On the Redundancy of Two-Dimensional Balanced Codes

Erik Ordentlich, Ron M. Roth*
Computer Systems Laboratory
HPL-97-143
December, 1997

E-mail: eor@hpl.hp.com
ronny@cs.technion.ac.il

balanced arrays, DC-free codes, two-dimensional coding

Let $A_{n \times m}$ be the set of binary $n \times m$ arrays in which each row, and respectively each column, has the same number of 0's and 1's. We prove the lower bound

$$\log_2 |A_{n \times m}| \geq nm - 1/2 \, (n \log_2 (2m) + m \log_2 (2n)).$$

We also show that this bound is tight up to an additive term $O(n + \log m)$.

Internal Accession Date Only

*On sabbatical leave from HP Laboratories Israel, Computer Science Department, Technion, Haifa 32000, Israel.
Work supported in part by grant No. 95-00522 from the United–States–Israel Binational Sciences Foundation (BSF), Jerusalem, Israel.

1 Introduction

In this work, we consider the enumeration problem of two-dimensional balanced binary $n \times m$ arrays, in which each row, and respectively each column, has the same number of 0's and 1's (n and m are even).

By a binary n-vector we refer to a vector in $\mathbb{R}^n$ with entries restricted to $\{0, 1\}$. A binary n-vector $\mathbf{v}$ is called *balanced* if n is even and half of the entries of $\mathbf{v}$ are 1's. Much is known about codes that map unconstrained input sequences to one-dimensional balanced binary n-vectors. Those codes go also by the names DC-free or zero-disparity codes [10]. We denote the set of all balanced binary n-vectors by $\mathcal{A}_n$; clearly,

$$|\mathcal{A}_n| \;=\; \binom{n}{n/2} .$$

The ratio $|\mathcal{A}_n|/2^n = 2^{-n}\binom{n}{n/2}$ will be denoted by λ_n.

The *redundancy* of a set $C \subseteq \{0,1\}^n$ is defined by $n - \log_2 |C|$. The redundancy of $\mathcal{A}_n$, denoted ρ_n, is given by

$$\rho_n \;=\; n - \log_2 |\mathcal{A}_n| \;=\; -\log_2 \lambda_n \; . \tag{1}$$

It is known that

$$\frac{1}{\sqrt{2n}} \;\le\; \lambda_n \;\le\; \frac{1}{\sqrt{\frac{\pi}{2}n}} \tag{2}$$

(see [5], [8, p. 309]). A very efficient encoding algorithm due to Knuth [5] maps unconstrained binary words into $\mathcal{A}_n$ with redundancy $\lceil \log_2 n \rceil$. See also improvements by Al-Bassam and Bose [1], and Tallini, Capocelli, and Bose [12].

Less has been known about the redundancy of two-dimensional balanced arrays. By a binary $n \times m$ array we mean an $n \times m$ array whose columns are binary n-vectors. A binary $n \times m$ array , is called *balanced* if n and m are both even and each one of the rows and columns of , is balanced. We denote by $\mathcal{A}_{n\times m}$ the set (or the code) of all balanced $n \times m$ arrays. The redundancy of $\mathcal{A}_{n\times m}$, denoted $\rho_{n\times m}$, is given by

$$\rho_{n\times m} \;=\; nm \;-\; \log_2 |\mathcal{A}_{n\times m}| \; .$$

An efficient coding algorithm into a subset of $\mathcal{A}_{n\times m}$ is presented in [11] that has redundancy $n \log_2 m + m \log_2 n + O(n + m \log\log n)$. In its simpler version, the algorithm in [11] balances the rows using one of the algorithms in [1], [5], or [12]; by trading those algorithms with the (more computationally complex) enumerative coding of $\mathcal{A}_m$, the redundancy can be reduced to $\frac{1}{2}(n \log_2 m) + m \log_2 n + O(n + m \log\log n)$.

In Section 2 we prove the upper bound

$$\rho_{n\times m} \;\le\; n\rho_m \;+\; m\rho_n \;\le\; \tfrac{1}{2}\Big(n \log_2(2m) \;+\; m \log_2(2n)\Big) \; ,$$

and in Section 3 we show that this bound is tight up to an additive term $O(n + \log m)$. This bound implies that requiring balanced rows in a binary array does not "interfere" with requiring balanced columns. Note, however, that those requirements are not independent: for instance, if all n rows in a binary $n \times m$ array are balanced, and $m-1$ of the columns are balanced as well, then so must be the remaining column.

The computation of the redundancy of two-dimensional balanced arrays can be relevant to the coding application that we outline next. In currently-available magnetic and optical memory devices, data is recorded along tracks, thus treating the recording device as one-dimensional. Recent proposals for the design of optical storage—in particular holographic memory—try to take advantage of the fact that the recording device is two-dimensional (or even three-dimensional), thereby increasing the recording density [4], [9]. The new approach, however, introduces new types of constraints on the data—those constraints now become multi-dimensional in nature, rather than one-dimensional. The specific constraints to be used in the recently suggested recording techniques are yet to be crystallized. Nevertheless, experiments reported on holographic memory, and experience gathered in other existing optical devices, suggest that 0's and 1's in the recorded data need to be balanced within certain areas or patterns. The set $\mathcal{A}_{n\times m}$ may turn out to be useful for that purpose.

2 Upper bound on the redundancy of $\mathcal{A}_{n\times m}$

In this section we prove the following upper bound on $\rho_{n\times m}$.

Proposition 2.1 *For every even positive integers n and m,*

$$\rho_{n\times m} \;\le\; n\rho_m \;+\; m\rho_n \;\le\; \tfrac{1}{2}\Big(n\log_2(2m) \;+\; m\log_2(2n)\Big)\;.$$

Proposition 2.1 is a direct corollary of the following lower bound on the size of $\mathcal{A}_{n\times m}$, combined with (1) and (2).

Proposition 2.2 *For every even positive integers n and m,*

$$|\mathcal{A}_{n\times m}| \;\ge\; 2^{nm}\lambda_m^n\lambda_n^m\;.$$

Proposition 2.2 is a special case of Lemma 2.4 which we state and prove below.

We introduce some notations that will be used hereafter in this work.

Let , be a binary $n \times m$ array (not necessarily balanced). The *row type* of , is an integer n-vector $\mathbf{w} = (w_1, \ldots, w_n)$ where w_i is the sum of the entries of the ith row of , .

For an integer n-vector $\mathbf{w} = (w_1, \ldots, w_n)$, define $\mathcal{R}_m(\mathbf{w})$ to be the set of all binary $n \times m$ arrays whose row type is $\mathbf{w}$. Clearly,

$$|\mathcal{R}_m(\mathbf{w})| \;=\; \prod_{i=1}^{n} \binom{m}{w_i}$$

(we define $\binom{m}{w} = 0$ if $w < 0$ or $w > m$).

For even n and an integer n-vector $\mathbf{w}$, denote by $\mathcal{U}_m(\mathbf{w})$ the set of all arrays in $\mathcal{R}_m(\mathbf{w})$ whose columns are balanced. For even m we have $\mathcal{A}_{n\times m} = \mathcal{U}_m((m/2)\cdot \mathbf{1}_n)$, where $\mathbf{1}_n$ denotes the all-one vector in $\mathbb{R}^n$.

For a real vector $\mathbf{y}$, we denote by $\|\mathbf{y}\| = \|\mathbf{y}\|_1$ the sum of the absolute values of the entries of $\mathbf{y}$ and by $\|\mathbf{y}\|_\infty$ the largest absolute value of any entry of $\mathbf{y}$. The support of $\mathbf{y}$ will be denoted by $\mathsf{supp}(\mathbf{y})$. Note that when $\mathbf{y}_1$ and $\mathbf{y}_2$ are binary m-vectors, then $\|\mathbf{y}_1 - \mathbf{y}_2\|$ is the number of positions on which they differ. The set $\{1, 2, \ldots, n\}$ will be denoted by $\langle n \rangle$.

Lemma 2.3 *Let $X_1, \ldots, X_n$ be independent Bernoulli random variables taking on $\{0, 1\}$ with probabilities $\mathsf{Prob}\{X_i = 1\} = p_i$, $i \in \langle n \rangle$, and suppose that $\sum_{i=1}^n p_i = n/2$. Then,*

$$\mathsf{Prob}\Big\{\sum_{i=1}^{n} X_i = n/2\Big\} \;\geq\; \lambda_n \;,$$

with equality holding if and only if $p_i = \frac{1}{2}$ for all i.

Lemma 2.3 follows from a result due to Hoeffding [7]. For the sake of completeness, we provide a proof of Lemma 2.3 in Appendix A (see Proposition 3.6 therein). The proof we present is simpler than the one in [7], as Lemma 2.3, which is what we need here, is less general than Hoeffding's result.

Lemma 2.4 *Let n and m be positive integers, n even, and let $\mathbf{w}$ be an integer n-vector with $\|\mathbf{w}\| = nm/2$. Then,*

$$|\mathcal{U}_m(\mathbf{w})| \;\geq\; \lambda_n^m \cdot |\mathcal{R}_m(\mathbf{w})| \;.$$

Proof. Consider the uniform measure Q on the elements of $\mathcal{R}_m(\mathbf{w})$; namely,

$$Q(,\,) \;=\; \begin{cases} |\mathcal{R}_m(\mathbf{w})|^{-1} & \text{if }, \;\in \mathcal{R}_m(\mathbf{w}) \\ 0 & \text{otherwise} \end{cases} \;. \tag{3}$$

It suffices to show that, with respect to this measure,

$$\mathsf{Prob}_Q\{,\;\in \mathcal{U}_m(\mathbf{w})\} \;\geq\; \lambda_n^m \;.$$

For $j \in \langle m \rangle$, let $\mathbf{c}_j$ denote the jth column of the random array , $\in \mathcal{R}_m(\mathbf{w})$, and let $\mathcal{B}_j$ denote the event that $\mathbf{c}_j$ is balanced. The key step in our proof is showing that for $j \in \langle m \rangle$,

$$\mathsf{Prob}_Q \left\{ \mathcal{B}_j \;\middle|\; \mathbf{c}_1{=}\mathbf{v}_1, \ldots, \mathbf{c}_{j-1}{=}\mathbf{v}_{j-1} \right\} \;\geq\; \lambda_n \;, \tag{4}$$

where $(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1})$ is any $(j{-}1)$-tuple of balanced vectors in $\mathcal{A}_n$ for which we have $\mathsf{Prob}_Q \{\mathbf{c}_1{=}\mathbf{v}_1, \ldots, \mathbf{c}_{j-1}{=}\mathbf{v}_{j-1}\} > 0$. The left-hand side of (4) is the conditional probability (implied by the measure Q) that $\mathbf{c}_j$ is balanced, given that columns $\mathbf{c}_1$ through $\mathbf{c}_{j-1}$ are equal respectively to the balanced vectors $\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}$. For $j = 1$, the inequality (4) becomes

$$\mathsf{Prob}_Q \{\mathcal{B}_1\} \;\geq\; \lambda_n \;. \tag{5}$$

Indeed, suppose that (4) holds. Then, computing the probability that the first j columns of , are balanced, we obtain

$$\begin{aligned}
&\mathsf{Prob}_Q \{\mathcal{B}_1, \ldots, \mathcal{B}_{j-1}, \mathcal{B}_j\} \\
&\quad = \sum_{(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}) \in \mathcal{A}_n^{j-1}} \mathsf{Prob}_Q \{\mathcal{B}_j, \mathbf{c}_1{=}\mathbf{v}_1, \ldots, \mathbf{c}_{j-1}{=}\mathbf{v}_{j-1}\} \\
&\quad = \sum_{(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}) \in \mathcal{A}_n^{j-1}} \mathsf{Prob}_Q \left\{ \mathcal{B}_j \;\middle|\; \mathbf{c}_1{=}\mathbf{v}_1, \ldots, \mathbf{c}_{j-1}{=}\mathbf{v}_{j-1} \right\} \cdot \mathsf{Prob}_Q \{\mathbf{c}_1{=}\mathbf{v}_1, \ldots, \mathbf{c}_{j-1}{=}\mathbf{v}_{j-1}\} \\
&\quad \overset{(4)}{\geq} \lambda_n \cdot \sum_{(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}) \in \mathcal{A}_n^{j-1}} \mathsf{Prob}_Q \{\mathbf{c}_1{=}\mathbf{v}_1, \ldots, \mathbf{c}_{j-1}{=}\mathbf{v}_{j-1}\} \\
&\quad = \lambda_n \cdot \mathsf{Prob}_Q \{\mathcal{B}_1, \ldots, \mathcal{B}_{j-1}\}
\end{aligned}$$

(the summations are over all $(j{-}1)$-tuples of balanced vectors in $\mathcal{A}_n$). By induction on j we thus obtain

$$\mathsf{Prob}_Q \{\mathcal{B}_1, \ldots, \mathcal{B}_j\} \;\geq\; \lambda_n^j \;, \quad j \in \langle m \rangle \;.$$

In particular,

$$\mathsf{Prob}_Q \{, \in \mathcal{U}_m(\mathbf{w})\} \;=\; \mathsf{Prob}_Q \{\mathcal{B}_1, \ldots, \mathcal{B}_m\} \;\geq\; \lambda_n^m \;,$$

as desired.

Returning to the proof of (4), we assume that the first $j{-}1$ columns of , are equal to $\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}$, and we let m_i be the number of 1's in the first $j{-}1$ positions of the ith row of , (with $m_i = 0$ if $j = 1$); note that the condition $\mathsf{Prob}_Q \{\mathbf{c}_1{=}\mathbf{v}_1, \ldots, \mathbf{c}_{j-1}{=}\mathbf{v}_{j-1}\} > 0$ implies that $m_i \leq w_i$ for all $i \in \langle n \rangle$. It is easy to see that

$$\mathsf{Prob}_Q \left\{ \mathcal{B}_j \;\middle|\; \mathbf{c}_1{=}\mathbf{v}_1, \ldots, \mathbf{c}_{j-1}{=}\mathbf{v}_{j-1} \right\} \;=\; \mathsf{Prob} \left\{ \sum_{i=1}^{n} X_i = n/2 \right\} , \tag{6}$$

where the X_i are independent Bernoulli random variables taking on $\{0, 1\}$ with probabilities $\mathsf{Prob}\{X_i = 1\} = p_i = (w_i{-}m_i)/(m{-}j{+}1)$. Note further that since $\mathbf{v}_\ell$ is balanced for every

$\ell \in \langle j{-}1 \rangle$, then $\sum_{i=1}^{n} m_i = (j{-}1)(n/2)$. Recalling that $\|\mathbf{w}\| = nm/2$ we thus have,

$$\begin{aligned} \sum_{i=1}^{n} p_i \;&=\; \frac{1}{m{-}j{+}1} \sum_{i=1}^{n} (w_i - m_i) \;&=\; \frac{nm}{2(m{-}j{+}1)} \;-\; \frac{1}{m{-}j{+}1} \sum_{i=1}^{n} m_i \\ &&=\; \frac{nm}{2(m{-}j{+}1)} \;-\; \frac{n(j{-}1)}{2(m{-}j{+}1)} \\ &&=\; \frac{n}{2} \,. \end{aligned}$$

Incorporating this and (6) into Lemma 2.3 yields (4). □

Proposition 2.2 can be generalized as follows. Let α be a rational number in the open interval $(0,1)$, and let n and m be positive integers such that both αn and αm are integers. Denote by $\mathcal{A}_{n\times m,\alpha}$ the set of all balanced $n \times m$ arrays in which the number of 1's in each row is αm, and the number of 1's in each column is αn. Then,

$$|\mathcal{A}_{n\times m,\alpha}| \;\geq\; 2^{-nmH(\alpha)} \cdot \binom{m}{\alpha m}^{n} \binom{n}{\alpha n}^{m} \;=\; 2^{nmH(\alpha)} \lambda_{m,\alpha}^{n} \lambda_{n,\alpha}^{m} \,, \tag{7}$$

where $H : [0,1] \to [0,1]$ is the entropy function

$$H(x) \;=\; -x \log_2 x - (1{-}x) \log_2 (1{-}x) \tag{8}$$

(with $H(0) = H(1) = 0$), and $\lambda_{n,\alpha} = 2^{-nH(\alpha)} \binom{n}{\alpha n}$. The proof of (7) is carried out by replacing Lemma 2.3 with Proposition 3.6 which we state and prove in Appendix A. Indeed, it can be verified that using Proposition 3.6, we can generalize the inequality of Lemma 2.4 to read

$$|\mathcal{U}_{m,\alpha}(\mathbf{w})| \;\geq\; \lambda_{n,\alpha}^{m} \cdot |\mathcal{R}_m(\mathbf{w})| \,, \tag{9}$$

where $\|\mathbf{w}\| = \alpha nm$ and $\mathcal{U}_{m,\alpha}(\mathbf{w})$ stands for all arrays in $\mathcal{R}_m(\mathbf{w})$ in which each column has αn entries equaling 1. The bound (7) is obtained by plugging $\mathbf{w} = (\alpha m) \cdot \mathbf{1}_n$ in (9) and recalling that $|\mathcal{R}((\alpha m) \cdot \mathbf{1}_n)| = 2^{mnH(\alpha)} \lambda_{m,\alpha}^{n}$.

It is known that [8, p. 309]

$$\lambda_{n,\alpha} \;\geq\; \frac{1}{\sqrt{8n\alpha(1{-}\alpha)}} \,.$$

So, from (7) we obtain the bound

$$\log_2 |\mathcal{A}_{n\times m,\alpha}| \;\geq\; nmH(\alpha) \;-\; \tfrac{1}{2}\Big(n \log_2(\beta m) \;+\; m \log_2(\beta n) \Big) \,,$$

where $\beta = 8\alpha(1{-}\alpha)$.

Estimates on $|\mathcal{A}_{n\times m,\alpha}|$ exist in the literature for the case where α goes to zero as n and m go to infinity. See [3, p. 48] and the references therein (e.g., [2]).

3 Lower bound on the redundancy of $\mathcal{A}_{n\times m}$

In this section, we prove the following lower bound on $\rho_{n\times m}$.

Proposition 3.1 *For every even positive integers n and m,*

$$\rho_{n\times m} \;\geq\; n\rho_m \;+\; m\rho_n \;-\; O(n+\log m)\;.$$

Note that there is asymmetry between n and m in the bound of Proposition 3.1, so transposition of the arrays may yield a better bound (note, however, that the presentation of the bounds here is not suitable for specific values of n and m, since we will not be explicit in the constant multipliers of the $O(\cdot)$ expressions).

Throughout this section, n and m will be even positive integers and t_m will denote the value $\lfloor\sqrt{m}\rfloor$. We denote by $\mathcal{D}_{n\times m}$ the set of all integer n-vectors $\mathbf{w}$ such that $\|\mathbf{w}\| = mn/2$ and $\|\mathbf{w} - (m/2)\cdot\mathbf{1}_n\|_\infty \leq t_m$. Let $\mathbf{w}_{\min}$ be a vector $\mathbf{w}\in\mathcal{D}_{n\times m}$ for which $|\mathcal{U}_m(\mathbf{w})|$ is minimal, and define $\tau_{n\times m}$ by

$$\tau_{n\times m} \;=\; nm \;-\; \log_2|\mathcal{U}_m(\mathbf{w}_{\min})|\;.$$

The proof of Proposition 3.1 will be carried out through a sequence of lemmas. The first two lemmas lead to a lower bound on $\tau_{n\times m}$, and the remaining lemmas provide a lower bound on $\rho_{n\times m}$ in terms of $\tau_{n\times m}$.

Lemma 3.2

$$|\mathcal{D}_{n\times m}| \;\geq\; \frac{(2t_m+1)^{n-1}}{n-1}\;.$$

Proof. Let $\mathcal{X}_{(n-1)\times m}$ denote the set of all integer $(n-1)$-vectors $\mathbf{v} = (v_1,\ldots,v_{n-1})$ such that $\|\mathbf{v} - (m/2)\cdot\mathbf{1}_{n-1}\|_\infty \leq t_m$. For such a vector $\mathbf{v}$ and an index $i\in\langle n-1\rangle$, let $\mathbf{v}_i$ denote the vector $(m-v_1,\ldots,m-v_i,v_{i+1},\ldots,v_{n-1})$; namely, $\mathbf{v}_i$ is obtained from $\mathbf{v}$ by changing the first i entries into the respective entries in $m\cdot\mathbf{1}_{n-1}-\mathbf{v}$. Generalizing the balancing technique of Knuth in [5], it can be shown that for every $\mathbf{v}\in\mathcal{X}_{(n-1)\times m}$ there is at least one index $i\in\langle n-1\rangle$ such that $\left|\|\mathbf{v}_i\| - m(n-1)/2\right| \leq t_m$. Let $i(\mathbf{v})$ denote the first such index i and let $\mathbf{w}(\mathbf{v})$ be the n-vector obtained by appending $mn/2 - \|\mathbf{v}_{i(\mathbf{v})}\|$ as an nth entry to $\mathbf{v}_{i(\mathbf{v})}$. The mapping

$$\mathbf{v}\mapsto\mathbf{w}(\mathbf{v})$$

sends $\mathcal{X}_{(n-1)\times m}$ to a subset of $\mathcal{D}_{n\times m}$. Furthermore, each element of $\mathcal{D}_{n\times m}$ has at most $n-1$ pre-images in $\mathcal{X}_{(n-1)\times m}$. Hence, $|\mathcal{D}_{n\times m}| \geq |\mathcal{X}_{(n-1)\times m}|/(n-1) = (2t_m+1)^{n-1}/(n-1)$. □

Lemma 3.3

$$\begin{aligned}\tau_{n\times m} &\geq m\rho_n + (n-1)\log_2(2t_m+1) - \log_2(n-1)\\ &= n\rho_m + m\rho_n - O(\log m + \log n)\,.\end{aligned}$$

Proof. The set of all binary $n \times m$ arrays whose columns are balanced can be written as $\bigcup_{\mathbf{w}} \mathcal{U}_m(\mathbf{w})$, where the union is taken over all integer n-vectors $\mathbf{w}$. Now, $\mathcal{U}_m(\mathbf{w})$ is nonempty only when $\|\mathbf{w}\| = mn/2$, and $\mathcal{U}_m(\mathbf{w})$ and $\mathcal{U}_m(\mathbf{w}')$ are disjoint when $\mathbf{w} \neq \mathbf{w}'$. So,

$$\sum_{\mathbf{w}\,:\,\|\mathbf{w}\|=nm/2} |\mathcal{U}_m(\mathbf{w})| = \Big|\bigcup_{\mathbf{w}} \mathcal{U}_m(\mathbf{w})\Big| = |\mathcal{A}_n|^m\,. \tag{10}$$

On the other hand,

$$|\mathcal{U}_m(\mathbf{w}_{\min})| \leq \frac{1}{|\mathcal{D}_{n\times m}|} \sum_{\mathbf{w}\in\mathcal{D}_{n\times m}} |\mathcal{U}_m(\mathbf{w})| \leq \frac{1}{|\mathcal{D}_{n\times m}|} \sum_{\mathbf{w}\,:\,\|\mathbf{w}\|=nm/2} |\mathcal{U}_m(\mathbf{w})| \tag{11}$$

Combining (10) and (11) yields

$$|\mathcal{U}_m(\mathbf{w}_{\min})| \leq \frac{|\mathcal{A}_n|^m}{|\mathcal{D}_{n\times m}|}\,,$$

and by taking logarithms we obtain

$$\tau_{n\times m} \geq m\rho_n + \log_2 |\mathcal{D}_{n\times m}|\,.$$

The result now follows from Lemma 3.2, (1), and (2). □

Let $\mathbf{w} = (w_1, \ldots, w_n)$ and $\mathbf{w}' = (w'_1, \ldots, w'_n)$ be two vectors in $\mathcal{D}_{n\times m}$. We say that $(\mathbf{w}, \mathbf{w}')$ is an *incremental pair* if the following conditions hold:

1. There are indexes $i, \ell \in \langle n\rangle$ such that $w'_i + 1 = w_i \leq m/2 \leq w_\ell = w'_\ell - 1$.
2. $w_j = w'_j$ for all $j \in \langle n\rangle \setminus \{i, \ell\}$.

The next lemma is proved in Appendix B.

Lemma 3.4 *Let $(\mathbf{w}, \mathbf{w}')$ be an incremental pair. Then*

$$\frac{|\mathcal{U}_m(\mathbf{w}')|}{|\mathcal{U}_m(\mathbf{w})|} \geq 1 - O\left(1/\sqrt{m}\right)\,.$$

Lemma 3.5

$$\rho_{n\times m} = \tau_{n\times m} - O(n)\,.$$

Proof. Let $\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_h$ be a shortest sequence of distinct elements of $\mathcal{D}_{n\times m}$ such that $\mathbf{w}_0 = (m/2)\cdot \mathbf{1}_n$, $\mathbf{w}_h = \mathbf{w}_{\min}$, and $(\mathbf{w}_{j-1}, \mathbf{w}_j)$ is an incremental pair for every $j \in \langle h\rangle$. It is easy to see that h is bounded from above by $t_m n/2 \le \sqrt{m}\cdot n/2$. Hence, by Lemma 3.4 we have

$$\frac{|\mathcal{U}_m(\mathbf{w}_{\min})|}{|\mathcal{U}_m((m/2)\cdot \mathbf{1}_n)|} \;=\; \prod_{j=1}^{h} \frac{|\mathcal{U}_m(\mathbf{w}_j)|}{|\mathcal{U}_m(\mathbf{w}_{j-1})|} \;\ge\; \left(1 - O\left(1/\sqrt{m}\right)\right)^{\sqrt{m}\cdot n/2} \;=\; \exp(-O(n))\;,$$

where m is assumed to be at least some value m_0 for which the term $1-O\left(1/\sqrt{m}\right)$ is positive (note that for $m < m_0$ the claim holds trivially). Taking logarithms, we obtain the desired result. □

Proof of Proposition 3.1. Combine Lemmas 3.3 and 3.5. □

Appendix A

For a vector $\mathbf{p} = (p_1, \ldots, p_n) \in \mathbb{R}^n$ and an integer k, $0 \le k \le n$, define

$$S_k(\mathbf{p}) \;=\; \sum_{I\subseteq\langle n\rangle\,:\,|I|=k} \prod_{i\in I} p_i \prod_{i\in\langle n\rangle\setminus I} (1-p_i)\;,$$

and $S_k(\mathbf{p}) = 0$ if $k < 0$ or $k > n$. The closed unit n-dimensional real hyper-cube $[0,1]\times[0,1]\times\cdots\times[0,1]$ will be denoted by $[0,1]^n$, and the respective open hyper-cube will be denoted by $(0,1)^n$. We also define $\mathcal{C}_k^{(n)} = \{\mathbf{p}\in[0,1]^n : \|\mathbf{p}\| = k\}$.

The quantity $S_k(\mathbf{p})$ equals $\mathsf{Prob}\left\{\sum_{i=1}^n X_i = k\right\}$, where $X_1, \ldots, X_n$ are independent Bernoulli random variables taking on $\{0,1\}$ with $\mathsf{Prob}\{X_i = 1\} = p_i$. In particular, $S_k(\mathbf{p}) \le 1$ for every $\mathbf{p}\in[0,1]^n$.

Recalling the definition of the entropy function in (8), we prove the following result.

Proposition 3.6 *Let k and n be integers, $0 \le k \le n$. For every $\mathbf{p}\in\mathcal{C}_k^{(n)}$,*

$$S_k(\mathbf{p}) \;\ge\; \binom{n}{k}\left(\frac{k}{n}\right)^k\left(\frac{n-k}{n}\right)^{n-k} \;=\; \binom{n}{k}\cdot 2^{-nH(k/n)}\;,$$

with equality holding if and only if $\mathbf{p} = (k/n)\cdot\mathbf{1}_n$.

In particular, if n is an even positive integer, then for every $\mathbf{p}\in\mathcal{C}_{n/2}^{(n)}$,

$$S_{n/2}(\mathbf{p}) \;\ge\; \binom{n}{n/2}\cdot 2^{-n} = \lambda_n\;,$$

with equality holding if and only if $\mathbf{p} = (1/2)\cdot\mathbf{1}_n$.

Lemma 3.7 *For $0 \leq k \leq n$, let $\frac{\partial}{\partial p_i} S_k(\mathbf{p})$ be the partial derivative with respect to p_i of the mapping $(p_1, \ldots, p_n) \mapsto S_k(p_1, \ldots, p_n)$ when defined over $\mathbb{R}^n$. Then,*

$$\sum_{i=1}^{n} p_i(1-p_i) \frac{\partial S_k(\mathbf{p})}{\partial p_i} \;=\; (k - \|\mathbf{p}\|) S_k(\mathbf{p}) \; .$$

Proof. For a vector $\mathbf{p} = (p_1, \ldots, p_n) \in \mathbb{R}^n$, define the generating polynomial $S(x; \mathbf{p})$ in the indeterminate x by

$$S(x; \mathbf{p}) \;=\; \sum_{k=0}^{n} S_k(\mathbf{p}) \cdot x^k \; .$$

The generating polynomial can also be written as

$$S(x; \mathbf{p}) \;=\; \prod_{i=1}^{n} (1-p_i + p_i x) \; .$$

Taking partial derivatives of $S(x; \mathbf{p})$ with respect to p_i yields

$$\frac{\partial}{\partial p_i} S(x; \mathbf{p}) \;=\; (x-1) \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (1-p_j + p_j x) \;=\; \frac{(x-1) S(x; \mathbf{p})}{1-p_i + p_i x} \; , \quad i \in \langle n \rangle \; . \tag{12}$$

Multiplying (12) by $p_i(1-p_i)$ and summing over i, we obtain

$$\begin{aligned}
\sum_{i=1}^{n} p_i(1-p_i) \frac{\partial}{\partial p_i} S(x; \mathbf{p}) \;&=\; \sum_{i=1}^{n} \frac{p_i(1-p_i)(x-1) S(x; \mathbf{p})}{1-p_i + p_i x} && (13) \\
&=\; \sum_{i=1}^{n} \frac{(p_i x - p_i(1-p_i + p_i x)) S(x; \mathbf{p})}{1-p_i + p_i x} \\
&=\; x \cdot \sum_{i=1}^{n} \frac{p_i S(x; \mathbf{p})}{1-p_i + p_i x} \;-\; \sum_{i=1}^{n} p_i S(x; \mathbf{p}) \\
&=\; x \frac{\partial}{\partial x} S(x; \mathbf{p}) \;-\; \|\mathbf{p}\| \, S(x; \mathbf{p}) \; . && (14)
\end{aligned}$$

The lemma follows by equating the coefficient of x^k in (14) to its counterpart in the left-hand side of (13). □

Lemma 3.8 [6, p. 52] *For $r \in \langle n \rangle$ and any vector $\mathbf{p} \in (0,1)^n$,*

$$(S_{r-1}(\mathbf{p}))^2 \;>\; S_{r-2}(\mathbf{p}) \cdot S_r(\mathbf{p}) \; .$$

Proof of Proposition 3.6. The cases $k \in \{0, n\}$ are trivial since $|\mathcal{C}_0^{(n)}| = |\mathcal{C}_n^{(n)}| = 1$. Therefore, we assume from now on that $0 < k < n$. The set $\mathcal{C}_k^{(n)}$ is compact; so, the

mapping $\mathbf{p} \mapsto S_k(\mathbf{p})$ over $\mathcal{C}_k^{(n)}$ attains a minimum (with value less than 1) at some point $\mathbf{q} = (q_1, \ldots, q_n) \in \mathcal{C}_k^{(n)}$. Without loss of generality we can assume that $q_i \in (0,1)$ for $i \in \langle m \rangle$ and $q_i \in \{0,1\}$ for $i \in \langle n \rangle \setminus \langle m \rangle$; note that $m > 0$ (or else $S_k(\mathbf{q})$ would be 1). We denote by $\mathbf{q}'$ and $\mathbf{q}''$ the vectors $(q_1, \ldots, q_m)$ and $(q_{m+1}, q_{m+2}, \ldots, q_n)$, respectively.

Define the mapping $\Psi_k : \mathbb{R}^n \to \mathbb{R}$ by

$$\Psi_k(p_1, \ldots, p_n) \;=\; S_k(k - \textstyle\sum_{j=2}^n p_j, p_2, p_3, \ldots, p_n)$$

(Ψ_k does not depend on p_1; nevertheless, for the sake of having simpler notations we inserted p_1 as a redundant variable). For every real $\mathbf{p}$ on the line $\|\mathbf{p}\| = k$ we have

$$\frac{\partial \Psi_k(\mathbf{p})}{\partial p_i} \;=\; \frac{\partial S_k(\mathbf{p})}{\partial p_i} \;-\; \frac{\partial S_k(\mathbf{p})}{\partial p_1}\;, \quad i \in \langle n \rangle\;. \tag{15}$$

If we fix $p_i = q_i$, $i \in \langle n \rangle \setminus \langle m \rangle$, then the mapping $\mathbf{p}' \mapsto \Psi_k(\mathbf{p}', \mathbf{q}'')$, over $\mathbb{R}^m$, must have a local minimum at $\mathbf{p}' = \mathbf{q}'$. Hence, by (15) we have

$$\frac{\partial S_k(\mathbf{p})}{\partial p_i}\Big|_{\mathbf{p}=\mathbf{q}} = \frac{\partial S_k(\mathbf{p})}{\partial p_1}\Big|_{\mathbf{p}=\mathbf{q}}\;, \quad i \in \langle m \rangle\;. \tag{16}$$

This, together with Lemma 3.7, yields

$$\frac{\partial S_k(\mathbf{p})}{\partial p_1}\Big|_{\mathbf{p}=\mathbf{q}} \cdot \sum_{i=1}^m q_i(1-q_i) \;=\; \sum_{i=1}^n q_i(1-q_i)\,\frac{\partial S_k(\mathbf{p})}{\partial p_i}\Big|_{\mathbf{p}=\mathbf{q}} = \;(k - \|\mathbf{q}\|)S_k(\mathbf{q}) \;=\; 0\;.$$

Since $\sum_{i=1}^m q_i(1-q_i) \neq 0$ we thus have

$$\frac{\partial S_k(\mathbf{p})}{\partial p_i}\Big|_{\mathbf{p}=\mathbf{q}} = \frac{\partial S_k(\mathbf{p})}{\partial p_1}\Big|_{\mathbf{p}=\mathbf{q}} = \;0\;, \quad i \in \langle m \rangle\;. \tag{17}$$

We show next that $m = n$ by proving that $q_n \notin \{0,1\}$. For a vector $\mathbf{p} = (p_1, \ldots, p_n) \in \mathbb{R}^n$ and integers ℓ and i, $1 < i \leq n$, let $S_{\ell;i} = S_{\ell;i}(\mathbf{p})$ denote the expression $S_\ell(p_2, p_3, \ldots, p_{i-1}, p_{i+1}, \ldots, p_n)$. We define $S_{0;2} = 1$ if $n = 2$, and let $S_{\ell;i} = 0$ if $\ell > n-2$ or $\ell < 0$. Note that $S_{\ell;i}$ does not depend on p_1 or p_i. We have

$$S_k(\mathbf{p}) \;=\; p_1 p_i S_{k-2;i} + (p_1(1-p_i) + p_i(1-p_1))S_{k-1;i} + (1-p_1)(1-p_i)S_{k;i}\;.$$

Taking partial derivatives with respect to p_1 and p_i, we obtain

$$\frac{\partial S_k(\mathbf{p})}{\partial p_1} \;=\; p_i S_{k-2;i} + (1-2p_i)S_{k-1;i} + (p_i-1)S_{k;i} \tag{18}$$

$$\frac{\partial S_k(\mathbf{p})}{\partial p_i} \;=\; p_1 S_{k-2;i} + (1-2p_1)S_{k-1;i} + (p_1-1)S_{k;i}\;. \tag{19}$$

Now, suppose to the contrary that $q_n = 0$ and compute $S_{k-2;n}$, $S_{k-1;n}$, and $S_{k;n}$ for $\mathbf{p} = \mathbf{q}$. By (17) and (18) we obtain

$$\frac{\partial S_k(\mathbf{p})}{\partial p_1}\Big|_{\mathbf{p}=\mathbf{q}} = S_{k-1;n} - S_{k;n} = 0 \tag{20}$$

i.e., $S_{k-1;n} = S_{k;n}$. Also, the partial derivative $\frac{\partial}{\partial p_n}\Psi_k(\mathbf{p})$ at $\mathbf{p} = \mathbf{q}$ must be nonnegative, or else we could increase q_n to some small $\epsilon > 0$ (and decrease q_1 by ϵ) to obtain a vector $\mathbf{q}_\epsilon \in \mathcal{C}_k^{(n)}$ such that $S_k(\mathbf{q}_\epsilon) < S_k(\mathbf{q})$, thereby contradicting the minimality of $\mathbf{q}$. Hence, by (15), (19), and (20) we have

$$\frac{\partial \Psi_k(\mathbf{p})}{\partial p_n}\Big|_{\mathbf{p}=\mathbf{q}} = \frac{\partial S_k(\mathbf{p})}{\partial p_n}\Big|_{\mathbf{p}=\mathbf{q}} = q_1(S_{k-2;n} - S_{k-1;n}) \geq 0 \ .$$

So, $S_{k-2;n} \geq S_{k-1;n} = S_{k;n} \geq 0$, or

$$S_{k-1;n}^2 \leq S_{k-2;n} \cdot S_{k;n} \ . \tag{21}$$

On the other hand, observe that $S_{\ell;n} = S_{\ell-\|\mathbf{q}''\|}(q_2, q_3, \ldots, q_m)$ for every integer ℓ. Noting that $0 < \|\mathbf{q}'\| = k - \|\mathbf{q}''\| < m$ and that $(q_2, q_3, \ldots, q_m) \in (0,1)^{m-1}$, we can apply Lemma 3.8 to the vector $(q_2, q_3, \ldots, q_m)$ with $r = k - \|\mathbf{q}''\|$ to obtain

$$S_{k-1;n}^2 > S_{k-2;n} \cdot S_{k;n} \ ,$$

thus contradicting (21). Hence, we cannot have $q_n = 0$.

A similar contradiction results if we assume that $q_n = 1$ (in this case, the partial derivative $\frac{\partial}{\partial p_n}\Psi_k(\mathbf{p})$ at $\mathbf{p} = \mathbf{q}$ must be nonpositive). Thus, we must have $m = n$, and $\mathbf{q}$ is therefore a local minimum of $\mathbf{p} \mapsto \Psi_k(\mathbf{p})$. By (17), (18), and (19) it follows that the vector $(S_{k-2;i}, S_{k-1;i}, S_{k;i})^T$, when computed for $\mathbf{p} = \mathbf{q}$, belongs to the right null space of the array

$$A(q_1, q_i) = \begin{pmatrix} q_i & 1-2q_i & q_i-1 \\ q_1 & 1-2q_1 & q_1-1 \end{pmatrix} \ .$$

On the other hand, the vector $(1,1,1)^T$ is also in the right null space of $A(q_1, q_i)$. However, Lemma 3.8, when applied to the vector $(q_2, q_3, \ldots, q_{i-1}, q_{i+1}, \ldots, q_n) \in (0,1)^{n-2}$ with $r = k$, implies that the vectors $(S_{k-2;i}, S_{k-1;i}, S_{k;i})$ and $(1,1,1)$ are linearly independent. Therefore, the rank of $A(q_1, q_i)$ is less than 2, which is possible only when $q_1 = q_i$. Since i is any index between 2 and n, it follows that all the entries of $\mathbf{q}$ are equal. And, since $\|\mathbf{q}\| = k$, we must have $q_i = k/n$ for all $i \in \langle n \rangle$. Finally, by symmetry it follows that $\mathbf{q} = (k/n) \cdot \mathbf{1}_n$ indeed satisfies (17). □

It is worthwhile pointing out that the mappings $\mathbf{p} \mapsto S_k(\mathbf{p})$ are generally not $\cup$-convex over $\mathcal{C}_k^{(n)}$. For example, let $\mathbf{p}_1 = (.1, .1, .9, .9)$, $\mathbf{p}_2 = (0, .2, .9, .9)$, and $\mathbf{p}_3 = (.2, 0, .9, .9)$. Then $\mathbf{p}_1 = (\mathbf{p}_2 + \mathbf{p}_3)/2$, yet $S_2(\mathbf{p}_1) > (S_2(\mathbf{p}_2) + S_2(\mathbf{p}_3))/2 = S(\mathbf{p}_2)$.

Appendix B

We provide here the proof of Lemma 3.4. For a nonnegative integer vector $\mathbf{v} = (v_1, v_2)$ with $v_1 \le v_2$, denote by $\mathcal{R}_m(\mathbf{v}, r)$ the set of all pairs of binary m-vectors $(\mathbf{y}_1, \mathbf{y}_2)$ such that $(\|\mathbf{y}_1\|, \|\mathbf{y}_2\|) = \mathbf{v}$ and $|\mathsf{supp}(\mathbf{y}_1 - \mathbf{y}_2)| = \|\mathbf{y}_1 - \mathbf{y}_2\| = 2r + v_2 - v_1$. We have

$$|\mathcal{R}_m(\mathbf{v}, r)| \;=\; \binom{m}{v_2}\binom{v_2}{v_1 - r}\binom{m - v_2}{r} \,. \tag{22}$$

In particular, $\mathcal{R}_m(\mathbf{v}, r)$ is nonempty if and only if $0 \le r \le \min\{v_1, m - v_2\}$.

Lemma 3.9 *Let $\mathbf{v} = (v_1, v_2)$ be an integer vector such that $m/2 - t_m \le v_1 \le m/2 \le v_2 \le m/2 + t_m$. If $s \le m/4 - t_m$, then*

$$\frac{\sum_{r \le s} |\mathcal{R}_m(\mathbf{v}, r)|}{|\mathcal{R}_m(\mathbf{v})|} \;\le\; 2^{m(H(2s/m)-1)+o(m)} \,.$$

Proof. Write $\Delta = v_2 - v_1$. It is easy to see that

$$\sum_{r \le s} |\mathcal{R}_m(\mathbf{v}, r)| \;\le\; \binom{m}{v_2} \sum_{k \le 2s+\Delta} \binom{m}{k} \,.$$

Recalling that $|\mathcal{R}_m(\mathbf{v})| = \binom{m}{v_1}\binom{m}{v_2}$, we thus have

$$\frac{\sum_{r \le s} |\mathcal{R}_m(\mathbf{v}, r)|}{|\mathcal{R}_m(\mathbf{v})|} \;\le\; \frac{\sum_{k \le 2s+\Delta} \binom{m}{k}}{\binom{m}{v_1}} \,.$$

We now combine this inequality with the lower bound

$$\binom{m}{v_1} \;\ge\; \frac{2^{mH(v_1/m)}}{\sqrt{8v_1(1 - v_1/m)}} \;=\; 2^{mH(v_1/m)-o(m)}$$

and the following upper bound that holds for $\sigma = 2s + \Delta \le m/2$,

$$\sum_{k \le \sigma} \binom{m}{k} \;\le\; 2^{mH(\sigma/m)}$$

(see [8, p. 310]). This yields

$$\frac{\sum_{r \le s} |\mathcal{R}_m(\mathbf{v}, r)|}{|\mathcal{R}_m(\mathbf{v})|} \;\le\; 2^{m(H(2s/m+2t_m/m)-H(1/2+t_m/m))+o(m)} \;=\; 2^{m(H(2s/m)-1)+o(m)} \,,$$

where we have used the continuity of $H(x)$ and that $H(1/2) = 1$ and $t_m/m = O\left(1/\sqrt{m}\right) = o(1)$. $\square$

For a k-vector $\mathbf{y}$ and a nonempty subset B of $\langle k \rangle$, we denote by $(\mathbf{y})_B$ the subvector of $\mathbf{y}$ indexed by B.

Let $\mathbf{w} = (w_1, \ldots, w_n) \in \mathcal{D}_{n \times m}$ and suppose that $w_1 \leq m/2 \leq w_2$ (in fact, there are always $i, \ell \in \langle n \rangle$ such that $w_i \leq m/2 \leq w_\ell$; we assume here that $i = 1$ and $\ell = 2$). We will use the notation $\mathbf{w}_{\langle 2 \rangle}$ for the vector $(\mathbf{w})_{\langle 2 \rangle} = (w_1, w_2)$. Also, the rows of an $n \times m$ array $,$ will be denoted by $[,]_1, \ldots, [,]_n$. Let $(\mathbf{y}_1, \mathbf{y}_2)$ be a pair in $\mathcal{R}_m(\mathbf{w}_{\langle 2 \rangle}, r)$ and consider the set

$$\mathcal{U}_m(\mathbf{w}; \mathbf{y}_1, \mathbf{y}_2) \;=\; \{, \;\in \mathcal{U}_m(\mathbf{w}) \;:\; ([,]_1, [,]_2) = (\mathbf{y}_1, \mathbf{y}_2)\} \;.$$

The set of all arrays $, \in \mathcal{U}_m(\mathbf{w})$ with $\|[,]_1 - [,]_2\| = 2r + w_2 - w_1$ is invariant under a fixed permutation on the columns of its elements. Therefore, the size of $\mathcal{U}_m(\mathbf{w}; \mathbf{y}_1, \mathbf{y}_2)$ depends on r, but not on the particular choice of $(\mathbf{y}_1, \mathbf{y}_2) \in \mathcal{R}_m(\mathbf{w}_{\langle 2 \rangle}, r)$. We denote that size by $V_m(\mathbf{w}, r)$ and prove the following result.

Lemma 3.10 *Let $\mathbf{w} = (w_1, \ldots, w_n) \in \mathcal{D}_{n \times m}$ with $w_1 \leq m/2 \leq w_2$. Then $V_m(\mathbf{w}, r)$ is nondecreasing for values of r in the range*

$$0 \;\leq\; r \;\leq\; \min\{w_1, m - w_2\} \;. \tag{23}$$

Proof. Assume that both r and $r+1$ lie in the range (23). Let $(\mathbf{y}_1, \mathbf{y}_2) \in \mathcal{R}_m(\mathbf{w}_{\langle 2 \rangle}, r)$ be such that $(\mathbf{y}_1)_{\langle 2 \rangle} = (\mathbf{y}_2)_{\langle 2 \rangle} = (0, 1)$; the existence of such a pair follows from the assumption that $r+1$ satisfies (23). Let $\mathbf{y}_2'$ be the binary m-vector obtained from $\mathbf{y}_2$ by flipping the bits indexed by $\langle 2 \rangle$; that is, $(\mathbf{y}_2')_{\langle 2 \rangle} = (1, 0)$ and $(\mathbf{y}_2')_{\langle m \rangle \setminus \langle 2 \rangle} = (\mathbf{y}_2)_{\langle m \rangle \setminus \langle 2 \rangle}$. Clearly, the pair $(\mathbf{y}_1, \mathbf{y}_2')$ is in $\mathcal{R}_m(\mathbf{w}_{\langle 2 \rangle}, r+1)$ and $V_m(\mathbf{w}, r+1) = |\mathcal{U}_m(\mathbf{w}; \mathbf{y}_1, \mathbf{y}_2')|$.

Define a mapping

$$\eta \;:\; \mathcal{U}_m(\mathbf{w}; \mathbf{y}_1, \mathbf{y}_2) \;\rightarrow\; \mathcal{U}_m(\mathbf{w}; \mathbf{y}_1, \mathbf{y}_2')$$

where $, ' = \eta(,)$ is an $n \times m$ array obtained as follows:

1. $[, ']_2 = \mathbf{y}_2'$.
2. Let U be the set of row indexes $b \in \langle n \rangle \setminus \langle 2 \rangle$ for which $([,]_b)_{\langle 2 \rangle} \in \{(0, 1), (1, 0)\}$. Denoting the first column of $,$ by $\mathbf{c}_1$ and the first two columns of $, '$ by $\mathbf{c}_1'$ and $\mathbf{c}_2'$,

   $$(\mathbf{c}_1')_U \;=\; \mathbf{1}_{|U|} - (\mathbf{c}_2')_U \;=\; \chi((\mathbf{c}_1)_U) \;,$$

   where χ is a particular 1–1 mapping from the set of all binary $(n-2)$-vectors $\mathbf{y}$ with $\|\mathbf{y}\| = n/2$ into the set $\mathcal{A}_{n-2}$.

3. The remaining entries of $,'$ (including the row $[,']_1$) are the same as in $,$.

It is easy to check that η is 1–1 and that $,'$ is in $\mathcal{U}_m(\mathbf{w};\mathbf{y}_1,\mathbf{y}_2')$. Hence,

$$V_m(\mathbf{w},r) \;=\; |\mathcal{U}_m(\mathbf{w};\mathbf{y}_1,\mathbf{y}_2)| \;\le\; |\mathcal{U}_m(\mathbf{w};\mathbf{y}_1,\mathbf{y}_2')| \;=\; V_m(\mathbf{w},r{+}1)\;,$$

as desired. □

Proof of Lemma 3.4 Assume without loss of generality that $\mathbf{w}$ and $\mathbf{w}'$ are such that $w_1'+1 = w_1 \le m/2 \le w_2 = w_2'-1$. Write $\Delta = w_2 - w_1$, and let $\mathcal{U}_m(\mathbf{w},r)$ be the set of all arrays in $\mathcal{U}_m(\mathbf{w})$ with $||[,]_1 - [,]_2|| = 2r+\Delta$. Then

$$|\mathcal{U}(\mathbf{w},r)| \;=\; |\mathcal{R}_m(\mathbf{w}_{\langle 2\rangle},r)|\cdot V_m(\mathbf{w},r)\;.$$

Observing that $V_m(\mathbf{w},r) = V_m(\mathbf{w}',r{-}1)$ and using (22), we obtain

$$\frac{|\mathcal{U}_m(\mathbf{w},r{-}1)|}{|\mathcal{U}_m(\mathbf{w},r)|} \;=\; \frac{r}{\Delta+r+1}\;.$$

Letting $L = \min\{w_1, m-w_2\}$, we have

$$\begin{aligned}
\frac{|\mathcal{U}_m(\mathbf{w}')|}{|\mathcal{U}_m(\mathbf{w})|} &= \frac{\sum_{r=1}^{L}|\mathcal{U}_m(\mathbf{w}',r{-}1)|}{\sum_{r=0}^{L}|\mathcal{U}_m(\mathbf{w},r)|}\\
&= \frac{\sum_{r=0}^{L}(r/(\Delta+r+1))|\mathcal{U}_m(\mathbf{w},r)|}{\sum_{r=0}^{L}|\mathcal{U}_m(\mathbf{w},r)|}\\
&\ge \frac{\sum_{r=0}^{L}(r/(\Delta+r+1))|\mathcal{R}_m(\mathbf{w}_{\langle 2\rangle},r)|}{\sum_{r=0}^{L}|\mathcal{R}_m(\mathbf{w}_{\langle 2\rangle},r)|}\;,
\end{aligned}$$

where the last step follows from the monotonicity of $|V_m(\mathbf{w},r)|$ as stated in Lemma 3.10. Now,

$$\begin{aligned}
\frac{\sum_{r=0}^{L}(r/(\Delta+r+1))|\mathcal{R}_m(\mathbf{w}_{\langle 2\rangle},r)|}{\sum_{r=0}^{L}|\mathcal{R}_m(\mathbf{w}_{\langle 2\rangle},r)|} &\ge \frac{\sum_{r=\lceil m/8\rceil}^{L}(r/(\Delta+r+1))|\mathcal{R}_m(\mathbf{w}_{\langle 2\rangle},r)|}{\sum_{r=0}^{L}|\mathcal{R}_m(\mathbf{w}_{\langle 2\rangle},r)|}\\
&\ge \frac{(m/8)}{\Delta+(m/8)+1}\cdot\frac{\sum_{r=\lceil m/8\rceil}^{L}|\mathcal{R}_m(\mathbf{w}_{\langle 2\rangle},r)|}{\sum_{r=0}^{L}|\mathcal{R}_m(\mathbf{w}_{\langle 2\rangle},r)|}\\
&= \left(1-O\left(1/\sqrt{m}\right)\right)\left(1-2^{m(H(1/4)-1)+o(m)}\right)\;,
\end{aligned}$$

where the last step follows from Lemma 3.9. The result now follows. □

4 References

[1] S. Al-Bassam, B. Bose, *On balanced codes, IEEE Trans. Inform. Theory,* IT-36 (1990), 406–408.

[2] A. Békéssy, P. Békéssy, J, Komlós, *Asymptotic enumeration of regular matrices, Studia Sci. Math. Hungar.,* 7 (1972), 343–353.

[3] B. Bollobás, *Random Graphs,* Academic Press, London, 1985.

[4] D. Brady, D. Psaltis, *Control of volume holograms, J. Opt. Soc. Am. A,* 9 (1992), 1167–1182.

[5] D.E. Knuth, *Efficient balanced codes, IEEE Trans. Inform. Theory,* IT-32 (1986), 51–53.

[6] G.H. Hardy, J.E. Littlewood, G. Pólya, *Inequalities,* Cambridge University Press, Cambridge, 1952.

[7] W. Hoeffding, *On the distribution of the number of successes in independent trials, Ann. Math. Statist.,* 27 (1956), 713–721.

[8] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes,* North Holland, Amsterdam, 1977.

[9] D. Psaltis, M.A. Neifeld, A. Yamamura, S. Kobayashi, *Optical memory disks in optical information processing, Applied Optics,* 29 (1990), 2038–2057.

[10] K.A. Schouhamer Immink, *Coding Techniques for Digital Recorders,* Prentice Hall, New York, 1991.

[11] R. Talyansky, T. Etzion, R.M. Roth, *Efficient code constructions for certain two-dimensional constraints, Proc. IEEE Int'l Symp. Inform. Theory,* Ulm, Germany (June 1997), p. 387.

[12] L.G. Tallini, R.M. Capocelli, B. Bose, *Design of some new balanced codes, IEEE Trans. Inform. Theory,* IT-42 (1996), 790–802.