On Ensembles of Low-Density Parity-Check Codes: Asymptotic Distance Distributions

Simon Litsyn, *Senior Member, IEEE,* and Vladimir Shevelev

***Abstract*—We derive expressions for the average distance distributions in several ensembles of regular low-density parity-check codes (LDPC). Among these ensembles are the standard one defined by matrices having given column and row sums, ensembles defined by matrices with given column sums or given row sums, and an ensemble defined by bipartite graphs.**

***Index Terms*—Distance distributions, low-density parity-check codes(LDPC).**

I. Introduction

Low-density parity-check codes (LDPC) attracted a great deal of attention recently due to their impressive performance under iterative decoding. However, there is no complete understanding of the structure of LDPC, and knowledge of such characteristics as the minimum distance and distance distribution could definitely facilitate our analysis of the best possible performance of such codes in different channels (see, e.g., [11], [13]). Moreover, information about the possible distance distributions provides estimates on the gap between performance of these codes under maximum likelihood and iterative decoding algorithms.

In this paper, we solve the problem of estimation of the average distance distribution (or weight enumerator function) in several ensembles of LDPC. This problem was addressed in many papers, starting with Gallager's original work [5]. However, the average distance distribution seems to be unknown even for the ensemble of codes defined by the parity-check matrices having fixed (and equal) number of ones in every column and row.

In the paper, we deal with the following cases: classical ensemble with all columns and rows of given weight (suggested by [5]), ensembles with all columns of fixed weight, with all columns obtained as a result of fixed times flipping of one of the coordinates with uniform probability (suggested by [9]), and the ensemble derived from bipartite graphs (suggested by [14]). It is worth mentioning that we deal in this paper only with *regular* ensembles, in the sense that all columns of the parity-check matrix have the same nature. More precisely, any permutation of columns of a parity-check matrix in the ensemble produces another matrix belonging to the same ensemble. The issue of irregular codes will be dealt with in the future. Also, we are planning to elaborate on the obtained bounds by estimating their standard deviations thus allowing to estimate the probability that a randomly generated code will have a distance distribution close to the expected one (for finite and infinitely growing lengths).

II. Ensembles of LDPC

Let H be a collection of binary parity-check matrices of size $m \times n$, where $m \leq n$. Every such matrix defines a code of rate $R \geq 1 - \frac{m}{n}$. Let k and ℓ be given numbers, independent of n.

The following ensembles of codes are considered.

- **Ensemble A:** Matrix H is chosen with uniform probability from the ensemble of $m \times n$ $(0,1)$-matrices having k ones in each row and ℓ ones in each column (or, in other words, having row sums equal k and column sums equal ℓ).
- **Ensemble B:** The matrix is composed of ℓ strips (each strip is of size $\frac{m}{\ell} \times n$). The first strip is the k-fold concatenation of the identity matrix I_k of size $k \times k$. The other strips are obtained by permuting at random the columns of the first strip.
- **Ensemble C:** Matrix H is chosen with uniform probability from the ensemble of $m \times n$ $(0,1)$-matrices with column sums equal ℓ.
- **Ensemble D:** Matrix H is generated starting from the all-zero matrix by flipping ℓ bits (not necessarily distinct) with uniform probability in each column.
- **Ensemble E:** Matrix H is chosen with uniform probability from the ensemble of $m \times n$ $(0,1)$-matrices with row sums equal k.
- **Ensemble F:** Matrix H is generated starting from the all-zero matrix by flipping k bits (not necessarily distinct) with uniform probability in each row;
- **Ensemble G:** Matrix H is generated starting from the all-zero matrix by flipping each entry with probability $k/n = \ell/m$.
- **Ensemble H:** Matrix H is generated using a random regular bipartite $m \times n$ graph (perhaps with parallel edges) with left degree k and right degree ℓ, such that $h_{i,j} = e$ if there are e edges connecting the ith left node with the jth right node, otherwise $h_{i,j} = 0$.

Manuscript received November 28, 2000; revised November 25, 2001. This work was supported in part by the Israeli Science Foundation under Grant 553-00. The work of V. Shevelev was supported in part by the Israeli Ministry of Absorption.

S. Litsyn is with the Department of Electrical Engineering–Systems, Tel-Aviv University, Ramat-Aviv 69978, Tel-Aviv, Israel (e-mail: litsyn@eng.tau.ac.il).

V. Shevelev is with the Department of Mathematics, Ben Gurion University, Beer-Sheva 84105, Israel (e-mail: shevelev@bgumail.bgu.ac.il).

Communicated by R. Koetter, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(02)01998-3.

III. Main Results

Let $\{\mathcal{C}_n\}$ be an ensemble of codes of length n defined by matrices of size $m \times n$. For a code $C \in \mathcal{C}_n$ we define the distance distribution as an $(n+1)$-vector

$$B(C) = (B_0(C) = 1,\, B_1(C),\, \dots,\, B_n(C))$$

where

$$B_i = |\{\mathbf{c} \in C\colon \mathrm{wt}(\mathbf{c}) = i\}|, \qquad i = 0,\, 1,\, \dots,\, n \tag{1}$$

where $\mathrm{wt}(\cdot)$ is the Hamming weight. The average ensemble distance distribution then is

$$B(\mathcal{C}_n) = (B_0(\mathcal{C}_n),\, B_1(\mathcal{C}_n),\, \dots,\, B_n(\mathcal{C}_n))$$

and is defined by

$$B_i(\mathcal{C}_n) := B_i = \frac{1}{|\mathcal{C}_n|} \sum_{C \in \mathcal{C}_n} B_i(C). \tag{2}$$

Let for $\theta \in [0,\, 1]$

$$H(\theta) = \lim_{n \to \infty} \frac{1}{n} \ln \binom{n}{\theta n} = -\theta \ln \theta - (1-\theta) \ln(1-\theta)$$

be the natural entropy.

In the following theorem we summarize results of the paper.

Theorem 1: Let $\alpha := m/n$, $\alpha \in (0,\, 1)$. For $\theta \in (0,\, 1)$ the average distance distributions

$$b_\theta := \lim_{n \to \infty} \frac{1}{n} \ln B_{\theta n} := H(\theta) + p_\theta^\alpha$$

in Ensembles A and B are determined by the following expressions.

- **Ensemble A:**
  Let
  $$p_\theta^\alpha = \alpha \ln \left(\frac{(1+t)^k + (1-t)^k}{2t^{\theta k}} \right) - \alpha k H(\theta) \tag{3}$$
  where t is the only positive root of
  $$\frac{(1+t)^{k-1} + (1-t)^{k-1}}{(1+t)^k + (1-t)^k} = 1 - \theta.$$
  Then, for k even
  $$b_\theta = H(\theta) + p_\theta^\alpha \tag{4}$$
  and for k odd
  $$b_\theta = \begin{cases} H(\theta) + p_\theta^\alpha, & \text{if } \theta \in \big(0,\, \frac{k-1}{k}\big) \\ -\infty, & \text{otherwise.} \end{cases} \tag{5}$$
- **Ensemble B:**
  The same as in Ensemble A.

In other ensembles

$$b_\theta = H(\theta) + p_\theta^\alpha \tag{6}$$

and p_θ^α is defined as follows.

- **Ensemble C:**
  $$p_\theta^\alpha = -\alpha \ln 2 + \alpha H(t) + \theta \ell \ln(1-2t) \tag{7}$$
  where t is the only root of
  $$(1-2t) \ln \frac{1-t}{t} = 2\, \frac{\theta \ell}{\alpha}. \tag{8}$$
- **Ensemble D:**
  The same as in Ensemble C.
- **Ensemble E:**
  $$p_\theta^\alpha = \alpha \ln \left(\frac{1 + (1-2\theta)^k}{2} \right). \tag{9}$$
- **Ensemble F:**
  The same as in Ensemble E.
- **Ensemble G:**
  $$p_\theta^\alpha = \alpha \ln \left(\frac{1 + e^{-2k\theta}}{2} \right). \tag{10}$$
- **Ensemble H:**
  The same as in Ensemble A.

To compare, for the ensemble of random codes defined by the binary $m \times n$ matrices without restrictions, we have the well-known normalized binomial distribution

$$b_\theta = H(\theta) - \alpha \ln 2. \tag{11}$$

Notice that in all the ensembles whenever we let k or ℓ tend to ∞, the average distance distribution converges to the binomial one.

IV. Average Distance Distribution in Ensemble A

Consider the ensemble of all $m \times n$ $(0,1)$-matrices with $m \leq n$, and having all row sums equal k and column sums equal ℓ. In other words, for every matrix $A = [a_{ij}]$, $i = 1,\, \dots,\, m$, $j = 1,\, \dots,\, n$, from this ensemble we have

$$\sum_{i=1}^{m} a_{ij} = \ell, \qquad \text{for every } j = 1,\, \dots,\, n$$
$$\sum_{j=1}^{n} a_{ij} = k, \qquad \text{for every } i = 1,\, \dots,\, m.$$

Counting the total number of ones in the matrices in two ways (by rows and by columns) we conclude that $mk = n\ell$. Let

$$\alpha := \frac{m}{n} = \frac{\ell}{k}, \qquad 0 < \alpha \leq 1. \tag{12}$$

We will denote the described ensemble by $\Lambda_n^{k,\,\alpha}$. Let $w = \theta n$, $0 < \theta < 1$, and denote the subset of the matrices from $\Lambda_n^{k,\,\alpha}$ having an even sum of the first w elements in every row as $\Lambda_{n,\,\theta}^{k,\,\alpha}$. In other words

$$\sum_{j=1}^{w} a_{ij} \in \{0,\, 2,\, 4,\, \dots\}, \qquad \text{for every } i = 1,\, \dots,\, m.$$

This condition yields that

$$\alpha k \theta n = \ell w \equiv 0 \bmod 2. \tag{13}$$

Another possible description of the matrices of this subset is that the componentwise modulo-2 sum of their first w columns is the all-zero column vector of size m (and, thus, the vector $1^w 0^{n-w}$ is a codeword).

Our **problem** is to estimate the number of such matrices $|\Lambda_{n,\theta}^{k,\alpha}|$.

We will make an extensive use of the following result due to [12]. Let $K=(k_1, k_2, \ldots, k_n)$, $L=(\ell_1, \ell_2, \ldots, \ell_n)$, where k_i and ℓ_i are nonnegative integers, and let $N_n^{K,L}$ stand for the ensemble of square $n \times n$ matrices with row sums k_i and column sums ℓ_i.

Theorem 2 (O'Neil): Let $n \to \infty$, and

$$\max_{1\le i\le n}\{k_i, \ell_i\} \le (\ln n)^{\frac{1}{4}-\varepsilon}, \qquad \varepsilon > 0 \tag{14}$$

$$|\{i\colon k_i = 0 \text{ or } \ell_i = 0\}| = O(\ln n). \tag{15}$$

Then, for $\delta > 0$

$$\left|N_n^{K,L}\right| = \frac{\left(\sum_{i=1}^n k_i\right)!}{\prod_{i=1}^n k_i!\ell_i!} \times \exp\left(\frac{-1}{2\left(\sum_{i=1}^n k_i\right)^2}\left(\sum_{i=1}^n k_i(k_i-1)\sum_{i=1}^n \ell_i(\ell_i-1)\right)\right) \cdot \left(1+o\left(n^{-1+\delta}\right)\right). \tag{16}$$

In 1977, Good and Crook [6] demonstrated that Theorem 2 is valid even without condition (15). Thus, it is quite straightforward to generalize it to rectangular matrices. Let again $K=(k_1, k_2, \ldots, k_m)$ and $L=(\ell_1, \ell_2, \ldots, \ell_n)$, $\Lambda_{m,n}^{K,L}$ be the ensemble of rectangular $m \times n$ matrices $m \le n$, with row sums k_i, $i=1, 2, \ldots, m$, and column sums ℓ_j, $j = 1, 2, \ldots, n$.

Theorem 3: Let $m \to \infty$, and

$$\max\left\{\max_{1\le i\le m} k_i, \max_{1\le j\le n} \ell_j\right\} \le (\ln n)^{\frac{1}{4}-\varepsilon}, \qquad \varepsilon > 0. \tag{17}$$

Then, for $\delta > 0$

$$\left|\Lambda_{m,n}^{K,L}\right| = \frac{\left(\sum_{i=1}^m k_i\right)!}{\prod_{i=1}^m k_i! \prod_{i=1}^n \ell_i!} \times \exp\left(\frac{-1}{2\left(\sum_{i=1}^m k_i\right)^2}\left(\sum_{i=1}^m k_i(k_i-1)\sum_{i=1}^n \ell_i(\ell_i-1)\right)\right) \cdot \left(1+o\left(n^{-1+\delta}\right)\right). \tag{18}$$

Proof: Indeed, assume

$$k_{m+1} = k_{m+2} = \cdots = k_n = 0.$$

Then (17) implies (14), (14) implies (16), and (18) follows therefrom. □

Let

$$P_{n,\theta}^{k,\alpha} = \frac{\left|\Lambda_{n,\theta}^{k,\alpha}\right|}{\left|\Lambda_n^{k,\alpha}\right|} \tag{19}$$

be the proportion of the matrices from the set $\Lambda_{n,\theta}^{k,\alpha}$ in the ensemble $\Lambda_n^{k,\alpha}$.

Theorem 4: Let t be the (only) positive root of

$$\frac{(1+t)^{k-1}+(1-t)^{k-1}}{(1+t)^k+(1-t)^k} = 1-\theta. \tag{20}$$

Then, for $0 < \theta < 1$ and k even

$$\lim_{n\to\infty}\frac{1}{n}\ln P_{n,\theta}^{k,\alpha} = \alpha\ln\left(\frac{(1+t)^k+(1-t)^k}{2t^{\theta k}}\left((1-\theta)^{1-\theta}\theta^\theta\right)^k\right) \tag{21}$$

$$P_{n,\theta}^{k,\alpha} = P_{n,1-\theta}^{k,\alpha} \tag{22}$$

and for k odd

$$\lim_{n\to\infty}\frac{1}{n}\ln P_{n,\theta}^{k,\alpha} = \begin{cases} \alpha\ln\left(\frac{(1+t)^k+(1-t)^k}{2t^{\theta k}}\left((1-\theta)^{1-\theta}\theta^\theta\right)^k\right), \\ \qquad \text{if } 0<\theta\le\frac{k-1}{k} \\ -\infty, \qquad \text{otherwise.}\end{cases} \tag{23}$$

A. Proof of Theorem 4

Let us sketch the proof. The treatment depends on parity of k. Given a weight w, our goal is to find the number of matrices from the ensemble such that the submatrix consisting of the first w columns has even row sums. Given the proportions of different row sums in this submatrix (they can be equal only for $0, 2, \ldots, 2[k/2]$) we also know the distribution of the row sums in the complementary right submatrix. Using the generalization of the result by O'Neil, it is possible to count the number of matrices having corresponding row sums distributions in the left and right submatrices. Summing over all possible distributions we obtain an expression for the total number of the matrices, and thus an estimate for the sought probability. The proof is accomplished by finding the maximizing left row sums distribution.

1) The Case of Even k: Let $A \in \Lambda_{n,\theta}^{k,\alpha}$. For a w, fixed, the matrix naturally partitions to two submatrices A^{left} and A^{right} of size $m \times w$ and $m \times (n-w)$ consisting, respectively, of the first w columns and the last $n-w$ columns of A. Let m_i be the number of rows in A^{left} with sums equal to i, where $i \in \{0, 2, 4, \ldots, k\}$. Consequently, A^{right} has m_i rows with sums $k-i$, and the following equalities are valid:

$$\begin{aligned} m_0+m_2+m_4+\cdots+m_k &= \alpha n \\ 2m_2+4m_4+\cdots+km_k &= \alpha k\theta n. \end{aligned} \tag{24}$$

Clearly, $m_i \ge 0$.

Denote the set of all possible matrices A^{left} by $L_{n,\theta}^{k,\alpha}$ and the set of all possible matrices A^{right} by $R_{n,\theta}^{k,\alpha}$. Then evidently

$$\left|\Lambda_{n,\theta}^{k,\alpha}\right| = \sum\binom{\alpha n}{m_0, m_2, \ldots, m_k}\left|L_{n,\theta}^{k,\alpha}\right|\left|R_{n,\theta}^{k,\alpha}\right| \tag{25}$$

where the sum is taken over all solutions $m_0, m_2, \ldots, m_k$ of (24) and

$$\binom{\alpha n}{m_0, m_2, \ldots, m_k} = \frac{(\alpha n)!}{\prod_{i=0}^{k/2} m_{2i}!}$$

is a multinomial coefficient.

Lemma 1: The following holds:

$$\left|L_{n,\theta}^{k,\alpha}\right| = g(n)\,\frac{(\alpha k\theta n)!}{(\alpha k)!^{\theta n} 2!^{m_2} 4!^{m_4} \cdots k!^{m_k}} \tag{26}$$

where for n sufficiently large

$$\frac{1}{2} e^{-\frac{k(k\alpha-1)}{2\theta}} \le g(n) \le 2e^{-\frac{k\alpha-1}{2}} \tag{27}$$

and

$$\left|R_{n,\theta}^{k,\alpha}\right| = h(n)\,\frac{(\alpha k(1-\theta)n)!}{(\alpha k)!^{(1-\theta)n} 2!^{m_{k-2}} 4!^{m_{k-4}} \cdots k!^{m_0}} \tag{28}$$

where for n sufficiently large

$$\frac{1}{2} e^{-\frac{k(k\alpha-1)}{2(1-\theta)}} \le h(n) \le 2e^{-\frac{k\alpha-1}{2}}. \tag{29}$$

Proof: To prove (26) and (27) we take into consideration that (14) is valid, thus from Theorem 3 it follows that for $\delta > 0$

$$\begin{aligned}\left|L_{n,\theta}^{k,\alpha}\right| = &\frac{(\alpha k\theta n)!}{(\alpha k)!^{\theta n} 2!^{m_2} 4!^{m_4} \cdots k!^{m_k}}\\ &\cdot \exp\Bigg(\frac{-1}{2(\alpha k\theta n)^2}\, k\alpha(k\alpha-1)\\ &\qquad \cdot \theta n(2m_2 + 12m_4 + \cdots + k(k-1)m_k)\Bigg)\\ &\cdot \left(1 + o\left(n^{-1+\delta}\right)\right).\end{aligned}$$

However, (24) implies that

$$k\alpha\theta n \le 2m_2 + 12m_4 + \cdots + k(k-1)m_k \le k^2\alpha n.$$

Thus, (26) and (27) follow.

To prove (28) and (29), we transform the conditions (24) into

$$\begin{aligned} m_0 + m_2 + \cdots + m_{k-2} + m_k &= \alpha n\\ km_0 + (k-2)m_2 + \cdots + 2m_{k-2} &= \alpha k(1-\theta)n. \end{aligned} \tag{30}$$

Then from Theorem 3 for $\delta > 0$

$$\begin{aligned}&\left|R_{n,\theta}^{k,\alpha}\right|\\ &= \frac{(\alpha k(1-\theta)n)!}{(\alpha k)!^{(1-\theta)n} k!^{m_0} (k-2)!^{m_2} \cdots 2!^{m_{k-2}}}\\ &\quad\cdot \exp\Bigg(\frac{-1}{2(\alpha k(1-\theta)n)^2}\, k\alpha(k\alpha-1)(1-\theta)n\\ &\qquad \cdot (k(k-1)m_0 + (k-2)(k-3)m_2 + \cdots + 2m_{k-2})\Bigg)\\ &\quad\cdot \left(1 + o\left(n^{-1+\delta}\right)\right).\end{aligned}$$

However, (30) implies that

$$k\alpha(1-\theta)n \le k(k-1)m_0 + \cdots + 2m_{k-2} \le k^2\alpha n,$$

and (28), (29) follow. □

For $n \to \infty$ we use notation $a_n \overset{\ln}{\sim} b_n$ if $\ln a_n \sim \ln b_n$, and say that a_n and b_n are logarithmically equivalent.

Lemma 1 and (25) imply

$$\begin{aligned}\left|\Lambda_{n,\theta}^{k,\alpha}\right| \overset{\ln}{\sim} &\frac{(\alpha k\theta n)!(\alpha k(1-\theta)n)!}{(\alpha k)!^n}\\ &\cdot \sum \frac{(\alpha n)!}{m_0!(0!k!)^{m_0} m_2!(2!(k-2)!)^{m_2} \cdots m_k!(k!0!)^{m_k}}\end{aligned} \tag{31}$$

where the summation is over all $m_0, m_2, \ldots, m_k$ satisfying (24).

Lemma 2:

$$\left|\Lambda_n^{k,\alpha}\right| \overset{\ln}{\sim} \frac{(nk\alpha)!}{(k!)^{n\alpha}(\alpha k)!^n}. \tag{32}$$

Proof: From Theorem 3, we conclude that for $n \to \infty$ and $\delta > 0$

$$\begin{aligned}\left|\Lambda_n^{k,\alpha}\right| \sim &\frac{(nk\alpha)!}{(k!)^{n\alpha}(\alpha k)!^n}\\ &\cdot \exp\left(-\frac{(k-1)(k\alpha-1)}{2}\right) \cdot \left(1 + o\left(n^{-1+\delta}\right)\right)\end{aligned}$$

and (32) follows. □

Lemma 3:

$$\begin{aligned}P_{n,\theta}^{k,\alpha} \overset{\ln}{\sim} &\frac{1}{\binom{nk\alpha}{n\theta k\alpha}} \sum \binom{\alpha n}{m_0, m_2, \ldots, m_k}\\ &\cdot \binom{k}{2}^{m_2} \binom{k}{4}^{m_4} \cdots \binom{k}{k-2}^{m_{k-2}}\end{aligned} \tag{33}$$

where the summation is over all $m_0, m_2, \ldots, m_k$ satisfying (24).

Proof: Follows from (19), and (31), (32). □

Corollary 1:

$$P_{n,\theta}^{k,\alpha} \overset{\ln}{\sim} P_{n\alpha,\theta}^{k,1}. \tag{34}$$

□

By (34), it suffices to accomplish the calculations for $\alpha = 1$ assuming

$$\Lambda_n^k := \Lambda_n^{k,1}, \quad \Lambda_{n,\theta}^k := \Lambda_{n,\theta}^{k,1}, \quad P_{n,\theta}^k := P_{n,\theta}^{k,1}. \tag{35}$$

Let us estimate the right-hand side of (33). By Stirling

$$\ln \binom{nk}{n\theta k} \sim knH(\theta). \tag{36}$$

Denote

$$\begin{aligned}M_{n,\theta}^k := \max &\binom{n}{m_0, m_2, \ldots, m_k} \binom{k}{2}^{m_2}\\ &\cdot \binom{k}{4}^{m_4} \cdots \binom{k}{k-2}^{m_{k-2}}\end{aligned} \tag{37}$$

where the maximum is over all $m_0, m_2, \ldots, m_k$ satisfying (24) with $\alpha = 1$, i.e.,

$$\begin{aligned} m_0 + m_2 + m_4 + \cdots + m_k &= n\\ 2m_2 + 4m_4 + \cdots + km_k &= k\theta n. \end{aligned} \tag{38}$$

Lemma 4:

$$P_{n,\theta}^k \overset{\ln}{\sim} \exp(-knH(\theta)) \cdot M_{n,\theta}^k. \tag{39}$$

Proof: Since m_i's are at most n (see the first equation of (38)), the number of summands in the sum in the right-hand side of (33) is at most $n^{\frac{k}{2}+1}$. Each of the summands is at most $M^k_{n,\theta}$, and thus the sum is at least $M^k_{n,\theta}$ and at most $n^{\frac{k}{2}+1}M^k_{n,\theta}$. To show the logarithmic equivalence it is left to show that $M^k_{n,\theta}$ is exponential in n. Indeed, since

$$\binom{n}{m_0,\, m_2,\, \dots,\, m_k} \le \left(\frac{k}{2}+1\right)^n$$

and

$$\binom{k}{2i} \le \binom{k}{k/2}$$

then

$$M^k_{n,\theta} \le \left(\left(\frac{k}{2}+1\right)\binom{k}{k/2}\right)^n.$$

On the other hand, choose $m_2 = n/2$, and assign to all the remaining m_i's arbitrary values in such a way that (38) is satisfied. Then, clearly,

$$M^k_{n,\theta} \ge \binom{k}{2}^{n/2}$$

and we are done. □

Before we continue the proof of Theorem 4, let us compare the considered distribution with the multinomial one.

2) Multinomial Distribution and an Example: By Lemmas 3 and 4, we reduced the problem to computing logarithmical asymptotics of

$$\ln M^k_{n,\theta} = \max \ln \frac{n!}{m_0! m_2! \cdots m_k!}\binom{k}{2}^{m_2} \cdot \binom{k}{4}^{m_4} \cdots \binom{k}{k-2}^{m_{k-2}} \tag{40}$$

under conditions (38). By

$$\binom{k}{0} + \binom{k}{2} + \cdots \binom{k}{k} = 2^{k-1}$$

we may rewrite (40) as

$$\ln M^k_{n,\theta} = \max \ln \frac{2^{(k-1)n} n!}{m_0! m_2! \cdots m_k!} p_0^{m_0} p_2^{m_2} \cdots p_k^{m_k} \tag{41}$$

where

$$p_{2i} = \frac{\binom{k}{2i}}{2^{k-1}}, \qquad i = 0, 1, \dots, k/2, \sum_{i=0}^{k/2} p_{2i} = 1. \tag{42}$$

Under condition

$$m_0 + m_2 + \cdots + m_k = n \tag{43}$$

the distribution

$$P_{m_0, m_2, \dots, m_k} = \frac{n!}{m_0! m_2! \cdots m_k!} p_0^{m_0} p_2^{m_2} \cdots p_k^{m_k}$$

is multinomial. If $(n+1)p_{2i}$ is an integer then $P_{m_0, m_2, \dots, m_k}$ attains maximum at

$$m_{2i} = (n+1)p_{2i} - \delta_{i,j} \tag{44}$$

for any $j \in \{0, 1, \dots, k/2\}$. In this case

$$\begin{aligned} m_0 + m_2 + \cdots + m_k &= (n+1)\sum_{i=0}^{k/2} p_{2i} - \sum_{i=0}^{k/2} \delta_{i,j} \\ &= n + 1 - 1 = n \end{aligned}$$

and (43) holds.

Recall that the second condition of (38) should hold as well in our case. However, in general, it is not true for the numbers defined in (44).

Let us give an example when the second condition is also valid. Let k be a multiple of 4, $n+1$ be a multiple of 2^{k-1}, and $\theta = 1/2$. Assume

$$m_{2i} = (n+1)p_{2i} - \delta_{i,k/4}. \tag{45}$$

Then, by (42) and (45)

$$\begin{aligned} 2m_2 + 4m_4 + \cdots + km_k &= -\frac{k}{2} + (n+1)\sum_{i=1}^{k/2} 2i \frac{\binom{k}{2i}}{2^{k-1}} \\ &= -\frac{k}{2} + \frac{n+1}{2^{k-1}} \sum_{i=1}^{k/2} k\binom{k-1}{2i-1} \\ &= -\frac{k}{2} + \frac{(n+1)k}{2^{k-1}} \cdot 2^{k-2} \\ &= \frac{nk}{2} \end{aligned}$$

and the second condition in (38) is valid.

Substituting (45) into (40) (and taking into account (42)), and by

$$\begin{aligned} m_{2i}! &\overset{\ln}{\sim} \ln\left(\frac{\binom{k}{2i}}{2^{k-1}}(n+1)\right)! \\ &\overset{\ln}{\sim} (n+1)\frac{\binom{k}{2i}}{2^{k-1}} \ln \frac{\binom{k}{2i}}{2^{k-1}} + (n+1)\frac{\binom{k}{2i}}{2^{k-1}} \ln(n+1) \\ &\quad - \frac{\binom{k}{2i}}{2^{k-1}}(n+1) \end{aligned}$$

we obtain

$$\begin{aligned} \ln M^k_{n,1/2} &\sim n\ln n - n - \frac{n+1}{2^{k-1}} \sum_{i=0}^{k/2} \binom{k}{2i} \ln\binom{k}{2i} \\ &\quad + \frac{n+1}{2^{k-1}}(k-1)\ln 2 \sum_{i=0}^{k/2}\binom{k}{2i} \\ &\quad - (n+1)\ln(n+1) + n + 1 \\ &\quad + (n+1)\sum_{i=0}^{k/2} \frac{\binom{k}{2i}}{2^{k-1}} \ln\binom{k}{2i} \\ &\sim n(k-1)\ln 2. \end{aligned}$$

From Lemmas 3 and 4 (for $\alpha = 1$ and $\theta = 1/2$), we conclude that

$$\ln P^k_{n,1/2} \sim -kn\ln 2 + ((k-1)\ln 2)n = -n\ln 2$$

or

$$\lim_{n\to\infty} \frac{1}{n} \ln P^k_{n,1/2} = -\ln 2. \tag{46}$$

This result is a particular case of Theorem 4 since for $\theta = 1/2$, (20) has the unique positive solution $t = 1$.

Since the second condition of (38) is in general invalid for the choice of m_{2i}'s given by (44), the numbers m_{2i} providing maximum to $M_{n,\theta}^k$ are different from (45).

Now we pass to an accomplishment of the proof of Theorem 4.

3) End of the Proof to Theorem 4 for k Even: Let us exclude from (38) m_0 and m_k

$$\begin{aligned} m_k &= \mu_k \\ &:= \theta n - \frac{2}{k}\, m_2 - \frac{4}{k}\, m_4 - \cdots - \frac{k-2}{k}\, m_{k-2} \\ m_0 &= \mu_0 \\ &:= (1-\theta)n - \frac{k-2}{k}\, m_2 - \frac{k-4}{k}\, m_4 - \cdots - \frac{2}{k}\, m_{k-2}. \end{aligned} \tag{47}$$

From (47) we have

$$\begin{aligned} \ln M_{n,\theta}^k \sim \max\Big\{ & n\ln n - n - \mu_0 \ln \mu_0 + \mu_0 - m_2 \ln m_2 + m_2 \\ & - m_4 \ln m_4 + m_4 - \cdots - m_{k-2} \ln m_{k-2} \\ & + m_{k-2} - \mu_k \ln \mu_k + \mu_k + m_2 \ln \binom{k}{2} \\ & + m_4 \ln \binom{k}{4} + \cdots + m_{k-2} \ln \binom{k}{k-2} \Big\} \\ = \max\Big\{ & n\ln n - \mu_0 \ln \mu_0 - m_2 \ln m_2 - m_4 \ln m_4 \\ & - \cdots - m_{k-2} \ln m_{k-2} - \mu_k \ln \mu_k \\ & + m_2 \ln \binom{k}{2} + m_4 \ln \binom{k}{4} \\ & + \cdots + m_{k-2} \ln \binom{k}{k-2} \Big\}. \end{aligned} \tag{48}$$

Equating the partial derivatives to zero we derive (after straightforward simplifications) a system of equations for $m_2, m_4, \ldots, m_{k-2}$

$$\begin{aligned} \frac{k-2}{k} \ln \mu_0 - \ln m_2 + \frac{2}{k} \ln \mu_k + \ln \binom{k}{2} &= 0 \\ \frac{k-4}{k} \ln \mu_0 - \ln m_4 + \frac{4}{k} \ln \mu_k + \ln \binom{k}{4} &= 0 \\ &\cdots \\ \frac{2}{k} \ln \mu_0 - \ln m_{k-2} + \frac{k-2}{k} \ln \mu_k + \ln \binom{k}{k-2} &= 0. \end{aligned} \tag{49}$$

Solving the system of the first and ith equation in $\ln \mu_k$ and $\ln \mu_0$ for every $i = 2, 3, \ldots, k/2 - 1$, we find

$$\frac{k-2}{k}\, m_2 + \frac{k-4}{k}\, m_4 + \cdots + \frac{2}{k}\, m_{k-2} = (1-\theta)n - \left(\frac{m_2}{\binom{k}{2}}\right)^{i/(i-1)} \left(\frac{\binom{k}{2i}}{m_{2i}}\right)^{1/(i-1)} \tag{50}$$

$$\frac{2}{k}\, m_2 + \frac{4}{k}\, m_4 + \cdots + \frac{k-2}{k}\, m_{k-2} = \theta n - \left(\frac{\binom{k}{2}}{m_2}\right)^{(k-2i)/2(i-1)} \left(\frac{m_{2i}}{\binom{k}{2i}}\right)^{(k-2)/2(i-1)}. \tag{51}$$

Set

$$\frac{m_4}{m_2} = t_4, \quad \frac{m_6}{m_2} = t_6, \quad \cdots \quad \frac{m_{k-2}}{m_2} = t_{k-2}. \tag{52}$$

Then, by (50)

$$\frac{k-2}{k} + t_4\, \frac{k-4}{k} + \cdots + t_{k-2}\, \frac{2}{k} + \frac{\binom{k}{2i}^{1/(i-1)}}{\binom{k}{2}^{i/(i-1)} t_{2i}^{1/(i-1)}} = \frac{(1-\theta)n}{m_2}. \tag{53}$$

From (53) we see that

$$C_{k,n} := \left(\frac{\binom{k}{2}}{\binom{k}{2i}}\, t_{2i}\right)^{1/(i-1)} \tag{54}$$

does not depend on i. Therefore,

$$t_{2i} = C_{k,n}^{i-1}\, \frac{\binom{k}{2i}}{\binom{k}{2}}. \tag{55}$$

From (52) and (55) it follows that to solve the system (49) we need to find $C_{k,n}$ and m_2. Rewriting (51) using (52)

$$\frac{2}{k} + t_4\, \frac{4}{k} + \cdots + t_{k-2}\, \frac{k-2}{k} + \frac{\binom{k}{2}^{\frac{k-2i}{2(i-1)}} t_{2i}^{\frac{k-2}{2(i-1)}}}{\binom{k}{2i}^{\frac{k-2}{2(i-1)}}} = \frac{\theta n}{m_2} \tag{56}$$

dividing (56) by (53), and taking into account (55) after simplifications, we get

$$C_{k,n}^{k/2} + \sum_{i=1}^{\frac{k}{2}-1} \left(\binom{k-1}{2i} - g \binom{k-1}{2i-1} \right) C_{k,n}^{\frac{k}{2}-i} - g = 0 \tag{57}$$

where

$$g = \frac{\theta}{1-\theta}. \tag{58}$$

However, it is easy to see that

$$\sum_{i=1}^{\frac{k}{2}-1} \binom{k-1}{2i} x^{\frac{k}{2}-i} = \frac{\sqrt{x}}{2} \left(\left(\sqrt{x}+1\right)^{k-1} + \left(\sqrt{x}-1\right)^{k-1} \right) - x^{k/2} \tag{59}$$

$$\sum_{i=1}^{\frac{k}{2}-1} \binom{k-1}{2i-1} x^{\frac{k}{2}-i} = \frac{1}{2} \left(\left(\sqrt{x}+1\right)^{k-1} + \left(\sqrt{x}-1\right)^{k-1} \right) - 1. \tag{60}$$

Set

$$t := \sqrt{C_{k,n}}. \tag{61}$$

From (57)–(61) it follows that

$$\frac{t\left((t+1)^{k-1} + (t-1)^{k-1}\right)}{(t+1)^{k-1} - (t+1)^{k-1}} = \frac{\theta}{1-\theta}. \tag{62}$$

Since $k-1$ is odd

$$\frac{(1+t)^{k-1} + (1-t)^{k-1}}{(1+t)^k + (1-t)^k} = 1 - \theta. \tag{63}$$

Thus, we arrived at the equation in Theorem 4.

Now we are in a position to accomplish solution of (49). By (54) and (61)

$$t_{2i} = \frac{\binom{k}{2i}}{\binom{k}{2}} t^{2(i-1)} \tag{64}$$

and since

$$\frac{\binom{k}{2i}^{1/(i-1)}}{\binom{k}{2}^{i/(i-1)} t_{2i}^{1/(i-1)}} = \frac{1}{t^2\binom{k}{2}} \tag{65}$$

then by (53)

$$\frac{1}{t^2\binom{k}{2}} \sum_{i=0}^{\frac{k}{2}-1} \binom{k-1}{2i} t^{2i} = \frac{(1-\theta)n}{m_2}.$$

Alternatively

$$\frac{1}{2t^2\binom{k}{2}} \left((1+t)^{k-1} + (1-t)^{k-1}\right) = \frac{(1-\theta)n}{m_2}. \tag{66}$$

Thus,

$$m_2 = \frac{2(1-\theta)\binom{k}{2}t^2 n}{(1+t)^{k-1} + (1-t)^{k-1}}. \tag{67}$$

By (52) and (64)

$$m_{2i} = \frac{2(1-\theta)\binom{k}{2i}t^{2i} n}{(1+t)^{k-1} + (1-t)^{k-1}}. \tag{68}$$

Notice also that (52) and (65) yield

$$\left(\frac{m_2}{\binom{k}{2}}\right)^{i/(i-1)} \left(\frac{\binom{k}{2i}}{m_{2i}}\right)^{1/(i-1)} = \frac{m_2}{t^2\binom{k}{2}}$$

$$\begin{aligned} &\left(\frac{\binom{k}{2}}{m_2}\right)^{\frac{k-2i}{2(i-1)}} \left(\frac{m_{2i}}{\binom{k}{2i}}\right)^{\frac{k-2}{2(i-1)}} \\ &= \frac{\left(\left(\frac{\binom{k}{2}}{m_2}\right)^{\frac{1}{i-1}} \left(\frac{m_{2i}}{\binom{k}{2i}}\right)^{\frac{1}{i-1}}\right)^{k/2}}{\left(\frac{\binom{k}{2}}{m_2}\right)^{\frac{i}{i-1}} \left(\frac{m_{2i}}{\binom{k}{2i}}\right)^{\frac{1}{i-1}}} \\ &= \frac{t^k}{\frac{t^2\binom{k}{2}}{m_2}} = \frac{t^{k-2}m_2}{\binom{k}{2}} \end{aligned}$$

and thus by (47), (50), (51), (67), (68), we have

$$\mu_0 = \frac{2(1-\theta)n}{(1+t)^{k-1} + (1-t)^{k-1}} \tag{69}$$

$$\mu_k = \frac{2(1-\theta)t^k n}{(1+t)^{k-1} + (1-t)^{k-1}}. \tag{70}$$

Now, by (48) and (67)–(70) after simplifications we have

$$\begin{aligned} &\ln M_{n,\theta}^k \\ &\sim n\ln n - \frac{2(1-\theta)n\ln n}{(1+t)^{k-1} + (1-t)^{k-1}} \\ &\quad - \frac{2(1-\theta)n}{(1+t)^{k-1} + (1-t)^{k-1}} \ln \frac{2(1-\theta)}{(1+t)^{k-1} + (1-t)^{k-1}} \\ &\quad - \frac{2(1-\theta)t^k n\ln n}{(1+t)^{k-1} + (1-t)^{k-1}} - \frac{2(1-\theta)t^k n}{(1+t)^{k-1} + (1-t)^{k-1}} \\ &\quad \cdot \ln \frac{2(1-\theta)t^k}{(1+t)^{k-1} + (1-t)^{k-1}} - \frac{2(1-\theta)n\ln n}{(1+t)^{k-1} + (1-t)^{k-1}} \\ &\quad \cdot \sum_{i=1}^{\frac{k}{2}-1} \binom{k}{2i} t^{2i} - \frac{2(1-\theta)n}{(1+t)^{k-1} + (1-t)^{k-1}} \\ &\quad \cdot \sum_{i=1}^{\frac{k}{2}-1} \binom{k}{2i} t^{2i} \ln \frac{2(1-\theta)t^{2i}}{(1+t)^{k-1} + (1-t)^{k-1}}. \end{aligned} \tag{71}$$

Let us compute the coefficient at $n\ln n$ in the last expression. We have

$$\begin{aligned} &1 - \frac{2(1-\theta)}{(1+t)^{k-1} + (1-t)^{k-1}} - \frac{2(1-\theta)t^k}{(1+t)^{k-1} + (1-t)^{k-1}} \\ &\quad + \frac{2(1-\theta)}{(1+t)^{k-1} + (1-t)^{k-1}} \left(1 + t^k - \sum_{i=0}^{k/2} \binom{k}{2i} t^{2i}\right) \\ &= 1 - \frac{2(1-\theta)}{(1+t)^{k-1} + (1-t)^{k-1}} \sum_{i=0}^{k/2} \binom{k}{2i} t^{2i} \\ &= 1 - \frac{(1-\theta)((1+t)^k + (1-t)^k)}{(1+t)^{k-1} + (1-t)^{k-1}}. \end{aligned}$$

However, by (63), the last expression equals 0. From this, and as well from the following equalities:

$$\sum_{i=1}^{\frac{k}{2}-1} \binom{k}{2i} t^{2i} = -1 - t^k + \sum_{i=0}^{k/2} \binom{k}{2i} t^{2i}$$

$$2i\binom{k}{2i} = k\binom{k-1}{2i-1}$$

we conclude

$$\begin{aligned} \ln M_{n,\theta}^k \sim &- \frac{2(1-\theta)n}{(1+t)^{k-1} + (1-t)^{k-1}} \\ &\cdot \left(\sum_{i=0}^{k/2} \binom{k}{2i} t^{2i} \ln \frac{2(1-\theta)}{(1+t)^{k-1} + (1-t)^{k-1}} \right. \\ &\left. + (k\ln t) \sum_{i=1}^{k/2} \binom{k-1}{2i-1} t^{2i} \right). \end{aligned} \tag{72}$$

However,

$$\sum_{i=0}^{k/2} \binom{k}{2i} t^{2i} = \frac{(1+t)^k + (1-t)^k}{2} \tag{73}$$

$$\sum_{i=1}^{k/2} \binom{k-1}{2i-1} t^{2i} = t \cdot \frac{(1+t)^{k-1} - (1-t)^{k-1}}{2} \tag{74}$$

and from (72)

$$\begin{aligned} \ln M_{n,\theta}^k \sim -(1-\theta)n &\left(\frac{(1+t)^k + (1-t)^k}{(1+t)^{k-1} + (1-t)^{k-1}} \right. \\ &\cdot \ln \frac{2(1-\theta)}{(1+t)^{k-1} + (1-t)^{k-1}} \\ &\left. + \frac{(1+t)^{k-1} - (1-t)^{k-1}}{(1+t)^{k-1} + (1-t)^{k-1}} kt\ln t \right). \end{aligned}$$

Taking into account (62) and (63) we find

$$\begin{aligned}\ln M_{n,\theta}^{k} &\sim -(1-\theta)n\left(\frac{1}{1-\theta}\ln\frac{2(1-\theta)}{(1+t)^{k-1}+(1-t)^{k-1}}\right.\\ &\qquad\left.+\frac{\theta}{1-\theta}\,k\ln t\right)\\ &= n\ln\frac{(1+t)^{k-1}+(1-t)^{k-1}}{2(1-\theta)t^{k\theta}}. \qquad (75)\end{aligned}$$

And, finally, by (63)

$$\frac{(1+t)^{k-1}+(1-t)^{k-1}}{1-\theta}=(1+t)^{k}+(1-t)^{k}$$

and from (75) we have

$$\ln M_{n,\theta}^{k}\sim n\ln\frac{(1+t)^{k}+(1-t)^{k}}{2t^{k\theta}}. \qquad (76)$$

From (33)–(39) we finally have (21) of Theorem 4.

4) The Case of Odd k: In this subsection, we keep all the notations of Section IV-A1. Consider $m_0, m_2, \ldots, m_{k-1}$ satisfying

$$\begin{aligned}m_0+m_2+m_4+\cdots+m_{k-1}&=\alpha n\\ 2m_2+4m_4+\cdots+(k-1)m_{k-1}&=\alpha k\theta n. \qquad (77)\end{aligned}$$

From (77) we have

$$\begin{aligned}m_{k-1}&=\mu_{k-1}\\ &:=\alpha\frac{k}{k-1}\theta n-\frac{2}{k-1}m_2-\frac{4}{k-1}m_4-\cdots-\frac{k-3}{k-1}m_{k-3} \qquad (78)\\ m_0&=\mu_0\\ &:=\alpha\left(1-\frac{k}{k-1}\theta\right)n-\frac{k-3}{k-1}m_2-\frac{k-5}{k-1}m_4\\ &\qquad-\cdots-\frac{2}{k-1}m_{k-3}. \qquad (79)\end{aligned}$$

Since $m_0\geq 0$, then (79) yields

$$0<\theta\leq\frac{k-1}{k}. \qquad (80)$$

Otherwise, $P_{n,\theta}^{k,\alpha}=0$. Restriction (80) is an important distinction of the case when k is odd (see (23)). Thus, we assume in what follows that (80) is valid. As it is easy to check, Lemmas 1–4 hold also for odd k's (with a minor change of notation). For example, (33) has the following form:

$$\begin{aligned}P_{n,\theta}^{k,\alpha}&\overset{\ln}{\sim}\frac{1}{\binom{nk\alpha}{n\theta k\alpha}}\sum\binom{\alpha n}{m_0,\, m_2,\, \ldots,\, m_{k-1}}\\ &\qquad\cdot\binom{k}{2}^{m_2}\binom{k}{4}^{m_4}\cdots\binom{k}{k-1}^{m_{k-1}}. \qquad (81)\end{aligned}$$

Therefore, similarly to above, we have to determine the asymptotics of

$$\begin{aligned}\ln M_{n,\theta}^{k}&=\max\ln\frac{n!}{m_0!m_2!\cdots m_{k-1}!}\binom{k}{2}^{m_2}\\ &\qquad\cdot\binom{k}{4}^{m_4}\cdots\binom{k}{k-1}^{m_{k-1}} \qquad (82)\end{aligned}$$

under condition (77) or (78), (79) when $\alpha=1$. Similarly to (48), we find

$$\begin{aligned}\ln M_{n,\theta}^{k}=\max\Big\{&n\ln n-\mu_0\ln\mu_0-m_2\ln m_2\\ &-m_4\ln m_4-\cdots-m_{k-3}\ln m_{k-3}\\ &-\mu_{k-1}\ln\mu_{k-1}+m_2\ln\binom{k}{2}\\ &+m_4\ln\binom{k}{4}+\cdots+m_{k-2}\ln\binom{k}{k-3}\\ &+\mu_{k-1}\ln k\Big\}. \qquad (83)\end{aligned}$$

Equating partial derivatives to 0, after some simplifications we obtain a system of equations for $m_2, m_4, \ldots, m_{k-3}$

$$\begin{aligned}&\frac{k-3}{k-1}\ln\mu_0-\ln m_2+\frac{2}{k-1}\ln\mu_{k-1}+\ln\binom{k}{2}\\ &\qquad-\frac{2}{k-1}\ln k=0\\ &\frac{k-5}{k-1}\ln\mu_0-\ln m_4+\frac{4}{k-1}\ln\mu_{k-1}+\ln\binom{k}{4}\\ &\qquad-\frac{4}{k-1}\ln k=0\\ &\qquad\cdots\\ &\frac{2}{k-1}\ln\mu_0-\ln m_{k-3}+\frac{k-3}{k-1}\ln\mu_{k-1}+\ln\binom{k}{k-3}\\ &\qquad-\frac{k-3}{k-1}\ln k=0. \qquad (84)\end{aligned}$$

From the first and the ith equations we find

$$\begin{aligned}&\frac{k-3}{k-1}m_2+\frac{k-5}{k-1}m_4+\cdots+\frac{2}{k-1}m_{k-3}\\ &\quad=\left(1-\frac{k}{k-1}\theta\right)n-\left(\frac{m_2}{\binom{k}{2}}\right)^{i/(i-1)}\\ &\qquad\cdot\left(\frac{\binom{k}{2i}}{m_{2i}}\right)^{1/(i-1)} \qquad (85)\\ &\frac{2}{k-1}m_2+\frac{4}{k-1}m_4+\cdots+\frac{k-3}{k-1}m_{k-3}\\ &\quad=\frac{k}{k-1}\theta n-k\left(\frac{\binom{k}{2}}{m_2}\right)^{(k-2i-1)/2(i-1)}\\ &\qquad\cdot\left(\frac{m_{2i}}{\binom{k}{2i}}\right)^{(k-3)/2(i-1)}. \qquad (86)\end{aligned}$$

Set

$$\frac{m_4}{m_2}=t_4,\quad\frac{m_6}{m_2}=t_6,\quad\cdots\quad\frac{m_{k-3}}{m_2}=t_{k-3}. \qquad (87)$$

Then, by (85)

$$\begin{aligned}&\frac{k-3}{k-1}+t_4\frac{k-5}{k-1}+\cdots+t_{k-3}\frac{2}{k-1}+\frac{\binom{k}{2i}^{1/(i-1)}}{\binom{k}{2}^{i/(i-1)}t_{2i}^{1/(i-1)}}\\ &\qquad=\frac{\left(1-\frac{k}{k-1}\theta\right)n}{m_2}. \qquad (88)\end{aligned}$$

From (88) we see that

$$C_{k,\,n} := \left(\frac{\binom{k}{2}}{\binom{k}{2i}}\, t_{2i}\right)^{1/(i-1)} \tag{89}$$

does not depend on i. Therefore,

$$t_{2i} = C_{k,\,n}^{i-1}\, \frac{\binom{k}{2i}}{\binom{k}{2}}. \tag{90}$$

From (87) and (90) it follows that to solve the system (84) it is left to find $C_{k,\,n}$ and m_2. Rewriting (75) using (76)

$$\begin{aligned} &\frac{2}{k-1} + t_4\, \frac{4}{k-1} + \cdots + t_{k-3}\, \frac{k-3}{k-1} \\ &\qquad + k\, \frac{\binom{k}{2}^{\frac{k-2i-1}{2(i-1)}}\, t_{2i}^{\frac{k-3}{2(i-1)}}}{\binom{k}{2i}^{\frac{k-3}{2(i-1)}}} = \frac{\frac{k}{k-1}\,\theta n}{m_2} \end{aligned} \tag{91}$$

dividing (91) by (88), and taking into account (90) after simplifications we get an equation in $C_{k,\,n}$ which is essentially distinct from the corresponding one (57) in the case of even k

$$\begin{aligned} &hk(k-1)C_{k,\,n}^{(k-1)/2} + k \sum_{j=1}^{(k-3)/2} \\ &\cdot \left((h+1)\binom{k-1}{2j-1} - \binom{k-1}{2j}\right) C_{k,\,n}^{j} - k + 1 = 0 \end{aligned} \tag{92}$$

where

$$h = \frac{1 - \frac{k}{k-1}\,\theta}{\frac{k}{k-1}\,\theta}. \tag{93}$$

It is easy to verify that

$$\begin{aligned} &\sum_{j=1}^{(k-3)/2} \binom{k-1}{2j} x^j \\ &\quad = \frac{(1+\sqrt{x}\,)^{k-1} + (1-\sqrt{x}\,)^{k-1}}{2} - x^{(k-1)/2} - 1 \end{aligned} \tag{94}$$

$$\begin{aligned} &\sum_{j=1}^{(k-3)/2} \binom{k-1}{2j-1} x^j \\ &\quad = \sqrt{x}\left(\frac{(1+\sqrt{x}\,)^{k-1} - (1-\sqrt{x}\,)^{k-1}}{2}\right) - (k-1)x^{(k-1)/2}. \end{aligned} \tag{95}$$

Set

$$t := \sqrt{C_{k,\,n}}. \tag{96}$$

From (92)–(96) we have

$$\frac{t\left((1+t)^{k-1} - (1-t)^{k-1}\right)}{(1+t)^{k-1} + (1-t)^{k-1}} = \frac{k-1}{hk+1} = g := \frac{\theta}{1-\theta}. \tag{97}$$

Again (see (63)) this yields

$$\frac{(1+t)^{k-1} + (1-t)^{k-1}}{(1+t)^k + (1-t)^k} = 1 - \theta. \tag{98}$$

Thus, for k odd we have obtained the same (63) as in Theorem 4. Now we are in a position to accomplish the solution of (84). By (96) and (90)

$$t_{2i} = \frac{\binom{k}{2i}}{\binom{k}{2}}\, t^{2(i-1)} \tag{99}$$

and by (88)

$$\frac{1}{t^2\binom{k}{2}} \sum_{i=0}^{(k-3)/2} \binom{k}{2i} \frac{k-2i-1}{k-1}\, t^{2i} = \frac{\left(1 - \frac{k}{k-1}\,\theta\right) n}{m_2}. \tag{100}$$

On the other hand

$$\begin{aligned} &\sum_{i=0}^{(k-3)/2} \binom{k}{2i} \frac{k-2i-1}{k-1}\, t^{2i} \\ &\quad = \sum_{i=0}^{(k-3)/2} \binom{k}{2i} t^{2i} - \sum_{i=1}^{(k-3)/2} \frac{2i}{k-1} \binom{k}{2i} t^{2i} \\ &\quad = \sum_{i=0}^{(k-3)/2} \binom{k}{2i} t^{2i} - \frac{k}{k-1} \sum_{i=1}^{(k-3)/2} \binom{k-1}{2i-1} t^{2i} \\ &\quad = \frac{(1+t)^k + (1-t)^k}{2} - kt^{k-1} \\ &\qquad - \frac{k}{k-1}\left(\frac{t}{2}\left((1+t)^{k-1} - (1-t)^{k-1}\right) - (k-1)t^{k-1}\right) \\ &\quad = \frac{(1+t)^k + (1-t)^k}{2} - \frac{kt}{2(k-1)}\left((1+t)^{k-1} - (1-t)^{k-1}\right) \end{aligned}$$

(by (97))

$$\begin{aligned} &\quad = \frac{(1+t)^k + (1-t)^k}{2} - \frac{k\theta}{2(k-1)(1-\theta)} \\ &\qquad \cdot \left((1+t)^{k-1} + (1-t)^{k-1}\right) \end{aligned}$$

(by (98))

$$\quad = \left((1+t)^{k-1} + (1-t)^{k-1}\right)\left(\frac{1}{2(1-\theta)} - \frac{k\theta}{2(k-1)(1-\theta)}\right)$$

(by (100))

$$\quad = t^2\binom{k}{2} \frac{k-1-k\theta}{k-1} \cdot \frac{n}{m_2}$$

and

$$m_2 = \frac{2(1-\theta)\binom{k}{2} t^2 n}{(1+t)^{k-1} + (1-t)^{k-1}} \tag{101}$$

which (surprisingly for the authors!) coincides with (67). From (87) and (99)

$$m_{2i} = \frac{2(1-\theta)\binom{k}{2i} t^{2i} n}{(1+t)^{k-1} + (1-t)^{k-1}}. \tag{102}$$

Now from (101) and (102)

$$\left(\frac{m_2}{\binom{k}{2}}\right)^{i/(i-1)} \left(\frac{\binom{k}{2i}}{m_{2i}}\right)^{1/(i-1)} = \frac{m_2}{t^2\binom{k}{2}} \tag{103}$$

and

$$\left(\frac{\binom{k}{2}}{m_2}\right)^{\frac{k-2i-1}{2(i-1)}} \left(\frac{m_{2i}}{\binom{k}{2i}}\right)^{\frac{k-3}{2(i-1)}} = \frac{t^{k-3} m_2}{\binom{k}{2}}. \tag{104}$$

From (78), (79) when $\alpha = 1$, (85), (86), and (101)–(104) we find

$$\mu_0 = \frac{2(1-\theta)n}{(1+t)^{k-1}+(1-t)^{k-1}} \tag{105}$$

$$\mu_{k-1} = \frac{kt^{k-3}m_2}{\binom{k}{2}} = \frac{2(1-\theta)t^{k-1}kn}{(1+t)^{k-1}+(1-t)^{k-1}}. \tag{106}$$

Further, from (83) using (101), (102), (105), and (106) we deduce after some transformations

$$\begin{aligned}\ln M^k_{n,\theta} \sim{}& n\ln n\\ &- \frac{2(1-\theta)n\ln n}{(1+t)^{k-1}+(1-t)^{k-1}}\\ &- \frac{2(1-\theta)n}{(1+t)^{k-1}+(1-t)^{k-1}}\ln\frac{2(1-\theta)}{(1+t)^{k-1}+(1-t)^{k-1}}\\ &- \frac{2(1-\theta)kt^{k-1}n\ln n}{(1+t)^{k-1}+(1-t)^{k-1}} - \frac{2(1-\theta)kt^{k-1}n}{(1+t)^{k-1}+(1-t)^{k-1}}\\ &\cdot \ln\frac{2(1-\theta)t^{k-1}}{(1+t)^{k-1}+(1-t)^{k-1}} - \frac{2(1-\theta)n\ln n}{(1+t)^{k-1}+(1-t)^{k-1}}\\ &\cdot \sum_{i=1}^{(k-3)/2}\binom{k}{2i}t^{2i} - \frac{2(1-\theta)n}{(1+t)^{k-1}+(1-t)^{k-1}}\\ &\cdot \sum_{i=1}^{(k-3)/2}\binom{k}{2i}t^{2i}\ln\frac{2(1-\theta)t^{2i}}{(1+t)^{k-1}+(1-t)^{k-1}}.\end{aligned} \tag{107}$$

Let us compute the coefficient at $n\ln n$ in the last expression. We have

$$\begin{aligned}1 &- \frac{2(1-\theta)}{(1+t)^{k-1}+(1-t)^{k-1}} - \frac{2(1-\theta)kt^{k-1}}{(1+t)^{k-1}+(1-t)^{k-1}}\\ &+ \frac{2(1-\theta)}{(1+t)^{k-1}+(1-t)^{k-1}}\\ &\cdot \left(1 + kt^{k-1} - \sum_{i=0}^{(k-1)/2}\binom{k}{2i}t^{2i}\right)\\ &= 1 - \frac{2(1-\theta)}{(1+t)^{k-1}+(1-t)^{k-1}}\sum_{i=0}^{(k-1)/2}\binom{k}{2i}t^{2i}\\ &= 1 - \frac{(1-\theta)((1+t)^k+(1-t)^k)}{(1+t)^{k-1}+(1-t)^{k-1}}.\end{aligned}$$

However, by (98) the last expression equals 0. From this, as well as from the following equalities:

$$\sum_{i=1}^{(k-3)/2}\binom{k}{2i}t^{2i} = -1 - t^{k-1} + \sum_{i=0}^{(k-1)/2}\binom{k}{2i}t^{2i}$$

$$2i\binom{k}{2i} = k\binom{k-1}{2i-1},$$

we conclude that

$$\begin{aligned}\ln M^k_{n,\theta} \sim{}& -\frac{2(1-\theta)n}{(1+t)^{k-1}+(1-t)^{k-1}}\\ &\cdot \left(\sum_{i=0}^{(k-1)/2}\binom{k}{2i}t^{2i}\ln\frac{2(1-\theta)}{(1+t)^{k-1}+(1-t)^{k-1}}\right.\\ &\left. + (k\ln t)\sum_{i=1}^{(k-1)/2}\binom{k-1}{2i-1}t^{2i}\right).\end{aligned} \tag{108}$$

However,

$$\sum_{i=0}^{(k-1)/2}\binom{k}{2i}t^{2i} = \frac{(1+t)^k+(1-t)^k}{2} \tag{109}$$

$$\sum_{i=1}^{(k-1)/2}\binom{k-1}{2i-1}t^{2i} = t\cdot\frac{(1+t)^{k-1}-(1-t)^{k-1}}{2}. \tag{110}$$

Comparison of (108)–(110), (97), (98) with corresponding (72)–(74), (62), (63) shows that further computations are not dependent on the parity of k. Thus, for $0 < \theta \le (k-1)/k$ we have (the same as in Section IV-A1)

$$\ln M^k_{n,\theta} \sim n\ln\frac{(1+t)^k+(1-t)^k}{2t^{k\theta}} \tag{111}$$

and (23) of Theorem 4 follows. □

B. *Study of (20)*

What is left in the proof is to show that the following equation

$$\frac{(1+t)^{k-1}+(1-t)^{k-1}}{(1+t)^k+(1-t)^k} = 1-\theta \tag{112}$$

has a unique positive solution. In the subsequent theorem, we not only prove this statement, but also find intervals for the root to exist.

Theorem 5:

a) For k even and any $\theta \in (0, 1]$, (112) possesses the unique positive root t_θ such that $t_\theta \in [\theta/(1-\theta), 1]$ for $\theta \le 1/2$, and $t_\theta \in (1, \theta/(1-\theta))$ for $\theta > 1/2$.

b) For k odd and any $\theta \in (0, (k-1)/k]$, (112) possesses the unique positive root t_θ such that $t_\theta \in [\theta/(1-\theta), 1]$ for $\theta \le 1/2$, and $t_\theta \in [\theta/(1-\theta), +\infty)$ for $\theta \in (1/2, (k-1)/k]$.

Proof: Set

$$z := \frac{1-t}{1+t}, \qquad a := 1-2\theta. \tag{113}$$

Then the considered equation transforms into

$$f(z) := az^k - z^{k-1} - z + a = 0. \tag{114}$$

Notice that for $t > 0$ we have $|z| < 1$.

a) Let k be even. Assume $\theta \in (0, 1/2]$. Then from (113) it follows that $a \in [0, 1)$. If $z \in [0, 1)$, that corresponds to $t \in (0, 1]$, then

$$\begin{aligned}f'(z) &= akz^{k-1} - (k-1)z^{k-2} - 1\\ &\le kz^{k-2} - (k-1)z^{k-2} - 1\\ &= z^{k-2} - 1 < 0.\end{aligned} \tag{115}$$

Furthermore, since $f(0) = a > 0$, $f(1) = 2(a-1) < 0$, then $f(z)$ has the unique root in the interval $[0, 1)$. It is possible to find more accurately its location if one takes into account that

$$f(a) = a^{k+1} - a^{k-1} < 0 \tag{116}$$

and thus it is located in $[0, a)$. However, since for $z = a = 1-2\theta$ we have $t = \theta/(1-\theta)$, the only positive root $t_\theta \in [\theta/(1-\theta), 1]$. The value of the root $z = 0$

corresponds to $\theta = 1/2$, $a = 0$, $t = 1$. If, however, $z \in (-1, 0)$, then denoting $\zeta := -z \in (0, 1)$, we have

$$f'(z) = -ak\zeta^{k-1} - (k-1)\zeta^{k-2} - 1 < 0.$$

Since $f(-1) = 2(1+a) > 0$, $f(0) = a > 0$, then $f(z) \geq a > 0$. Thus, for $|z| < 1$ we have the unique root in the interval $[0, a)$, that corresponds to a unique positive value $t \in [\theta/(1-\theta), 1]$.

Now, let $\theta \in (1/2, 1]$, then $a \in [-1, 0)$. If $z \in [0, 1)$ then

$$f'(z) = akz^{k-1} - (k-1)z^{k-2} - 1 < -1.$$

Since $f(0) = a < 0$, $f(1) = 2(a-1) < 0$, then $f(z) \leq a < 0$ and there are no roots in the interval $[0, 1)$. If $z \in (-1, 0)$ then denoting $\zeta := -z \in (0, 1)$, we have

$$\begin{aligned} f'(z) &= -ak\zeta^{k-1} - (k-1)\zeta^{k-2} - 1 \\ &< k\zeta^{k-2} - (k-1)\zeta^{k-2} - 1 \\ &= \zeta^{k-2} - 1 < 0. \end{aligned}$$

Furthermore, since $f(-1) = 2(1+a) \geq 0$, $f(0) = a < 0$, then $f(z)$ has the unique root in the interval $[-1, 0)$ that corresponds to a unique value of $t > 1$. It is possible to find its location more accurately if one takes into account that

$$f(a) = a^{k+1} - a^{k-1} \geq 0 \tag{117}$$

for $a \in [-1, 0)$. Therefore, $f(z)$ has a root in $[a, 0)$, which corresponds $t_\theta \in (1, \theta/(1-\theta)]$.

b) Let k be odd. Assume $\theta \in (0, 1/2]$. Then $a \in [0, 1)$. If $z \in [0, 1)$, then (115) is valid, and since $f(0) = a \geq 0$, $f(1) = 2(a-1) < 0$, then $f(z)$ has the unique root in the interval $[0, 1)$. It is possible to specify its location by taking into account that

$$f(a) = a^{k+1} - a^{k-1} \leq 0 \tag{118}$$

i.e., it is located in $[0, a]$, which corresponds to $t_\theta \in [\theta/(1-\theta), 1]$. The value of the root $z = 0$ corresponds to $\theta = 1/2$, $a = 0$, $t = 1$. If, however, $z \in (-1, 0)$, then denoting $\zeta := -z \in (0, 1)$, we have for $f(z)$

$$\begin{aligned} f(z) &= -a\zeta^{k} - \zeta^{k-1} + \zeta + a \\ &= a\left(1 - \zeta^{k}\right) + \zeta\left(1 - \zeta^{k-2}\right) > 0. \end{aligned}$$

Thus, $f(z)$ does not have roots in the interval $z \in (-1, 0)$. Now, let $\theta \in (1/2, (k-1)/k]$, then, by (113), $a \in [-(k-2)/k, 0)$. First of all, let us show that for $z \in [0, 1)$, $f(z) \neq 0$. Indeed, $f(0) = a < 0$, $f(1) = 2(a-1) < 0$, and evidently

$$f'(z) = akz^{k-1} - (k-1)z^{k-2} - 1 \leq -1;$$

we are done.

Finally, let $z \in (-1, 0)$. Then (114) is equivalent to

$$\lambda(z) := \frac{z^{k-1} + z}{z^k + 1} = a. \tag{119}$$

Since

$$\lambda(0) = 0,\ \lambda(-1) = \lim_{z \to -1+0} \lambda(z) = -(k-2)/k$$

it is sufficient to show that $\lambda'(z) > 0$. Indeed, then $\lambda(z)$ is monotonous and varies in the same limits as a. This means that (119) has a unique solution for every a. We will prove that

$$\begin{aligned} \mu(z) &:= -\lambda'(z)(z^k + 1)^2 \\ &= z^{2k-2} + (k-1)z^k - (k-1)z^{k-2} - 1 < 0 \\ &\qquad\qquad (z \in (-1, 0)). \end{aligned}$$

Indeed, $\mu(0) = -1$, $\mu(-1) = 0$, and it is sufficient to demonstrate that $\mu'(z) < 0$. We have

$$\frac{\mu'(z)}{(k-1)z^{k-3}} = \nu(z) := 2z^k + kz^2 - (k-2).$$

We have $\nu(0) = -(k-2)$, $\nu(-1) = 0$, and it is sufficient to show that for $z \in (-1, 0)$, $\nu'(z) < 0$. We have

$$\frac{\nu'(z)}{2k} = z^{k-1} + z < -z + z = 0.$$

Furthermore, the root of (119) $z_a \leq a$. Indeed, if $z > a$, then, since $\lambda'(z) > 0$, we have

$$\frac{z^{k-1} + z}{z^k + 1} > \frac{a^{k-1} + a}{a^k + 1} > a. \tag{120}$$

Thus, the root $z_a \in [a, 0)$ corresponds to the unique root t_θ

$$t_\theta \in [\theta/(1-\theta), +\infty). \tag{121}$$

□

Remark 1: In the case of odd k the value $\theta = (k-1)/k$ (or $a = -(k-2)/k$) corresponds to the limiting case $z = -1$, which in turn corresponds to the limiting case $t = +\infty$. Indeed, for odd k

$$\lim_{t \to +\infty} \frac{(1+t)^{k-1} + (1-t)^{k-1}}{(1+t)^k + (1-t)^k} = \lim_{t \to +\infty} \frac{2t^{k-1}}{2\binom{k}{k-1}t^{k-1}} = \frac{1}{k}.$$

Analogously, for k even, $\theta \to 1 - 0$ $(a = -1 + 0)$ we have $z \to -1 + 0$, and correspondingly, $t = +\infty$.

Remark 2: From (20), it follows that for $k \to \infty$

$$\frac{1}{1+t} = 1 - \theta, \qquad t = \frac{\theta}{1-\theta}.$$

Then by (21)

$$\lim_{k \to \infty} \lim_{n \to \infty} \frac{1}{n} P_{n,\theta}^{k,\alpha} = -\alpha \ln 2.$$

Remark 3: Checking (as in the example of Section IV-A2) that the condition (38) holds for $\theta = 1/2$, $t = 1$. Indeed, from (67), (68), (101), (102) we have

$$\begin{aligned} \sum_{i=1}^{\lfloor k/2 \rfloor} 2im_{2i} &= \sum_{i=1}^{\lfloor k/2 \rfloor} 2i\, \frac{\binom{k}{2i}n}{2^{k-1}} \\ &= \frac{nk}{2^{k-1}} \sum_{i=1}^{\lfloor k/2 \rfloor} \binom{k-1}{2i-1} \\ &= \frac{nk}{2^{k-1}}\, 2^{k-2} = \frac{nk}{2}. \end{aligned}$$

Therefore, we have a multinomial distribution with

$$p_{2i} = \frac{\binom{k}{2i}}{2^{k-1}}, \qquad i = 1, 2, \ldots, \lfloor k/2 \rfloor.$$

It is known, see e.g., [2], that $m_{2i} = np_{2i}$ provides maximum probability in multinomial distribution. Moreover, these values provide maximum under an extra condition

$$\sum_{i=1}^{\lfloor k/2 \rfloor} 2im_{2i} = nk\theta.$$

Thus,

$$\max_{\theta \in (0,1)} M_{n,\theta}^{k} = M_{n,1/2}^{k} \overset{\ln}{\sim} 2^{(k-1)n}. \tag{122}$$

Analogously, it is possible to show that the function $M_{n,\theta}^{k}$ is monotonously increasing in the interval $\theta \in (0, 1/2]$ and is monotonously nonincreasing in the interval $\theta \in [1/2, 1]$.

Remark 4: For $\alpha = 1/k$ when $\ell = 1$, n is a multiple of k, $m = n/k$. This case is interesting in two ways. First, for $\alpha = 1/k$, (33) becomes an exact equality. Second, for $P_{n,\theta}^{k,1/k}$ there exists an alternative representation. We state these facts as a theorem.

Theorem 6:

a) For even k

$$P_{n,\theta}^{k,1/k} = \frac{1}{\binom{n}{\theta n}} \sum \binom{n/k}{m_0, m_2, \ldots, m_k} \cdot \binom{k}{2}^{m_2} \binom{k}{4}^{m_4} \cdots \binom{k}{k-2}^{m_{k-2}} \tag{123}$$

where the summation is over all nonnegative m_0, $m_2, \ldots, m_k$ satisfying (24) for $\alpha = 1/k$.

For odd k

$$P_{n,\theta}^{k,1/k} = \frac{1}{\binom{n}{\theta n}} \sum \binom{n/k}{m_0, m_2, \ldots, m_{k-1}} \cdot \binom{k}{2}^{m_2} \binom{k}{4}^{m_4} \cdots \binom{k}{k-1}^{m_{k-1}} \tag{124}$$

where the summation is over all nonnegative m_0, $m_2, \ldots, m_{k-1}$ satisfying (77) for $\alpha = 1/k$.

b) For any k

$$P_{n,\theta}^{k,1/k} = \frac{1}{\binom{n}{\theta n}} \sum \binom{k}{i_1} \binom{k}{i_2} \cdots \binom{k}{i_{n/k}} \tag{125}$$

where the summation is over even $i_1, i_2, \ldots, i_{n/k} \in [0, k]$ under condition

$$\sum_{j=1}^{n/k} i_j = \theta n. \tag{126}$$

Proof: The expressions (123) and (124) are proved in a similar way, thus, we will prove only (123). Assume k is even. First of all, notice that

$$\left|\Lambda_n^{k,1/k}\right| = \binom{n}{k}\binom{n-k}{k}\binom{n-2k}{k} \cdots \binom{k}{k} = \frac{n!}{(k!)^{n/k}}. \tag{127}$$

Let, as in Section IV-A1, m_i stand for the number of rows in the matrix A^{left} with row sums equal i, where i is an even nonnegative number not exceeding k. Correspondingly, A^{right} has m_i rows with sums $k-i$. Here it is possible to compute $|L_{n,\theta}^{k,1/k}|$, $|R_{n,\theta}^{k,1/k}|$. We have

$$\begin{aligned}
&\left|L_{n,\theta}^{k,1/k}\right| \\
&= \binom{\theta n}{2}\binom{\theta n - 2}{2}\binom{\theta n - 4}{2} \cdots \binom{\theta n - 2(m_2-1)}{2} \\
&\quad \cdot \binom{\theta n - 2m_2}{4}\binom{\theta n - 2m_2 - 4}{4} \cdots \binom{\theta n - 2m_2 - 4(m_4-1)}{4} \\
&\quad \cdot \binom{\theta n - 2m_2 - \cdots - (k-2)m_{k-2}}{k} \\
&\quad \cdot \binom{\theta n - 2m_2 - \cdots - (k-2)m_{k-2} - k}{k} \\
&\quad \cdot \cdots \cdot \binom{\theta n - 2m_2 - \cdots - (k-2)m_{k-2} - k(m_k-1)}{k} \\
&= \frac{(\theta n)!}{(2!)^{m_2}(4!)^{m_4} \cdots (k!)^{m_k}(\theta n - 2m_2 - 4m_4 - \cdots - km_k)!}.
\end{aligned}$$

By (24) for $\alpha = 1/k$

$$\theta n - 2m_2 - 4m_4 - \cdots - km_k = 0.$$

Therefore,

$$\left|L_{n,\theta}^{k,1/k}\right| = \frac{(\theta n)!}{(2!)^{m_2}(4!)^{m_4} \cdots (k!)^{m_k}}. \tag{128}$$

Analogously, see the equation at the bottom of the page. However, by (30) for $\alpha = 1/k$

$$(1-\theta)n - km_0 - (k-2)m_2 - \cdots - 2m_{k-2} = 0.$$

$$\begin{aligned}
\left|R_{n,\theta}^{k,1/k}\right| &= \binom{(1-\theta)n}{k}\binom{(1-\theta)n - k}{k} \cdots \binom{(1-\theta)n - k(m_0-1)}{k} \\
&\quad \cdot \binom{(1-\theta)n - km_0}{k-2}\binom{(1-\theta)n - km_0 - (k-2)}{k-2} \cdot \cdots \cdot \binom{(1-\theta)n - km_0 - (k-2)(m_2-1)}{k-2} \\
&\quad \cdot \cdots \cdot \binom{(1-\theta)n - km_0 - (k-2)m_2 - \cdots - 4m_{k-4}}{2} \\
&\quad \cdot \binom{(1-\theta)n - km_0 - \cdots - 4m_{k-4} - 2}{2} \cdot \cdots \cdot \binom{(1-\theta)n - km_0 - \cdots - 4m_{k-4} - 2(m_{k-2}-1)}{2} \\
&= \frac{((1-\theta n)!}{(k!)^{m_0}((k-2)!)^{m_2} \cdots (2!)^{m_{k-2}}((1-\theta)n - km_0 - (k-2)m_2 - \cdots - 2m_{k-2})!}.
\end{aligned}$$

Therefore,

$$\left|R_{n,\theta}^{k,1/k}\right| = \frac{((1-\theta n)!}{(k!)^{m_0}((k-2)!)^{m_2}\cdots(2!)^{m_{k-2}}}. \tag{129}$$

Now

$$P_{n,\theta}^{k,1/k} = \sum \binom{n/k}{m_0,\,\ldots,\,m_k} \frac{\left|L_{n,\theta}^{k,1/k}\right| \left|R_{n,\theta}^{k,1/k}\right|}{\left|\Lambda_n^{k,1/k}\right|} \tag{130}$$

where the summation is over all $m_0, m_2, \ldots, m_k$ satisfying (24) for $\alpha = 1/k$. From (127)–(130), we find (131), shown at the bottom of the page, and (123) follows from (131) by the first restriction in (24) when $\alpha = 1/k$.

We proceed to prove claim b) of the theorem. Although the equivalence of (123) and (124) to (125) is straightforward, in what follows we will provide an independent direct proof of (125). Let there be j_i ones, $i = 1, 2, \ldots, n/k$, in the first θn entries and the ith row of the considered $m \times n$ matrix. Taking into account that in every column there is exactly a unique one, there are

$$\binom{\theta n}{j_1}\binom{\theta n - j_1}{j_2}\cdots\binom{\theta n - j_1 - j_2 - \cdots - j_{\frac{n}{k}-1}}{j_{n/k}}$$

ways to do it. Here $j_1, j_2, \ldots, j_{n/k}$ are even nonnegative numbers not exceeding k and satisfying

$$\sum_{i=1}^{n/k} j_i = \theta n.$$

Simultaneously, since all the row sums equal k, in the last $(1-\theta)n$ entries of the ith row there are $k - j_i$ ones, $i = 1, 2, \ldots, n/k$. Such choice can be done in

$$\binom{(1-\theta)n}{k-j_1}\binom{(1-\theta)n-(k-j_1)}{k-j_2} \cdot \cdots \cdot \binom{(1-\theta)n-(k-j_1)-(k-j_2)-\cdots-(k-j_{\frac{n}{k}-1})}{k-j_{n/k}}$$

ways.

By (127), see the second equation at the bottom of the page, and since

$$\begin{aligned} \theta n - j_1 - j_2 - \cdots - j_{n/k} &= 0 \\ (1-\theta)n - (k-j_1) - (k-j_2) - \cdots - (k-j_{n/k}) &= 0 \end{aligned}$$

finally we have

$$\begin{aligned} P_{n,\theta}^{k,1/k} &= \frac{1}{\binom{n}{\theta n}} \sum_{\substack{j_1+j_2+\cdots+j_{n/k}=\theta n \\ j_i \equiv 0 \bmod 2}} \\ &\quad \cdot \frac{k!}{j_1!(k-j_1)!}\,\frac{k!}{j_2!(k-j_2)!}\cdots\frac{k!}{j_{n/k}!(k-j_{n/k})!} \\ &= \frac{1}{\binom{n}{\theta n}} \sum_{\substack{j_1+j_2+\cdots+j_{n/k}=\theta n \\ j_i \equiv 0 \bmod 2}} \binom{k}{j_1}\binom{k}{j_2}\cdots\binom{k}{j_{n/k}} \end{aligned}$$

and thus we have proved (125). □

Lemma 3 yields the following corollary.

Corollary 2:

$$P_{n,\theta}^{k,\alpha} \overset{\ln}{\sim} P_{nk\alpha,\theta}^{k,1/k}. \tag{132}$$

□

Moreover, by (125) and (132) we have

$$P_{n,\theta}^{k,\alpha} \overset{\ln}{\sim} \frac{1}{\binom{nk\alpha}{n\theta k\alpha}} \sum \binom{k}{i_1}\binom{k}{i_2}\cdots\binom{k}{i_{n/k}} \tag{133}$$

where the summation is over

$$i_1, i_2, \ldots, i_{n\alpha} \in \{0, 2, \ldots, 2[k/2]\}$$

under condition that

$$\sum_{j=1}^{n\alpha} i_j = \theta n k\alpha. \tag{134}$$

In contrast with the sum appearing in Lemma 3, having order $O(1)$, the order of the sum (133) is $O(n)$, which complicates drastically its study. In particular, it is not logarithmically equivalent to its maximal summand (in which, when θk is even, $i_1 = i_2 = \cdots = i_{n\alpha} = \theta k$). Indeed, for instance, when $\alpha = 1$, $\theta = 1/2$, $k \equiv 0 \bmod 4$, the maximal summand is $\binom{k}{k/2}^n$ and, by (122)

$$\binom{k}{k/2}^n < M_{n,1/2}^k \overset{\ln}{\sim} 2^{(k-1)n}$$

since

$$\binom{k}{k/2} < 2^{k-1} = \binom{k}{0} + \binom{k}{2} + \cdots + \binom{k}{k/2} + \cdots + \binom{k}{k}.$$

$$\begin{aligned} P_{n,\theta}^{k,1/k} &= \sum \binom{n/k}{m_0,\,\ldots,\,m_k} \cdot \frac{(\theta n)!((1-\theta)n)!(k!)^{n/k}}{n!(k!)^{m_0}((k-2)!2!)^{m_2}((k-4)!4!)^{m_4}\cdots(2!(k-2)!)^{m_{k-2}}(k!)^{m_k}} \\ &= \frac{1}{\binom{n}{\theta n}} \sum \binom{n/k}{m_0,\,\ldots,\,m_k} \frac{(k!)^{n/k}}{(k!)^{m_0+m_2+\cdots+m_k}} \binom{k}{2}^{m_2}\binom{k}{4}^{m_4}\cdots\binom{k}{k-2}^{m_{k-2}}. \end{aligned} \tag{131}$$

$$\begin{aligned} P_{n,\theta}^{k,1/k} = &\sum_{\substack{j_1+j_2+\cdots+j_{n/k}=\theta n \\ j_i \equiv 0 \bmod 2}} \frac{(k!)^{n/k}}{n!}\,\frac{(\theta n)!}{j_1!j_2!\cdots j_{n/k}!(\theta n - j_1 - j_2 - \cdots - j_{n/k})!} \\ &\cdot \frac{((1-\theta)n)!}{(k-j_1)!(k-j_2)!\cdots(k-j_{n/k})!((1-\theta)n-(k-j_1)-(k-j_2)-\cdots-(k-j_{n/k}))!}. \end{aligned}$$

However, by Lemmas 3 and 4, (133) with $\alpha = 1$, as well as from (111) we have the following.

Corollary 3:

$$\ln \sum_{\substack{i_1+\cdots+i_n=\theta nk \\ i_j\in\{0,2,\ldots,2[k/2]\}}} \binom{k}{i_1}\binom{k}{i_2}\cdots\binom{k}{i_n} \sim n \ln \frac{(1+t)^k+(1-t)^k}{2t^{\theta k}} \tag{135}$$

where t is the root of (20) in Theorem 4. □

C. Study of $P_{n,\theta}^{k,\alpha}$ as a Function of θ

Let us study

$$\mathcal{P}(\theta) := \lim_{n\to\infty} \frac{1}{n} \ln P_{n,\theta}^{k,\alpha}$$

as a function in θ. By Theorem 5, the function $t(\theta)$ is invertible.

Assume that k is even. We have

$$\begin{aligned}\Gamma_{k,t}(\theta) &:= \frac{d}{d\theta}\left[\ln\left((1+t)^k+(1-t)^k\right) - \theta k \ln t - kH(\theta)\right] \\ &= k\left(\frac{1}{\theta'_t}\left(\frac{(1+t)^{k-1}-(1-t)^{k-1}}{(1+t)^k+(1-t)^k} - \frac{\theta}{t}\right)\right. \\ &\qquad \left. + \ln\frac{\theta}{t(1-\theta)}\right).\end{aligned} \tag{136}$$

By (63) we have

$$\frac{(1+t)^{k-1}-(1-t)^{k-1}}{(1+t)^k+(1-t)^k} = \frac{\theta}{t} \tag{137}$$

and

$$\Gamma_{k,t}(\theta) = k \ln \frac{\theta}{t(1-\theta)}. \tag{138}$$

Thus, the function $\mathcal{P}(\theta)$ has the unique stationary point satisfying

$$\frac{\theta}{t_\theta(1-\theta)} = 1.$$

However, by (62), it is equivalent, when k is even, to

$$\frac{\theta/(1-\theta)}{t_\theta} = \frac{(1+t_\theta)^{k-1}-(1-t_\theta)^{k-1}}{(1+t_\theta)^{k-1}+(1-t_\theta)^{k-1}}.$$

Therefore, in the stationary point $t_\theta = 1$ and $\theta = 1/2$. From Theorem 5, it follows that if $\theta < 1/2$ then

$$\frac{\theta}{t_\theta(1-\theta)} < 1$$

and by (138), $\Gamma_{k,t}(\theta) < 0$. Analogously, for $\theta > 1/2$

$$\frac{\theta}{t_\theta(1-\theta)} > 1$$

and $\Gamma_{k,t}(\theta) > 0$. This means that for k even

$$\min_{\theta\in(0,1]} \mathcal{P}(\theta) = \mathcal{P}\left(\tfrac{1}{2}\right) = -\alpha \ln 2. \tag{139}$$

Let now k be odd. Then from (98) it again follows that

$$\frac{(1+t)^{k-1}-(1-t)^{k-1}}{(1+t)^k+(1-t)^k} = \frac{\theta}{t} \tag{140}$$

and

$$\Gamma_{k,t}(\theta) = k \ln \frac{\theta}{t(1-\theta)}$$

with the only stationary point $t_\theta = 1$, $\theta = 1/2$. However, for $\theta < 1/2$ as well as for $\theta > 1/2$ by Theorem 5 we have

$$\frac{\theta}{t_\theta(1-\theta)} < 1, \qquad \Gamma_{k,t}(\theta) < 0.$$

In this case, there is no extremum and $\mathcal{P}(\theta)$ is everywhere monotonously decreasing. Furthermore

$$\min_{\theta\in(0,(k-1)/k]} \mathcal{P}(\theta) = \mathcal{P}\left(\frac{k-1}{k}\right).$$

In what follows we will prove that

$$\begin{aligned}\mathcal{P}\left(\frac{k-1}{k}\right) &= \alpha k\left(\frac{1}{k}\ln\frac{1}{k} + \left(1-\frac{1}{k}\right)\ln\left(1-\frac{1}{k}\right)\right) - \alpha \ln 2 \\ &= \alpha((k-1)\ln(k-1) - k\ln k) - \alpha \ln 2.\end{aligned}$$

Then

$$\lim_{k\to\infty} \min_{\theta\in(0,(k-1)/k]} \mathcal{P}(\theta) = -\infty.$$

We summarize the results in the following theorem.

Theorem 7: If k is even then

$$\lim_{n\to\infty} \frac{1}{n} \ln P_{n,\theta}^{k,\alpha}$$

has the only extremum (minimum) in the interval $(0, 1)$ at $\theta = 1/2$, when it is equal to $-\alpha \ln 2$.

If k is odd then this limit is monotonously decreasing and attains the minimum equal $-\infty$. □

Remark 5: Actually the last theorem means that in the case of even k the distance distribution is always greater than the distance distribution of a random code (normalized binomial distribution) but in the point $\theta = 1/2$, where both distributions coincide. For an odd k, the distance distribution is greater than the binomial one for $\theta < 1/2$, and is less than the binomial one for $\theta > 1/2$. In $\theta = 1/2$ they coincide. □

Let us further study the concavity of $\mathcal{P}(\theta)$. Since

$$-\frac{1-\theta}{\theta'_t} = \frac{1}{(\ln(1-\theta))'_t}$$

then from (138) it follows that

$$\frac{\theta(1-\theta)}{k} \frac{d}{d\theta} \Gamma_{k,t}(\theta) = 1 + \frac{\theta/t}{(\ln(1-\theta))'_t}. \tag{141}$$

Taking into account (137) and (20), we find that

$$\begin{aligned}&\frac{\theta/t}{(\ln(1-\theta))'_t} \\ &\quad = -\frac{(1+t)^{2k-2}-(1-t)^{2k-2}}{(1+t)^{2k-2}-(1-t)^{2k-2}+4(k-1)(1-t^2)^{k-2}t}.\end{aligned} \tag{142}$$

Let k be even. Then $(1-t^2)^{k-2} > 0$ and (142) yields

$$\frac{\theta/t}{(\ln(1-\theta))'_t} > -1.$$

Then by (141) we have

$$\frac{d}{d\theta}\Gamma_{k,\,t}(\theta) > 0$$

and the function is ∪-concave in all the interval $\theta \in (0,\,1)$. Moreover, for $\theta \to 1-0$, $t \to \infty$, and

$$\begin{aligned}\lim_{t\to+\infty} \mathcal{P}(\theta) &= \alpha \ln \lim_{t\to+\infty} t^{k(1-\theta)} = k\alpha \lim_{t\to+\infty} \frac{1-\theta}{\frac{1}{\ln t}}\\ &= k\alpha \lim_{t\to+\infty} \frac{-1}{\frac{-1}{t\ln^2 t\, t'_\theta}}\\ &= k\alpha \lim_{t\to+\infty} (t\ln^2 t)\theta'_t. \qquad (143)\end{aligned}$$

By (20)

$$\theta'_t = \frac{(1+t)^{2k-2} - (1-t)^{2k-2} + 4(k-1)t(1-t^2)^{k-2}}{((1+t)^k + (1-t)^k)^2}. \qquad (144)$$

Therefore (when $t \to \infty$)

$$\theta'_t = O\left(\frac{t^{2k-3}}{t^{2k}}\right) = O\left(\frac{1}{t^3}\right). \qquad (145)$$

Now, from (143) we have that

$$\lim_{t\to+\infty} \mathcal{P}(\theta(t)) = 0.$$

Next, when $\theta \to +0$, $t \to +0$, from (144) we find

$$\lim_{t\to+0} \mathcal{P}(\theta(t)) = -k\alpha \lim_{t\to+0} \theta \ln t = 0.$$

Now, let k be odd. Then from (142) it follows for $t < 1$

$$\frac{\theta/t}{(\ln(1-\theta))'_t} > -1$$

and from (141)

$$\frac{d}{d\theta}\Gamma_{k,\,t}(\theta) > 0$$

and when $t > 1$

$$\begin{aligned}\frac{\theta/t}{(\ln(1-\theta))'_t} &< -1\\ \frac{d}{d\theta}\Gamma_{k,\,t}(\theta) &< 0.\end{aligned}$$

Thus, at $t = 1$, corresponding to $\theta = 1/2$, we have the point of change of concavity. Moreover, to the left of $\theta = 1/2$ the function $\mathcal{P}(\theta)$ is ∪-concave, and to the right of $\theta = 1/2$ the function $\mathcal{P}(\theta)$ is ∩-concave.

When $\theta \to \frac{k-1}{k} - 0$, $t \to +\infty$ and

$$\begin{aligned}\lim_{t\to+\infty} \mathcal{P}(\theta(t)) &= \alpha k \ln\left(\left(\frac{1}{k}\right)^{\frac{1}{k}}\left(1-\frac{1}{k}\right)^{1-\frac{1}{k}}\right) - \alpha\ln 2\\ &\quad + \lim_{t\to+\infty} \alpha(k(1-\theta)) - 1)\ln t\\ &= \alpha k \lim_{t\to+\infty} \theta'_t \ln^2 t\\ &\quad + \alpha((k-1)\ln(k-1) - k\ln k) - \alpha\ln 2.\end{aligned}$$

However, by (144)

$$\theta'_t = O\left(\frac{t^{2k-4}}{t^{2k-2}}\right) = O\left(\frac{1}{t^2}\right)$$

and

$$\lim_{t\to+\infty} \mathcal{P}(\theta(t)) = \alpha((k-1)\ln(k-1) - k\ln k) - \alpha\ln 2.$$

Therefore, in this case, $\mathcal{P}(\theta)$ is monotonously decreasing from 0 to $\alpha((k-1)\ln(k-1) - k\ln k) - \alpha\ln 2$ changing at $\theta = 1/2$ concavity from down to up. Notice also that

$$\lim_{k\to+\infty}\lim_{t\to+\infty} \mathcal{P}(\theta(t)) = -\infty$$

and this accomplishes the proof of Theorem 7 for odd k.

V. Average Distance Distribution in Ensemble B

This ensemble was suggested by Gallager in [5] and is defined as follows. Let A be a k-fold concatenation of the $k \times k$ identity matrix. Then

$$H = \begin{pmatrix} A \\ P_1(A) \\ \cdots \\ P_{\ell-1}(A)\end{pmatrix}$$

where $P_i(A)$ is a matrix obtained by a random column permutation of A. Clearly, every such matrix H has k ones in every row and ℓ ones in every column, i.e., Ensemble B is a subensemble of Ensemble A.

Comparison of the final results of the previous section with [5, Theorem 2.3] shows that they are identical (up to a somewhat more precise analysis in the case of odd k's in the previous section). This is a very surprising (at least for the authors) fact, since the proof techniques are very different. Moreover, Ensembles A and B are different in the sense that Ensemble A contains matrices which cannot be derived from a matrix from Ensemble B using permutations of rows and columns. Indeed, consider, e.g., matrices of size 4×6 with column sums 2 and row sums 3. By definition, for every row in a matrix from Ensemble B there is another row having support nonintersecting with the support of the initial row. For example, a typical matrix from Ensemble B is

$$\left(\begin{array}{cccccc} 1 & 1 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 1 & 1\\ \hline 1 & 0 & 1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1 & 0 & 1\end{array}\right).$$

However, in the following matrix belonging to Ensemble A

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0\\ 1 & 0 & 0 & 1 & 1 & 0\\ 0 & 0 & 1 & 0 & 1 & 1\\ 0 & 1 & 0 & 1 & 0 & 1\end{pmatrix}$$

the support of each row intersects the supports of all other rows, and this property is clearly invariant under rows and column permutations.

VI. Average Distance Distribution in Ensemble C

Ensemble C is defined by matrices having ℓ ones in every column. Let $\Delta_n^{\ell,\,\alpha}$ stand for the ensemble of such $m \times n$ matrices with $\alpha := m/n$. Our goal is to find an expression for the distance distribution component B_w where $w = \theta n$. Let $\Delta_{n,\,\theta}^{\ell,\,\alpha}$

represent the ensemble of matrices from $\Delta_n^{\ell,\alpha}$ having the property that, for all rows, the sum of the first w entries in the row is even (and thus, the vector $1^w 0^{n-w}$ is a codeword). Finally, let

$$P_{n,\theta}^{\ell,\alpha} := \frac{\left|\Delta_{n,\theta}^{\ell,\alpha}\right|}{\left|\Delta_n^{\ell,\alpha}\right|}. \qquad (146)$$

Evidently

$$B_{\theta n} = \binom{n}{\theta n} P_{n,\theta}^{\ell,\alpha}. \qquad (147)$$

For estimation of $|\Delta_{n,\theta}^{\ell,\alpha}|$, methods standard for the random walks on hypercube can be applied, see, e.g., [3], [7]. However, we will demonstrate how an elementary method of generating functions gives the sought result.

We will need the following definition. The binary Krawtchouk polynomial is

$$K_\ell^{(m)}(x) = \sum_{i=0}^{\ell} (-1)^i \binom{x}{i}\binom{m-x}{\ell-i}. \qquad (148)$$

It may be defined also by the following generating function:

$$\sum_{\ell=0}^{\infty} K_\ell^{(m)}(x) z^\ell = (1-z)^x (1+z)^{m-x}. \qquad (149)$$

For a survey of properties of Krawtchouk polynomials see [8], and also [1, Sec. 2.3], [10, Sec. 5.7].

Theorem 8:

$$P_{n,\theta}^{\ell,\alpha} = \frac{1}{2^m}\left(\sum_{j=0}^{m}\binom{m}{j}\left(K_\ell^{(m)}(j)\right)^{\theta n}\right)\binom{m}{\ell}^{-\theta n}. \qquad (150)$$

Proof: Let $w = \theta n$. Assume that $(1+z_i)$ is the generating function for appearance of one in the ith coordinate of a row-vector of size w. Then

$$g(x) = \frac{\prod_{i=1}^{w}(1+z_i) + \prod_{i=1}^{w}(1-z_i)}{2}$$

is the generating function for row-vectors of size w and even weight (for example, $z_2 z_3 z_8 z_9$ corresponds to the binary vector having one in the second, third, eighth, and ninth coordinates). Then $g^m(x)$ is the generating function for $m \times w$ matrices with even row sums. The number of such matrices with column sums equal ℓ is represented by the coefficient at $z_1^\ell z_2^\ell \cdots z_w^\ell$. However, by (149)

$$\begin{aligned} g^m(x) &= \frac{1}{2^m}\sum_{j=0}^{m}\binom{m}{j}\left(\prod_{i=1}^{w}(1+z_i)\right)^j\left(\prod_{i=1}^{w}(1-z_i)\right)^{m-j} \\ &= \frac{1}{2^m}\sum_{j=0}^{m}\binom{m}{j}\prod_{i=1}^{w}(1+z_i)^j(1-z_i)^{m-j} \\ &= \frac{1}{2^m}\sum_{j=0}^{m}\binom{m}{j}\prod_{i=1}^{w}\left(\sum_{\ell=0}^{m} K_\ell^m(j) z_i^\ell\right) \\ &= \frac{1}{2^m}\sum_{j=0}^{m}\binom{m}{j} \\ &\quad\cdot\left(\cdots + \left(K_\ell^{(m)}(j)\right)^w \left(z_1^\ell z_2^\ell \cdots z_w^\ell\right) + \cdots\right). \end{aligned}$$

Therefore,

$$\left|\Delta_{n,\theta}^{\ell,\alpha}\right| = \frac{1}{2^m}\left(\sum_{j=0}^{m}\binom{m}{j}\left(K_\ell^{(m)}(j)\right)^{\theta n}\right)\binom{m}{\ell}^{n(1-\theta)}.$$

Since

$$\left|\Delta_n^{\ell,\alpha}\right| = \binom{m}{\ell}^n$$

we arrive at the claimed conclusion. □

Remark 6: It is known that for an arbitrary polynomial $f(x)$ of degree at most m one can find the unique expansion in the basis of Krawtchouk polynomials

$$f(x) = \sum_{i=0}^{m} \phi_i(f) K_i^{(m)}(x).$$

In particular

$$\phi_0(f) = \frac{1}{2^m}\sum_{j=0}^{m}\binom{m}{j} f(j).$$

Therefore,

$$P_{n,\theta}^{\ell,\alpha} = \phi_0\left(\left(K_\ell^{(m)}\right)^{\theta n}\right)\binom{m}{l}^{-\theta n}. \qquad (151)$$

Now let us study the asymptotic behavior of the expression in Theorem 8 under assumption that n tends to infinity, $m = \alpha n$ for $\alpha \in (0, 1)$, and ℓ is a constant independent of n.

Under these assumptions

$$\begin{aligned} K_\ell^{(m)}(x) &= \frac{(m-2x)^\ell}{\ell!} + O(m^{\ell-1}) \\ \binom{m}{\ell} &= \frac{m^\ell}{\ell!} + O(m^{\ell-1}). \end{aligned}$$

Thus,

$$\begin{aligned} &\lim_{n\to\infty}\frac{1}{n}\ln P_{n,\theta}^{\ell,\alpha} \\ &\quad = -\alpha\ln 2 + \max_{\eta\in[0,1]}\{\alpha H(\eta) + \theta\ell\ln(1-2\eta)\}. \qquad (152) \end{aligned}$$

Differentiating in η we have that the maximum is achieved at η satisfying

$$(1-2\eta)\ln\frac{1-\eta}{\eta} = 2\,\frac{\theta\ell}{\alpha}. \qquad (153)$$

On the right-hand side of the last expression we have a positive constant, while on the left-hand side there is a function monotonously decreasing from ∞ at $\eta = 0$ to 0 at $\eta = 1/2$. Thus, (153) has a unique solution in the interval $(0, 1/2)$, and we have proved the corresponding of Theorem 1.

VII. Average Distance Distribution in Ensemble D

Recall that Ensemble D is defined by the following procedure. We start from the all-zero column-vector of size m. We repeat the following operation ℓ times (ℓ is a constant independent of n): flip one of the m coordinates with uniform probability. As a result, we have a column-vector of weight at most ℓ with the parity of the weight equal to the one of ℓ. Generating such vectors independently n times yields an $m \times n$ matrix H.

Clearly, the described procedure is equivalent to the following: generate $n\ell$ column-vectors of size m and of weight 1, Sum up (coordinate-wise modulo 2) the ℓ consecutive vectors with numbers $1, 2, \dots, \ell$; $\ell+1, \ell+2, \dots, 2\ell$; $\dots$, thus getting n column-vectors constituting the parity-check matrix H.

Thus, the problem reduces to estimation of the proportion of $(0, 1)$-matrices of size $m \times n\ell$ with column sums equal 1 and having the sum (coordinate-wise modulo 2) of the first $\theta n\ell$ columns equal the all-zero vector. This is a particular case of the problem for Ensemble C. By (150) and $K_1^{(m)}(x) = m-2x$, we have here

$$P_{n\ell,\theta}^{\ell,\alpha} = \frac{1}{2^m}\sum_{j=0}^{m}\binom{m}{j}\left(1-2\frac{j}{m}\right)^{\theta n\ell}. \tag{154}$$

The corresponding expression was earlier derived in [9] using different arguments.

VIII. Average Distance Distribution in Ensemble E

Recall that Ensemble E is defined by binary $m \times n$ matrices with row sums equal to k, where k is a constant independent of n. Consider the probability that the first $w = \theta n$ columns of such a matrix sum up (coordinate-wise modulo 2) to the all-zero vector. The probability that the number of ones is even in the first w positions in a vector of length n and weight k is

$$P = \frac{1}{\binom{n}{k}}\sum_{j=0}^{\lfloor k/2\rfloor}\binom{w}{2j}\binom{n-w}{k-2j}. \tag{155}$$

For n tending to ∞ it reduces to

$$P = \sum_{j=0}^{\lfloor k/2\rfloor}\frac{\theta^{2j}(1-\theta)^{k-2j}k!}{(2j)!(k-2j)!} + o(1) = \frac{1+(1-2\theta)^k}{2} + o(1). \tag{156}$$

To have the desired property we need this event to hold for m rows. Since these events are independent then the sought probability is

$$P_{n,\theta}^{k,\alpha} = P^m \tag{157}$$

and the corresponding claim of Theorem 1 follows.

IX. Average Distance Distribution in Ensemble F

Recall that Ensemble F is defined by the following procedure. We start from the all-zero vector of size n and flip one entry with uniform probability. Repeating this k times we obtain a vector of weight at most k. Now, generating m such vectors, we compose from them an $m \times n$ matrix.

Consider the probability that the generated vector has an even number of ones in the first $w = \theta n$ coordinates. Since the probability that flipping happens at the first w positions is θ, the sought probability is

$$P = \sum_{j=0}^{\lfloor k/2\rfloor}\binom{k}{2j}\theta^{2j}(1-\theta)^{k-2j} = \frac{1+(1-2\theta)^k}{2}. \tag{158}$$

The probability that the described happens in m independent events is P^m, and we arrive at the corresponding claim of Theorem 1.

X. Average Distance Distribution in Ensemble G

Recall that Ensemble G is generated by $m\times n$ binary matrices where each entry is 1 with probability $\varepsilon = k/n$. The probability that there is an even number of ones in the first $w = \theta n$ positions of a row is

$$P = \frac{1+(2\varepsilon-1)^w}{2}. \tag{159}$$

Furthermore, if w is even

$$\lim_{n\to\infty} P = \frac{1+e^{-2k\theta}}{2}. \tag{160}$$

The probability of the sought event is P^m, and we arrive at the corresponding conclusion in Theorem 1.

XI. Average Distance Distribution in Ensemble H

Recall that Ensemble H is defined by the following model. Let G be an $m\times n$ regular bipartite graph with left degree k and right degree ℓ, perhaps with parallel edges. To generate such graph, one just enumerates the edges on the left part and on the right part of the graph, and connects them randomly (using a permutation). It is easy to see that this model corresponds to the following procedure: generate a random $m \times n\ell$ binary matrix with column sums equal 1 and row sums equal k; sum up (regular summation) the consecutive ℓ columns with numbers $1, 2, \dots, \ell$; $\ell+1, \ell+2, \dots, 2\ell, \dots$, to get an $m \times n$ matrix H (with entries being $0, 1, \dots, \ell$); construct a bipartite graph from H by putting e parallel edges between the ith node on the left and the jth vertex on the right if and only if $h_{i,j} = e$. Thus, the problem reduces to estimation of probability that the first $\theta\ell n$ columns of a binary $m \times \ell n$ matrix with row sums k and column sums 1, sum up (coordinate-wise modulo 2) to the all-zero column. This is a particular case of the problem considered in regards to Ensemble A, and a direct check shows that the expressions are equivalent.

XII. The Distance Distributions for Constant Distances

Theorem 1 provides a classification of Ensembles A–H according to the behavior of considered probability p_θ^α for $w = n\theta$ $(0 < \theta < 1)$. The equivalence classes are

- A, B, H
- C, D
- E, F
- G

In this section, we restrict ourselves to the study of this probability for the first ensembles in each group, i.e., A, C, E, and G, when w is a constant independent of n.

A. Ensemble A

Assume

$$\alpha k w \equiv 0 \bmod 2. \tag{161}$$

Under this condition, the following analysis does not depend on the parity of k, thus we assume, for instance, that k is even. The expression (33) reduces to

$$P_{n,w}^{k,\alpha} \overset{\ln}{\sim} \frac{1}{\binom{nk\alpha}{wk\alpha}} \sum \binom{\alpha n}{m_0, m_2, \dots, m_k} \cdot \binom{k}{2}^{m_2} \binom{k}{4}^{m_4} \cdots \binom{k}{k-2}^{m_{k-2}} \tag{162}$$

where the summation is over all integral nonnegative m_0, $m_2, \dots, m_k$, satisfying the conditions

$$m_0 + m_2 + \cdots + m_k = \alpha n \tag{163}$$

$$2m_2 + 4m_4 + \cdots + km_k = \alpha kw. \tag{164}$$

By (164) we have

$$\frac{\binom{k}{2}^{m_2}}{m_2!} \frac{\binom{k}{4}^{m_4}}{m_4!} \cdots \frac{\binom{k}{k-2}^{m_{k-2}}}{m_{k-2}!} \frac{(m_2 + m_4 + \cdots + m_k)!}{m_k!} \le C_{k,w,\alpha} = \mathrm{const}(n).$$

Therefore, (162) and (163) yield

$$P_{n,w}^{k,\alpha} \overset{\ln}{\sim} \mathcal{A}_{n,w}^{k,\alpha} := \frac{1}{\binom{nk\alpha}{wk\alpha}} \sum \binom{\alpha n}{m_2 + m_4 + \cdots + m_k}. \tag{165}$$

However, (164) yields

$$\alpha w \le m_2 + m_4 + \cdots + m_k \le \frac{\alpha kw}{2}$$

and, since the number of summands is $O(1)$, then we have

$$c_1 n^{-\alpha w(k-1)} \le \mathcal{A}_{n,w}^{k,\alpha} \le c_2 n^{-\frac{\alpha kw}{2}}. \tag{166}$$

B. Ensemble C

Let w be even. Similarly to Ensemble A, we partition any matrix from Ensemble C into two submatrices (left and right), the first one having w columns. We denote the corresponding classes by $L_{n,w}^{\ell,\alpha}$, $R_{n,w}^{\ell,\alpha}$, so that the total number of the matrices in the ensemble is

$$\left|\Lambda_{n,w}^{\ell,\alpha}\right| = \sum \binom{\alpha n}{m_0, m_2, \dots, m_w} \left|L_{n,w}^{\ell,\alpha}\right| \left|R_{n,w}^{\ell,\alpha}\right| \tag{167}$$

where the sum is over all

$$m_0 + m_2 + m_4 + \cdots + m_w = \alpha n \tag{168}$$

$$2m_2 + 4m_4 + \cdots + wm_w = \ell w. \tag{169}$$

Moreover, as in Lemma 1

$$\left|L_{n,w}^{\ell,\alpha}\right| = g(n) \frac{(\ell w)!}{(\ell!)^w 2!^{m_2} 4!^{m_4} \cdots w!^{m_w}}. \tag{170}$$

Here, $g(n)$ is $O(1)$. Furthermore, evidently

$$\left|R_{n,w}^{\ell,\alpha}\right| = \binom{\alpha n}{\ell}^{n-w}. \tag{171}$$

From (167), (170), and (171) we conclude that

$$\begin{aligned} \left|\Lambda_{n,w}^{\ell,\alpha}\right| &\overset{\ln}{\sim} \sum \binom{\alpha n}{m_0, m_2, \dots, m_w} \cdot \frac{(\ell w)!}{(\ell!)^w 2!^{m_2} 4!^{m_4} \cdots w!^{m_w}} \binom{\alpha n}{\ell}^{n-w} \\ &= \sum \frac{(\alpha n)!}{m_0!(m_2 + \cdots + m_w)!} \cdot \frac{(\ell w)!(m_2 + \cdots + m_w)!}{(\ell!)^w 2!^{m_2} 4!^{m_4} \cdots w!^{m_w}} \binom{\alpha n}{\ell}^{n-w}. \end{aligned} \tag{172}$$

However, by (169)

$$\ell \le m_2 + m_4 + \cdots + m_w \le \frac{\ell w}{2}$$

and we have

$$\frac{(\ell w)!}{\ell!^{w-1} w!^{\frac{\ell w}{2}}} \le \frac{(\ell w)!(m_2 + \cdots + m_w)!}{(\ell!)^w 2!^{m_2} 4!^{m_4} \cdots w!^{m_w}} \le \frac{(\ell w)! \left(\frac{\ell w}{2}\right)!}{2^\ell}. \tag{173}$$

Since the total number of the matrices in the ensemble is $\binom{\alpha n}{\ell}^n$, by (173) we have

$$P_{n,w}^{\ell,\alpha} \overset{\ln}{\sim} \mathcal{B}_{n,w}^{\ell,\alpha} := \binom{\alpha n}{\ell}^{-w} \sum \binom{\alpha n}{m_2 + \cdots m_w}. \tag{174}$$

Furthermore

$$\binom{\alpha n}{\ell}^{-w} = O(n^{-\ell w})$$

$$\binom{\alpha n}{m_2 + \cdots m_w} = O(n^{m_2 + \cdots + m_w})$$

and we conclude

$$c_3 n^{-\ell(w-1)} \le \mathcal{B}_{n,w}^{\ell,\alpha} \le c_4 n^{-\frac{\ell w}{2}}. \tag{175}$$

C. Ensemble E

For an arbitrary row the probability P that it contains an even number of ones in the first w columns is

$$\begin{aligned} P &= \frac{1}{\binom{n}{k}} \sum_{j=0}^{\lfloor k/2 \rfloor} \binom{w}{2j} \binom{n-w}{k-2j} \\ &= \frac{1}{\binom{n}{k}} \sum_{s=0,2,\dots,2[k/2]} \binom{w}{s} \binom{n-w}{k-s} \\ &\sim \frac{\binom{n-w}{k}}{\binom{n}{k}} = \prod_{t=0}^{k-1} \frac{n-w-t}{n-t}. \end{aligned}$$

Thus, taking into account that the number of rows is $m = \alpha n$, the probability we are interested in is

$$P_{n,w}^{k,\alpha} = e^{-\alpha k(w+(k-1)/2)}(1 + o(1)). \tag{176}$$

This means that the proportion of words of constant weight belonging to a code from the ensemble is a constant independent of n.

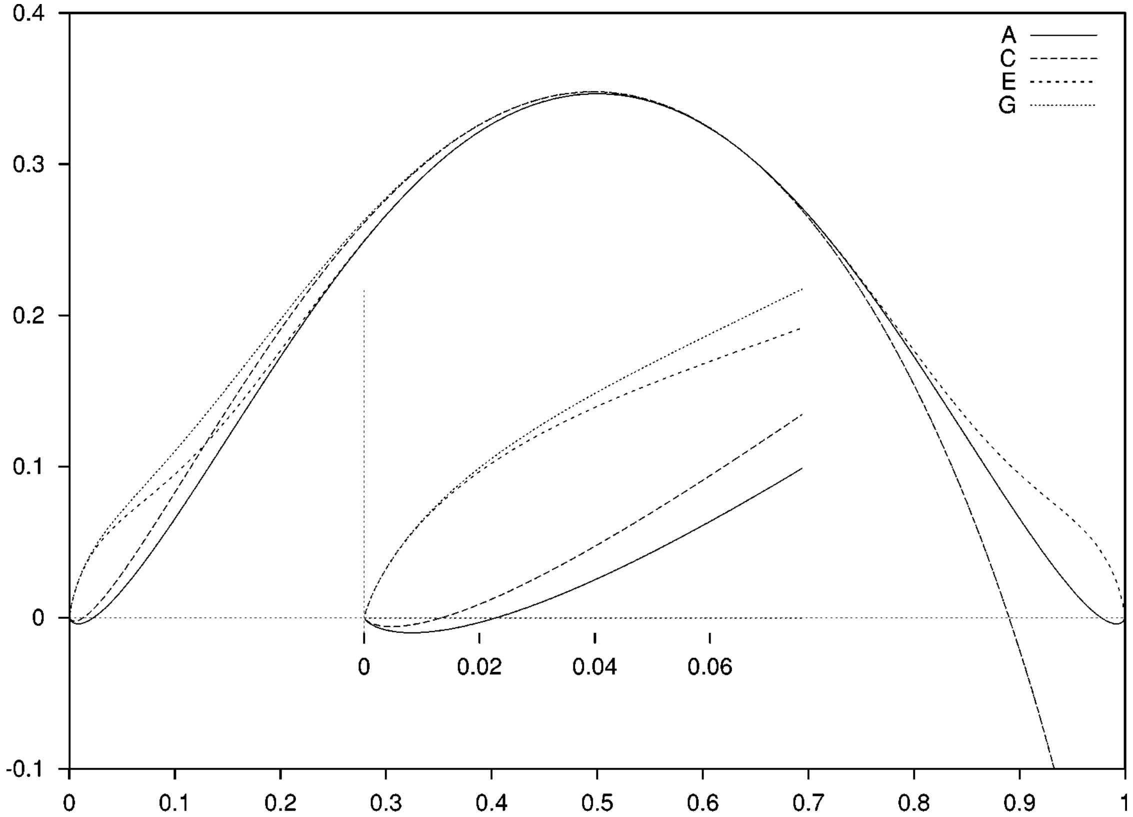

Fig. 1. Distance distributions for $(\ell, k) = (3, 6)$.

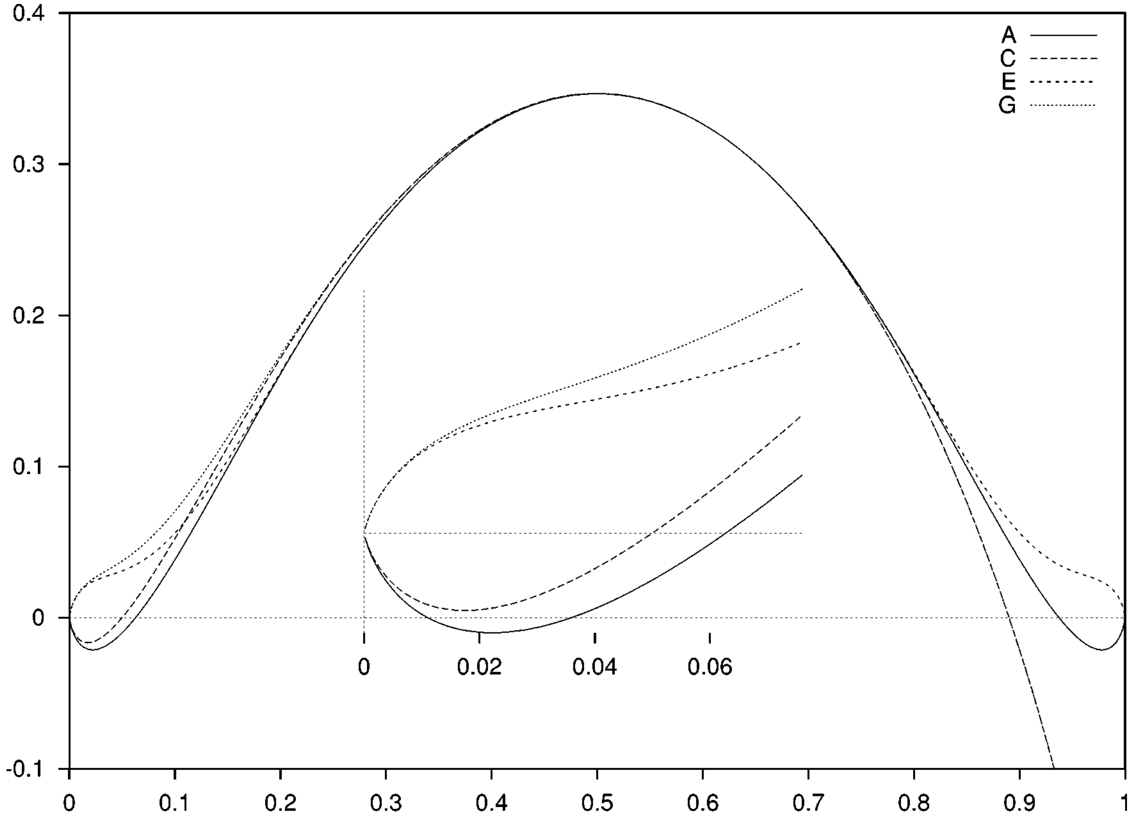

Fig. 2. Distance distributions for $(\ell, k) = (4, 8)$.

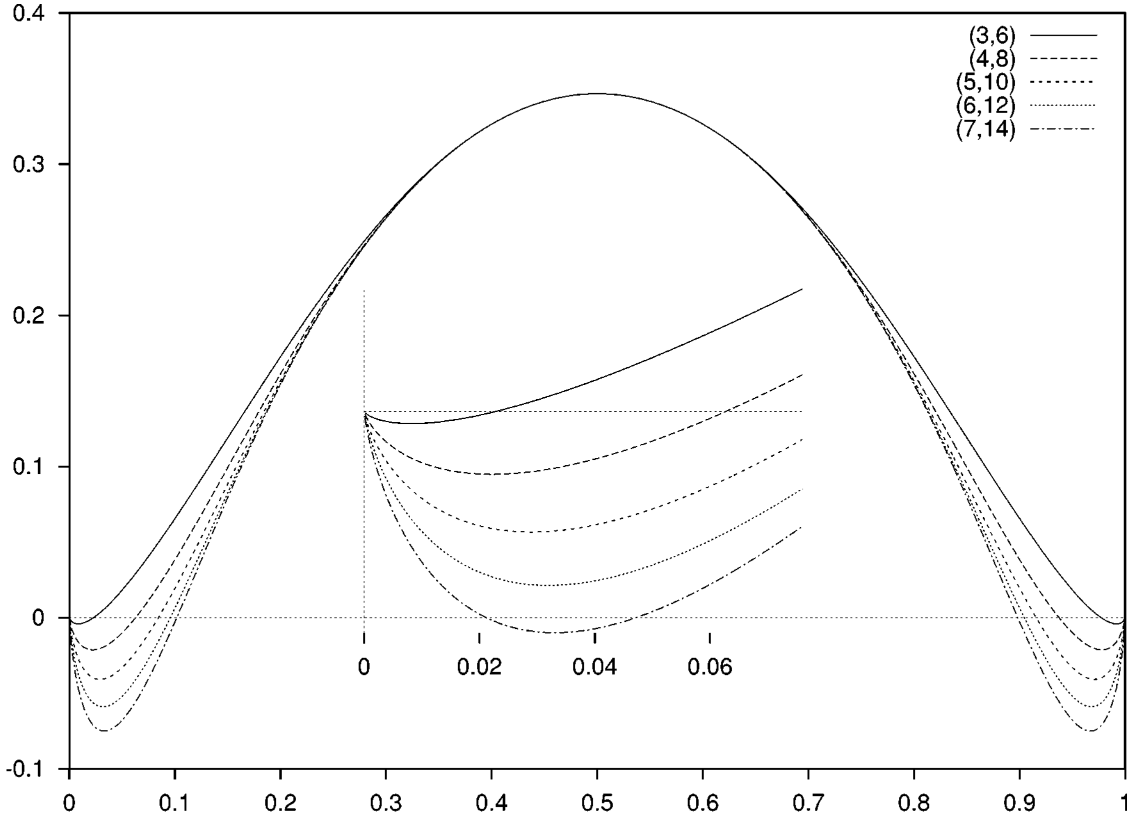

Fig. 3. Distance distributions for Ensemble A.

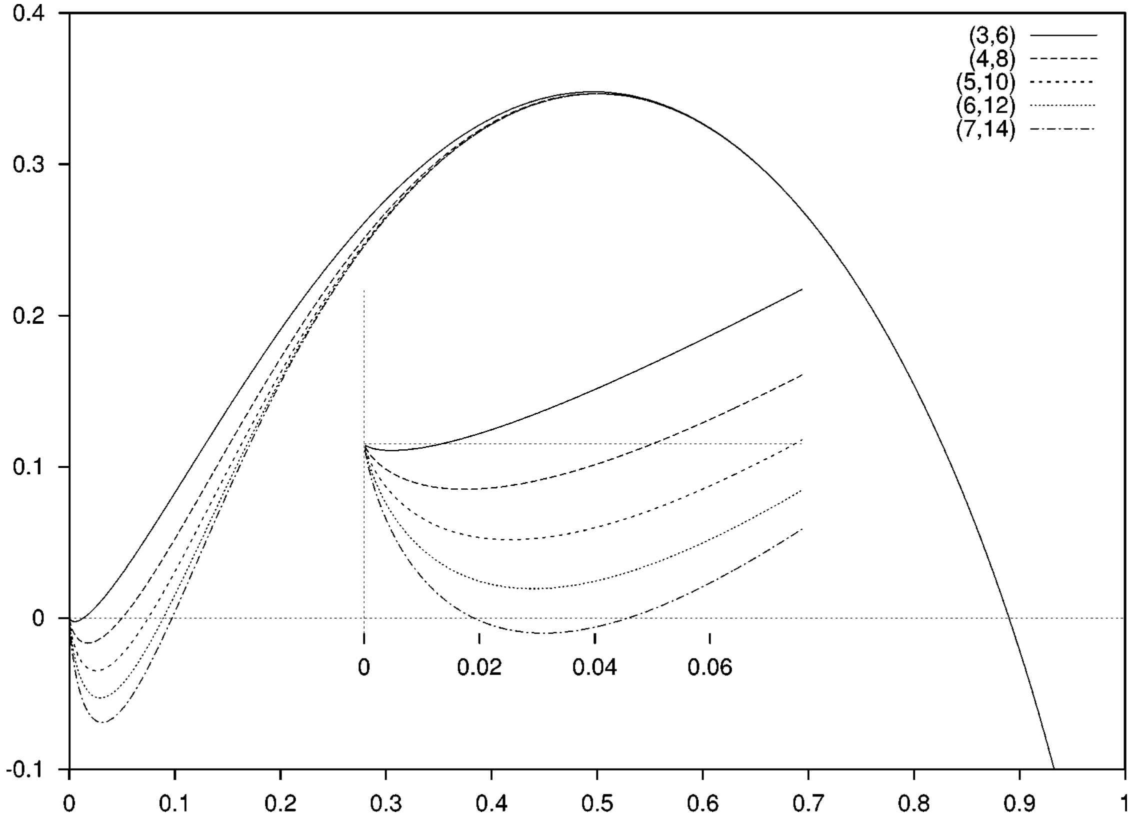

Fig. 4. Distance distributions for Ensemble C.

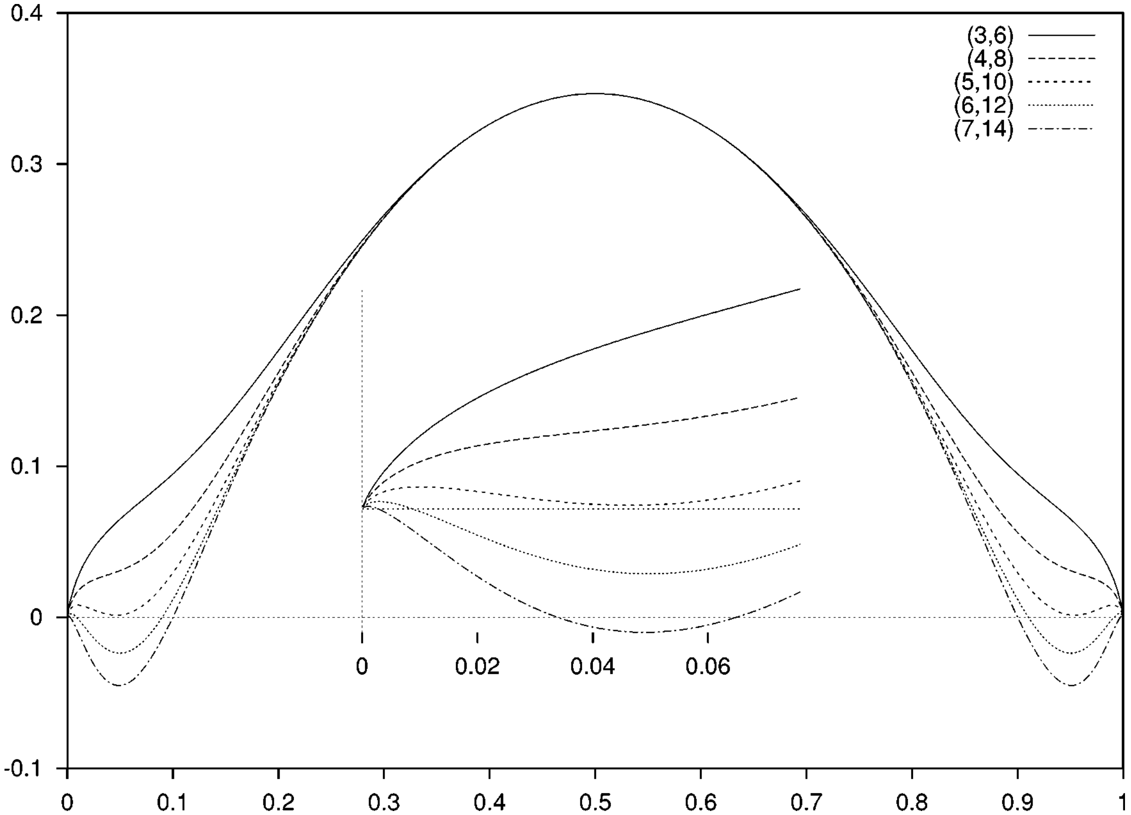

Fig. 5. Distance distributions for Ensembles E.

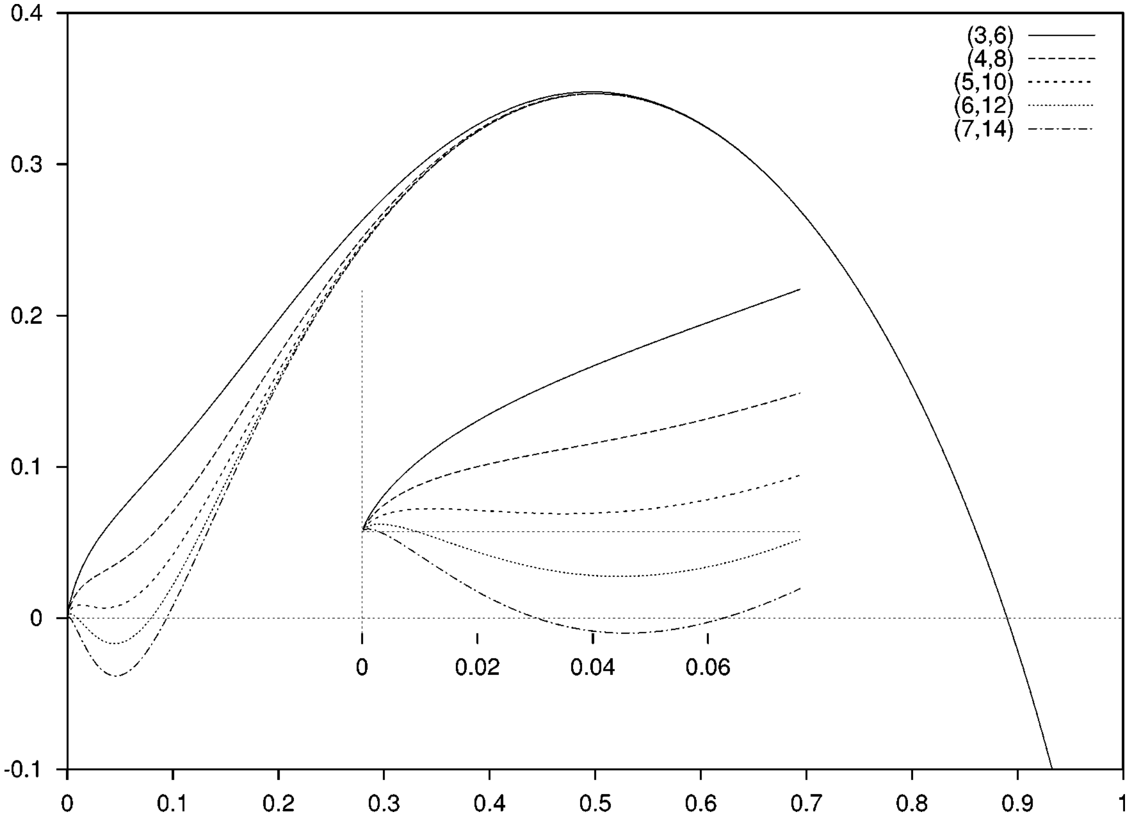

Fig. 6. Distance distributions for Ensembles G.

D. Ensemble G

The probability P that arbitrary row contains an even number of ones in the first w columns is

$$\begin{aligned} P &= \sum_{s=0}^{[w/2]} \binom{w}{2s} \left(\frac{k}{n}\right)^{2s} \left(1 - \frac{k}{n}\right)^{w-2s} \\ &= \frac{1 + \left(2\,\frac{k}{n} - 1\right)^{w}}{2} \\ &= \begin{cases} \frac{1+\left(1-\frac{2k}{n}\right)^{w}}{2}, & \text{for } w \text{ even} \\ \frac{1-\left(1-\frac{2k}{n}\right)^{w}}{2} \sim \frac{kw}{n}, & \text{for } w \text{ odd.} \end{cases} \end{aligned}$$

Raising it to power $m = \alpha n$ we have

$$P_{n,\,w}^{k,\,\alpha} = \begin{cases} e^{-\alpha k w}(1 + o(1)), & \text{for } w \text{ even} \\ O\left(\left(\frac{kw}{n}\right)^{\alpha n}\right), & \text{for } w \text{ odd.} \end{cases} \tag{177}$$

XIII. Discussion

In the paper, we derived expressions for the distance distributions in several ensembles of LDPC. The ensembles are defined in Section II. As it can be seen from the main theorem (Theorem 1), essentially there are four distinct ensembles of the codes, represented by Ensembles A, C, E, and G. In Figs. 1 and 2, we give graphs of the (normalized) distance distributions in the four ensembles of rate $1/2$ for $(\ell, k) = (3, 6)$, and $(\ell, k) = (4, 8)$. In Figs. 3–6, we demonstrate dependence of the behavior of the distance distributions in the ensembles of codes of rate $1/2$ when $(\ell, k) = (3–7, 6–14)$.

Ensembles A and C have the minimum distance growing linearly in n, while Ensembles E and G have relative distance tending to 0 when n grows. Ensembles E and G both have worse minimum distance than Ensembles A and C, because it is inevitable that these ensembles will make columns with no 1's in them, so the code will have codewords of weight 1. Ensembles G and C have slightly higher peaks at relative distance $1/2$ because their matrices have some blank rows, so the code rate is slightly higher.

Acknowledgment

S. Litsyn is grateful to D. Burshtein and G. Miller for enjoyable discussions. The authors are indebted to D. MacKay and anonymous referees for comments and suggestions which helped to improve the paper. D. MacKay kindly provided them with the illustrative graphs of the distance distributions.

References

[1] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: Elsevier, 1997.

[2] H. Cramer, *Mathematical Methods of Statistics*. Princeton, NJ: Princeton Univ. Press, 1966.

[3] P. Diaconis, R. L. Graham, and J. A. Morrison, "Asymptotic analysis of a random walk on a hypercube with many dimensions," *Random Struct. Algor.*, vol. 1, pp. 51–72, 1990.

[4] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.

[5] ——, *Low Density Parity Check Codes*. Cambridge, MA: M.I.T Press, 1963.

[6] I. J. Good and J. F. Crook, "The enumeration of arrays and a generalization related to contingency tables," *Discr. Math.*, vol. 19, no. 1, pp. 23–45, 1977.

[7] M. Kac, "Random walk and the theory of Brownian motion," *Amer. Math. Monthly*, vol. 54, pp. 369–391, 1947.

[8] I. Krasikov and S. Litsyn, "A survey of binary Krawtchouk polynomials," in *Codes and Association Schemes*, ser. DIMACS, A. Barg and S. Litsyn, Eds., 2001, vol. 56, pp. 199–212.

[9] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, pp. 399–431, Mar. 1999.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: Elsevier, 1977.

[11] G. Miller and D. Burshtein, "Bounds on the maximum likelihood decoding error probability of low density parity check codes," *IEEE Trans. Inform. Theory*, to be published.

[12] P. E. O'Neil, "Asymptotics and random matrices with row-sum and column-sum restrictions," *Bull. Amer. Math. Soc.*, vol. 75, pp. 1276–1282, 1969.

[13] I. Sason and S. Shamai (Shitz), "Improved upper bounds on the ensemble performance of ML decoded low density parity check codes," *IEEE Commun. Lett.*, vol. 4, pp. 89–91, Mar. 2000.

[14] T. Richardson and R. Urbanke, "The capacity of low-density parity check codes under message-passing decoding," *IEEE Trans. Inform. Theory*, vol. 47, pp. 599–618, Feb. 2001.