \text{for } \alpha \geqslant 4 \end{cases} = \max(\alpha, \bar{\alpha}), \tag{1.3}$$

that the cases $\alpha = 2, 3$ (and also the break point $\alpha = 4$ to a certain extent) show exceptional behaviour.

Insight can be gained from the following examples

Example 2. $(\alpha \geqslant 4)$.

$$A = \left\{1, \ldots, \left\lfloor \frac{\alpha}{2} \right\rfloor\right\}^m, \qquad B = \left\{\left\lfloor \frac{\alpha}{2} \right\rfloor + 1, \ldots, \alpha\right\}^m.$$

Example 3. $(\alpha = 2, 3, 4)$.

$$A = \{1, \ldots, \alpha\}^m, \qquad B = \{(11 \ldots 1)\}.$$

They satisfy $(\vec{H})$ (and thus (4-WP)) and $|A||B| = \alpha^{*m}$ (tightness of the bound). *Example 2 also satisfies* $(\vec{H})$ and thus Theorem 1 implies the extension of Theorem [1] to the cases with $\alpha \geqslant 4$. However, here the best choice for δ is $\delta = n$ rather than $\delta = \lfloor \frac{n}{2} \rfloor$.

Theorem 1 also implies the result of Theorem [1] for even m, whereas the case with m odd requires an additional argument (see Section 3).

The case $\alpha = 3$ has the most complex structure with respect to ($\vec{\mathrm{H}}$). Here the optimal bound is not of the form β^m. It will be treated in another paper, which is concerned also with the *Lee metric.* Notice that for $\alpha = 3$ the Hamming and Lee distances are *equal.* In this case we encounter already problems which are typical for ($\bar{\mathrm{L}}$), the case of constant Lee-distance code pairs. A discussion about this and also several other problems can be found in Section 4.

2. The Main Inequality

Theorem 1. *If* (A, B); $A, B \subset \mathscr{X}^m$; *satisfies* (4-WP), *then with* α^* *as defined in* (1.3)

$$|A||B| \leqslant \alpha^{*m}, \qquad m \in \mathbb{N},$$

and the bound is best.

The proof is based on two Lemmas.

Lemma 1. [Inheritance of (4-WP)]. *Let* $m \geqslant 2$. *If* (A, B); $A, B \subset \mathscr{X}^m$; *satisfies* (4-WP), *then for any* A_i, $i \in I \subset \mathscr{X}$ *and any* B_j, $j \in \mathscr{X}$, $(\bigcup_i A_i, B_j)$ *satisfies* (4-WP).

Here by symmetry the roles of the A_is and the B_js are exchangeable.

Proof. For $a \in A_i$, $a' \in A_k$; $b, b' \in B_j$ by assumption

$$\begin{aligned} 1, 2 \neq {} & d(ia, jb) - d(ia, jb') + d(ka', jb') - d(ka', jb) \\ = {} & d(a, b) - d(a, b') + d(a', b') - d(a', b), \end{aligned}$$

because $d(i, j) - d(i, j) + d(k, j) - d(k, j) = 0$ for $k = i$ as well as for $k \neq i$.

Define now the non-negative numbers k, s and t by

$$k = |\{1 \leqslant i \leqslant \alpha : |A_i||B_i| > 0\}|, \tag{2.1}$$

$$s = |\{1 \leqslant i \leqslant \alpha : |A_i| > 0\}| - k, \; t = |\{1 \leqslant i \leqslant \alpha : |B_i| > 0\}| - k. \tag{2.2}$$

After *relabelling* we have

$$\begin{aligned} &|A_i||B_i| > 0, && \text{for} \quad 1 \leqslant i \leqslant k; \\ &|A_i| > 0, && \text{for} \quad 1 \leqslant i \leqslant k + s; \\ &|B_i| > 0, && \text{for} \quad 1 \leqslant i \leqslant k \quad \text{and} \quad k + s < i \leqslant k + s + t. \end{aligned} \tag{2.3}$$

Lemma 2. (Disjointness property). *Let* $m \geqslant 2$. *If* (A, B); $A, B \subset \mathscr{X}^m$; *satisfies* (4-WP) and *if* $k + s$, $k + t \geqslant 2$, *then for* $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant \alpha$, $i \neq j$:
(*a*) $A_i \cap A_j = \varnothing$, *and*
(*b*) $B_i \cap B_j = \varnothing$.

Proof. By symmetry it suffices to show (a), that is, $A_i \cap A_j \neq \varnothing$ contradicts (4-WP). By our definitions $B_i \neq \varnothing$ and since $k + t \geqslant 2$ there exists an $l \neq i$ with $B_l \neq \varnothing$. Choose now $a \in A_i \cap A_j$, $b_i \in B_i$, $b_l \in B_l$ and notice that

$$\begin{aligned} & d(ia, lb_l) - d(ia, ib_i) + d(ja, ib_i) - d(ja, lb_l) \\ = {} & d(i, l) + d(j, i) - d(j, l) = 2 - d(j, l). \end{aligned}$$

This contradicts (4-WP).

PROOF OF THEOREM 1 BY INDUCTION ON m.

$m = 1$: If $A \cap B = \varnothing$, then $|A||B| \leqslant \bar{\alpha} \leqslant \max(\alpha, \bar{\alpha}) = \alpha^*$, and if $A \cap B = \varnothing$, then the assumption $A \supset \{i, j\}$, $B \supset \{i, l\}$ with $i \neq j, l$ leads to the contradiction

$$d(i, l) - d(i, j) + d(j, i) - d(j, l) = 1 - 0 + 1 - d(j, l) \in \{1, 2\}.$$

Therefore in this case $|A||B| \leqslant \alpha \leqslant \alpha^*$.

$m - 1 \to m$: If in Lemma 2 the hypothesis $k + s$, $k + t \geqslant 2$ does not hold, then

$$|A||B| \leqslant \alpha \max_{i,j} |A_i||B_j|,$$

and since, as a special case of Lemma 1, (A_i, B_j) satisfies (4-WP), we have by induction hypothesis

$$|A||B| \leqslant \alpha\alpha^{*m-1} \leqslant \alpha^{*m}.$$

In the case $k + s, k + t \geqslant 2$ we consider the scheme specified by the definitions (2.1)–(2.3) with the following subdivision

	$A_1 \dots A_k A_{k+1}$	$A_{k+2} \dots A_{k+s}$
B_1		
⋮	I	II
B_k		
B_{k+s+1}		II
⋮	I	
B_{k+s+t}		III

Clearly $|A||B| = \text{I} + \text{II} + \text{III}$, where

$$I = \sum_{i=1}^{k+1} |A_i| \left(\sum_{j=1}^{k} |B_j| + \sum_{j=k+s+1}^{k+s+t} |B_j| \right)$$

$$= \left| \bigcup_{i=1}^{k+1} A_i \right| \left(\sum_{j=1}^{k} |B_j| + \sum_{j=k+s+1}^{k+s+t} |B_j| \right) \qquad \text{(by Lemma 2)}$$

$$\leqslant (k + t)\alpha^{*m-1} \qquad \text{(by Lemma 1 and the induction hypothesis).}$$

$$\text{II} = \sum_{i=k+2}^{k+s} |A_i| \left| \left(\bigcup_{i=1}^{k} B_i \right) \cup B_{k+s+1} \right| \qquad \text{(by Lemma 2)}$$

$$\leqslant (s - 1)\alpha^{*m-1} \qquad \text{(by Lemma 1 and the induction hypothesis).}$$

$$\text{III} = \sum_{i=k+2}^{k+s} |A_i| \sum_{j=k+s+2}^{k+s+t} |B_j| \leqslant (s - 1)(t - 1)\alpha^{*m-1}$$

(by Lemma 1 and the induction hypothesis).

Since $(k + t) + (s - 1)(t - 1) = k + st$, and since

$$k + st \leqslant \begin{cases} (k + s)t \leqslant \bar{\alpha}, & \text{for } t \geqslant 1, \\ k \leqslant \alpha & \text{for } t = 0, \end{cases}$$

we conclude that

$$|A||B| \leqslant \max(\alpha, \bar{\alpha})\alpha^{*m-1} = \alpha^{*m}. \tag{2.5}$$

Remark. P. Delsarte and P. Piret gave in [2] for $\alpha = 2$ the congruence condition:

$$d(a, b) \equiv r \bmod 4, \qquad \text{for some } r \in \{0, 1, 2, 3,\} \quad \text{and all} \quad a \in A, b \in B.$$

Since $4r \bmod 4 \equiv 0 \bmod 4 \not\equiv 2 \bmod 4$, this is a very special case of the 4-words condition.

3. A Proof of Theorem [1] Via One-sided Constant Distance Code Pairs

It is clear from (1.2) that Theorem 1 and Examples 2 and 3 yield:

Corollary 1. *If* (A, B); $A, B \subset \mathscr{X}^m$; *satisfies* $(\vec{\mathrm{H}})$; *then for* $m \in \mathbb{N}$

$$|A||B| \leqslant \alpha^{*m},$$

and the bound is best.

A Simple Proof for the Case $\alpha = 2$. The case $m = 1$ is trivial. For an m-pair (A, B), either $B_j = \varnothing$, for some j, and then inductively

$$|A||B| = |A_1||B_{j'}| + |A_2||B_{j'}| \leqslant 2 \cdot 2^{m-1}, \qquad j' \neq j,$$

or we have $A_1 \cap A_2 = \varnothing$, because otherwise for $a \in A_1 \cap A_2$, $b \in B_1$, $b' \in B_2$ by $(\vec{\mathrm{H}})$

$$d(1a, 1b) = d(1a, 2b') \tag{3.1}$$

$$d(2a, 1b) = d(2a, 2b') \tag{3.2}$$

and (3.2) implies $d(1a, 1b) + 1 = d(1a, 2b') - 1$, a contradiction to (3.1).

Notice now that $(A_1 \dot{\cup} A_2, B_j)$ is an $(m - 1)$-pair and that therefore

$$|A||B| \leqslant |A_1 \dot{\cup} A_2|(|B_1| + |B_2|) \leqslant 2 \cdot 2^{m-1}.$$

Theorem [1] from Corollary 1 ($\alpha = 2$). Only the case m odd remains to be proved. We denote the complement of an $a \in \{0, 1\}^m$ by a^c. For a set $A \subset \{0, 1\}^m$ we define $A^c = \{a^c : a \in A\}$. Since for any $a, b \in \{0, 1\}^m$

$$d(a^c, b) + d(a, b) = m, \tag{3.3}$$

for any (m, δ)-pair (A, B) the pair $(A \cup A^c, B)$ is an m-pair and for odd m also $A \cap A^c = \varnothing$. Therefore by Corollary 1

$$2|A||B| = |A \cup A^c||B| \leqslant 2^m.$$

Corollary 2. (Extension of Theorem [1]). *If* (A, B); $A, B \subset \mathscr{X}^m$; *satisfies* $(\bar{\mathrm{H}})$, *then for* $m \in \mathbb{N}$ *and all* $\alpha \geqslant 2$

$$|A||B| \leqslant \alpha^{*m}.$$

The bound is best for $\alpha \neq 2, 3$.

Proof. Since $(\bar{\mathrm{H}})$ implies $(\vec{\mathrm{H}})$, Corollary 2 is a special case of Corollary 1. Tightness of the bound for $\alpha \geqslant 4$ follows from Example 3. We know already that for $\alpha = 2$ the bound is also tight for even m, however, for m odd it is not, because here α^{*m-1} is tight. Finally the bound is not tight for $\alpha = 3$, because $(A, B) = (\{1, 2\}, \{3\})$ is an optimal configuration in case $m = 1$ and $|A||B| = 2 < 3 = \alpha^*$.

For a further discussion of the exceptional behaviour of the cases $\alpha = 2, 3$ see Section 4.

4. Directions for Further Investigations

We sketch here possible extensions of the results of the paper and state some specific problems.

(1) From Hamming to General Distortion Measures

In information theory, any function $D: \mathscr{X} \times \hat{\mathscr{X}} \to \mathbb{R}_+$ is called a distortion measure and $D: \mathscr{X}^m \times \hat{\mathscr{X}}^m \to \mathbb{R}$ is of *sum-type*, if $D(x^m, \hat{x}^m) = \Sigma_{t=1}^m D(x_t, \hat{x}_t)$. Quite generally one can study the sizes of sets $A \subset \mathscr{X}^m$, $b \subset \hat{\mathscr{X}}^m$ meeting a fixed finite set of constraints in terms of the mutual distances. In particular for the familiar (4-WP) Inheritance Lemma 1 extends to every sum-type distortion measure.

Lemma 2 extends to accurate ($D(x, x) = 0$ for $x \in \mathscr{X}$) and symmetric ($D(x, x') = D(x', x)$ for all $x, x' \in \mathscr{X} = \hat{\mathscr{X}}$) sum-type distortion measures, if

$$\Delta(i, j, l) = D(i, j) + D(i, l) - D(j, l) \neq 0, \tag{Δ}$$

for all $i, j, l \in \mathscr{X}$, with $i \neq j, l$, *and* if the generalized four word property is defined by

$$D(a, b) - D(a, b') + D(a', b') - D(a', b) \notin \{\Delta(i, j, l): i \neq j, l\} \tag{G4-WP}$$

Inspection of the proof of Theorem 1 shows that the bound α^{*m} (but not tightness!) holds in this greater generality.

Problem 1. The generalized (4-WP) above holds for constant distance code pairs (A, B), if the *metric space* $(\mathscr{X}, D)$ has no degenerate triangles, that is, (Δ) holds.

Establish *tight* bounds on $|A||B|$!

Problem 2. We have mentioned in the introduction for the Hamming case the weaker 4-words property (4-WWP).

For every $\alpha \geqslant 2$ and $m \in \mathbb{N}$ study

$$\max \{|A||B|: A, B \subset \mathscr{X}^m \text{ satisfies (4-WWP)}\}.$$

(2) Lee Metric

Notice that (Δ) is satisfied for instance by every ultrametric, but *not* by the *Lee metric* for $\alpha \geqslant 4$ and also not by the Taxi metric (a name used for the L^1-metric, if the space is finite).

It is remarkable that the cases $\alpha = 2, 3$, which showed exceptional behaviour for constant distance Hamming code pairs, are exactly those where the Lee and the Hamming metric are identical.

Problem 3. What are the exact bounds for
(a) constant distance
(b) one-sided constant distance
code pairs in the Lee case?

In particular for $\alpha = 3$ in the circumstances of (a) we *conjecture*: for $m \geqslant 10 \max_d \binom{m}{d} 2^d$ is tight.

Notice that the case $\alpha = 4$ is solved, because the Hamming metric on $\mathscr{X}^2$ is isomorphic to the Lee metric on $\{1, 2, 3, 4\}$.

PROBLEM 4. What are the answers to the questions in Problem 3 for the Taxi metric?

PROBLEM 5. What are the substitutes for the (4-WP) in the Lee resp. Taxi case*.

A solution to these problems may give hints how to proceed with the program described in (1).

(3) SPECIFIC DISTANCES, FREQUENCY CONSTRAINTS

For a metric D define

$$D_\alpha(m, \delta) = \max\{|A||B| : (A, B) \text{ is } (m, \delta)\text{-pair}\}.$$

PROBLEM 6. Determine $D_\alpha(m, \delta)$ in the case D is (a) the Hamming metric, (b) the Lee metric and (c) the Taxi metric.

PROBLEM 7. We say that (A, B); $A, B \subset \mathscr{X}^m$; is of constant frequency type, if

$$f_{i,j}(a, b) = |\{t: (a_t, b_t) = (i, j)\}|$$

does not depend on $(a, b) \in A \times B$. What are the configurations maximizing $|A||B|$?

(4) MORE THAN TWO CODES

The questions raised in so far can be asked for tuples of sets $A, B, \ldots \subset \mathscr{X}^m$. Already if only constraints on pairs are imposed, there is a multitude of problems.

(5) FROM SYMMETRIC DIFFERENCE TO OTHER BOOLEAN OPERATIONS FOR SETS AND MULTISETS

The Hamming space $(\{0, 1\}^m, d)$ is isomorphic to $(\mathscr{P}(\{1, \ldots, m\}), |\Delta|)$, where $|\Delta|(a, b)$ denotes the cardinality of the symmetric difference for two subsets a, b of $\{1, \ldots, m\}$. One might consider $|\cup|(a, b) = |a \cup b|$ and other Boolean operations and ask questions in the spirit of the preceding paragraphs for sets (and also multisets).

There is of course already an extensive literature on problems of this or a similar kind, but some of the questions seem to be new.

REFERENCES

1. R. Ahlswede, A. El Gamal and K. F. Pang, A two-family extremal problem in Hamming space, *Discrete Math.* **49** (1984), 1–5.
2. P. Delsarte and P. Piret, An extension of an inequality by Ahlswede, El Gamal and Pang for pairs of binary codes, *Discrete Math.* **55** (1985), 313–315.
3. J. I. Hall and J. H. van Lint, Constant distance code pairs, *Proc. Kon. Ned. Akad. v. Wet.* (*A*) (1) **88** (1985), 41–45.

Received 25 October 1984

RUDOLF AHLSWEDE AND MICHAEL MÖRS
Fakultät für Mathematik, Universität Bielefeld,
Postfach 86 40, 4800 Bielefeld 1, F.R.G.

*In a recent paper 'A bound of sizes of code pairs satisfying the strong 4-words property for the Lee distance' Cai Ning showed that for $A, B \subset \{1, 2, \ldots, \alpha\}^n$ ($\alpha \geqslant 2$; $n \in \mathbb{N}$), which satisfy for the Lee distance λ

$$\lambda(a, b) - \lambda(a, b') + \lambda(a', b') - \lambda(a', b) = 0, \text{ for all } a, a' \in A;\ b, b' \in B,$$

$$|A||B| = (\max\{\alpha, (\lfloor \alpha/4 \rfloor + 1)(\lceil \lfloor \alpha/2 \rfloor /2 \rceil + 1)\})^n$$

and that this bound is best possible.