COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
52. COMBINATORICS, EGER (HUNGARY), 1987

On Code Pairs with Specified Hamming Distances

R. AHLSWEDE

1. Introduction, results and conjectures

Our results concern code pairs with specified constant Hamming distances, code pairs and also codes with specified parity of the distances, and applications to the two-way complexity of the Hamming distance function as well as the parity function thereof. Finally we state some conjectures and discuss relations of this work to the theory of multi-user source coding. The proofs of the theorems are given in subsequent sections.

a.) Constant distance code pairs

We continue the investigations of [1] and [4]. The main results of those papers are stated here as Theorems [1], [4] for comparison with the new results of the present paper. We need a few definitions.

$\mathcal{X}_\alpha = \{1, 2, \ldots, \alpha\}$ is a finite set of alphabet. The pair (A, B), $A, B \subset \mathcal{X}_\alpha^n$, is called an (n, δ)-system (or constant distance code pair with parameters n, δ), if for the Hamming distance function d

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

Let $S_\alpha(n, \delta)$ denote the set of those systems. We consider the functions

$$M_\alpha(n, \delta) = \max\{|A| \cdot |B| :\ (A, B) \in S_\alpha(n, \delta)\} \tag{1.1}$$

$$M_\alpha(n) = \max_{0 \le \delta \le n} M_\alpha(n, \delta). \tag{1.2}$$

The discovery of [1] was

Theorem [1].

$$M_2(n) = \begin{cases} 2^n & \text{, if } n \text{ is even} \\ 2^{n-1} & \text{, if } n \text{ is odd.} \end{cases}$$

By now several proofs exist (c.f. [2], [3], [4], [8]), which are simpler than the two original proofs (by a 1-step and a 2-step induction on n) based on frequency arguments. However, this seemingly unnecessary complicated approach is presently the only one we know to yield the sharper results in Theorem 1 below.

In trying to characterize $M_\alpha(n)$ for $\alpha \geq 3$ the authors of [4] found a quite general inequality.

(A, B), $A, B \subset \mathcal{X}_\alpha^n$, is said to satisfy the 4-words property, if

(4-WP) $\quad d(a,b) - d(a,b') + d(a',b') - d(a,b') \neq 1, 2$ for all $a, a' \in A$; $b, b' \in B$.

Theorem [4]. *If (A, B), $A, B \in \mathcal{X}_\alpha^n$, $n \in \mathbb{N}$, satisfies (4-WP), then*

$$|A| \cdot |B| \leq \alpha^{*n}, \quad \text{where} \quad \alpha^* = \begin{cases} \alpha & \text{for } \alpha = 2, 3, 4 \\ \lfloor \frac{\alpha}{2} \rfloor \cdot \lceil \frac{\alpha}{2} \rceil & \text{for } \alpha \geq 4, \end{cases}$$

and the bound is best (within this class).

The inequality is also best for the subclass of one-sided equidistant pairs (A, B), i.e.,

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

For two sided equidistant pairs (A, B), i.e.,

$(\overline{H})$ $\qquad d(a,b) = \delta$ for some δ and all $a \in A$, $b \in B$,

the inequality is best for $\alpha \geq 4$ and $\alpha = 2$, is n is even. A detailed discussion and the necessary examples can be found in [4].

Our new result are for specified distances, that is, for the functions $M_\alpha(n, d)$. They are expressed in term of the following two functions:

(1.3) $$F_2(n, \delta) = \max_{d_1 + d_2 = \delta} (2!\,2)^{d_1} \binom{n - 2d_1}{d_2}$$

(1.4) $$F_3(n, \delta) = \max_{2\ell + d = \delta} (3!\,3)^{\ell} \binom{n - 3\ell}{d} 2^d$$

$$F_\alpha(n,\delta) = \max_{d_1+d_2=\delta} \overline{\alpha}^{d_1} \binom{n-d_1}{d_2} (\alpha-1)^{d_2} \text{ for } \alpha \geq 4 \text{ where } \overline{\alpha} = \left\lfloor \frac{\alpha}{2} \right\rfloor \cdot \left\lceil \frac{\alpha}{2} \right\rceil. \quad (1.5)$$

Theorem 1.* *For $n \in \mathbb{N}$, $0 \leq \delta \leq n$*

(a) $$M_2(n,\delta) = F_2(n,\delta)$$

(b) $$M_\alpha(n,d) = F_\alpha(n,\delta) \text{ for } \alpha = 4,5.$$

Conjecture 1.

(c) $$M_3(n,\delta) = F_3(n,\delta)$$

(d) $$M_\alpha(n,d) = F_\alpha(n,\delta) \text{ for } \alpha \geq 6.$$

Notice that for $\alpha \geq 6$ the structure of the formula for $M_\alpha(n,d)$, which we firmly believe to be correct, is the same as in the case $\alpha = 4,5$. A really startling phenomenon is, that our proof for these cases, which uses again an averaging argument to establish the existence of a configuration on which an (in this case 1-step) induction can be performed, breaks down for $\alpha \geq 6$.

It ought to be mentioned that (a) can be derived from Theorem 4 in [6] with the help of (a) in Lemma 2.1. This was missed in [6] and also the proof of this Theorem 4 is unnecessarily complicated. The idea to combine two competing extremal configurations (as specified below) was suggested by us earlier.

Configurations yielding $M_\alpha(n,d) \geq F_\alpha(n,\delta)$

We define now the basic extremal configurations from which pairs (A,B) with $|A| \cdot |B| = F_\alpha(n,\delta)$ can be build. Let m be a positive integer.

$$E_1(\alpha,m) = \{(11\ldots1),\ldots,(\alpha\alpha\ldots\alpha)\} \subset \mathcal{X}_\alpha^m \quad (1.6)$$

$$E_2(\alpha) = \{(\sigma(1)\sigma(2)\ldots\sigma(\alpha)) : \sigma \in \mathcal{S}_\alpha\} \subset \mathcal{X}_\alpha, \quad (1.7)$$

where $\mathcal{S}_\alpha$ are the permutations on $\mathcal{X}_\alpha$.

$$E_3(\alpha,m,d) = \{x^m \in \mathcal{X}_\alpha^m : d(x^m,(11\ldots1)) = d\} \quad (1.8)$$

$$E_4(\alpha) = \{1,2,\ldots,\beta\},\ \overline{E}_4(\alpha) = \{\beta+1,\ldots,\alpha\}, \text{ where } \beta = \left\lfloor \frac{\alpha}{2} \right\rfloor. \quad (1.9)$$

---

* Presented at the 2. Internat. Workshop on Information Theory, Gränna, Sweden, April 14–19, 1985 and the Tagung "Kombinatorik", Oberwolfach, West Germany, January 19–25, 1986.

$\underline{\alpha = 2:}$ Define

$$A = E_1(2,2)^{d_1} * E_1(1, n-2d_1) \text{ and}$$
$$B = E_2(2)^{d_1} * E_3(2, n-2d_1, d_2).$$

Notice that $d(a,b) = d_1 + d_2$ for $a \in A$, $b \in B$ and that $|A| = 2^{d_1}$, $|B| = 2^{d_1}\binom{n-2d_1}{d_2}$. Thus for fixed n, δ an optimal choice of d_i gives $|A| \cdot |B| = F_2(n,\delta)$.

$\underline{\alpha = 3:}$ Define

$$A = E_1(3,3)^{\ell} * E_1(1, n-3\ell) \text{ and}$$
$$B = E_2(3)^{\ell} * E_3(3, n-3\ell, d).$$

Now we have $d(a,b) = 2\ell + d$ for $a \in A$, $b \in B$ and $|A| = 3^{\ell}$, $|B| = (3!)^{\ell}\binom{n-3\ell}{d}2^d$. For fixed n, δ an optimal choice of d, ℓ with $2\ell + d = \delta$ gives $|A| \cdot |B| = F_3(n,\delta)$.

$\underline{\alpha \geq 4:}$ Define

$$A = E_4(\alpha)^{d_1} * E_1(1, n-d_1) \text{ and}$$
$$B = \overline{E}_4(\alpha)^{d_1} * E_3(\alpha, n-d_1, d_2).$$

Here we have again $d(a,b) = d_1 + d_2$ for $a \in A$, $b \in B$ and $|A| = \lfloor \frac{\alpha}{2} \rfloor^{d_1}$, $|B| = \lceil \frac{\alpha}{2} \rceil^{d_1}\binom{n-d_1}{d_2}(\alpha-1)^{d_2}$.

An optimal choice of d_i subject to the constraint $d_1 + d_2 = \delta$ gives finally $|A| \cdot |B| = F_\alpha(n,\delta)$.

There are of course many configurations isomorphic to the basic configurations and optimal configurations are not even unique up to isomorphism.

Example 1. $\alpha = 4$, $n = 4$, $\delta = 3$.
Here $\max\limits_{d_1+d_2=3} a^{d_1}\binom{4-d_1}{d_2}3^{d_2} = 108$ and for $d_2 = 0$ $\binom{4}{3}3^3 = 108$. However, also for $d_2 = 1$ $4\binom{3}{2}3^2 = 108$.

Notice also that for $\alpha \geq 4$ the configurations $E_1(\alpha, m)$ and $E_3(\alpha, m, d)$ are superseded by $E_4(\alpha)$, resp. $\overline{E}_4(\alpha)$. This must have consequences for the methods of proof for the converses $M_\alpha(n,d) \leq F_\alpha(n,\delta)$.

b.) On parity of the Hamming distance

It is convenient to introduce the function

$$\psi(n) = \begin{cases} 0, & \text{if } n \text{ is even} \\ 1, & \text{if } n \text{ is odd,} \quad n \in \mathbb{N}. \end{cases} \tag{1.10}$$

We consider the parity function $\Pi : \cup_{n=1}^{\infty} \mathcal{X}_\alpha^n \times \mathcal{X}_\alpha^n \to \{0,1\}$ defined by

$$\Pi(x^n, y^n) = \psi(d(x^n, y^n)). \tag{1.11}$$

The pair (A,B) $A, B \in \mathcal{X}_\alpha^n$, is said to have i-parity, if

$$\Pi(a,b) = i \quad \text{for all} \quad a \in A,\ b \in B. \tag{Π^i}$$

For $i = 1, 2$ let $P_\alpha^i(n)$ denote the set of those i-parity pairs and define

$$Q_\alpha^i(n) = \max\{|A| \cdot |B| : (A, B) \in P_\alpha^i(n);\ i = 1, 2\} \tag{1.12}$$

$$Q_\alpha(n) = \max(Q_\alpha^0(n), Q_\alpha^1(n)). \tag{1.13}$$

Estimates for these quantities are derived from the solution of a problem for pairs with a more general parity property.

Analogously to the property $(\vec{H})$ we introduce the property of one-sided equiparity for a pair (A, B) $A, B \in \mathcal{X}_\alpha$:

$$\Pi(a, b) = \Pi(a, b') \text{ for every } a \in A \text{ and all } b, b' \in B, \tag{$\vec{\Pi}$}$$

and we denote the set of those pairs by $\vec{P}_\alpha(n)$ and define

$$\vec{Q}(n) = \max\{|A| \cdot |B| : (A, B) \in \vec{P}_\alpha(n)\}. \tag{1.14}$$

The following concept and result of some independent interest are needed for the proof of the next Theorem.

For $B \in \mathcal{X}_2^n$ and $X \subset \{1, 2, \ldots, n\}$ we say that B has *parity on* X, if the projection $\mathrm{Proj}_X B$ on $\prod_{t \in X} \mathcal{X}_2^t$ contains only sequences with an odd *or* only sequences with an even number of ones.

Lemma. (Blockwise parity property)

$$\sum_{\substack{X \subset \{1,2,\ldots,n\} \\ B \text{ has parity on } X}} 2^{|X|}|B| \le (2^n + 1)2^{n-1} \quad \text{for every} \quad B \in \mathcal{X}_2^n.$$

The right-hand bound is assumed, for instance, if B equals the set of all sequences with an even number of ones.

Next we state

Theorem 2. *For* $n \in \mathbb{N}$

(a) $$\vec{Q}_\alpha(n) = \overline{\alpha}^n \quad \text{for} \quad \alpha \ge 4$$

(b) $$\vec{Q}_2(n) = 2 \cdot 4^{n-1}$$

(c) $$\vec{Q}_3(n) = (2^n + 1)2^{n-1}.$$

Another result of a similar kind is for i-parity pairs.

Theorem 3. *For* $n \in \mathbb{N}$

(a) $$Q_\alpha^i(n) = \overline{\alpha}^n, \quad \text{if} \quad \psi(n) = i \quad (\alpha \ge 4;\ i = 0, 1)$$

(a′) $$\overline{\alpha}^{n-1} \le Q_\alpha^i(n) < \overline{\alpha}^n, \quad \text{if} \quad \psi(n) \ne i \quad (\alpha \ge 4;\ i = 0, 1)$$

(a″) $$Q_\alpha(n) = \overline{\alpha}^n$$

(b) $$Q_2(n) = Q_2^0(n) = Q_2^1(n) = 4^{n-1}.$$

For $\alpha = 3$ we have

Conjecture 2. Proved by Zhang

$$(c) \qquad Q_3^i(n) = (2^{n-1}+1)(2^{n-1}+1), \quad \text{if} \quad \psi(n) = i = 0$$

$$(c') \qquad Q_3^i(n) = (2^{n-1}+1)2^{n-1}, \quad \text{if} \quad \psi(n) = i = 1$$

$$(c'') \qquad Q_3^i(n) = 2^{n-1} \cdot 2^{n-1}, \quad \text{if} \quad \psi(n) \neq i \quad \text{and} \quad n \neq 3.$$

Remarks

The lower bound in (a') is not tight

$\alpha = 4, \quad n = 2, \quad i = 1$

Here $Q_4^1(2) = M_4(2,1)$ and by Theorem 1

$$M_4(2,1) = \max_{d_1+d_2=1} 4^{d_1} \binom{2-d_1}{d_2} 3^{d_2} = 6;$$

however, $4 < 6 < 16$.

An exceptional case in (c'') is for $n = 3, \quad i = 0$

$$A = \{111, 222, 333\}, \quad B = \{\text{all permutations of } 123\}.$$

Here $|A| \cdot |B| = 18$ and it can be shown by inspection that this is the optimal value. However, $2^2 \cdot 2^2 = 16 < 18 = 2^2(2^2+1) = 20$.

c.) On parity for one family

A well-known unsolved problem is to characterize equidistant codes of maximal length. $A \subset \mathcal{X}_\alpha^n$ is equidistant code, if

$$(1.15) \qquad d(a,a') = \delta \quad \text{for all} \quad a, a' \in A \quad \text{with} \quad a \neq a'.$$

One approach to the solution might be to study sets $A \subset \mathcal{X}_\alpha^n$ with

$$(1.16) \qquad d(a,a') \equiv \gamma \bmod m \quad \text{for all} \quad a, a' \in A \quad \text{with} \quad a \neq a'.$$

We consider here the case $m = 2$ and say that A has i-parity $(i = 0, 1)$, if

$$(1.17) \qquad \Pi(a,a') = i \quad \text{for} \quad a, a' \in A \quad \text{with} \quad a \neq a'.$$

In case $i = 0$ the condition $a \neq a'$ can, of course, be dropped. For this reason the cases $i = 0$ and $i = 1$ show quite different behaviour.

We are now interested in the quantities

$$q_\alpha^i(n) = \max\{|A| : A \subset \mathcal{X}_\alpha^n \text{ has } i\text{-parity}\}, \quad i = 0, 1. \tag{1.18}$$

Theorem 4. *For* $n \in \mathbb{N}$

(a) $$q_2^0(n) = 2^{n-1}$$

(b) $$q_\alpha^0(n) = \alpha^{\lfloor n/2 \rfloor} \text{ for } \alpha \geq 4$$

(c) $$q_3^0(n) = 2^{n-1} + 1 - \psi(n).$$

Remarks on $q_\alpha^1(n)$

It seems to be harder to characterize $q_\alpha^1(n)$.

For $\alpha = 2$ obviously $q_\alpha^1(n) = 2$ for all $n \in \mathbb{N}$, because A cannot contain two sequences such that both contain an even (or odd) number of ones. A first question is therefore whether $q_\alpha^1(n) \to \infty$ $(n \to \infty)$ for $\alpha \geq 3$.

B. Voigt answered this in the affirmative by providing the following construction.

Suppose that $a = \{a_1, \ldots, a_\gamma\} \subset \mathcal{X}_\alpha^\ell$, $\gamma \geq 3$ *odd,* has 1-parity, then A^*, the set of sequences obtained by concatenation from the row sequences in the following scheme, has again 1-parity and $|A^*| = |A| + 2$.

a_1	a_1	$\ldots$	a_γ
a_1	a_2	$\ldots$	$a_{\gamma-1}$
a_1	a_3	$\ldots$	$a_{\gamma-1}$
..	..	$\ldots$	$\ldots$
a_1	a_γ	$\ldots$	a_1
a_2	a_1	$\ldots$	a_1
a_2	a_2	$\ldots$	a_2

In the right upper subscheme the cyclic permutations of $a_1 \ldots a_\gamma$ are listed.

With γ odd also $\gamma + 2$ is odd and one can reiterate.

For γ odd (resp., even) one can start with $a_1 \ldots a_\gamma = 1 \ldots \gamma$ and $\gamma = \alpha$ (resp., $\gamma = \alpha - 1$). The lengths of the sequences increase of course very rapidly. We have only started to get exact results for $q_\alpha^1(n)$. One general bound is readily obtained:

$$q_\alpha^1(n) \leq \alpha \cdot q_\alpha^1(n-2), \quad n \geq 3. \tag{1.19}$$

For this just notice that for $ij \neq i'j'$ with $\Pi(ij, i'j') = 0$ necessarily $A_{ij} \cap A_{i'j'} = \emptyset$ and therefore

$$A = |A_{11} \dot{\cup} A_{22} \dot{\cup} \ldots \dot{\cup} A_{\alpha\alpha}| + |A_{12} \dot{\cup} A_{23} \dot{\cup} \ldots \dot{\cup} A_{\alpha 1}| + \cdots + |A_{1\alpha} \dot{\cup} A_{21} \dot{\cup} \ldots \dot{\cup} A_{\alpha(\alpha-1)}| \leq \alpha \cdot q_\alpha^1(n-2).$$

The first values of q_3^1, obtained by inspection, are

$$q_3^1(1) = 3, \quad q_3^1(2) = 3, \quad q_3^1(3) = 4 \tag{1.20}$$

and those values are assumed for

$$\{1,2,3\}, \quad \{11,12,13\}, \quad \{111,112,233,333\}.$$

By (1.19) $q_3^1(4) \leq 9$ and actually equality holds for

$$\{1\} \times \{123,231,312\} \cup \{2\} \times \{132,321,213\} \cup \{3\} \times \{111,222,333\}.$$

These examples may help to find the general pattern.

d.) Applications to two-way communication complexity

After Abelson had raised the issue of information transfer in distributed computations [11], Yao did his pioneering work on two-way communication complexity [5]. His success is mainly due to his limitation to functions $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ with $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ finite, which made a combinatorial treatment possible. A natural improvement of Yao's model [10] led to a very smooth form of Yao's lower bound for the two-way complexity $C(f; 1 \leftrightarrow 2)$, which we now state without proof. $S \times T$ $(S \subset \mathcal{X},\ T \subset \mathcal{Y})$ is called f-monochromatic, if f is constant on $S \times T$. A k-decomposition of f is a partition $S = \{S_1 \times T_1, \ldots, S_k \times T_k\}$ of $\mathcal{X} \times \mathcal{Y}$ into f-monochromatic rectangles.

For the decomposition number

$$D(f) \triangleq \min\{k: \text{ there exists a } k\text{–decomposition of } f\}$$

Yao's inequality (in the improved form of [10]) states

$$C(f;\ 1 \leftrightarrow 2) \geq \log_2 D(f). \tag{1.21}$$

We have not yet defined $C(f;\ 1 \leftrightarrow 2)$. It is actually a quantity which can be understood without any reference to computing in the context of an abstract multi-user source coding theory (see [12]).

The specifica here are:

1.) No probabilistic assumption on the source $(\mathcal{X}, \mathcal{Y}, f)$

2.) Correct decoding for all source outputs.

The communication model is as follows:

$\mathcal{X}$ outputs x and $\mathcal{Y}$ outputs y. A person $P_{\mathcal{X}}$ observes x and another person $P_{\mathcal{Y}}$ observes y. They can transmit messages to each other alternatively over a binary channel with zero error probability. Their goal is to find out the value $f(x, y)$ with minimal worst case transmission time. This quantity is denoted by $C(f;\ 1 \leftrightarrow 2)$.

Similar as in classical source coding there is a multitude of other communication models one might consider.

El Gamal and Pang [6] have investigated $C(f;\ 1 \leftrightarrow 2)$ for a particular function: $\mathcal{X} = \mathcal{Y} = \{0,1\}^n$, $\mathcal{Z} = \{0, 1, \ldots, n\}$; $f = d_n$, the Hamming distance function. Their result is

Theorem. [6]. $\left|C(d_n;\ 1 \leftrightarrow 2) - n - \lceil \log_2(n+1) \rceil\right| \leq 1$ *for all* $n \in \mathbb{N}$.

There is a trivial general bound on $C(f;\ 1 \leftrightarrow 2)$. Suppose that $P_{\mathcal{X}}$ transmits the output x of $\mathcal{X}$ to $P_{\mathcal{Y}}$, who in the knowledge of x and y calculates $f(x, y)$ and transmits this value to $P_{\mathcal{X}}$; then obviously $\lceil \log_2 |\mathcal{X}| \rceil + \lceil \log_2 |\mathcal{Z}| \rceil$ bits suffice, i.e.,

$$C(f;\ 1 \leftrightarrow 2) \leq \lceil \log_2 |\mathcal{X}| \rceil + \lceil \log_2 |\mathcal{Z}| \rceil. \tag{1.22}$$

Thus, in particular, for $\mathcal{X} = \mathcal{X}_\alpha^n$

$$C(d_n;\ 1 \leftrightarrow 2) \leq \lceil \log_2 \alpha \rceil + \lceil \log_2(n+1) \rceil. \tag{1.23}$$

This together with a lower bound, which is readily obtained from Theorem 1(b) and inequality (1.21), gives

Theorem 5. *For* $\alpha = 4, 5$ *and* $n \in \mathbb{N}$

$$\left|C(d_n;\ 1 \leftrightarrow 2) - \lceil \log_2 \alpha \rceil - \lceil \log_2(n+1) \rceil\right| \leq 1.$$

This derivation follows the lines of [6], but is more direct and shorter. Replacement of (b) and (a) in Theorem 1 would give Theorem [6] by the analogous argument.

We consider next $C(\Pi_n;\ 1 \leftrightarrow 2)$, where Π_n is the restriction of Π on $\mathcal{X}_\alpha^n \times \mathcal{X}_\alpha^n$.

For this we use first a general, but naive, lower bound on $D(f)$. Denoting the size of the largest monochromatic rectangle of f by $M(f)$, we clearly have $D(f) \geq |\mathcal{X}| \cdot |\mathcal{Y}| \cdot M(f)^{-1}$ and thus by (1.21)

$$C(f;\ 1 \leftrightarrow 2) \geq \lceil \log_2 |\mathcal{X}| \cdot |\mathcal{Y}| \cdot M(f)^{-1} \rceil \tag{1.24}$$

For $f = \Pi_n$ $M(\Pi_n) = Q_\alpha(n)$ and thus by Theorem 3

$$C(\Pi_n;\ 1 \leftrightarrow 2) \geq \begin{cases} 2 & \text{for } \alpha = 2 \\ 2n & \text{for } \alpha = 4 \end{cases} \tag{1.25}$$

For $\alpha = 2$ the bound is easily seen to be tight and for $\alpha \neq 2, 4$ it is too bad to be stated.

The upper bound (1.22) gives

$$\lceil n \cdot \log_2 \alpha \rceil + 1 \geq C(\Pi_n;\ 1 \leftrightarrow 2) \tag{1.26}$$

and thus for $\alpha = 4$ the lower and upper bound differ by 1 bit only. A slightly refined estimate of $D(\Pi_n)$ gives

Theorem 6. *For $\alpha = 4$ and $n \in \mathbb{N}$*

$$C(\Pi_n;\ 1 \leftrightarrow 2) = 2n + 1.$$

This lends credit to

Conjecture 3. *For all $\alpha \geq 3$ and $n \in \mathbb{N}$*

$$C(\Pi_n;\ 1 \leftrightarrow 2) = \lceil n \cdot \log_2 \alpha \rceil + 1.$$

In the same spirit we believe in

Conjecture 4. *For all $\alpha \geq 2$ and $n \in \mathbb{N}$*

$$C(d_n;\ 1 \leftrightarrow 2) = \lceil n \cdot \log_2(\alpha) \rceil + \lceil \log_2(n+1) \rceil.$$

e.) Discussion

We have mentioned already that the theory of communication complexity can be viewed as a part of (abstract) multi-user source coding theory. There is also a connection to already existing results ([9]), which have been obtained independently. In order to understand these connections we begin with the notion of one-way communication complexity $C(f;\ 1 \leftrightarrow 2)$, which is defined as the minimal number of bits to be transmitted form P_X to P_Y so that P_Y can compute f. For the parity function Π_n in case $\alpha \geq 3$

$$C(\Pi_n;\ 1 \leftrightarrow 2) = \lceil n \cdot \log_2 \alpha \rceil, \tag{1.27}$$

because for any $x^n, x'^n \in \mathcal{X}_\alpha^n$ there is a $y^n \in \mathcal{X}^n$ with $z\Pi(x^n, y^n) \neq \Pi(x'^n, y^n)$ and therefore every output of $\mathcal{X}_\alpha^n$ has to be encoded individually.

The problems studied in [9] include the following. Suppose that $(X_t, Y_t)_{t=1}^{\infty}$ is a discrete memoryless correlated source, where $X^n = X_1 \dots X_n$ (resp., $Y^n = Y_1 \dots Y_n$) takes values in $\mathcal{X}^n$ (resp., $\mathcal{Y}^n$), and suppose that $f : \cup_{n=1}^{\infty}(\mathcal{X}^n \times \mathcal{Y}^n) \to \mathbb{N}$ is to be computed with probability tending to 1 as $n \to \infty$ correctly by $P_{\mathcal{Y}}$, who observes Y^n. How much information has $P_{\mathcal{X}}$, who observes X^n, to transmit so that the necessary rate of transmission is $H(X|Y)$, the conditional entropy. Assuming that $\mathcal{X} = \mathcal{Y}$ and that the random variables X_t, Y_t are independent and take all there values with equal probability the result (the so-called 1-Bit Theorem) implies that

$$\lim_{n\to\infty} \frac{1}{n} C(\Pi_n;\ 1 \leftrightarrow 2) = \log_2 \alpha \quad \text{for} \quad \alpha \geq 3. \tag{1.28}$$

A yet unsolved problem is concerned with the situation, where both $P_{\mathcal{X}}$ and $P_{\mathcal{Y}}$ can inform a third person, say P_f, about their source outputs. What are the necessary rates of transmission to enable P_f to compute f with probability approaching 1 as $n \to \infty$? Conversely, this problem can be considered in a purely combinatorial setting. An encoding in this case is a product of partitions of $\mathcal{X}^n$ and $\mathcal{Y}^n$, with monochromatic members. This in turn is a special case of what has been called in [12] a strict coloring of orthogonal hypergraphs.

The interest in distributive computing gives a new impetus to sources coding theory and promises a fruitful exchange of ideas and methods. There are numerous open problems, many of them fall into the mathematical domain of combinatorial extremal theory.

For example, what is $D(f)$ for the function

$$f(x^n, y^n) = \begin{cases} 1 & \text{if } d(x^n, y^n) \geq \delta \\ 0 & \text{if } d(x^n, y^n) < \delta? \end{cases}$$

Finally, we ask "For which class of functions is Yao's lower bound asymptotically tight?"

2. Proof of Theorem 1

Our first auxiliary result concerns a recursion formula for $F_\alpha(n, \delta)$.

Lemma 2.1.

(a) $$F_2(n, \delta) = F_2(n-2, \delta-1) \cdot \max(4, \frac{n(n-1)}{\delta(n-\delta)}) \quad \text{for} \quad n \geq 3,\ 1 \leq \delta \leq n-1.$$

(b) $$F_\alpha(n, \delta) = F_\alpha(n-1, \delta-1) \cdot \max(\overline{\alpha}, \frac{n(\alpha-1)}{\delta}) \quad \text{for} \quad \alpha \geq 4;\ n \geq 2,\ 1 \leq \delta \leq n.$$

Proof. We show first that the left side expressions do not exceed the right side expressions. This easier part of the result is actually not needed in the proof of Theorem 1.

Choose d_1, d_2 with $d_1 + d_2 = \delta$ such that

$$F_2(n,\delta) = 2^{2d_1}\binom{n-2d_1}{d_2}. \tag{2.1}$$

In case $d_1 = 0$ we have

$$F_2(n,\delta) = \binom{n}{\delta} = \binom{n-2}{\delta-1}\frac{n(n-1)}{\delta(n-\delta)} \le F_2(n-2,\delta-1)\frac{n(n-1)}{\delta(n-\delta)}$$

and in case $d_1 \ge 1$ we have

$$F_2(n,\delta) = 2^2 \cdot 2^{2(d_1-1)}\binom{n-2-2(d_1-1)}{d_2} \le 4 \cdot F_2(n-2,\delta-1).$$

Similarly, if for $\alpha \ge 4$

$$F_\alpha(n,\delta) = \overline{\alpha}^{d_1}\binom{n-d_1}{d_2}(\alpha-1)^{d_2}, \tag{2.2}$$

then we have in case $d_1 = 0$

$$F_\alpha(n,\delta) = \binom{n}{\alpha}(\alpha-1)^\delta = \frac{n(\alpha-1)}{\delta}\binom{n-1}{\delta-1}(\alpha-1)^{\delta-1} \le \frac{n(\alpha-1)}{\delta}F_\alpha(n-1,\delta-1)$$

and in case $d_1 \ge 1$

$$F_\alpha(n,\delta) = \overline{\alpha}^{d_1}\binom{n-d_1}{d_2}(\alpha-1)^{d_2} = \overline{\alpha}\,\overline{\alpha}^{d_1-1}\binom{(n-1)-(d_1-1)}{d_2}(\alpha-1)^{d_2} \le$$
$$\le \overline{\alpha}\cdot F_\alpha(n-1,\delta-1).$$

Next we prove the reverse inequality for (b).

Let d_1, d_2, $d_1 + d_2 = \delta - 1$, be such that

$$F_(n-1,\delta-1) = \overline{\alpha}^{d_1}\binom{n-1-d_1}{d_2}(\alpha-1)^{d_2}, \tag{2.3}$$

then $\overline{\alpha}\cdot F_\alpha(n-1,\delta-1) = \overline{\alpha}^{d_1+1}\binom{n-(d_1+1)}{d_2}(\alpha-1)^{d_2} \le F_\alpha(n,\delta)$, because $(d_1+1)+d_2 = \delta$. Furthermore, since

$$\frac{n(\alpha-1)}{\delta}\cdot F_\alpha(n-1,\delta-1) = \overline{\alpha}^{d_1}\binom{n-1-d_1}{d_2}\frac{n}{\delta}(\alpha-1)^{d_2+1},$$

it suffices to show that

$$\binom{n-1-d_1}{d_2}\frac{n}{\delta} \le \binom{n-d_1}{d_2+1}. \tag{2.4}$$

Since $\binom{n-1-d_1}{d_2}\frac{n}{\delta} = \binom{n-d_1}{d_2+1} \le \frac{d_2+1}{n-d_1} \cdot \frac{n}{\delta}$, it suffices to show that

$$\frac{n}{n-d_1} \le \frac{\delta}{d_2+1} = \frac{\delta}{\delta-d_1}. \tag{2.5}$$

But this is true, because for $x \ge y \ge 0$, $z \ge 0$ $\frac{x+z}{y+z} \le \frac{x}{y}$.

Finally we prove the reverse inequality in (a).

Suppose that

$$F_2(n-2,\delta-1) = 2^{2d}\binom{n-2-2d}{\delta-1-d}, \tag{2.6}$$

then $4 \cdot F_2(n-2,\delta-1) = 2^{2(d+1)}\binom{n-2(d+1)}{\delta-(d+1)} \le F_2(n,\delta)$ and we are left with the case

$$4 < \frac{n(n-1)}{\delta(n-\delta)}. \tag{2.7}$$

By (2.6) $F_2(n-2,\delta-1)\frac{(n-2d)(n-2d-1)}{(\delta-d)(n-d-\delta)} = 2^{2d}\binom{n-2d}{\delta-d} \le F_2(n,\delta)$ and it remains to be seen that under the condition (2.7)

$$\frac{(n-2d)(n-2d-1)}{(\delta-d)(n-d-\delta)} \ge \frac{n(n-1)}{\delta(n-\delta)}. \tag{2.8}$$

This inequality is equivalent to

$$\delta(n-\delta)[n^2-4nd+4d^2-n+2d] \ge (n^2-n)[(n-\delta)\delta-(n-\delta)d-\delta d+d^2],$$

which can be simplified to

$$\delta(n-\delta)[-4nd+4d^2+2d] \ge n(n-1)[-nd+d^2].$$

Since $n \ge d$, this is equivalent to

$$\frac{n(n-1)}{\delta(n-\delta)} \ge \frac{-4nd+4d^2+2d}{-nd+d^2} = 4-\frac{2}{n-d},$$

and the truth of this inequality is ensured by (2.7). ■

Next we state our results involving frequencies, which are obtained by an averaging procedure. For this we adopt a notation, which will be used many times in the paper.

For a set $C \subset \mathcal{X}^n$, elements $i, j \in \mathcal{X}$, and a set $I \subset \mathcal{X}$ define

$$(2.9) \quad C_i^t = \{(c_1, \dots, c_{t-1}, c_{t+1}, \dots, c_n) : (c_1, \dots, c_{t-1}, i, c_{t+1}, \dots, c_n) \in C\} \subset \mathcal{X}^{n-1} \quad (1 \le t \le n, \ n \ge 2)$$

$$(2.10) \quad C^t(I) = \{(c_1, c_2, \dots, c_n) \in C : \ c_t \in I\} \subset C \subset \mathcal{X}^n \quad (1 \le t \le n, \ n \ge 2)$$

$$(2.11) \quad C_{ij}^{st} = \{(c_1, \dots, c_{s-1}, c_{s+1}, \dots, c_{t-1}, c_{t+1}, \dots, c_n) : (c_1, \dots, c_{s-1}, i, c_{s+1}, \dots, c_{t-1}, j, c_{t+1}, \dots, c_n) \in C\} \subset \subset \mathcal{X}^{n-2} \quad (1 \le s, t \le n, \ s \ne t \ n \ge 3).$$

$$(2.12) \quad \mathcal{P}_\beta(\mathcal{X}_\alpha) \text{ is the family of subsets of } \mathcal{X}_\alpha \text{ of cardinality } \beta = \lfloor \frac{\alpha}{2} \rfloor.$$

Lemma 2.2. *For $(A, B) \in S_2(n, \delta)$ there exist $s, t \in \{1, 2, \dots, n\}$ such that*

$$(|A_{11}^{st}| + |A_{22}^{st}|)(|B_{12}^{st}| + |B_{21}^{st}|) + (|A_{12}^{st}| + |A_{21}^{st}|)(|B_{11}^{st}| + |B_{22}^{st}|) \ge \frac{\delta(n-\delta)}{n(n-1)} \cdot |A| \cdot |B|.$$

Proof. Set $C^{st}(ij) = \{(c_1, \dots, c_n) \in C : \ c_s = i, c_t = j\}$. Then $|C^{st}(ij)| = |C_{ij}^{st}|$ and using the indicator function for sets, we can write

$$\sum_{s \ne t} (|A_{11}^{st}| + |A_{22}^{st}|)(|B_{12}^{st}| + |B_{21}^{st}|) + (|A_{12}^{st}| + |A_{21}^{st}|)(|B_{11}^{st}| + |B_{22}^{st}|) =$$

$$= \sum_{\substack{(x^n, y^n) \in (A,B) \\ s \ne t}} (1_{A_{11}(st)}(x^n) + 1_{A_{22}(st)}(x^n))(1_{B_{12}(st)}(y^n) + 1_{B_{21}(st)}(y^n)) +$$

$$+ (1_{A_{12}(st)}(x^n) + 1_{A_{21}(st)}(x^n))(1_{B_{11}(st)}(y^n) + 1_{B_{22}(st)}(y^n)).$$

Since for $x^n \in A, \quad y^n \in B \quad d(x^n, y^n) = \delta$, the contribution of (A, B) is $|A| \cdot |B| \cdot \delta \cdot (n - \delta)$ and since there are $\binom{n}{2}$ pairs (s, t), there is one pair with a contribution $\binom{n}{2}^{-1} |A| \cdot |B| \cdot \delta \cdot (n - \delta)$. ■

The other auxiliary result of this kind, used for the proof of Theorem 1(b), is

Lemma 2.3. *For $(A, B) \in S_\alpha(n, \delta)$ there exists a $t \in \{1, 2, \dots, n\}$ with*

$$\frac{1}{2} \sum_{I \in \mathcal{P}_\beta(\mathcal{X}_\alpha)} |A^t(I)| \cdot |B^t(I^c)| + |A^t(I^c)| \cdot |B^t(I)| \ge |A| \cdot |B| \cdot \frac{\delta}{n(\alpha-1)} \cdot \frac{\overline{\alpha}}{\alpha} \cdot \binom{\alpha}{\beta}.$$

Here $I^c = \mathcal{X}_\alpha \backslash I$.

Proof.

$$\sum_{t=1}^{n} \sum_{I \in \mathcal{P}_\beta(\mathcal{X}_\alpha)} |A^t(I)| \cdot |B^t(I^c)|$$

$$= \sum_{t=1}^{n} \sum_{I \in \mathcal{P}_\beta(\mathcal{X}_\alpha)} \sum_{x^n \in A, y^n \in B} 1_{A^t(I)}(x^n) 1_{B^t(I^c)}(y^n)$$

$$= \sum_{x^n \in A, y^n \in B} \sum_{t=1}^{n} \sum_{I \in \mathcal{P}_\beta(\mathcal{X}_\alpha)} 1_{A^t(I)}(x^n) 1_{B^t(I^c)}(y^n)$$

$$= \sum_{x^n \in A, y^n \in B} \delta \binom{\alpha - 2}{\beta - 1} = |A| \cdot |B| \cdot \delta \cdot \binom{\alpha - 2}{\beta - 1}.$$

By symmetry also

$$\sum_{t=1}^{n} \sum_{I \in \mathcal{P}_\beta(\mathcal{X}_\alpha)} |A^t(I^c)| \cdot |B^t(I)| = |A| \cdot |B| \cdot \delta \cdot \binom{\alpha - 2}{\beta - 1}.$$

Therefore there exists a t with

$$\frac{1}{2} \sum_{I \in \mathcal{P}_\beta(\mathcal{X}_\alpha)} |A^t(I)| \cdot |B^t(I^c)| + |A^t(I^c)| \cdot |B^t(I)| \geq |A| \cdot |B| \frac{\delta}{n} \binom{\alpha - 2}{\lfloor \frac{\alpha}{2} \rfloor - 1}$$

and the result follows with the identity

$$\binom{\alpha}{\lfloor \frac{\alpha}{2} \rfloor} = \frac{\alpha(\alpha - 1)}{\lfloor \frac{\alpha}{2} \rfloor \lceil \frac{\alpha}{2} \rceil} \binom{\alpha - 2}{\lfloor \frac{\alpha}{2} \rfloor - 1}. \quad \blacksquare$$

Proof of (a) in Theorem 1

The cases $\delta = 0$ and $\delta = n$, which are not covered by Lemma 1(a), are verified directly.

$$M_2(n, 0) = F_2(n, 0) = 1, \quad M_2(n, n) = F_2(n, n) = 1. \tag{2.13}$$

For the other cases we proceed by induction on n.

Among the cases $n = 1, 2$, $\delta \neq 0, n$, not settled in (2.13) there is only the case

$$M_2(2, 1) = F_2(1, 1) = 4. \tag{2.14}$$

An optimal configuration here is $(A, B) = (\{00, 11\}, \{10, 01\})$.

$\underline{n - 2 \to n}$: We use the sets $A^{st}_{\epsilon\delta}$, $B^{st}_{\epsilon\delta}$ with the property stated in Lemma 2.2. Since no misunderstanding is possible we omit the indices s, t. Let us consider the scheme

	A_{11} A_{22}	A_{12} A_{21}
B_{11} B_{22}	I	II
B_{12} B_{21}	III	IV

The convention here is that
$I = (|A_{11}| + |A_{22}|)(|B_{11}| + |B_{22}|)$, etc.

Lemma 2.2 says that

$$|A| \cdot |B| \leq \frac{1}{2} \frac{n(n-1}{\delta(n-\delta)} (II + III). \tag{2.15}$$

Without loss of generality we can assume that

$$II \leq III. \tag{2.16}$$

Case: $A_{11} \cap A_{22} \neq \emptyset$
Since $d(a_{11}, b_{\varepsilon\varepsilon}) \neq d(a_{22}, b_{\varepsilon\varepsilon})$, necessarily $B_{11} = B_{22} = \emptyset$ and thus $I = II = 0$.

If now $B_{12} \cap B_{21} \neq \emptyset$, then by the same argument $A_{12} = A_{21} = \emptyset$ and thus also $IV = 0$. Therefore
$|A| \cdot |B| = III \leq 4 \cdot M_2(n-2, \delta-1) = 4 \cdot F_2(n-2, \delta-1)$ (by induction hypothesis) $\leq F_2(n, \delta)$ (by Lemma 2.1(a)).

If on the other hand $B_{12} \cap B_{21} = \emptyset$, then $A_{\varepsilon\varepsilon}, B_{12} \cup B_{21}) \in S_2(n-2, \delta-1)$ for $\varepsilon = 1, 2$ and therefore $III \leq 2 \cdot M_2(n-2, \delta-1)$. Since $II = 0$, we conclude that $II + III \leq 2 \cdot M_2(n-2, \delta-1) = 2 \cdot F_2(n-2, \delta-1)$ and that by (2.15)

$$|A| \cdot |B| \leq \frac{n(n-1)}{\delta(n-1)} F_2(n-2, \delta-1).$$

Finally, by Lemma 2.1(a) $|A| \cdot |B| \leq F_2(n, \delta)$.

Case: $A_{11} \cap A_{22} = \emptyset$
If now $B_{12} \cap B_{21} \neq \emptyset$, then, as previously, $A_{12} = A_{21} = \emptyset$, thus $II = 0$, $II + III = III \leq 2 \cdot M_2(n-2, \delta-1)$ and $|A| \cdot |B| \leq F_2(n, \delta)$. Finally, if $B_{12} \cap B_{21} = \emptyset$, then

$$(A_{11} \dot{\cup} A_{22},\ B_{12} \dot{\cup} B_{21}) \in S_2(n-2, \delta-2)$$

and thus $III \leq M_2(n-2, \delta-1$. By (2.16) $II + III \leq 2 \cdot M_2(n-2, \delta-1)$ and the proof can be completed as before. ■

Proof of (b) in Theorem 1: $\alpha = 4$

Since $\mathcal{P}_\beta(\mathcal{X}_\alpha)| = \binom{\alpha}{\beta}$, it follows from Lemma 2.3 that for some $I \in \mathcal{P}_\beta(\mathcal{X}_\alpha)$

$$|A^t(I)| \cdot |B^t(I^c)| + |A^t(I^c)| \cdot |B^t(I)| \geq \frac{2\delta}{n(\alpha-1)} \cdot \frac{\overline{\alpha}}{\alpha} \cdot |A| \cdot |B|. \tag{2.17}$$

In case $\alpha = 4$ we can assume that after relabelling $I = \{1,2\}$, $I^c = \{3,4\}$. We omit again the index t and consider the scheme

	A_1 A_2	A_3 A_4
B_1 B_2	I	II
B_3 B_4	III	IV

For $\alpha = 4$ the inequality (2.17) can be written in the form

$$\begin{aligned} |A| \cdot |B| &= \frac{3n}{2\delta}[(|A_1| + |A_2|)(|B_3| + |B_4|) + (|A_3| + |A_4|)(|B_1| + |B_2|)] \quad (2.18) \\ &\leq \frac{3n}{2\delta}(II + III). \end{aligned}$$

If now in the proof of Theorem 1(a) we perform the following substitutions:
$11 \to 1$, $22 \to 2$, $12 \to 3$, $21 \to 4$, $A_{11} \to A_1$, $B_{11} \to B_1$, etc.;
$F_2(n,\delta) \to F_4(n,\delta)$, $F_2(n-2,\delta-1) \to F_2(n-1,\delta-1)$;
(2.15) $\to$ (2.18); and finally Lemma 2.1(a) $\to$ Lemma 2.1(b), then all arguments literally apply. Here it is also essential that $\overline{\alpha} = 4$ for all $\alpha = 4$. The case $n = 1$ is done by inspection. ■

How far does the approach go?

Before we prove Theorem 1 for $\alpha = 5$, we shall investigate how far the averaging procedure in Lemma 2.3 can go. This is no detour, because most of the argument is needed for proving the positive result for $\alpha = 5$ (in the case $K = 1$ below) anyhow. It turns out that the procedure can be successful only if

$$\left\lfloor \frac{\alpha-1}{2} \right\rfloor \cdot \left\lceil \frac{\alpha-1}{2} \right\rceil \leq \alpha - 1. \tag{2.19}$$

Notice that this condition is satisfied for $\alpha = 4$ and for $\alpha = 5$ with equality! For $\alpha \geq 6$ the approach has to fail even if we work with the average $G = E + \overline{E}$, where

$$E = \sum_{I \in \mathcal{P}_\beta(\mathcal{X}_\alpha)} |A^t(I)| \cdot |B^t(I^c)| \tag{2.20}$$

$$\overline{E} = \sum_{I \in \mathcal{P}_\beta(\mathcal{X}_\alpha)} |A^t(I^c)| \cdot |B^t(I)| \tag{2.21}$$

and

$$\frac{1}{2} G \geq |A| \cdot |B| \cdot \frac{\delta}{n(\alpha - 1)} \cdot \frac{\overline{\alpha}}{\alpha} \cdot \binom{\alpha}{\beta}. \tag{2.22}$$

Henceforth we drop again the index t and we calculate G by using a familiar scheme (see [4]).

Define the non-negative numbers K, S and T by

$$K = |\{1 \leq i \leq \alpha : \ |A_i| \cdot |B_i| > 0\}| \tag{2.23}$$

$$S = |\{1 \leq i \leq \alpha : \ |A_i| > 0\}| - K, \qquad T = |\{1 \leq i \leq \alpha : \ |B_i| > 0\}| - K. \tag{2.24}$$

After relabelling we have

$$\begin{aligned} &|A_i| \cdot |B_i| > 0 \ \text{ for } \ 1 \leq i \leq K; \ \ |A_i| > 0 \ \text{ for } \ 1 \leq i \leq K + S \ \text{ and} \\ &|B_i| > 0 \ \text{ for } \ 1 \leq i \leq K \ \text{ and } \ K + S \leq i \leq K + S + T. \end{aligned} \tag{2.25}$$

One readily verifies

Lemma 2.4. (Special case of Lemma 2 in [4]) *Let $n \geq 2$. If $(A, B) \in S_\alpha(n, \delta)$ and if $K + S, \ K + T \geq 2$, then for $1 \leq i \leq K, \ 1 \leq j \leq \alpha, \ i \neq j$*

$$(a) \qquad A_i \cap A_j = \emptyset \quad \text{and} \quad (b) \qquad B_i \cap B_j = \emptyset. \qquad \blacksquare$$

We use the notation

$$X = \{1, 2, \ldots, K\}, \ \ Y = \{K + 1, \ldots, K + S\}, \tag{2.26}$$

$$Z = \{K + S + 1, \ldots, K + S + T\}.$$

It is also clear that the replacement of A_i for $i \in Y$ by $C = \cup_{i \in Y} A_i$ and of B_i for $i \in Z$ by $D = \cup_{i \in Z} B_i$ leads again to a pair in $S_\alpha(n, \delta)$. We can enlarge Y so that $K + S + T = \alpha$.

Evaluation of E

For $I \in \mathcal{P}_\beta(\mathcal{X}_\alpha)$ we define

$$U = I \cap X, \quad V = I \cap Y, \quad W = I \cap Z. \tag{2.27}$$

We use also the abbreviations

$$a(J) = \sum_{i \in J} |A_i|, \quad b(J) = \sum_{j \in J} |B_j| \quad \text{for} \quad J \in \mathcal{X}. \tag{2.28}$$

With these conventions we can write

$$E = \sum_{\substack{U \subset X,\, V \subset Y,\, W \subset Z \\ |U|+|V|+|W|=\beta}} [a(U) + |V| \cdot |C|] \cdot [b(x \backslash U) + |Z \backslash W| \cdot |D|]. \tag{2.29}$$

Application of the distributive law leads to four sums, which we denote by E_1, E_2, E_3, and E_4.

$$E_1 = \sum_{\substack{U \subset X,\, V \subset Y,\, W \subset Z \\ |U|+|V|+|W|=\beta}} \cdot a(U) \cdot b(X \backslash U) = \sum_{\substack{U \subset X, \ell \\ |U|+\ell=\beta}} \binom{S+T}{\ell} a(U) \cdot b(X \backslash U)$$

$$= \sum_{\substack{U \subset X \\ 1 \le |U| \le \min(\beta, K-1)}} \binom{\alpha - K}{\beta - |U|} \cdot a(U) \cdot b(X \backslash U)$$

$$E_2 = \sum_{\substack{U \subset X,\, V \subset Y,\, W \subset Z \\ |U|+|V|+|W|=\beta}} a(U) \cdot |Z \backslash W| \cdot |D|$$

$$= \sum_{\substack{U \subset X \\ |U|+|V|+|W|=\beta}} \binom{S}{|V|} \binom{T}{|W|} (T - |W|) \cdot a(U) \cdot |D|$$

$$= \sum_{\substack{U \subset X \\ |U|+|V|+|W|=\beta}} \binom{S}{|V|} \binom{T-1}{|W|} \cdot T \cdot a(U) \cdot |D|$$

$$= \sum_{\substack{U \subset X \\ 1 \le |U| \le \beta}} \binom{\alpha - K - 1}{\beta - |U|} \cdot T \cdot a(U) \cdot |D|$$

$$E_3 = \sum_{\substack{U\subset X,\, V\subset Y,\, W\subset Z \\ |U|+|V|+|W|=\beta}} b(X\backslash U)\cdot|V|\cdot|C|$$

$$= \sum_{\substack{U\subset X \\ |U|+|V|+|W|=\beta}} \binom{S}{|V|}\binom{T}{|W|}\cdot|V|\cdot b(X\backslash U)\cdot|C|$$

$$= \sum_{\substack{U\subset X \\ |U|+|V|+|W|=\beta}} \binom{S-1}{|V|-1}S\binom{T}{|W|}\cdot b(X\backslash U)\cdot|C|$$

$$= \sum_{\substack{U\subset X \\ |U|\le\min(\beta,K-1)}} \binom{\alpha-K-1}{\beta-|U|-1}\cdot b(X\backslash U)\cdot S\cdot|C|$$

$$E_4 = \sum_{\substack{U\subset X,\, V\subset Y,\, W\subset Z \\ |U|+|V|+|W|=\beta}} |V|\cdot|C|\cdot|Z\backslash W|\cdot|D|$$

$$= \sum_{\substack{U\subset X \\ |U|+|V|+|W|=\beta}} \binom{S}{|V|}\binom{T}{|W|}\cdot|V|\cdot|Z\backslash W|\cdot|C|\cdot|D|$$

$$= \sum_{\substack{U\subset X \\ |U|+|V|+|W|=\beta}} \binom{S-1}{|V|-1}\binom{T-1}{|W|}\cdot S\cdot T\cdot|C|\cdot|D|$$

$$= \sum_{\substack{U\subset X \\ |U|\le\beta-1}} \binom{\alpha-K-2}{\beta-|U|-1}\cdot S\cdot T\cdot|C|\cdot|D|.$$

Now notice that in the extremal configuration $E_1(1, n-d_1)$ defined in Section 1 the case $K = 1$ arises. Does an induction based on Lemma 2.3 and Lemma 2.1(b) work in this case?

We have here by the constraints imposed on U

$$E_1 = 0, \quad E_2 = \binom{\alpha-2}{\beta-1}\cdot T\cdot|A_1|\cdot|D|,$$

$$E_3 = \binom{\alpha-2}{\beta-1}|B_1|\cdot S\cdot|C|,$$

$$E_4 = \binom{\alpha-3}{\beta-1}S\cdot T\cdot|C|\cdot|D| + \binom{\alpha-3}{\beta-2}S\cdot T\cdot|C|\cdot|D| = \binom{\alpha-2}{\beta-1}S\cdot T\cdot|C|\cdot|D|,$$

and

$$E = \binom{\alpha-1}{\beta-1}(|A_1|\cdot T\cdot|D| + |B_1|\cdot S\cdot|C| + S\cdot|C|\cdot T\cdot|D|). \tag{2.30}$$

Notice the complete symmetry of the formula in A and B! Thus $E = \overline{E}$ and $\frac{1}{2}G = E$ in this case.

By Lemma 2.1(b) and Lemma 2.3 (resp., 2.22) *sufficient* for the induction to work would be

$$E \leq F_\alpha(n-1, \delta-1) \cdot \frac{\overline{\alpha}}{\alpha} \cdot \binom{\alpha}{\beta}. \tag{2.31}$$

By (2.30) this means that for

$$\lambda = |A_1| \cdot T \cdot D + |B_1| \cdot S \cdot |C| + S \cdot |C| \cdot T \cdot |D|$$

we must have

$$\lambda \leq F_\alpha(n-1, \delta-1)(\alpha-1). \tag{2.32}$$

We can write λ in the form

$$\begin{aligned}\lambda &= S \cdot |C| \cdot (B_1| + |D|) + (|A_1| + |C|) \cdot T \cdot |D| \\ &\quad + (S-1) \cdot T \cdot |C| \cdot |D| - S \cdot |C| \cdot |D| \\ &= S \cdot |C| \cdot (|B_1| + |D|) + (|A_1| + |C|) \cdot T \cdot |D| + (ST - S - T) \cdot |C| \cdot |D|.\end{aligned}$$

Since $C, (B_1 \cup D))$, $(A_1 \cup C, D)$, $(C, D) \in S_\alpha(n-1, \delta-1)$ an induction hypothesis gives

$$\lambda \leq [S + T + (ST - S - T)]F_\alpha(n-1, \delta-1) \leq \left\lfloor \frac{\alpha-1}{2} \right\rfloor \cdot \left\lceil \frac{\alpha-1}{2} \right\rceil \cdot F_\alpha(n-1, \delta-1).$$

We see that (2.32) holds if (2.19) holds.

Proof of (b) in Theorem 1: $\alpha = 5$

The induction beginning for $n = 1$ is done by inspection. For the induction step it is sufficient by (2.31) to establish

$$E \leq F_5(n-1, \delta-1) \cdot 12. \tag{2.33}$$

For this we go through the cases defined by the value of K.

$\underline{K = 5}$: Since $S = T = 0$, we have $E_2 = E_3 = E_4 = 0$. Therefore,

$$E = E_1 = \sum_{\substack{U \subset \{1,2,\ldots,5\} \\ 1 \leq |U| \leq 2}} \binom{5-5}{2-|U|} \cdot a(U) \cdot b(X \backslash U).$$

Since $(\cup_{i \in U} A_i, \cup_{i \in X \backslash U} B_i) \in S_5(n-1, \delta-1)$ and by Lemma 2.4

$$|\cup_{i \in U} A_i| = a(U); \quad |\cup_{i \in X \backslash U} B_i| = b(X \backslash U),$$

we get

$$E \le \binom{5}{2} \cdot M_5(n-1, \delta-1) \le 10 \cdot F_5(n-1, \delta-1)$$

(by induction hypothesis).

$\underline{K=4}$: Either $S=1$, $T=0$, or $S=0$, $T=1$. By symmetry it suffices to consider the first case. Then $E_2 = E_4 = 0$, and

$$\begin{aligned} E = E_1 + E_2 &= \sum_{\substack{U \subset \{1,2,3,4\} \\ 1 \le |U| \le 2}} \binom{1}{2-|U|} \cdot a(U) \cdot b(X \backslash U) \\ &\quad + \sum_{\substack{U \subset \{1,2,3,4\} \\ |U| \le 2}} \binom{0}{2-|U|-1} b(X \backslash U) \cdot S \cdot |C| \\ &\le \binom{4}{2} F_5(n-1, \delta-1) + \sum_{\substack{U \subset \{1,2,3,4\} \\ |U|=1}} (a(U) + |C|) \cdot b(X \backslash U). \end{aligned}$$

By lemma 2.4 and the induction hypothesis the second summand is smaller than $4 \cdot F_5(n-1, \delta-1)$ and therefore $E \le 10 \cdot F_5(n-1, \delta-1)$.

$\underline{K=3}$:

$$\begin{aligned} E_1 &= \sum_{\substack{U \subset \{1,2,3\} \\ 1 \le |U| \le 2}} \binom{2}{2-|U|} \cdot a(U) \cdot B(X \backslash U) \\ &= 2[|A_1|(|B_2| + |B_3|) + |A_2|(|B_1| + |B_3|) + |A_3|(|B_1| + |B_2|)] \\ &\quad + [(|A_1| + |A_2|)|B_3| + (|A_1| + |A_3|)|B_2| + (|A_2| + |A_3|)|B_1|] \\ E_2 &= 3[|A_1| + |A_2| + |A_3|] \cdot T \cdot |D| \\ E_3 &= 3[|B-1| + |B_2| + |B_3|] \cdot S \cdot |C| \\ E_4 &= 3 \cdot S \cdot T \cdot |C| \cdot |D|. \end{aligned}$$

$\underline{S=2,\ T=0}$:

$$\begin{aligned} E = E_1 + E_3 &= 3(|B_1| + |B_2|)(|A_3| + |C|) \\ &\quad + 3(|B_1| + |B_3|)(|A_2| + |C|) + 3(|B_2| + |B_3|)(|A_1| + |C|). \end{aligned}$$

Since $(B_1 \dot\cup B_2, A_3 \dot\cup C) \in S_5(n-1, \delta-1)$ etc., we get $E \le 9 \cdot F_5(n-1\delta-1)$.

$\underline{S=1,\ T=1}$: $E = E_1 + E_2 + E_3 + E_4$

$$E_2 = 3[|A_1| + |A_2| + |A_3|]|D| \quad E_3 = 3[|B_1| + |B_2| + |B_3|]|C| \quad .E_4 = 3|C| \cdot |D|$$

and E_1 as previously.

We can assume that $E_2 \le E_3$, because otherwise we can exchange the roles of A and B, Thus, by the previous case, $E_1 + E_2 + E_3 \le 9 \cdot F_5(n-1, \delta - 1)$, and since $E_4 \le 3 \cdot F_5(n-1, \delta-1)$, we get $E \le 12 \cdot F_5(n-1, \delta-1)$.

$S = 0,\ T = 2$: Since E_1 and E_2 are symmetric in A and B, replacement of E_3 by E_2 in the case $S = 2,\ T = 0$ gives again the bound $E \le 9 \cdot F_5(n-1, \delta-1)$.

$K = 2$:

$$E_1 = \sum_{\substack{U \subset \{1,2\} \\ |U|=1}} \binom{3}{2-|U|} \cdot a(U) \cdot b(X \backslash U) = 3[|A_1| \cdot |B_2| + |A_2| \cdot |B_1|]$$

$$E_2 = \sum_{\substack{U \subset \{1,2\} \\ 1 \le |U| \le 2}} \binom{2}{2-|U|} \cdot a(U) \cdot T \cdot |D| = 3[|A_1| + |A_2|] \cdot T \cdot |D|$$

$$E_3 = \sum_{\substack{U \subset \{1,2\} \\ |U| \le 1}} \binom{2}{1-|U|} \cdot b(X \backslash U) \cdot S \cdot |C| = 3[|B-1| + |B_2|] \cdot S \cdot |C|$$

$$E_4 = \sum_{\substack{U \subset \{1,2\} \\ |U| \le 1}} \binom{1}{1-|U|} S \cdot T \cdot |C| \cdot |D| = 3S \cdot T \cdot |C| \cdot |D|.$$

$S = 3,\ T = 0$:

$$E = E_1 + E_3 = 3|B_1|(|A_2| + |C|) + 3|B_2|(|A_1| + |C|) + 6(|B_1| + |B_2|)|C| \le 12 \cdot F_5(n-1, \delta-1).$$

$S = 2,\ T = 1$:

$$E = E_1 + E_2 + E_3 + E_4 = [E_1 + E_2 + \frac{E_3}{2} + E_4] + \frac{E_3}{2}$$
$$= 3(|B_1| + |D|)(|A_2| + |C|) + 3(|B_2| + |D|)(|A_1| + |C|) + 3(|B_1| + |B_2|)|C| \le 9 \cdot F_5(n-1, \delta-1).$$

The other cases are symmetrically the same.

$K = 1$: This case was done earlier, when we arrived at the condition (2.19).

$K = 0$: Here and only here the factor $\overline{\alpha} = 6$ comes into play!

$$|A| \cdot |B| = S \cdot T \cdot |C| \cdot |D| \le 6 \cdot |C| \cdot |D| \le 6 \cdot F_5(n-1, \delta-1). \quad \blacksquare$$

3. Proof of Theorem 2

Here and later we use the notation

(3.1) $\langle a|i\rangle =$ number of occurrences of i in the sequence a.

(3.2) $$\mathcal{E}_n = \{a \in \mathcal{X}_2^n : \langle a|1\rangle \text{ is even}\} \text{ and}$$
$$\mathcal{O}_n = \{a \in \mathcal{X}_2^n : \langle a|1\rangle \text{ is odd}\}.$$

Clearly,

(3.3) $$|\mathcal{E}_n| = |\mathcal{O}_n| = 2^{n-1}.$$

Notice that the pairs $(\mathcal{E}_n, \mathcal{E}_n)$, $(\mathcal{O}_n, \mathcal{O}_n)$ have 0-parity and that the pairs $(\mathcal{E}_n, \mathcal{O}_n)$, $(\mathcal{O}_n, \mathcal{E}_n)$ have 1-parity.

Therefore, $(\mathcal{E}_n \cup \mathcal{O}_n, \mathcal{E}_n)$ satisfies $(\vec{P})$ and by (3.3) we have

(3.4) $$\vec{Q}_2(n) \geq 2 \cdot 4^{n-1}.$$

Next notice that $(\mathcal{E}_n \cup \mathcal{O}_n \cup \{33\ldots3\}, \mathcal{E}_n)$ satisfies $(\vec{P})$ and therefore

(3.5) $$\vec{Q}_3(n) \geq (2^n + 1) \cdot 2^{n-1}.$$

Also, the pair $(\{1,\ldots,\beta\}^n, \{\beta+1,\ldots,\alpha\}^n)$ satisfies $(\vec{P})$ and therefore in particular

(3.6) $$\vec{Q}_\alpha(n) \geq \overline{\alpha}^n \text{ for } \alpha \geq 4.$$

The issue is now to establish the reverse inequalities in (2.23)–(2.25). The proof by induction on n is based on two Lemmas.

Lemma 3.1. *(Inheritance of $(\vec{P})$)*
If for $n \geq 2$ (A, B) $A, B \subset \mathcal{X}_\alpha^n$, satisfies $(\vec{P})$, then

(a) $(\cup_{i\in I} A_i, B_j)$ satisfies $(\vec{P})$ for every j, $I \subset \mathcal{X}_\alpha$.

(b) $(A_i \cup_{j\in J} B_j)$ satisfies $(\vec{P})$ for every $J \subset \mathcal{X}_\alpha$, $J \neq \mathcal{X}_\alpha$ and $\{i\} \subset \mathcal{X}_\alpha \backslash J$.

Proof.

(a) Since for any $ai \in A$ $\pi(ai, c)$ is independent of $c \in B$, this is also the case for every $bj \in B$. Thus $\pi(ai, bj)$ and consequently $\pi(a, b)$ are independent of $b \in B_j$.

(b) Since $\pi(ai, bj)$ is constant for all $b \in B_j$ and all $j \in J$, and since $\pi(i, j) = 1$ for all $j \in J$, $i \notin J$, we also have $\pi(a, b)$ constant for all $b \in \cup_{j\in J} B_j$.

Lemma 3.2. *(Disjointness property)*
If for $n \geq 2$ (A, B), $A, B \subset \mathcal{X}_\alpha^n$, *satisfies* $(\vec{P})$, *then for* $1 \leq i \leq K$, $1 \leq j \leq \alpha$

(a) $$B_i \cap B_j = \emptyset \text{ for } i \neq j$$

(b) $$A_i \cap A_j = \emptyset \text{ for } i \neq j, \text{ if } B_\ell \neq \emptyset \text{ for some } \ell \neq i, j.$$

Proof.

(a) If $b \in B_i \cap B_j$, then by $(\vec{P})$ for any $a \in A_i$ $\pi(ai, bi) = \pi(ai, bj)$, which contradicts $d(ai, bi) = d(ai, bj) - 1$.

(b) If $a \in A_i \cap A_j$, then by $(\vec{P})$ for any $b \in B_i$ and $b' \in B_\ell$ $\pi(ai, bi) = \pi(ai, b'\ell)$ and $\pi(aj, bi) = \pi(aj, b'l)$, which contradicts $\pi(i, i) \neq \pi(i, \ell)$ and $\pi(j, i) = \pi(j, \ell)$. ∎

Theorem 2 will be derived from

Lemma 3.3. *For every* $\alpha \geq 2$

(i) $$\vec{Q}_\alpha(1) \leq \alpha^* = \max(a, \overline{\alpha}).$$

For any (A, B), $A, B \subset \mathcal{X}_\alpha^n$ $(n \geq 2)$, *satisfying* $(\vec{P})$ *with parameters* K, S, T *in the basic scheme (2.23)–(2.25)*

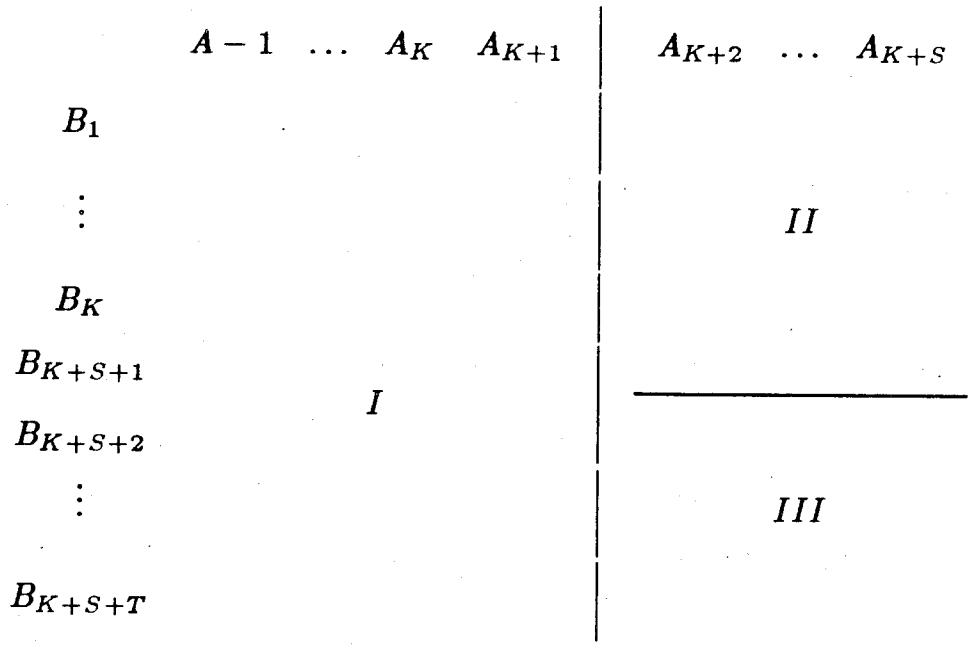
(ii) $$|A| \cdot |B| \leq \alpha^* \cdot \vec{Q}_\alpha(n-1), \text{ if } T \geq 1 \text{ or } K \geq 3$$

(iii) $$|A| \cdot |B| \leq [4 + \max(0, \alpha - 4)] \cdot \vec{Q}_\alpha(n-1), \text{ if } T = 0 \text{ and } K \leq 2.$$

Proof.

(i) If (A, B) satisfies $(\vec{P})$, then $|B| > 2$ implies in case $n = 1$ $A \cap B = \emptyset$. Therefore, $|A| \cdot |B| \leq \max(\alpha, \overline{\alpha})$.

(ii) We subdivide the basic scheme as follows



$$|A||B| = I + II + III.$$

Since $T \geq 1$ or $K \geq 3$ Lemma 3.2(b) applies and yields

$$A_i \cap A_j = \emptyset \text{ for } 1 \leq i \leq K,\ 1 \leq j \leq \alpha,\ i \neq j. \tag{3.7}$$

Now

$$\begin{aligned} I &= \sum_{i=1}^{K+1} |A_i| \Big(\sum_{j=1}^{K} |B_j| + \sum_{j=K+S+1}^{K+S+T} |B_j| \Big) \\ &= \Big| \bigcup_{i=1}^{K+1} A_i \Big| \Big(\sum_{j=1}^{K} |B_j| + \sum_{j=K+S+1}^{K+S+T} |B_j| \Big) \text{ (by (3.7))} \\ &\leq (K+T)\vec{Q}_\alpha(n-1) \end{aligned}$$

(by Lemma 3.1(a) and the definition of $\vec{Q}_\alpha(n-1)$),

$$II = \sum_{i=K+2}^{K+S} |A_i| \cdot |(\cup_{i=1}^{K} B_i) \cup B_{K+S+1}| \text{ (by Lemma 3.2(a))}$$

$$\leq (S-1)\vec{Q}_\alpha(n-1) \text{ (by Lemma 3.1(b))}$$

$$III = \sum_{i=K+2}^{K+S} |A_i| \sum_{j=K+S+2}^{K+S+T} |B_j| \leq (S-1)(T-1)\vec{Q}_\alpha(n-1).$$

Since $(K+T)+(S-1)+(S-1)(T-1)=K+ST$, and since

$$K+ST \leq \begin{cases} (K+S)T \leq \overline{\alpha} & \text{for } T \geq 1 \\ K \leq \alpha & \text{for } T=0, \end{cases}$$

we conclude that

$$|A| \cdot |B| \leq \max(\alpha, \overline{\alpha}) \vec{Q}_\alpha(n-1). \tag{3.8}$$

(iii) In case $T=0$, $K \leq 1$ obviously

$$|A| \cdot |B| = |B_1| \sum |A_i| \leq \alpha \cdot \vec{Q}_\alpha(n-1) \tag{3.9}$$

and the desired inequality follows.

In case $T=0$, $K=2$ we have by Lemma 3.2(b)

$$A_i \cap A_j = \emptyset \text{ for } i=1,2 \text{ and } j>2 \tag{3.10}$$

and by Lemma 3.2(a)

$$B_1 \cap B_2 = \emptyset. \tag{3.11}$$

Also, by Lemma 3.1(a)

$$|A_i \cup A_j| \cdot |B_\ell| \leq \vec{Q}_\alpha(n-1) \text{ for } i=1,2;\ \ell=1,2;\ j>2 \tag{3.12}$$

and therefore

$$[(|A_1|+|A_3|)+(|A_2|+|A_4|)] \cdot (|B_1|+|B_2|) \leq 4 \cdot \vec{Q}_\alpha(n-1). \tag{3.13}$$

Furthermore, by (3.11) and Lemma 3.1(b)

$$|A_i| \cdot |B_1 \cup B_2| \leq \vec{Q}_\alpha(n-1) \text{ for } i>2$$

and therefore

$$\sum_{i \geq 4} |A_i| \cdot (|B_1|+|B_2|) \leq \max(0, \alpha-4) \cdot \vec{Q}_\alpha(n-1). \tag{3.14}$$

Finally, (3.13) and (3.14) imply (iii). ■

Proof of Theorem 2 (a)

For $\alpha \geq 4$ we have $\alpha^* = \overline{\alpha}$ and therefore Lemma 3.3 implies inductively $\vec{Q}_\alpha(n) \leq \leq \overline{\alpha}^n$, which remained to be shown. ■

Proof of Theorem 2 (b)

For $\alpha = 2$ we have $\alpha^* = \alpha = 2$ and thus $\vec{Q}_2(1) \leq 2$ by (i) and then inductively $\vec{Q}_2(n) \leq 2 \cdot 4^{n-1}$ by (ii), (iii) of Lemma 3.3. ■

Proof of Theorem 2 (c)

Step 1: For $\alpha = 3$ we have $\alpha^* = \alpha = 3$. Using the function

$$F(n) = (2^n + 1) \cdot 2^{n-1} \quad \text{for} \quad n \geq 1 \tag{3.15}$$

we see that by Lemma 3.3(i) $\vec{Q}_3(1) \leq 3 = F(1)$ and the case $n = 1$ is settled.

Furthermore, in case $T =\geq 1$ or $K \geq 3$ by (ii) and in case $T = 0$ and $K \leq 1$ by (3.9) we have

$$|A| \cdot |B| \leq 3 \cdot \vec{Q}_3(n-1). \tag{3.16}$$

Since for all $n \geq 1$ it can be shown that

$$3 \cdot F(n-1) \leq F(n), \tag{3.17}$$

it would follow inductively that $\vec{Q}_3(n) \leq F(n)$ unless we have the condition

(K–T) For *all* $t = 1, 2, \ldots, n$ in the basic scheme the case $T = 0,;\ K = 2$ occurs.

Notice that in this case by (3.10) and (3.11) the conditions

$$(A) \qquad A_i^t \cap A_j^t = \emptyset \quad \text{for} \quad i = 1,2 \quad \text{and} \quad j = 3 \quad \text{for} \quad t = 1, 2, \ldots, n$$

$$(B) \qquad B_1^t \cap B_2^t = \emptyset \quad \text{for} \quad t = 1, 2, \ldots, n$$

also hold automatically. Furthermore, we can replace A by A^* by defining for a fixed t $A_i^{*t} = A_1^t \cup A_2^t$ for $i = 1, 2$ and $A_3^{*t} = A_3^t$. These operations can only increase cardinalities and after finitely many iterations we achieve the condition

$$(C) \qquad A_1^t = A_2^t \quad \text{for} \quad t = 1, 2 \ldots n,$$

if we use the letter A again. Of course, we can assume that this new A and the old B satisfy again (K–T), because otherwise we are in cases for which the result is inductively already established.

Notice that (K–T) implies $B \subset \{1,2\}^n$.

We speak of *critical case,* if for $A, B) \in \vec{P}_3(n)$

$$(D) \qquad B \subset \{1,2\}^n \quad \text{and} \quad A \quad \text{satisfies (C).}$$

Step 2: An equivalent formulation for the critical case
For $Y \subset \{1,2,\ldots,n\}$ we define

$$^{Y}A = \{a = (a_1,\ldots,a_n) \in A:\ a_i = 3 \text{ iff } i \in Y\}.$$

Notice that in the critical case by (C) ^{Y}A contains *all* sequences in $\mathcal{X}_3^n$ with a 3 exactly in the positions Y. Obviously,

$$^{Y}A \cap {}^{Y'}A = \emptyset \text{ for } Y \neq Y' \text{ and } |^{Y}A| = 2^{n-|Y|}, \text{ if } {}^{Y}A \neq \emptyset.$$

Now since $B \subset \{1,2\}^n$ and $(A,B) \in \vec{P}_3(n)$ we must have the condition

(E) For all Y with $^{Y}A \neq \emptyset$ B has *parity on* $X = \{1,2,\ldots,n\}\backslash Y$ (as defined in Section 1)

and, conversely, (E) implies $(A,B) \in \vec{P}_3(n)$.

Finally, for a *given* $B \subset \{1,2\}^n$ *the* optimal A is obtained when we choose $^{Y}A \neq \emptyset$, if B has parity on X. Then

$$|A| = \sum_{\substack{X \subset \{1,2,\ldots,n\} \\ B \text{ has parity on } X}} 2^{|X|} \cdot |B|,$$

and the critical case is settled by the Lemma.

Step 3: Proof of the Lemma
First we write the sum

$$|A| = \sum_{\substack{X \subset \{1,2,\ldots,n\} \\ B \text{ has parity on } X}} 2^{|X|} \cdot |B|$$

in a more symmetric form. Both $\mathcal{X}_2^n = \{1,2\}^n$ and $\mathcal{P}(\{1,\ldots,n\})$, the family of subsets of $\{1,2,\ldots,n\}$, are canonically isomorphic to $\{0,1\}^n$. In the first case replace "2" by "0" and in the second case map X on $x = (x_1,\ldots,x_n)$, where for $t = 1,2,\ldots,n$

$$x_t = 1 \text{ exactly if } t \in X. \tag{3.18}$$

The property "B has parity on X" then reads

$$\sum_{t=1}^{n} b_t \cdot X_t \equiv i \mod 2 \text{ for some } i \in \{0,1\} \text{ and all } b = (b_1,\ldots,b_n) \in B \subset \{0,1\}^n. \tag{3.19}$$

This suggests to endow $\{0,1\}^n$ with the vector space structure over GF(2). Let us call this vector space $\mathbb{F}_2^n$. The Hamming weight of a vector $x = (x_1,\ldots,x_n) \in \mathbb{F}_2^n$ is

denoted by $w(x)$. The componentwise sum and product of two vectors are denoted by $x+y$ and xy.

(3.20) The inner product $x * y$ of x and y is $\sum_{t=1}^{n} x_t y_t$, where the addition is taken in GF(2).

Defining now for $i = 0, 1$

$$C_i = \{x \in \mathbb{F}_2^n : \ b * x = i \ \text{ for all } \ b \in B\}, \tag{3.21}$$

it follows from (3.19) that

$$|A| = \sum_{\substack{X \subset \{1,2,\ldots,n\} \\ B \text{ has parity on } X}} 2^{|X|} \cdot |B| = \sum_{x \in c_0 \cup C_1} 2^{w(x)} |B|. \tag{3.22}$$

The key observation now is that $C = C_0 = C_1$ is a linear subspace. This is a consequence of (3.21) and the simple, but useful identity

$$w(x+y) = w(x) + w(y) - 2 \cdot w(xy). \tag{3.23}$$

Furthermore, C_0 is a linear subspace, C_1 is an affine subspace of C, and $C_0 \cap C_1 = \emptyset$.

Also, by (3.21) we have that

$$B \subset C_0^{\perp}, \tag{3.24}$$

where $C_0^{\perp}$ denotes the orthogonal dual subspace of C_0. Since $(C_0^{\perp})^{\perp} = C_0$, we can replace B by the larger $C_0^{\perp}$ and get instead of (3.21)

$$C_i = \{x \in \mathbb{F}_2^n : \ c * x = i \ \text{ for all } \ c \in C_0^{\perp}\} \ \text{ for } \ i = 0, 1. \tag{3.25}$$

In order to prove the inequality it suffices therefore to prove

$$\sum_{cx \in C_0} 2^{w(c)} |C_0^{\perp}| + \sum_{c \in C_1} 2^{w(c)} |C_0^{\perp}| \leq (2^n + 1) 2^{n-1}. \tag{3.26}$$

If C_0 has dimension d, then $C_0^{\perp}$ has dimension $n-d$. Thus also $|C_0| = |C_1| = 2^d$, $|C_0^{\perp}| = 2^{n-d}$, and (3.26) is equivalent to

$$\frac{2}{|C|} \sum_{c \in C} 2^{w(c)} \leq 2^n + 1. \tag{3.27}$$

But this is true, because we can partition C into 2 element subsets so that the 0–vector and a vector with maximal weight are paired and arbitrarily otherwise. Notice that each pair contributes less than $2^n + 1$ to the sum $\sum_{c \in C} 2^{w(c)}$. Therefore the average contribution does not exceed $2^n + 1$.

Equality in (3.27) occurs only if $|C| = 2$ and C contains the vector with all components equal to 1. Inspection of the cases in the proof of Lemma 3.3 shows thus also that the optimal configuration described in (3.3) is unique up to relabelling. ■

4. Proof of Theorem 3

(a) For $\psi(n) = i$ the pair $(\{1,\dots,\beta\}^n,\ \{\beta+1,\dots,\alpha\}^n)$ is in $P_\alpha^i(n)$ and therefore $\vec{Q}_\alpha^i(n) \geq \overline{\alpha}^n$. The reverse inequality follows from Theorem 2(a) and the inequality $Q_\alpha^i(n) \leq \vec{Q}_\alpha(n)$.

(a'') This is a consequence of (a) and (a').

(b) This result follows immediately from the fact that for $a, a' \in \mathcal{E}_n,\ b, b' \in \mathcal{O}_n$

$$\Pi(a,a') = \Pi(b,a') = 0 \quad \text{and} \quad \Pi(a,b) = 1.$$

(a') The pair $(\{1,\dots,\beta\}^{n-1}\times\{1\},\ \{\beta+1,\dots,\alpha\}^{n-1}\times\{1\})$ is in $P_\alpha^i(n)$ for $\psi(n) \neq i$ and therefore $Q_\alpha^i(n) \geq \overline{\alpha}^{n-1}$. Also, by Theorem 3(b) $Q_\alpha^i(n) \leq \overline{\alpha}^n$. However, we have to prove strict inequality. This is used in the proof of Theorem 6.

Step1: Since (Π_i) implies $(\vec{\Pi})$ we can *follow* the proof of Theorem 3. We shall assume for $(A,B) \in P_\alpha^i(n)$ $(\alpha \geq 4;\ \psi(n) \neq i)$ that

$$|A| \cdot |B| = \overline{\alpha}^n = \vec{Q}_\alpha(n) \tag{4.1}$$

and shall arrive at a contradiction.

Case $T \geq 1$ or $K \geq 3$ Here $|A| \cdot |B| = \overline{\alpha}\vec{Q}_\alpha(n-1)$ only if $K + ST = \overline{\alpha}$ for $T \geq 1$ or $K = \alpha$ for $T = 0$ in case $\alpha = \overline{\alpha} = 4$.

In the first case necessarily $K = 0$. We summarize our findings in

$$\text{Either} \quad K = 0 \quad \text{or} \quad K = \alpha \quad \text{and} \quad \alpha = 4. \tag{4.2}$$

Case $T = 0,\ K_i \leq 1$ Inspection of (3.9) shows that $|A| \cdot |B| = |B_1| \cdot \sum_i |A_i|$ can get a better upper bound in our case.

Notice that $(B_1, A_j) \in P_\alpha^{i'}(n-1)$ with $\psi(n-1) \neq i'$ and therefore

$$|A| \cdot |B| \leq \vec{Q}_\alpha(n-1) + (\alpha-1) \cdot Q_\alpha^{i'}(n-1),\ \ i' \neq \psi(n-1), \tag{4.3}$$

Even in case $\alpha = 4$ this situation cannot arise if we assume inductively that $Q_\alpha^{i'}(n-1) < \vec{Q}_\alpha(n-1)$, the induction beginning being obviously satisfied.

Case $T = 0,\ K = 2$ Since $\alpha \leq \overline{\alpha}$ for $\alpha > 4$, here only the case $\alpha = 4$ is to be considered as can be seen from (3.13) and (3.14).

Here again we can improve the bound in (3.13) because $(A_2 \cup A_4, B_1) \in \in P_\alpha^{i'}(n-1)$. Thus only the situation described in (4.2) is to be considered.

Step 2: Now in case $K = 0$ we have $(A_i, B_j) \in P_\alpha^{i'}(n-1)$ again and inductively

$$Q_\alpha^i(n) \cdot \overline{\alpha} \cdot Q_\alpha^{i'}(n-1) < \overline{\alpha}\vec{Q}_\alpha(n-1) = \vec{Q}_\alpha(n).$$

Thus the proof is complete for $\alpha > 5$.

Step 3: We are left with $K = 4$, $\alpha = 4$. Here

$$|A| \cdot |B| = I = \Big|\bigcup_{i=1}^{4} A_i\Big| \cdot \sum_{j=1}^{4} |B_j| = 4 \cdot \vec{Q}_4(n-1)$$

only if

(4.4) $$|B_j| \text{ is independent of } j.$$

By the symmetry which we have *now* also

(4.5) $$|A_i| \text{ is independent of } i.$$

Furthermore, again by symmetry

(4.6) $$B_j \cap B_{j'} = \emptyset \text{ for } j \neq j'.$$

But then we can define A^*, B^* such that $A_1^* = A_2^* = A_1 \cup A_2$, $B_3^* = B_4^* = B_3 \cup B_4$. (A^*, B^*) is also in $P_\alpha^i(n)$ and by (4.4), (4.5)

(4.7) $$|A^*| \cdot |B^*| = |A| \cdot |B|.$$

But now we are in the case $K = 0$ discussed already in Step 2 and the proof is complete. ∎

5. Proof of Theorem 4

For all $\alpha \geq 2$ the cases $n = 1, 2$ are done by inspection.

(a) $A \subset \{1,2\}^n$ has 0–parity exactly if

(5.1) $$\langle a|1\rangle \equiv \langle a'|1\rangle \mod 2 \text{ for } a, a' \in A.$$

Clearly,

$$\mathcal{E}_n = \{a \in \{1,2\}^n : \langle a|1\rangle \text{ is even}\}$$

and

$$\mathcal{O}_n = \{a \in \{1,2\}^n : \langle a|1\rangle \text{ is odd}\}$$

have 0–parity and

(5.2) $$|\mathcal{E}_n| = |\mathcal{O}_n| = 2^{n-1}.$$

Thus we have not only shown that $q_2^0(n) = 2^{n-1}$, but also that $|\mathcal{E}_n|$ and $|\mathcal{O}_n|$ are the only optimal configurations.

(b) The examples $A = \{11, 22, \ldots, \alpha\alpha\}^k$ for $n = 2k$ and $A = \{11, 22, \ldots, \alpha\alpha\}^{k-1} \times \{1\}$ for $n = 2k-1$ show that $q_\alpha^0(n) \geq \alpha^{\lfloor n/2 \rfloor}$.

We show now first for $\alpha = 4$ and then for all $\alpha \geq 4$ the reverse inequality. The form of these examples suggests a 2-step induction. Choose any two components and define $A_{\epsilon\delta}$ as previously in Section 2. A first simple observation is stated as

Lemma 5.1. *For $A \subset \mathcal{X}_\alpha^n$, $n \geq 3$, with 0–parity*

$$A_{ij} \cap A_{i'j'} = \emptyset, \quad \text{if} \quad \Pi(ij, i'j') = 1.$$

Proof. For $a \in A_{ij} \cap A_{i'j'}$ and $\Pi(ij, i'j') = 1$ we have also $\Pi(aij, ai'j') = 1$. This contradicts the 0–parity of A.

We distinguish two cases.

Case I: There are $ij, i'j'$ with $\Pi(ij, i'j') =)$, $(i, j) \neq (i', j')$ and $A_{ij} \cap A_{i'j'} \neq \emptyset$.

After relabelling we can assume that $ij = 11$, $i'j' = 22$.

Lemma 5.2. *For $A \subset \mathcal{X}_\alpha^n$, $n \geq 3$, with 0–parity, $A_{11} \cap A_{22} \neq \emptyset$ implies $A_{1\varepsilon}$, $A_{\varepsilon 1}$, $A_{2\delta}$, $A_{\delta 2} = \emptyset$ for $\varepsilon, \delta \in \{3, 4, \ldots \alpha\}$.*

Proof. This follows from the fact that

$$\Pi(11, 2\delta) = \Pi(11, \delta 2) \neq \Pi(22, 2\delta) = \Pi(22, \delta 2) \quad \text{and}$$
$$\Pi(11, 2\varepsilon) = \Pi(11, \varepsilon 2) \neq \Pi(22, 2\varepsilon) = \Pi(22, \varepsilon 2)$$

for $\varepsilon, \delta \in \{3, 4, \ldots, \alpha\}$. ■

$\underline{\alpha = 4}$

By Lemma 5.2 we are left with the sets A_{11}, A_{22}; A_{12}, A_{21}; A_{33}, A_{44}; A_{34}, A_{43}. Next we can assume that $A_{11} = A_{22} = C$, say, because for $\varepsilon, \delta \in \{11, 22, 12, 21, 33, 44, 34, 43\}$

$$\Pi(11, \varepsilon\delta) = \Pi(22, \varepsilon\delta).$$

Similarly, we can assume that $A_{12} = A_{21} = D$, $A_{33} = A_{44} = E$, and $A_{34} = A_{43} = F$.

The properties of these sets are listed in

Lemma 5.3.

(0)	$C \cap D = \emptyset$,		$E \cap F = \emptyset$
(1)	$C \cap E = \emptyset$	or	$D = F = \emptyset$
(2)	$C \cap F = \emptyset$	or	$E = D = \emptyset$
(3)	$D \cap E = \emptyset$	or	$C = F = \emptyset$
(4)	$D \cap F = \emptyset$	or	$C = E = \emptyset$

Proof. (0) follows from Lemma 5.1.

By symmetry it suffices to prove (1). Notice that in case $C \cap E \neq \emptyset$ *and* $F \neq \emptyset$ for $a \in C \cap E$ and $f \in F$ $\Pi(a_{11}, f_{34}) \neq \Pi(a_{33}, f_{34})$, which contradicts the 0–parity of A. Thus $C \cap E \neq \emptyset$ implies $F = \emptyset$ and similarly $D = \emptyset$ ■

By relabelling we can assume now that

$$|C| + |E| \geq |C| + |F|, \ |D| + |E|, \ |D| + |F|. \tag{5.3}$$

Subcase 1: $\underline{C \cap E = \emptyset}$

Here we can build

$$A^* = \cup_{\varepsilon=1}^{4}(C \cup E)_{\varepsilon\varepsilon}. \tag{5.4}$$

This set has 0–parity and applying the induction hypothesis to $C \dot\cup E$ we get $|A^*| \leq q_4^0(n-2)$. The same bound holds also for $|A|$, because by (5.3)

$$|A^*| = 4 \cdot (|C| + |E|) \geq 2 \cdot (|C| + |D| + |E| + |F|) = |A|.$$

Subcase 2: $\underline{C \cap E \neq \emptyset}$

By Lemma 5.3(1) $F = D = \emptyset$ and we have $|A| = 2 \cdot |C| + 2 \cdot |E| \leq 4 \cdot q_4^0(n-2)$ by the induction hypothesis for C and for E.

Case II: $A_{ij} \cap A_{i'j'} = \emptyset$ for all $ij \neq i'j'$.

Notice that by Lemma 5.1 this is the only case left, if we are not in Case I. We can write

$$\begin{aligned} A = {} & |A_{11} \dot\cup A_{22} \dot\cup A_{33} \dot\cup A_{44}| + |A_{12} \dot\cup A_{23} \dot\cup A_{34} \dot\cup A_{41}| \\ & + |A_{13} \dot\cup A_{24} \dot\cup A_{31} \dot\cup A_{42}| + |A_{14} \dot\cup A_{21} \dot\cup A_{32} \dot\cup A_{43}|. \end{aligned}$$

Each summand is the cardinality of a 0–parity set in $\mathcal{X}_4^{n-2}$ and by induction hypothesis again $|A| \leq 4 \cdot q_4^0(n-2)$.

$\underline{\alpha \geq 4}$

Case II: $A_{ij} \cap A_{i'j'} = \emptyset$ for all $ij \neq i'j'$.

The same idea as before works.

$$\begin{aligned} |A| = {} & |A_{11} \dot\cup A_{22} \dot\cup \ldots \dot\cup A_{\alpha\alpha}| \\ & + |A_{12} \dot\cup A_{23} \dot\cup \ldots \dot\cup A_{\alpha 1} \\ & \vdots \\ & + |A_{12} \dot\cup A_{21} \dot\cup \ldots \dot\cup A_{\alpha(\alpha-1)}| \leq \alpha \cdot q_\alpha^0(n-2). \end{aligned}$$

Case I: Without loss of generality, $A_{11} \cap A_{22} \neq \emptyset$.

Here by Lemma 5.2 only the sets

$$A_{11}, A_{22};\ A_{21}, A_{12};\ A_{\varepsilon\delta}\ (\varepsilon, \delta \in \{3, 4, \ldots, \alpha\})$$

are possible non-empty.

Subcase 1: $A_{ij} \cap A_{i'j'} = \emptyset$ for all $i, j, i', j' \in \{3, 4, \ldots, \alpha\}$ with $ij \neq i'j'$.

By Lemma 5.2 we are left with

$$\mathcal{C} = \{A_{11}, A_{22}, A_{12}, A_{21}\} \quad \text{and} \quad \mathcal{D} = \{A_{\varepsilon\delta} :\ \varepsilon, \delta \in \{3, 4, \ldots, \alpha\}\}.$$

We can also assume that $A_{11} = A_{22}$, $A_{12} = A_{21}$. Suppose now that for some $X \in \mathcal{C}$ and $Y \in \mathcal{D}$ $X \cap Y \neq \emptyset$. Without loss of generality, $X = A_{11}$ and $Y = A_{33}$. Then by the parity property necessarily $A_{12} = A_{21} = \emptyset$ and therefore

$$\sum_{X \in \mathcal{C}} |X| \leq 2 \cdot q_\alpha^0(n-2). \tag{5.5}$$

Furthermore,

$$\begin{aligned}\sum_{Y \in \mathcal{D}} |Y| &= |A_{33} \,\dot\cup\, A_{44} \,\dot\cup \ldots \dot\cup\, A_{\alpha\alpha}| \\ &\quad + |A_{34} \,\dot\cup\, A_{45} \,\dot\cup \ldots \dot\cup\, A_{\alpha 3}| \\ &\quad \vdots \\ &\quad + |A_{3\alpha} \,\dot\cup\, A_{43} \,\dot\cup \ldots \dot\cup\, A_{\alpha(\alpha-1)}| \\ &\quad \leq (\alpha-2) \cdot q_\alpha^0(n-2)\end{aligned}$$

and thus $|A| \leq 2 \cdot q_\alpha^0(n-2) + (\alpha-2) \cdot q_\alpha^0(n-2)$.

In case $X \cap Y = \emptyset$ for all $X \in \mathcal{C}$, $Y \in \mathcal{D}$ consider the scheme

$$\begin{array}{llll} & |A_{11} \;\dot\cup & (A_{33} \,\dot\cup\, A_{44} \,\dot\cup \ldots \dot\cup & A_{\alpha\alpha})| \\ + & |A_{12} \;\dot\cup & (A_{34} \,\dot\cup\, A_{45} \,\dot\cup \ldots \dot\cup & A_{\alpha 3})| \\ + & & |A_{35} \,\dot\cup\, A_{46} \,\dot\cup \ldots \dot\cup & A_{\alpha 4}| \\ \vdots & \vdots & & \\ + & & |A_{3\alpha} \,\dot\cup\, A_{43} \,\dot\cup \ldots \dot\cup & A_{\alpha(\alpha-1)}| \;\leq (\alpha-2) \cdot q_\alpha^0(n-2). \end{array}$$

Since $|A_{22}| + |A_{21}| \leq 2 \cdot q_\alpha^0(n-2)$, we get again

$$|A| \leq \alpha \cdot q_\alpha^0(n-2).$$

Subcase 2: There are $i, j, i', j' \in \{3, 4, \ldots, \alpha\}$ such that $ij \neq i'j'$, $\Pi(ij, i'j') = 0$, and $A_{ij} \cap A_{i'j'} \neq \emptyset$.

Without loss of generality $ij = 33$, $i'j' = 44$. Again, by Lemma 5.2 we are left with

$$\mathcal{A} = A\{11, A_{22}, A_{12}, A_{21}, A_{33}, A_{44}, A_{34}, A_{43}\} \quad \text{and}$$
$$\mathcal{B} = \{A_{\varepsilon\delta} : \; \varepsilon, \delta \in \{5, 6, \ldots, \alpha\}\}.$$

Now we treat $\mathcal{A}$ exactly as earlier in case $\alpha = 4$, keeping in mind that now $q_4^0(n-2)$ is to be replaced by $q_\alpha^0(n-2)$ in the estimates. Thus

$$\sum_{X \in \mathcal{A}} |X| \leq 4 \cdot q_\alpha^0(n-2). \tag{5.6}$$

Finally, we treat $\mathcal{B}$ inductively by the same procedure as we treated $\{A_{\varepsilon\delta} : \varepsilon, \delta \in \{1, \ldots, \alpha\}\}$ until now and get $\sum_{Y \in \mathcal{B}} |Y| \leq (\alpha - 4) \cdot q_\alpha^0(n-2)$. Therefore here also

$$|A| = \sum_{X \in \mathcal{A}} |X| + \sum_{Y \in \mathcal{B}} |Y| \leq \alpha \cdot q_\alpha^0(n-2).$$

$\underline{\alpha = 3}$

This is the most intricate case. For n odd $A = \mathcal{E}_n$ has 0–parity and $|A| = 2^{n-1}$. For n even the set $A = \mathcal{E}_n \cup \{33\ldots3\}$ has also 0–parity and $|A| = 2^{n-1}+1$. We have to show that these numbers cannot be exceeded. Here again the 2-step induction is easy in

Case II: $A_{ij} \cap A_{i'j'} = \emptyset$ for all $ij \neq i'j'$.

$$\begin{aligned} |A| &= |A_{11} \,\dot\cup\, A_{22} \,\dot\cup\, A_{33}| + |A_{12} \,\dot\cup\, A_{23} \,\dot\cup\, A_{31}| \\ &\quad + |A_{13} \,\dot\cup\, A_{21} \,\dot\cup\, A_{32}| \leq 3 \cdot q_3^0(n-2). \end{aligned}$$

Obviously $3 \cdot 2^{n-3} \leq 2^{n-1}$ and also $3 \cdot (2^{n-3}+1) \leq 2^{n-1}+1$ for $n \geq 3$.

Case I: Without loss of generality $A_{11} \cap A_{22} \neq \emptyset$ and by Lemma 5.2 only the sets $C = A_{11} = A_{22}$, $D = A_{12} = A_{21}$, $E = A_{33}$ are possibly non-empty. As in the case $\alpha = 4$ we obtain

$$|A| \leq 4 \cdot q_3^0(n-2). \tag{5.7}$$

This settles the case n odd. For n even a more detailed discussions is needed. Lemma 5.3 implies

$$C \cap D = \emptyset, \quad C \cap E = \emptyset \quad \text{or} \quad D = \emptyset, \quad D \cap E = \emptyset \quad \text{or} \quad C = \emptyset. \tag{5.8}$$

If $C = \emptyset$ or $D = \emptyset$, then $|A| \leq 3 \cdot q_3^0(n-1)$ and we are done. Otherwise C, D, and E are disjoint. Since $C \,\dot\cup\, E$ and $D \,\dot\cup\, E$ have 0–parity, we have

$$|C \,\dot\cup\, E|, \ |D \,\dot\cup\, E| \leq q_3^0(n-2). \tag{5.9}$$

We distinguish two cases.

$\underline{|E| \geq 1}$

Since $|C|+|E|$, $|D|+|E| \leq 2^{n-3}+1$, we have $|C|$, $|D| \leq 2^{n-3}+1-|E|$. Therefore

$$\begin{aligned} |A| &= 2 \cdot |C| + 2 \cdot |D| + |E| \leq 2^{n-2} + 2 - 2 \cdot |E| + 2^{n-2} + 2 - 2 \cdot |E| + |E| \\ &= 2^{n-1} + 4 - 3 \cdot |E| \leq 2^{n-1} + 1 \end{aligned}$$

$\underline{|E| = 0}$

Here we look at other components as well. Partition the set of components $\{1, 2, \ldots, n\}$ into the sets $\{2,1\}$, $\{3,4\}$, $\{5,6\}, \ldots, \{n-1, n\}$.

Either for some pair of components a case $|E| \geq 1$ arises and are done by the previous arguments or it never does. But then after proper relabelling the letter 3 occurs in none of the schemes corresponding to those pairs of components. This means that no word in A has a 3 as letter.

Hence

$$A \subset \{1,2\}^n \quad \text{and} \quad |A| \leq q_2^0(n) = 2^{n-1}.$$

Remark. Notice that for $\alpha = 3$, $n = 4$ there are two essentially different 0–parity sets: $\{11, 22, 33\}^2$ and $\mathcal{E}_4 \cup \{3333\}$.

6. Proof of Theorems 5,6

In order to indicate the dependence on α we write $C_\alpha(d_n;\ 1 \leftrightarrow 2)$, $D_\alpha(d_n)$ for $C(d_n;\ 1 \leftrightarrow 2)$, $D(d_n)$.

We give now a lower bound on $D_\alpha(d_n)$, which together with (1.21) and (1.23) implies Theorem 5.

For this we define for $0 \leq \delta \leq n$

$$N_\alpha(n, \delta) = \left|\{(n^n, y^n) \in \mathcal{X}_\alpha^n \times \mathcal{X}_\alpha^n :\ d_n(x^n, y^n) = \delta\}\right| \tag{6.1}$$

and observe that

$$N_\alpha(n, \delta) = \alpha^n \binom{n}{\delta} (\alpha - 1)^\delta. \tag{6.2}$$

Now clearly

$$D_\alpha(d_n) \geq \sum_{\delta=0}^{n} \frac{N_\alpha(n, d)}{M_\alpha(n, \delta)}. \tag{6.3}$$

By Theorem 1 and Lemma 2.1(b) we have

$$M_\alpha(n, \delta) = F_\alpha(n, \delta) = \binom{n}{\delta} (\alpha - 1)^\delta, \quad \text{if } \overline{\alpha} \leq \frac{n(\alpha - 1)}{\delta}. \tag{6.4}$$

This, (6.3), and (6,2) imply

$$D_\alpha(d_n) \geq \sum_{\delta=0}^{\delta^*} \frac{n_\alpha(n, \delta)}{M_\alpha(n, \delta)} = (\delta^* + 1)\alpha^n \quad \text{for} \quad \delta^* = \left\lfloor \frac{n(\alpha - 1)}{\overline{\alpha}} \right\rfloor. \tag{6.5}$$

Therefore $\log D_\alpha(d_n) \geq \log(\delta^* + 1)\alpha^n$, and consequently $\log D_\alpha(d_n) \geq$ $\geq n \cdot \log \alpha + \log n + \log \frac{\alpha-1}{\overline{\alpha}}$.

Thus by (1.21)

$$C_\alpha(d_n;\ 1 \leftrightarrow 2) \geq \left\lceil n \cdot \log \alpha + \log n + \log \frac{\alpha - 1}{\overline{\alpha}} \right\rceil. \tag{6.6}$$

Now for $\alpha = 4$ $n \cdot \log 4 = 2n = \lceil n \cdot \log 4 \rceil$ and $\left|\lceil \log n + \log \frac{3}{4} \rceil - \lceil \log(n+1) \rceil\right| \leq$ ≤ 1, because $\log \frac{3}{4} > -1$ and $\lceil \log(n+1) \rceil > \lceil \log n \rceil$ only if $n = 2^k$, and then $\lceil \log(n+1) \rceil = k+1$, $\lceil \log n + \log \frac{3}{4} \rceil = k$. Thus by (1.23) and (6.6) the Theorem follows in case $\alpha = 4$.

For $\alpha = 5$ a slightly more technical argument gives again the 1 bit bound. A 2 bit bound obviously holds.

The proof of Theorem 6 consists of a modest refinement of the lower bound on $D_4(\Pi_n)$, which gave (1.25). It just so happens that for $\alpha = 4$ this bound is optimal. Define now for $i = 0, 1$

$$R^i_\alpha(n) = \left|\{(x^n, y^n) \in \mathcal{X}^n_\alpha \times \mathcal{X}^n_\alpha :\ \Pi(x^n, y^n) = i\}\right|. \tag{6.7}$$

Clearly $R^i_\alpha(n) > 1$ for $i = 0, 1$. Since $R^0_\alpha(n) + R^1_\alpha(N) = \alpha^{2n}$, we get for $\alpha = 4$ by (a), (a') in Theorem 3

$$D_4(\Pi_n) \geq \frac{R^0_4(n)}{Q^0_4(n)} + \frac{R^1_4(n)}{Q^1_4(n)} > 4^n.$$

Therefore $C_4(\Pi_n, 1 \leftrightarrow 2) \geq \lceil \log D_4(\Pi_n) \rceil \geq 2n + 1$.

Finally, (1.26) shows tightness of this bound. ■

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) **88**(1985), 41–45.

[4] R' Ahlswede and M. Moers, Inequalities for code pairs, *European J. Combinatorics*, **9**(1988), 175–181.

[5] A. Yao, Some complexity questions related to distributive computing, *Proc. 11th Ann. ACM Symp. Theory of Computing*, 1979, 209–219.

[6] A. El Gamal and K. F. Pang, Communication complexity of computing the Hamming distance, submitted to *SIAM J. on Computing*.

[7] Cai Ning, A bound of sizes of code pairs satisfying the strong 4-words property for Lee distance, *J. of System Science and Mathematical Science,* **6**(1986), 129–135.

[8] P. Frankl and V. Rödl, Forbidden intersections, Preprint, 1984.

[9] R. Ahlswede and I, Csiszár, To get a bit of information may be as hard as to get full information, *IEEE Transactions Inf. Theory,* IT-27, 1981, 398–408.

[10] C. H. Papadimitriou and M. Sipser, Communication complexity, *Proc. 14th Ann. ACM Symp. on Theory of Computing,* 1982, 201–214.

[11] H. Abelson, Lower bounds on Inf. Transfers in distributed computations, *Proc IEEE 19th Ann. Symp. on Foundations of Computer Science,* Ann Arbor, 1978, 151-158.

[12] A. El Gamal, A simple proof of the Ahlswede-Csiszár one-bit theorem, *IEEE Transactions Inf. Theory,* IT-29, 1983, 931–933.

[13] R. Ahlswede, Coloring hypergraphs: A new approach to multi-user source coding I, *J. Combinatorics, Information and System Sciences,* **4**(1979), 76–115; Part II, ibid. **5**(1980), 220–268.

[14] M. Deza, Une proprieté extrémale des plans projectifs finis dans une classe de code equidistants, *Discrete Math.,* **6**(1973) 343–352.

[15] H. van Lint, A theorem on equidistant codes, *Discrete Math.,* **6**(1973), 353–358.

[16] V. T. Sós, Irregularities of partitions (Ramsey theory, uniform distribution), Surveys in Combinatorics, invited papers for the 9th British Comb. Conf.: 1983, London Math. Society Lecture Note, Series 82, ed. E. K. Lloyd, Cambridge University Press, 1983.

[17] R. Ahlswede and Z. Zhang, Coding for write-efficient memory, submitted to *Information and Computation.*

Rudolf Ahlswede

Universität Bielefeld
Fakultät für Mathematik
Postfach 8640, 4800 Bielefeld 1
West Germany