5-2007

Random Vectors Over Finite Fields

Shannon Lockard
Clemson University, shannonlockard@gmail.com

RANDOM VECTORS OVER FINITE FIELDS

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Mathematical Sciences

---

by
Shannon Renee Lockard
May 2007

Accepted by:
Dr. Neil Calkin, Committee Chair
Dr. Kevin James
Dr. Gretchen Matthews
Dr. Wayne Goddard

ABSTRACT

The study of random objects is a useful one in many applications and areas of mathematics. The Probabilistic Method, introduced by Paul Erdős and his many collaborators, was first used to study the behavior of random graphs and later to study properties of random objects. It has developed as a powerful tool in combinatorics as well as finding applications in linear algebra, number theory, and many other areas. In this dissertation, we will consider random vectors, in particular, dependency among random vectors. We will randomly choose vectors according to a specified probability distribution. We wish to determine how many vectors must be generated before the vectors are almost surely dependent, that is, there is a high probability that a subset of the vectors is linearly dependent.

In Chapter 1, we will review previous work done in this area. A typical result in the study of random objects is a threshold function that describes the behavior of a given property of the objects. We will discuss previous threshold functions and methods used to find them. The results found for this problem before now have been for vectors of bounded or fixed weight. In Chapter 2, we will develop the methods we will use later on vectors of fixed weight. We will then use these methods in Chapter 3 to vary the probability model under which the vectors are generated. Instead of considering vectors of fixed weight, we will consider a general probability model for choosing the vectors: each position in a vector will be assigned a probability of containing a nonzero entry. Finally, in Chapter 4 we will specify a function for this probability. We will then find a threshold result for the specified probability model. This result will give a lower bound for the number of vectors needed before they are almost surely dependent.

ACKNOWLEDGMENTS

I would like to thank my advisor, Neil Calkin, for spending his time and energy to listen to and teach me. He has introduced me to countless ideas and given me many opportunities that have enabled me to develop as a researcher and a teacher. His never-ending ideas have taught me how to always have another question.

I also thank my committee for taking their time to talk with me and read my work. I thank Kevin James for being an excellent example in the classroom and always taking the time to talk to me when I had questions. I also thank Gretchen Matthews and Wayne Goddard for their questions and suggestions that have already given me new ideas to work on. Jim Peterson also deserves a great deal of thanks for being a wonderful teacher and encourager during my time here.

My time at Clemson would not be the same without the other graduate students and all the friends I have made here. They have always provided me with an outlet for ideas and questions; I have learned a great deal of math from the other students here. Office chats, card games, and frisbee on Fridays have kept me sane and I will remember these things fondly.

I owe my family a great deal for their support and prayers. They have always encouraged me, listened to me, and if possible, are more excited than I am that I've finished this chapter of my life. They have loved me unconditionally and I am honored to make them proud.

I also thank my husband for being an amazing support system for me as well. He has prayed with me, listened to my frustrations, celebrated my triumphs, encouraged me to continue when I didn't know how, and has been a wonderful example. He is an inspiration to me.

Finally, I would like to thank God, through whom all things are possible.

TABLE OF CONTENTS

Table of Contents (Continued)

LIST OF FIGURES

CHAPTER 1

Random Vector History

Since its introduction in the late 1940s [3], the Probabilistic Method has been a powerful tool, widely used in combinatorics and graph theory as well as finding applications in number theory, algebra, and computer science. Pioneered by Erdős and his many collaborators to study random graphs, probabilistic methods can often yield results not easily attainable with other methods. The key to the Probabilistic Method is its use of random objects, often applied to existence proofs or in finding threshold results. A random approach to a difficult problem can make the problem easier to tackle. For instance, determining if a graph is Hamiltonian is an NP-complete problem. However, it has been shown that a random graph is almost surely Hamiltonian if it has minimum degree 2. This type of threshold result is often the goal in studying random objects. In this dissertation, we will be investigating properties of random vectors. In particular, we will discuss the probability of dependency among a set of vectors randomly chosen according to a given probability model.

The majority of the literature in this area has focused on the dependencies found in random vectors of fixed weight or vectors of bounded weight, that is, vectors with weight at most h. The weight of a vector is taken here to be the number of nonzero entries of that vector. Although many variations and extensions have been studied, many aspects of the problem remain unanswered. Our main question is as follows.

Question: Choose l vectors randomly from a vector space based on a given probability distribution. How large must l be to ensure with high probability that a subset of the l vectors is linearly dependent?

Kolchin, Khokhlov, and Balakin have published a collection of papers that address this question under the guise of hypergraphs. In the first of these papers [11], Kolchin and Khokhlov studied the distribution of cycles in a random graph of

degree N. In [2], Balakin, Kolchin, and Khokhlov studied the number of hypercycles in hypergraphs. The results of these papers apply to vectors over $\mathbb{F}_2$. Kolchin found similar results for $\mathbb{F}_2$ by studying systems of random equations in [9] and their relation to hypergraphs. Kolchin and Khokhlov generalized the work on systems of equations to prime fields in [12]. Finally, Kolchin studied yet another system of random equations in [10] to analyze the question over general finite fields. Calkin took a more direct approach to the question in [5] and [6], giving a result similar to the main results in the previous papers although the models are slightly different. Cooper then generalized the question further in [7] to include random vectors over Abelian groups in addition to vector spaces over finite fields. Finally, in [13] Linial and Weitz considered the question motivated by coding theory applications.

In the remainder of the dissertation, k will be the length of the vectors and we will be choosing l vectors independently according to a specified probability distribution. We will regard the vectors as the rows of a matrix so that we will be considering an $l \times k$ matrix. From linear algebra we know this matrix is dependent for any $l > k$. Therefore, the interesting case for dependency is when $l \leq k$. As such, we will always assume that $l \leq k$.

We begin by summarizing the work done by Balakin, Kolchin, and Khokhlov on hypergraphs. A *hypergraph* $H = (V, E)$ is a generalization of a graph where V is a set of vertices and each edge in E, called a *hyperedge*, is a subset of the vertices. Although hypergraphs and hyperedges are generally considered to be non-empty, for this application we allow the empty hypergraph and hyperedge as well as multiple hyperedges. Each hypergraph with k vertices and l hyperedges is associated with an $l \times k$ binary matrix $A = (a_{ij})$ called the incidence matrix. A is defined as follows: if e_i is the i^{th} hyperedge in E and v_j is the j^{th} vertex of H, then

$$a_{ij} = \begin{cases} 1 & \text{if } v_j \in e_i \\ 0 & \text{otherwise.} \end{cases}$$

A subset of hyperedges $C = \{e_1, e_2, \ldots, e_m\}$ is a *hypercycle* if every vertex appearing in C appears in an even number of the hyperedges. In other words, the vectors representing $e_1, e_2, \ldots, e_m$ sum to the zero vector modulo 2. If C_1 and C_2 are both

hypercycles, the union of C_1 and C_2, denoted $C_1 \triangle C_2$, is defined to be the set of hyperedges contained in either C_1 or C_2 but not both. Finally, let $C_1, C_2, \ldots, C_s$ be a set of hypercycles and let $\epsilon_1, \epsilon_2, \ldots, \epsilon_s \in \{0, 1\}$. Then $C_1, C_2, \ldots, C_s$ are independent if

$$\epsilon_1 C_1 \triangle \epsilon_2 C_2 \triangle \cdots \triangle \epsilon_s C_s = \emptyset$$

if and only if $\epsilon_1 = \epsilon_2 = \cdots = \epsilon_s = 0$.

In [2], Balakin, Kolchin, and Khokhlov constructed a hypergraph with incidence matrix A whose rows are generated independently of each other. To construct a row, h positions are chosen uniformly with replacement in which to insert a 1. In doing this, it is possible for more than one 1 to be placed in any given position. If an odd number of 1's are placed in one position, then the final entry is a 1. Otherwise, a 0 is placed in that position. Notice that using this construction, each row contains at most h 1's. Balakin, Kolchin, and Khokhlov considered the total number of independent hypercycles, $s(A)$, of this hypergraph. Then the total number of nonempty hypercycles is $S(A) = 2^{s(A)} - 1$. They proved the following theorem about the expected number of hypercycles in the constructed hypergraph.

Theorem 1.1 *Let $h \geq 3$ be fixed, $l, k \to \infty$ in such a way that $l/k \to \alpha$. Then there exists a constant α_h such that $E(S(A)) \to 0$ for $\alpha < \alpha_h$ and $E(S(A)) \to \infty$ for $\alpha > \alpha_h$.*

A system of equations was given to find the exact value of α_h along with the following solutions:

$$\begin{aligned} \alpha_3 &= 0.8894\ldots, \quad \alpha_6 = 0.9969\ldots, \\ \alpha_4 &= 0.9671\ldots, \quad \alpha_7 = 0.9986\ldots, \\ \alpha_5 &= 0.9891\ldots, \quad \alpha_8 = 0.9995\ldots \end{aligned}$$

An asymptotic expression for α_h was also given as

$$\alpha_h \simeq 1 - \frac{e^{-h}}{\ln 2} - \frac{e^{-2h}}{\ln 2}\left(\frac{h^2}{2} + \frac{h}{\ln 2} - h - \frac{1}{2}\right). \tag{1.1}$$

Kolchin proved the same theorem in [9] by first forming the matrix A in terms of systems of linear equations and then considering the number of hypercycles found in the hypergraph represented by A. As in [2], the number of nonzero entries

of each row of A, equivalently, the number of variables included in the linear equation corresponding to the row, was at most h.

All the the papers above point out the connection between the dimension of the null space of the matrix A and the systems of linear equations or the number of independent hypercycles of the hypergraph represented by A. Recall that a subset of hyperedges, C, is a hypercycle if all of the vertices appearing in C have even degree. This is equivalent to saying that the sum of the rows corresponding to these hyperedges sum to the zero vector over $\mathbb{F}_2^k$. Thus the maximum number of distinct hypercycles is the number of independent subsets of the rows of A that sum to the zero vector. Observe that this corresponds exactly to a basis for the left null space of the matrix A. Thus the size of the null space of A is one more than the number of nonempty hypercycles in the hypergraph represented by A, since we account for the empty sum when considering the null space.

Calkin proved a similar threshold theorem using the left null space of a matrix rather than the concept of hypergraphs [5]. In this paper, the matrix A is formed by choosing binary vectors uniformly with replacement from the set of all vectors with weight exactly h. As a side note, the vectors chosen are actually used as the columns of A and the size of the right null space is calculated. Since we place the vectors as the rows of A, we will phrase Calkin's results in terms of the left null space.

Let r be the rank of A and $s = l - r$ the dimension of the left null space. Calkin showed the following threshold theorem for each $h \geq 3$.

Theorem 1.2

(a) If $\beta < \beta_h$ and $m = m(k) < \beta k$, then $E(2^s) \to 1$ as $k \to \infty$.

(b) If $\beta > \beta_h$ and $m = m(k) > \beta k$, then $E(2^s) \to \infty$ as $k \to \infty$.

As $h \to \infty$, the constant β_h is shown to be

$$\beta_h \sim 1 - \frac{e^{-h}}{\ln 2}.$$

The first few exact critical values are found to be

$$\beta_3 = 0.8894928\ldots, \quad \beta_7 = 0.9986504\ldots,$$
$$\beta_4 = 0.9671147\ldots, \quad \beta_8 = 0.9995102\ldots,$$
$$\beta_5 = 0.9891624\ldots, \quad \beta_9 = 0.9998209\ldots,$$
$$\beta_6 = 0.9962283\ldots, \quad \beta_{10} = 0.9999343\ldots$$

It appears that the only difference between Theorems 1.1 and 1.2 is in the finite limit of the expected value. Since $S(A)$ is defined to be the total number of non-empty hypercycles while the null space allows the zero vector, this difference is simply a matter of what is being considered. Even the exact solutions for the threshold values agree to four decimal places with the exception of α_6 and β_6. However, it is important to remember that the models are different. We go into more detail on this after discussing Calkin's method.

Calkin took a very different approach to proving this theorem than Balakin, Kolchin, and Khokhlov. He defined a Markov chain as follows: starting with the zero vector, add a single vector of weight h at each step and calculate the weight of the current vector sum. The states of the chain are in the set $\{0, 1, 2, \ldots, k\}$ and correspond to the possible weights of the vector sum. Calkin showed that the transition matrix of this Markov chain was diagonalizable and obtained explicit expressions for the eigenvalues and eigenvectors. He then found the probability that a subset of m vectors sums to the zero vector in $\mathbb{F}_2^k$. Thus the expected size of the left null space of the matrix whose rows are vectors of fixed weight h is

$$E(2^s) = \sum_{i=0}^{k} \frac{1}{2^k} \binom{k}{i} (1 + \lambda_i)^l,$$

where

$$\lambda_i = \sum_{t=0}^{h} (-1)^t \frac{\binom{i}{t}\binom{k-i}{h-t}}{\binom{k}{h}}$$

is the i^{th} eigenvalue of the transition matrix.

Estimating λ_i and in turn $E(2^s)$ gives the threshold theorem. Now let $p_{k,h}(l)$ be the probability that the l random vectors are linearly dependent. As a result of Theorem 1.2, Calkin also gives

Theorem 1.3 *For each h there is a constant β_h so that if $\beta < \beta_h$ then*

$$\lim_{k\to\infty} p_{k,h}(\beta k) = 0,$$

where β_h is as before.

Since $\beta_h \to 1$ very quickly, this theorem tells us that l must be very close to k in order to have a chance of choosing a set of linearly dependent vectors.

At this point we return to the observation that although the models of Balakin, Kolchin, and Khokhlov in [2, 9] are different than Calkin's in [5], the results look the same. Upon careful inspection, we see that as h grows, the asymptotic threshold values given for the two theorems are slightly different. Recall the approximate solution (1.1) given by Balakin, Kolchin, and Khokhlov as the threshold value:

$$\alpha_h \simeq 1 - \frac{e^{-h}}{\ln 2} - \frac{e^{-2h}}{\ln 2}\left(\frac{h^2}{2} + \frac{h}{\ln 2} - h - \frac{1}{2}\right),$$

as well as the asymptotic threshold value for β_h given by Calkin:

$$\beta_h \sim 1 - \frac{e^{-h}}{\ln 2}.$$

It is clear that these critical values are asymptotic. In fact, Calkin also gives the following expanded expression:

$$\beta_h \sim 1 - \frac{e^{-h}}{\ln 2} - \frac{e^{-2h}}{\ln 2}\left(\frac{h^2}{2} + \frac{h}{\ln 2} - h - \frac{1}{2}\right) + e^{-3h}O(h^4)$$

in [5], giving more evidence to imply these theorems are equivalent. We must recognize, though, that these are asymptotic solutions. Here lies the difference between the theorems: the thresholds are not actually identical, but are instead asymptotically equivalent.

This similarity between solutions comes directly from the similarity between models. In all of the papers, h positions are chosen uniformly and independently from k possible locations. However, in the former papers, the locations of the 1's are chosen with replacement while in the latter paper, they are chosen without replacement. Thus the vectors chosen in [2, 9] have weight at most h and the vectors in [5] have weight exactly h. Actually, we can express the first model in terms of

the second: to generate the vectors in the bounded weight model, take h random vectors of weight exactly 1 and add them together. Now, if λ_i is the i^{th} eigenvalue of the transition matrix generated for the problem with weight h vectors, let μ_i be the eigenvalue of the transition matrix of the problem with vectors of weight 1. Adding h vectors of weight 1 corresponds to raising the transition matrix for weight 1 vectors to the h^{th} power. We are thus interested in the i^{th} eigenvalue of this matrix, μ_i^h. Observe that

$$\begin{aligned}\mu_i &= \sum_{t=0}^{1}(-1)^t \frac{\binom{i}{t}\binom{k-i}{1-t}}{\binom{k}{1}} \\ &= \frac{1}{k}(k-i-i) \\ &= 1-\frac{2i}{k},\end{aligned}$$

so

$$\mu_i^h = \left(1-\frac{2i}{k}\right)^h.$$

To determine how close these two models are, we must compare μ_i^h and λ_i. Initial computations on Maple indicate that these two values are almost indistinguishable. Furthermore, in analyzing $E(2^s)$, Calkin gave the following lemma which will aid us.

Lemma 1.1

(a) $|\lambda_i| < 1$ *for all* $0 \le i \le k$.

(b) If $i > \frac{k}{2}$ *then* $\lambda_i = (-1)^h \lambda_{k-i}$.

(c) Let $0 < c < \frac{1}{2}$. *If* $i = ck$ *then*

$$\lambda_i = \left(1-\frac{2i}{k}\right)^h - \frac{4\binom{h}{2}}{k}\left(1-\frac{2i}{k}\right)^{h-2}\frac{i}{k}\left(1-\frac{i}{k}\right) + O\left(\frac{h^3}{c^2k^2}\right).$$

Notice the first term in the expression for λ_i in part (c) is μ_i^h. Since this is the dominant term in the expression, we see that λ_i approaches μ_i^h as $k \to \infty$. Thus the two different models are asymptotically the same, explaining the similarity in the threshold theorems.

Although the results are similar, the methods used by Balakin et al. and Calkin are completely different. The disadvantage of using hypergraphs to prove the

threshold theorems is in the limitations set on the matrix considered. By using an incidence matrix, we are forced to consider only vectors chosen from $\mathbb{F}_2$. However, Kolchin's use of linear equations and Calkin's Markov chain can be used to investigate results in other finite fields. Recall that Kolchin related a system of linear equations over $\mathbb{F}_2$ to a hypergraph in [9] to give a threshold theorem. Kolchin and Khokhlov considered the system of equations over $\mathbb{F}_p$, p prime, given by

$$x_{i_1(t)} + x_{i_2(t)} + \cdots + x_{i_h(t)} = b_t, \quad t = 1, \ldots, l,$$

where the values for $i_j(t)$ are uniformly randomly chosen from $\{1, 2, \ldots, k\}$ with replacement and the values for b_t are chosen from $\mathbb{F}_q$ with equal probability [12]. A_h is then defined to be the matrix corresponding to the system of equations. Observe by the formulation of the system each row of A_h will have at most h nonzero entries. A *critical set* is defined to be a set of rows and weights, $B = \{t_1, \ldots, t_m; \epsilon_1, \ldots, \epsilon_m\}$ such that

$$\epsilon_1 \mathbf{a}_{t_1} + \ldots \epsilon_m \mathbf{a}_{t_m} = \mathbf{0}$$

where $\mathbf{a}_t$ is the t^{th} row of A_r. Letting $S(A_r)$ be the total number of critical sets of A_r, they showed for $\mathbb{F}_p$:

Theorem 1.4 *Let $p \geq 3$ be prime, $h \geq 3$ be fixed, and let $l, k \to \infty$ in such a way that $l/k \to \alpha$. Then there exists a constant α_h such that $E(S(A_h)) \to 0$ if $\alpha < \alpha_h$ and $E(S(A_h)) \to \infty$ if $\alpha > \alpha_h$.*

The constant α_h is the first component of the vector which is the only solution of the following system of equations in three unknowns a, λ, and x:

$$\begin{aligned} \frac{1}{p}\, e^{\lambda}(1 + (p-1)e^{-p\lambda/(p-1)}) \left(\frac{ah}{ah - x}\right)^a e^{-x} &= 1, \\ \frac{(p-1)(ah-x)}{x} &= \left(\frac{\lambda}{x}\right)^h, \\ \lambda\, \frac{1 - e^{-p\lambda/(p-1)}}{1 + (p-1)e^{-p\lambda/(p-1)}} &= x. \end{aligned}$$

Finally, in [10], Kolchin generalized this approach even further and showed that the threshold exists for systems of equations over $\mathbb{F}_q$, $q \geq 3$. He considered the

system of linear equations given by

$$a_1^{(t)} x_{i_1(t)} + a_2^{(t)} x_{i_2(t)} + \cdots + a_h^{(t)} x_{i_h(t)} = b_t, \quad t = 1, \ldots, l$$

where the $i_j(t)$ and b_t are randomly chosen as before and the $a_j^{(t)}$ are uniformly randomly chosen from $\mathbb{F}_q$. The threshold theorem resulting from this generalized system of linear equations is identical to Theorem 1.4 with p replaced by q.

Calkin also generalized his method of computing the expected size of the null space to other finite fields in [6]. The process is the same: randomly choose l vectors independently and uniformly with replacement from the set of vectors in $\mathbb{F}_q^k$ that have h nonzero entries, and define a Markov chain based on the Hamming weight of the partial sums of the vectors. Setting up the transition matrix as before he found

$$\lambda_i = \sum_{t=0}^{h} (-1)^{h+t} \frac{\binom{i}{t}\binom{k-i}{h-t}(q-1)^t}{\binom{k}{h}(q-1)^k}$$

and

$$E(q^s) = \sum_{i=0}^{k} \frac{1}{q^k} \binom{k}{i} (1 + (q-1)\lambda_i)^l (q-1)^{k-i}.$$

Asymptotics of $E(q^s)$ gave the following generalized theorem.

Theorem 1.5 *For any q, $h \geq 3$ there is a constant β_h so that*

(a) If $\beta < \beta_h$ and $m = m(k) < \beta k$, then $E(q^s) \to 1$ as $k \to \infty$.

(b) If $\beta > \beta_h$ and $m = m(k) > \beta k$, then $E(q^s) \to \infty$ as $k \to \infty$.

Furthermore, $1 - \beta_h \sim \frac{(q-1)e^{-h}}{\ln q}$ as $k \to \infty$.

Again, the expected size of the left null space, $E(q^s)$, led to the following corollary about linear dependencies among the random vectors.

Corollary 1.1 *For any fixed h, q, if $\beta < \beta_h$ and $l < \beta_h k$, then, as $k \to \infty$, the probability that the vectors $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_l$ are linearly dependent tends to 0.*

Corollary 1.1 and Theorem 1.5 give a lower bound for the number of vectors needed to have a set of vectors in $\mathbb{F}_q^k$ that are linearly dependent. In addition, Kolchin and Khokhlov's calculation of this threshold value in [12, 10] agreed with the asymptotic expression for β_h in Theorem 1.5.

The original question of linearly dependent random vectors can be modified to obtain other interesting results. Cooper not only considered the question where the vector entries come from finite fields, but also generalized the problem to consider the case when the entries are elements of an Abelian group [7]. Like Calkin, he studied vectors of constant weight. However, it was necessary to employ different methods in order to gain more insight into the question regarding Abelian groups. Cooper gave an expression for the probability that a random sequence of vectors sums to the zero vector and estimated this probability in order to obtain a system of equations. For fixed k, the smallest positive solution to the system gave a lower bound on the threshold value for linear independence. On the other hand, for k tending to infinity, the lower bounds could be simplified to find the solution of one equation. For finite fields, Cooper found this threshold value to be α_q, the largest non-negative solution of

$$\alpha_q = 1 - \log_q \left(1 + (q-1)e^{-\alpha_q h}\right).$$

Furthermore,

$$\alpha_q \sim 1 - \frac{(q-1)e^{-h}}{\ln q},$$

the same result given by Calkin in [6].

The question of Abelian groups separates into two cases to specify the possibilities for the vector entries:

> **Case 1:** Each vector has h nonzero entries, all of which are a fixed element, γ, of the group such that the order of γ is t.
>
> **Case 2:** Each vector has h nonzero entries chosen uniformly at random from the nonzero elements of the group where the size of the group is t.

In both cases, as $h \to \infty$, a lower bound on the critical threshold value was found to be

$$\beta_h \sim \log_2 t$$

where t is as defined in the cases above.

Linial and Weitz have also studied rank and linear dependency among matrices where the rows are restricted [13]. The rows in their matrices were chosen uniformly from the vector space containing vectors with Hamming weight at most h, that is the vectors have at most h nonzero entries. Their variation is as follows: how large does the maximum weight need to be in order to ensure that the matrices behave like those where $h = n$, in other words, matrices whose rows are taken from $\mathbb{F}_q^k$ with no restrictions. Let E^l be the expected size of the null space of an $l \times k$ matrix whose rows are chosen uniformly over $\mathbb{F}_q$ with no restriction on weight. Linial and Weitz noted that

$$E^l = 1 + \frac{q^l - 1}{q^k}.$$

Now let E_h^l be the expected size of the null space where the rows have weight at most h. One of the main theorems in [13] is

Theorem 1.6 *Let $\Omega = \Omega_{h,l,k,q}$ be the probability space of $l \times k$ matrices over $\mathbb{F}_q$ with row weights at most h. Consider the rank r as a random variable on Ω. Then the expected cardinality of the kernel satisfies:*

$$E^l = 1 + \frac{q^l - 1}{q^k} \leq E(q^{l-r}) = E_h^l$$

with equality when $h = k$. Moreover, if $h \geq \ln k + \omega(1)$, then for every l,

$$E_h^l \leq (1 + o(1)) \left(1 + \frac{q^l - 1}{q^k}\right)$$

as $k \to \infty$.

This implies that when $h \geq \ln k + \omega(1)$,

$$E^l \leq E_h^l \leq (1 + o(1))E^l.$$

In other words, when h is large enough, the null space of matrices in $\Omega_{h,l,k,q}$ behaves roughly as it does when there are no restrictions on the rows of the matrices. To estimate E_h^l and prove this theorem, Linial and Weitz used upper and lower bounds on the probability that a sum of vectors gives the zero vector. As a corollary to this theorem, they gave

Corollary 1.2 *Let $\omega(k) \to \infty$ as $k \to \infty$. If $h \geq \ln k + \omega(k)$, then*

$$E(\min\{k,l\} - r) \leq \frac{q^{-|l-k|}}{\ln q} + o(1)$$

where r is the rank of the matrix.

This led to the results they were interested in.

Corollary 1.3 *If $h > \ln k + \omega(k)$ and if $|k-l| \geq \omega(k)$ then almost every matrix in $\Omega_{h,l,k,q}$ has full rank.*

Corollary 1.4 *If $h > \ln k + \omega(k)$ and if $r' \leq \min\{l,k\} - \omega(k)$ then $Pr(r \leq r') = o(1)$.*

This last corollary is especially interesting as it says that if h is large enough, the probability of not achieving full rank is very small.

The papers discussed all addressed some variation of the main question, the only differences being in the models and fields considered and in the methods used. There are still variations to this question to be studied. We will explore another of these variations by modifying the probability model. Instead of requiring the vectors to have constant or bounded weight, we will assign each element of the vectors a probability of having a 1 in that location. We will find an exact expression for the expected size of the null space of the matrix generated under this probability model following a method we outline using fixed weight vectors. Finally, we will use the exact expression to explore a specific probability model.

CHAPTER 2

More on Fixed Weight Vectors

2.1 Introduction

In Chapter 1 we saw lower bounds on a critical threshold value for our main question over both $\mathbb{F}_2$ and $\mathbb{F}_q$. For sets of vectors with size less than this critical value, previous authors showed that those vectors were almost surely independent, thus implying we would need to generate more vectors than the critical value before finding a dependent subset. Balakin, Kolchin, Khokhlov, and Calkin all took an approach that utilized a matrix and all authors discussed the importance of the null space of that matrix in their findings. In this chapter we will more thoroughly discuss the link between our question and the null space of a certain matrix. To explore this idea further, we will continue to work with vectors of fixed weight, as Calkin and Cooper did. We first describe the variables and assumptions we will be using.

Let $\mathcal{H}$ be the set of binary vectors of weight h over $\mathbb{F}_2^k$. Choose l vectors, $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_l$, uniformly from $\mathcal{H}$ with replacement and let $\mathcal{V} = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_l\}$. We define the matrix A such that the i^{th} row of A is the i^{th} vector chosen, i.e.

$$A = \begin{pmatrix} \mathbf{v}_1^T \\ \mathbf{v}_2^T \\ \vdots \\ \mathbf{v}_l^T \end{pmatrix}.$$

Observe that A is an $l \times k$ matrix and by construction, each row of A has weight h. Let r be the rank of A and $s = l - r$ the dimension of the left null space of A. Recall in [5] that Calkin found the following exact expression for the expected number of subsequences of $\mathcal{V}$ that sum to the zero vector:

$$E(2^s) = \sum_{i=0}^{k} \frac{1}{2^k} \binom{k}{i} (1 + \lambda_i)^l, \tag{2.1}$$

with

$$\lambda_i = \sum_{t=0}^{h} (-1)^t \frac{\binom{i}{t}\binom{k-i}{h-t}}{\binom{k}{h}}.$$

Alternatively, we can view $E(2^s)$ as the expected size of the left null space of A. To make this connection clear, consider $\mathbf{x}$ in the left null space of A. Since $\mathbf{x}$ is over $\mathbb{F}_2$, multiplying A by $\mathbf{x}^T$ on the left is equivalent to adding the rows of A corresponding to the 1's in $\mathbf{x}$. Since $\mathbf{x}^T A = \mathbf{0}$, the sum over $\mathbb{F}_2$ of the subset of rows is the zero vector, therefore the subset of rows is dependent. Thus there is a correspondence between the dependent subsets of $\mathcal{V}$ and the vectors in the left null space of A.

Now that we see there is a well-known concept from linear algebra connected to our question, we can use it to gain insight into the problem. In particular, we discuss the implication of having $E(2^s) = 1$. If the size of the null space is 1, then there is only one vector in the null space. In fact, we know exactly what vector that is, the zero vector. Therefore if $\mathbf{x}^T = (c_1, c_2, \ldots, c_l)$, then the only solution to $\mathbf{x}^T A = \mathbf{0}$, or

$$c_1\mathbf{v}_1 + \ldots c_l\mathbf{v}_l = \mathbf{0},$$

is $\mathbf{x} = \mathbf{0}$. In other words, $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_l$ are independent. So when the expected size of the left null space is close to 1, the vectors are almost surely independent, or there is a very small probability that they are dependent. As $E(2^s)$ increases, the probability that there exists a dependent subset of $\mathcal{V}$ also increases. Recall the threshold theorem for $E(2^s)$.

Theorem 2.1 (Calkin, [5])

(a) If $\beta < \beta_h$ and $l = l(k) < \beta k$, then $E(2^s) \to 1$ as $k \to \infty$.

(b) If $\beta > \beta_h$ and $l = l(k) > \beta k$, then $E(2^s) \to \infty$ as $k \to \infty$.

Furthermore, as $h \to \infty$,

$$\beta_h \sim 1 - \frac{e^{-h}}{\ln 2}.$$

This theorem says that we must choose at least $k \cdot (1 - e^{-h}/\ln 2)$ vectors of fixed weight h from $\mathbb{F}_2^k$ before obtaining a dependent set. Also, as $h \to \infty$, β_h rapidly approaches 1, so we must generate close to k vectors before we have a high probability of seeing dependence.

Calkin used a Markov chain to obtain the expression for $E(2^s)$ leading to Theorem 2.1. In this chapter, we will further exploit the importance of the null space by considering the right null space of A. This will lead to an interesting binomial identity as well as ideas that will be important in a later chapter with different probability models.

2.2 The Right Side of Calkin's Work

From linear algebra, we know that the left null space of a matrix A is the set of all vectors $\mathbf{x}$ such that $\mathbf{x}^T A = \mathbf{0}$. As stated before, when $\mathbf{x} \in \mathbb{F}_2^l$ as it is here, $\mathbf{x}$ being in the left null space is equivalent to the corresponding rows of A summing to the zero vector. On the other hand, the right null space of a matrix A is the set of all vectors $\mathbf{x}$ such that $A\mathbf{x} = \mathbf{0}$. When $\mathbf{x} \in \mathbb{F}_2^k$, we now need to determine when the corresponding columns sum to the zero vector. Although we are still adding a subset of vectors, we no longer know the weight of those vectors so a Markov chain is no longer convenient. Instead, we will need to be careful of where the nonzero entries are. To do this, we will fix a vector, $\mathbf{x}$, of weight r and determine how many of the vectors, or how many of the rows of A, have a certain number of entries in common with $\mathbf{x}$. This calculation will then be used to determine the probability that the columns corresponding to the nonzero entries of the vector sum to zero.

Lemma 2.1 *Fix $\mathbf{x} \in \mathbb{F}_2^k$ such that the weight of $\mathbf{x}$ is r. Choose $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_l$ randomly with replacement from $\mathbb{F}_2^k$ so that the weight of each $\mathbf{v}_i$ is h. Then the probability that the product of $\mathbf{v}_i$ and $\mathbf{x}$ is 0 for all i is*

$$Pr(\mathbf{v}_1^T\mathbf{x} = \mathbf{v}_2^T\mathbf{x} = \ldots = \mathbf{v}_l^T\mathbf{x} = 0) = \Theta^l,$$

where

$$\Theta = \frac{1}{\binom{k}{h}} \sum_{i=0}^{\lfloor h/2 \rfloor} \binom{r}{2i}\binom{k-r}{h-2i}.$$

Proof: Let $\mathcal{H} = \{\mathbf{v} \in \mathbb{F}_2^k \mid wt(\mathbf{v}) = h\}$. Clearly,

$$|\mathcal{H}| = \binom{k}{h}.$$

Now let $\mathcal{W} = \{\mathbf{v} \in \mathcal{H} \mid \mathbf{v}^T\mathbf{x} = 0\}$. To find the desired probability, we will first find the probability that a random vector is in $\mathcal{W}$, or

$$Pr(\mathbf{v}^T\mathbf{x} = 0) = \frac{|\mathcal{W}|}{|\mathcal{H}|}.$$

We begin by determining $|\mathcal{W}|$. Note that in order for $\mathbf{v}^T\mathbf{x} = 0$, $\mathbf{v}$ and $\mathbf{x}$ must have an even number of 1's in common, say $2i$ 1's in common. From the r 1's in $\mathbf{x}$, there are $\binom{r}{2i}$ ways to choose these common bits, leaving $h - 2i$ 1's in $\mathbf{v}$. The locations of these remaining 1's must be chosen from the locations of the $k - r$ 0's in $\mathbf{x}$ in order for the vector product to be 0. There are $\binom{k-r}{h-2i}$ ways to do this. Thus the number of vectors in $\mathcal{H}$ with $2i$ 1's in common with $\mathbf{x}$ is

$$\binom{r}{2i}\binom{k-r}{h-2i}.$$

Since $\mathbf{v}$ and $\mathbf{x}$ have an even number of 1's in common, and the common number ranges from 0 to h, we find

$$|\mathcal{W}| = \sum_{i=0}^{\lfloor h/2 \rfloor} \binom{r}{2i}\binom{k-r}{h-2i}.$$

Then

$$Pr(\mathbf{v}^T\mathbf{x} = 0) = \Theta = \frac{1}{\binom{k}{h}} \sum_{i=0}^{\lfloor h/2 \rfloor} \binom{r}{2i}\binom{k-r}{h-2i}.$$

Finally, since each $\mathbf{v}_i$ is chosen independently from $\mathbb{F}_2^k$, then $Pr(\mathbf{v}^T\mathbf{x} = 0)$ for any $\mathbf{v}$ chosen is independent of the other vectors already chosen. Thus

$$\begin{aligned} Pr(\mathbf{v}_1^T\mathbf{x} = \mathbf{v}_2^T\mathbf{x} = \ldots = \mathbf{v}_l^T\mathbf{x} = 0) &= Pr(\mathbf{v}_1^T\mathbf{x} = 0)Pr(\mathbf{v}_2^T\mathbf{x} = 0)\cdots Pr(\mathbf{v}_l^T\mathbf{x} = 0) \\ &= [Pr(\mathbf{v}_1^T\mathbf{x} = 0)]^l \\ &= \Theta^l \end{aligned}$$

as claimed. □

Alternatively, the result of this lemma could be stated as $Pr(A\mathbf{x} = \mathbf{0}) = \Theta^l$ where A is the previously discussed matrix.

Now that we know the probability that a fixed vector is in the null space of a random set of l vectors, we can use this to find an expression for the expected size of the right null space of A. To use Lemma 2.1, we will need to separate the vectors

in $\mathbb{F}_2^k$ by weight. We let t be the dimension of the right null space of A and denote the expected size of the null space by $E(2^t)$.

Proposition 2.1 *Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_l \in \mathbb{F}_2^k$ be chosen randomly such that the weight of each $\mathbf{v}_i$, $1 \leq i \leq l$, is h and let A be the matrix with $\mathbf{v}_i^T$ as the i^{th} row. Let t be the dimension of the right null space of A. Then*

$$E(2^t) = \sum_{r=0}^{k} \binom{k}{r} \Theta^l$$

where

$$\Theta = \frac{1}{\binom{k}{h}} \sum_{i=0}^{\lfloor h/2 \rfloor} \binom{r}{2i} \binom{k-r}{h-2i}$$

as before.

Proof: Observe that there are 2^k vectors in $\mathbb{F}_2^k$ and $\binom{k}{r}$ vectors of weight r in $\mathbb{F}_2^k$. Let $\{\mathbf{x}_i\}_{i=1}^{2^k}$ be the set of all vectors in $\mathbb{F}_2^k$ and define the random variable Y_i to be

$$Y_i = \begin{cases} 1 & \text{if } A\mathbf{x}_i = \mathbf{0} \\ 0 & \text{otherwise.} \end{cases}$$

By defining Y_i as an indicator variable in this way, we can use it to determine the size of the right null space,

$$|\{\mathbf{x}_i | A\mathbf{x}_i = \mathbf{0}\}| = \sum_{i=1}^{2^k} Y_i.$$

By linearity of expectation, the expected size of the null space is given by a sum of expected values:

$$\begin{aligned} E(2^t) &= E\left(\sum_{i=1}^{2^k} Y_i\right) \\ &= \sum_{i=1}^{2^k} E(Y_i). \end{aligned}$$

Then using the usual definition of the expected value of a random variable and the definition of the null space,

$$\begin{aligned} E(2^t) &= \sum_{i=1}^{2^k} 1 \cdot Pr(A\mathbf{x}_i = \mathbf{0}) \\ &= \sum_{i=1}^{2^k} Pr(\mathbf{v}_1^T\mathbf{x}_i = \mathbf{v}_2^T\mathbf{x}_i = \ldots = \mathbf{v}_l^T\mathbf{x}_i = 0). \end{aligned}$$

Regrouping the vectors above, we can sum over the weight of the $\mathbf{x}_i$. We are then able to use the result of Lemma 2.1. Thus

$$\begin{aligned} E(2^t) &= \sum_{i=1}^{2^k} Pr(\mathbf{v}_1^T\mathbf{x}_i = \mathbf{v}_2^T\mathbf{x}_i = \ldots = \mathbf{v}_l^T\mathbf{x}_i = 0) \\ &= \sum_{r=0}^{k} \binom{k}{r} Pr(\text{vector of weight } r \text{ is in null space of } A) \\ &= \sum_{r=0}^{k} \binom{k}{r} \Theta^l. \end{aligned}$$

Hence

$$E(2^t) = \sum_{r=0}^{k} \binom{k}{r} \Theta^l,$$

where Θ is the probability that a vector of weight r is in the right null space of the matrix A. □

This gives us an exact expression for the expected size of the right null space of A.

We have seen that the left null space of A is important to the problem at hand. In fact, we have given a direct correlation between the vectors in the left null space and subsets of dependent vectors. So why are we interested in the right null space? The following algebraic connection between $E(2^s)$ and $E(2^t)$ gives the answer.

Fact 2.1 *Suppose A is an $l \times k$ binary matrix and let s be the dimension of the left null space and t the dimension of the right null space. Then*

$$E(2^t) = 2^{k-l}E(2^s).$$

Proof: Suppose r is the rank of A. Then $s = l - r$ and let $t = k - r$. Thus $t = k - l + s$, giving

$$2^t = 2^{k-l}2^s.$$

So $E(2^t) = E(2^{k-l}) = 2^{k-l}E(2^s)$. □

This equality, along with equation (2.1) and Proposition 2.1, gives a combinatorial proof of the following binomial identity. We also give an algebraic proof below.

Corollary 2.1

$$2^l \sum_{i=0}^{k} \binom{k}{i} \left(\frac{1}{\binom{k}{h}} \sum_{j=0}^{\lfloor h/2 \rfloor} \binom{i}{2j} \binom{k-i}{h-2j} \right)^l \tag{2.2}$$

$$= \sum_{i=0}^{k} \binom{k}{i} \left(1 + \sum_{j=0}^{h} (-1)^j \frac{\binom{i}{j}\binom{k-i}{h-j}}{\binom{k}{h}} \right)^l \tag{2.3}$$

Proof: This identity certainly looks complicated, but the proof is actually quite straightforward. First notice that (2.2) can be rewritten as

$$\sum_{i=0}^{k} \frac{\binom{k}{i}}{\binom{k}{h}^l} \left(2 \sum_{j=0}^{\lfloor h/2 \rfloor} \binom{i}{2j} \binom{k-i}{h-2j} \right)^l = \sum_{i=0}^{k} \frac{\binom{k}{i}}{\binom{k}{h}^l} \left(\binom{k}{h} + \sum_{j=0}^{h} (-1)^j \binom{i}{j} \binom{k-i}{h-j} \right)^l .$$

If we can show

$$2 \sum_{j=0}^{\lfloor h/2 \rfloor} \binom{i}{2j} \binom{k-i}{h-2j} = \binom{k}{h} + \sum_{j=0}^{h} (-1)^j \binom{i}{j} \binom{k-i}{h-j},$$

we will obtain the desired result. Recall Vandermonde's identity:

$$\binom{a+b}{d} = \sum_{c=0}^{d} \binom{a}{c} \binom{b}{d-c}.$$

Replacing $\binom{k}{h}$ with the appropriate expression and adding the two sums gives the result.

$$\begin{aligned} \binom{k}{h} + \sum_{j=0}^{h} (-1)^j \binom{i}{j} \binom{k-i}{h-j} &= \sum_{j=0}^{h} \binom{i}{j} \binom{k-i}{h-j} + \sum_{j=0}^{h} (-1)^j \binom{i}{j} \binom{k-i}{h-j} \\ &= 2 \sum_{j=0}^{\lfloor h/2 \rfloor} \binom{i}{2j} \binom{k-i}{h-2j}. \end{aligned}$$

Hence (2.2) is true. □

Although we could find asymptotics for $E(2^t)$, this corollary tells us it is not necessary to do so. Theorem 2.1 gives a lower bound on the threshold value for the size of the left null space. This can be used in conjunction with Fact 2.1 to derive

a lower bound on a threshold value for the right null space. On one side of the threshold, $E(2^s)$ tends to 1 while $E(2^t)$ approaches 2^{k-l}. On the other side of the threshold, $E(2^s)$ as well as $E(2^t)$ go to infinity.

The relationship between the expected sizes of the left and right null space is particularly useful as it gives another expression with which to analyze and derive a threshold theorem. Although we don't need to find asymptotics for both expressions, for some probability models it may be difficult to obtain one for $E(2^s)$ or $E(2^t)$. If we are able to find one of these, the second follows by multiplying by the appropriate factor of 2. In addition, we can always use the simpler expression even if it is not the desired one for our application.

For our particular application, the size of the left null space is more useful to us as it is directly related to the question. However, we will be able to use this connection between the left and right null space as well as the idea behind proving Lemma 2.1 in the next chapter. There we will extend these results to vectors that do not have fixed weight and are chosen under a more general probability model.

CHAPTER 3

Vectors Under a Probability Distribution

3.1 Introduction

We have seen one type of generalization for the problem so far; Cooper considered vectors over Abelian groups in addition to finite fields. We saw that similar threshold results were found for this case. In this chapter and the next, we are interested in a different generalization of the question. We will continue to work over $\mathbb{F}_2$, but we will remove the restriction that the random vectors have fixed weight. Instead, we allow the weight of each vector to vary by assigning to each entry of a vector $\mathbf{v}$ a probability of having a 1 in that position. In other words,

$$Pr(\mathbf{v}[j] = 1) = \alpha_j.$$

The variables and set up will be the same as before: choose l vectors of length k and let A be the matrix having the i^{th} vector chosen as its i^{th} row. Let s be the dimension of the left null space of A and t the dimension of the right null space. Recall that we want to know how many vectors we need to choose to have a high probability that the vectors are dependent. In this chapter we will find exact expressions for the expected size of both the left and right null space.

3.2 The Right Null Space: Method 1

In Chapter 2 we found an expression for $E(2^t)$, the expected size of the right null space of A where the rows of A had fixed weight h. We first calculated the probability that a fixed vector, $\mathbf{x}$, with weight r was in the right null space by recognizing the fact that $\mathbf{x}$ and each row of A had to have an even number of 1's in common. We will follow the same outline in this chapter and begin by finding the probability that a fixed vector of weight r is in the null space.

With vectors of fixed weight, finding this probability was merely a matter of finding the number of ways that $\mathbf{x}$ and each vector $\mathbf{v}_i$ could have an even number

of 1's in common and then dividing by the total number of vectors in the space. With the new probability model, however, the matter is more complicated. Since the probability of having a 1 changes according to position, we must know where the 1's are in $\mathbf{x}$. The following lemma is similar to Lemma 2.1, but notice that we now specify the location of the 1's in $\mathbf{x}$.

Lemma 3.1 *Fix* $\mathbf{x} \in \mathbb{F}_2^k$ *with* $wt(\mathbf{x}) = r$ *and suppose* $\mathbf{x}[j_1] = \mathbf{x}[j_2] = \cdots = \mathbf{x}[j_r] = 1$. *Let* $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_l \in \mathbb{F}_2^k$ *with* $Pr(\mathbf{v}_i[j] = 1) = \alpha_j$ *for all* i. *Then*

$$Pr(\mathbf{v}_1^T\mathbf{x} = \mathbf{v}_2^T\mathbf{x} = \cdots = \mathbf{v}_l^T\mathbf{x} = 0) = \Theta_r^l$$

where

$$\Theta_r = \sum_{m=0}^{\lfloor r/2 \rfloor} \sum_{s_1=1}^{k} \sum_{s_2=s_1+1}^{k} \cdots \sum_{s_{2m}=s_{2m-1}+1}^{k} \prod_{\substack{t=1 \\ t \neq s_1,\ldots,s_{2m}}}^{r} \alpha_{j_{s_1}} \alpha_{j_{s_2}} \cdots \alpha_{j_{s_{2m}}} (1 - \alpha_{j_t}).$$

Proof: We will first find this probability for one vector $\mathbf{v} \in \mathbb{F}_2$, i.e.

$$Pr(\mathbf{v}^T\mathbf{x} = 0).$$

Assume $\mathbf{v}$ is chosen according to the α_j probability model, that is,

$$Pr(\mathbf{v}[j] = 1) = \alpha_j.$$

As in Lemma 2.1, $\mathbf{x}$ and $\mathbf{v}$ must have an even number of ones in common, so

$$Pr(\mathbf{v}^T\mathbf{x} = 0) = Pr(\mathbf{v} \text{ has } 2m \text{ ones in common with } \mathbf{x}).$$

If $\mathbf{v}$ has no ones in common with $\mathbf{x}$, then this is the probability that $\mathbf{v}$ has a 0 in each position where $\mathbf{x}$ has a 1. Thus

$$Pr(\mathbf{v} \text{ has 0 ones in common with } \mathbf{x}) = \prod_{t=1}^{r} (1 - \alpha_{j_t}).$$

If $\mathbf{v}$ has 2 ones in common with $\mathbf{x}$, then we need the probability that $\mathbf{v}[p] = \mathbf{v}[q] = 1$ for any pair $p, q \in \{j_1, j_2, \ldots, j_r\}$, $p \neq q$, and $\mathbf{v}[w] = 0$ for all other $w \in \{j_1, j_2, \ldots, j_r\}$, $w \neq p, q$. So

$$Pr(\mathbf{v} \text{ has 2 ones in common with } \mathbf{x}) = \sum_{s_1=1}^{r} \sum_{s_2=s_1+1}^{r} \prod_{\substack{t=1 \\ t \neq s_1, s_2}}^{r} \alpha_{j_{s_1}} \alpha_{j_{s_2}} (1 - \alpha_{j_t}).$$

The two sums run through all ordered pairs of indices in $\{j_1, j_2, \ldots, j_r\}$ and the product gives the probability that the remaining terms are 0. We continue this process to find that

$$\begin{aligned} &Pr(\mathbf{v} \text{ has } 2m \text{ ones in common with } \mathbf{x}) \\ &= \sum_{s_1=1}^{r} \sum_{s_2=s_1+1}^{r} \cdots \sum_{s_{2m}=s_{2m-1}+1}^{r} \prod_{\substack{t=1 \\ t \neq s_1, \ldots, s_{2m}}}^{r} \alpha_{j_{s_1}} \alpha_{j_{s_2}} \cdots \alpha_{j_{s_{2m}}} (1 - \alpha_{j_t}). \end{aligned}$$

The embedded sums indicate we are considering all possible ordered $2m-$tuples of 1's. Now, in order to have $\mathbf{v}^T\mathbf{x} = \mathbf{0}$, $\mathbf{v}$ and $\mathbf{x}$ must have $2m$ common 1's, where $0 \leq 2m \leq r$. Thus

$$Pr(\mathbf{v}^T\mathbf{x} = 0) = \sum_{m=0}^{\lfloor r/2 \rfloor} \sum_{s_1=1}^{r} \sum_{s_2=s_1+1}^{r} \cdots \sum_{s_{2m}=s_{2m-1}+1}^{r} \prod_{\substack{t=1 \\ t \neq s_1, \ldots, s_{2m}}}^{r} \alpha_{j_{s_1}} \alpha_{j_{s_2}} \cdots \alpha_{j_{s_{2m}}} (1 - \alpha_{j_t}).$$

Set $\Theta_r = Pr(\mathbf{v}^T\mathbf{x} = 0)$. Since the $\mathbf{v}_i$ are independent of each other and Θ_r is the same for each $\mathbf{v}_i$, $1 \leq i \leq l$,

$$Pr(\mathbf{v}_1^T\mathbf{x} = \mathbf{v}_2^T\mathbf{x} = \cdots = \mathbf{v}_l^T\mathbf{x} = 0) = \Theta_r^l.$$

□

With this lemma we can find the probability that a given vector is in the null space of A, as long as we know exactly what that vector is. When computing $E(2^t)$, we will construct a sum over all 2^k vectors in $\mathbb{F}_2^k$, as we did in Chapter 2. There, it was very convenient to regroup the terms and sum instead over the weight of the vectors. Lemma 3.1 doesn't allow us to do this. Therefore, we would like to generalize the result to all $\mathbf{x} \in \mathbb{F}_2^k$ with weight r. We do this in the following lemma.

Lemma 3.2 *Let $\mathbf{x} \in \mathbb{F}_2^k$ with weight $r > 0$. Let $\mathbf{v}_1, \mathbf{v}_2, \ldots \mathbf{v}_l \in \mathbb{F}_2^k$. Then*

$$Pr(\mathbf{v}_1^T\mathbf{x} = \mathbf{v}_2^T\mathbf{x} = \cdots = \mathbf{v}_l^T\mathbf{x} = 0) = \Psi_r^l$$

where

$$\Psi_r = \sum_{m=0}^{\lfloor r/2 \rfloor} \sum_{s_1=1}^{k} \sum_{s_2=s_1+1}^{k} \cdots \sum_{s_{2m}=s_{2m-1}+1}^{k} \sum_{\substack{t_1=1 \\ t_1 \neq s_i}}^{k} \sum_{\substack{t_2=t_1+1 \\ t_2 \neq s_i}}^{k} \cdots \sum_{\substack{t_{r-2m}=t_{r-2m-1}+1 \\ t_{r-2m} \neq s_i}}^{k} \alpha_{s_1}\alpha_{s_2}\cdots\alpha_{s_{2m}}(1-\alpha_{t_1})(1-\alpha_{t_2})\cdots(1-\alpha_{t_{r-2m}}).$$

Proof: For this proof, we want to enumerate the probability for all possible vectors $\mathbf{x}$ of weight r from $\mathbb{F}_2^k$. Again, $\mathbf{x}$ and $\mathbf{v}$, a vector generated under the probability model, must have an even number of 1's in common. As in Lemma 3.1, the probability of having $2m$ common 1's is

$$\sum_{s_1=1}^{k} \cdots \sum_{s_{2m}=s_{2m-1}+1}^{k} \alpha_{s_1}\cdots\alpha_{s_{2m}},$$

counting all possible ordered $2m-$tuples in $\mathbf{v}$. The remaining $r-2m$ 1's in $\mathbf{x}$ must correspond to 0's in $\mathbf{v}$, thus we must have $r-2m$ 0's in $\mathbf{v}$ in addition to the $2m$ 1's. We account for all possible combinations in

$$\sum_{\substack{t_1=1 \\ t_1 \neq s_i}}^{k} \cdots \sum_{\substack{t_{r-2m}=t_{r-2m-1}+1 \\ t_{r-2m} \neq s_i}}^{k} (1-\alpha_{t_1})\cdots(1-\alpha_{t_{2m}}).$$

Combining these two expressions, we find the probability of having $2m$ common 1's, $0 \leq m \leq \lfloor r/2 \rfloor$, to be

$$Pr(\mathbf{v}^T\mathbf{x}=0) = \sum_{m=0}^{\lfloor r/2 \rfloor} \sum_{s_1=1}^{k} \sum_{s_2=s_1+1}^{k} \cdots \sum_{s_{2m}=s_{2m-1}+1}^{k} \sum_{\substack{t_1=1 \\ t_1 \neq s_i}}^{k} \sum_{\substack{t_2=t_1+1 \\ t_2 \neq s_i}}^{k} \cdots \sum_{\substack{t_{r-2m}=t_{r-2m-1}+1 \\ t_{r-2m} \neq s_i}}^{k} \alpha_{s_1}\alpha_{s_2}\cdots\alpha_{s_{2m}}(1-\alpha_{t_1})\cdots(1-\alpha_{t_{r-2m}}).$$

Set $\Psi_r = Pr(\mathbf{v}^T\mathbf{x}=0)$. Since $\mathbf{v}_1,\ldots,\mathbf{v}_l$ are independent,

$$Pr(\mathbf{v}_1^T\mathbf{x} = \mathbf{v}_2^T\mathbf{x} = \cdots = \mathbf{v}_l^T\mathbf{x} = 0) = \Psi_r^l.$$

□

Before continuing, let's write out the first few terms of Ψ_r to get a handle on what the summands looks like. When $m=0$, the summand is not empty, rather

we find that it reduces to the sums indexed by t, or

$$\sum_{t_1=1}^{k} \cdots \sum_{t_r=t_{r-1}+1}^{k} (1-\alpha_{t_1}) \cdots (1-\alpha_{t_r}). \tag{3.1}$$

Since $\mathbf{v}$ must have a 0 in each position corresponding to a 1 in $\mathbf{x}$, we see that the summand gives the probability that this happens for any $\mathbf{x}$ of weight r, as it should. For example, if $k = 3$ and $r = 2$, there are $\binom{3}{2}$ vectors of weight 2 that may be in the null space. Then (3.1) becomes

$$(1-\alpha_1)(1-\alpha_2) + (1-\alpha_1)(1-\alpha_3) + (1-\alpha_2)(1-\alpha_3),$$

giving the probability of having the appropriate vectors $\mathbf{v}$ as rows in A. When $m = 1$, there are 2 common 1's between the rows of A and $\mathbf{x}$ of weight r while the remaining $r-2$ 1's in $\mathbf{x}$ correspond to 0's in $\mathbf{v}$. Then the summand is

$$\sum_{s_1=1}^{k} \sum_{s_2=s_1+1}^{k} \sum_{\substack{t_1=1 \\ t_1 \neq s_1,s_2}}^{k} \cdots \sum_{\substack{t_{r-2}=t_{r-3}+1 \\ t_{r-2} \neq s_1,s_2}}^{k} \alpha_{s_1}\alpha_{s_2}(1-\alpha_{t_1}) \cdots (1-\alpha_{t_{r-2}}). \tag{3.2}$$

For example, suppose $k = 4$ and $r = 3$. Then (3.2) is

$$\begin{aligned} &\alpha_1\alpha_2(1-\alpha_3) + \alpha_1\alpha_2(1-\alpha_4) + \alpha_1\alpha_3(1-\alpha_2) + \alpha_1\alpha_3(1-\alpha_4) \\ &+\alpha_2\alpha_3(1-\alpha_1) + \alpha_2\alpha_3(1-\alpha_4) + \alpha_2\alpha_4(1-\alpha_1) + \alpha_2\alpha_4(1-\alpha_3). \end{aligned}$$

This gives the probability of having any rows in A that correspond to vectors of weight 3 and having 2 1's in common.

We now have the probability that a fixed vector of weight r is in the right null space of A. The advantage of this lemma over the last is that we can now use this probability to find $E(2^t)$, using the same method as in Chapter 2.

Theorem 3.1

$$E(2^t) = 1 + \sum_{r=1}^{k} \Psi_r^l$$

where Ψ_r is as in Lemma 3.2.

Proof: Assume A is the $l \times k$ matrix with $\mathbf{v}_i$ as its i^{th} row. We wish to count the expected number of vectors from $\mathbb{F}_2^k$ in the right null space of A. We order the

vectors $\mathbf{x}_i \in \mathbb{F}_2^k$ and define the random variable Y_i to be

$$Y_i = \begin{cases} 1 & \text{if } A\mathbf{x}_i = \mathbf{0} \\ 0 & \text{otherwise.} \end{cases}$$

By linearity of expectation we find

$$E(2^t) = E\left(\sum_{i=1}^{2^k} Y_i\right) = \sum_{i=1}^{2^k} E(Y_i).$$

Substituting for $E(Y_i)$ and regrouping the terms by weight of $\mathbf{x}_i$ yields

$$\begin{aligned} E(2^t) &= \sum_{i=1}^{2^k} E(Y_i) \\ &= \sum_{i=1}^{2^k} Pr(A\mathbf{x}_i = \mathbf{0}) \\ &= \sum_{r=0}^{k} Pr(A\mathbf{x}_i = \mathbf{0} | \mathbf{x}_i \text{ has weight } r) \\ &= 1 + \sum_{r=1}^{k} Pr(A\mathbf{x}_i = \mathbf{0} | \mathbf{x}_i \text{ has weight } r). \end{aligned}$$

Finally, we replace the probability in the last line with the result from Lemma 3.2 to get

$$E(2^t) = 1 + \sum_{r=1}^{k} \Psi_r^l.$$

□

We now have an expression for the expected number of vectors in the right null space of A for a general probability model. Therefore the expected size of the left null space is

$$E(2^s) = 2^{l-k} E(2^t).$$

Finding asymptotics for $E(2^s)$ for a specific probability model would lead to the lower bound for l and the the threshold theorem we are searching for. However, the expression we have is clearly not easy to work with. The number and variability of embedded sums alone is enough to prompt us to find a more elegant expression to estimate.

3.3 The Right Null Space: Method 2

To find a different expression, we need a few preliminary lemmas. In Lemma 3.1, we specified the location of the 1's in the vector $\mathbf{x}$. There we saw that having a zero vector product depended largely on the behavior of the randomly generated vectors in those locations. In the next lemma, we will consider a vector of length t where every entry is a 1. We will then find the vector product of this vector with another generated by a probability model and give an expression for the probability that the product is zero.

Lemma 3.3 *Let* $\mathbf{b} = (b_1, b_2, \ldots, b_t)$ *where* $Pr(b_i = 1) = \beta_i$ *and let* $\mathbf{y} = \mathbf{1} \in \mathbb{F}_2^t$ *be the vector of all ones. Then*

$$Pr(\mathbf{b}^T\mathbf{y} = 0) = \frac{1}{2} + \frac{1}{2}\prod_{i=1}^{t}(1 - 2\beta_i).$$

Proof: Observe that

$$\mathbf{b}^T\mathbf{y} = \sum_{i=1}^{t} b_i y_i = \sum_{i=1}^{t} b_i.$$

Now let $P_t = Pr(\mathbf{b}^T\mathbf{y} = 0)$. We can write P_t recursively as follows.

$$\begin{aligned}
P_t &= Pr\left(\sum_{i=1}^{t} b_i y_i = 0\right) \\
&= Pr\left(\sum_{i=1}^{t} b_i = 0\right) \\
&= Pr\left(\sum_{i=1}^{t-1} b_i = 0\right) Pr(b_t = 0) + \left(\sum_{i=1}^{t-1} b_i = 1\right) Pr(b_t = 1) \\
&= P_{t-1}(1 - \beta_t) + (1 - P_{t-1})\beta_t \\
&= \beta_t + (1 - 2\beta_t)P_{t-1}
\end{aligned}$$

To find a closed form for P_t, we need to know P_0. When $t = 0$, $\mathbf{b}^T\mathbf{y}$ is an empty sum and therefore is 0. Thus $P_0 = Pr(\mathbf{b}^T\mathbf{y} = 0) = 1$, giving

$$P_1 = 1 - \beta_1 = \frac{1}{2} + \frac{1}{2}(1 - 2\beta_1).$$

This also verifies the definition $P_0 = 1$ since $\mathbf{b}^T\mathbf{y} = 0$ if and only if $\mathbf{b} = \mathbf{0}$ when $t = 1$. The probability of this happening is $1 - \beta_1$. We then use the recursive definition of

P_t to find

$$\begin{aligned} P_2 &= \beta_2 + (1-2\beta_2)P_1 \\ &= \beta_2 + (1-2\beta_2)\left(\frac{1}{2} + \frac{1}{2}(1-2\beta_1)\right) \\ &= \frac{1}{2} + \frac{1}{2}(1-2\beta_1)(1-2\beta_2). \end{aligned}$$

Now assume that

$$P_m = \frac{1}{2} + \frac{1}{2}(1-2\beta_1)(1-2\beta_2)\cdots(1-2\beta_m).$$

This leads to

$$\begin{aligned} P_{m+1} &= \beta_{m+1} + (1-2\beta_{m+1})P_m \\ &= \beta_{m+1} + (1-2\beta_{m+1})\left(\frac{1}{2} + \frac{1}{2}(1-2\beta_1)(1-2\beta_2)\cdots(1-2\beta_m)\right) \\ &= \frac{1}{2} + \frac{1}{2}(1-2\beta_1)(1-2\beta_2)\cdots(1-2\beta_m)(1-2\beta_{m+1}). \end{aligned}$$

With this we find

$$P_t = \frac{1}{2} + \frac{1}{2}\prod_{i=1}^{t}(1-2\beta_i)$$

by induction. □

To use this result in finding $E(2^t)$, we must generalize the lemma so that $\mathbf{y}$ is no longer the vector of all 1's, rather we want it to have length k with zero entries as well as 1's. We will again have to specify where the 1's are in $\mathbf{y}$ since the probability model of the random vector is so dependent on location. However, we will be able to use Lemma 3.3 whose result gives a much nicer closed form for the probability than the previous embedded sums. Since we are now considering vectors of length k, we return to vectors generated under the α_j probability model.

Corollary 3.1 *Let* $\mathbf{v} = (v_1, v_2, \ldots, v_k)$ *such that* $Pr(\mathbf{v}_j = 1) = \alpha_j$. *Let* $\mathbf{y}_S = (y_1, y_2, \ldots, y_k)$ *where* $S = \{j_1, j_2, \ldots, j_t\} \subseteq [k]$ *and* $y_i = 1$ *if and only if* $i \in S$. *Then*

$$Pr(\mathbf{v}^T\mathbf{y}_S = 0) = \frac{1}{2} + \frac{1}{2}\prod_{j\in S}(1-2\alpha_j).$$

Proof: Again observe that

$$\mathbf{v}^T\mathbf{y}_S = \sum_{i=1}^{k} v_i y_i = \sum_{j\in S} v_j y_j = \sum_{j\in S} v_j.$$

We see that $\mathbf{v}^T\mathbf{y}_S$ is equivalent to summing the terms of $\mathbf{v}$ corresponding to the 1's in $\mathbf{y}_S$. Therefore $\mathbf{v}$ and $\mathbf{Y}_S$ are reduced to the type of vectors seen in Lemma 3.3. The result immediately follows. □

We are now in a position to find the probability that a fixed vector is in the right null space of the matrix A. We know the probability that one row of A times the fixed vector $\mathbf{y}_S$ is zero. Since the vectors are chosen independently, the probability this is true for each row of A independent of what happens with the other rows. Therefore

$$\begin{aligned} Pr(A\mathbf{y}_S = 0) &= P_S^l \\ &= \left(\frac{1}{2} + \frac{1}{2}\prod_{j\in S}(1-2\alpha_j)\right)^l \\ &= 2^{-l}\sum_{w=0}^{l}\binom{l}{w}\prod_{j\in S}(1-2\alpha_j)^w \end{aligned}$$

by the binomial theorem. Finally, we have reached the probability we need in order to find a new expression for $E(2^t)$.

Theorem 3.2

$$E(2^t) = 2^{-l}\sum_{w=0}^{l}\binom{l}{w}\prod_{j=1}^{k}(1+(1-2\alpha_j)^w)$$

Proof: In order to find $E(2^t)$, we must add P_S^l for all possible subsets S of $[k]$, size 0 to k. This gives

$$\begin{aligned} E(2^t) &= \sum_S P_S^l \\ &= 2^{-l}\sum_S\sum_{w=0}^{l}\binom{l}{w}\prod_{j\in S}(1-2\alpha_j)^w \\ &= 2^{-l}\sum_{w=0}^{l}\binom{l}{w}\sum_S\prod_{j\in S}(1-2\alpha_j)^w. \end{aligned}$$

Consider $\sum_S\prod_{j\in S}(1-2\alpha_j)^w$. Since S runs through all possible subsets of $\{1,2,\ldots,k\}$, this is the sum of all possible products of $(1-2\alpha_j)^w$, where $1 \le j \le k$. By the

binomial therem, when we sum over all of the subsets we get $\prod_{j=1}^{k}(1+(1-2\alpha_j)^w)$, thus

$$\begin{aligned} E(2^t) &= 2^{-l}\sum_{w=0}^{l}\binom{l}{w}\sum_{S}\prod_{j\in S}(1-2\alpha_j)^w \\ &= 2^{-l}\sum_{w=0}^{l}\binom{l}{w}\prod_{j=1}^{k}(1+(1-2\alpha_j)^w)\,. \end{aligned}$$

□

This gives a new expression for $E(2^t)$ that is more manageable than the first. We point out here that the terms of the sum have no combinatorial interpretation when discussing the right null space of A, but are merely the result of rewriting the expression.

3.4 The Left Null Space

At this point, we can use Theorem 3.2 to find the expected size of the left null space. By Fact 2.1,

$$E(2^s) = 2^{-k}\sum_{r=0}^{l}\binom{l}{r}\prod_{j=1}^{k}(1+(1-2\alpha_j)^r). \tag{3.3}$$

This is is actually the expression we want to estimate to find a threshold theorem since it more directly relates to our question. However, it will be instructive to first construct the expected size of the left null space. The approach will be as before: fix a vector $\mathbf{x}$ and determine the probability $\mathbf{x}$ is in the left null space of A. Since the columns of A are independent of each other, we can write this probability as

$$Pr(\mathbf{x}^T A = \mathbf{0}) = \prod_{j=1}^{k} Pr(\mathbf{x}^T\mathbf{a}_j = 0),$$

where $\mathbf{a}_j$ is the j^{th} column of A. From this equation we see that the desired probability only relies on how $\mathbf{x}$ interacts with the individual columns of A. Since each entry in the j^{th} column has probability α_j of being a 1, we can concentrate on one column of A and then extend our results to the entire matrix. Thus we wish to compute

$$Pr(\mathbf{x}^T\mathbf{a}_j = 0).$$

We will again consider the number of common 1's to find this probability.

Fix the vector $\mathbf{x}$ and a probability α. Choose $\mathbf{a} = (a_1, a_2, \ldots, a_l)^T$ such that $Pr(a_i = 1) = \alpha$. Fixing α and choosing $\mathbf{a}$ in this way corresponds to fixing a column of A to determine the probability that we're interested in. Since $\mathbf{x}$ and $\mathbf{a}$ must have an even number of 1's in common, we need to know the weight of $\mathbf{x}$. For instance, if the weight of $\mathbf{x}$ is 0, $\mathbf{x}$ is the zero vector and $\mathbf{x}^T\mathbf{a} = 0$, independent of α. Thus

$$Pr(\mathbf{x}^T\mathbf{a} = 0) = 1.$$

If $wt(\mathbf{x}) = 1$, then $\mathbf{a}$ must have a 0 in the location corresponding to the 1 in $\mathbf{x}$ while the other entries of $\mathbf{a}$ may be either 0 or 1. Thus

$$Pr(\mathbf{x}^T\mathbf{a} = 0) = 1 - \alpha.$$

Now suppose $wt(\mathbf{x}) = 2$. In order to have $\mathbf{x}^T\mathbf{a} = 0$, then the two ones in $\mathbf{x}$ must be paired with two 1's from $\mathbf{a}$ or with two 0's, since we are working over $\mathbb{F}_2$. Since the probability that the vectors have two 1's in common is α^2 and the probability that $\mathbf{a}$ has two 0's where $\mathbf{x}$ has 1's is $(1-\alpha)^2$, we see that

$$Pr(\sum_{i=1}^{l} x_i a_i = 0) = (1-\alpha)^2 + \alpha^2.$$

If $wt(\mathbf{x}) = 3$, then $\mathbf{x}$ and $\mathbf{a}$ can again either have no 1's in common or two. If there are two common 1's, then there are $\binom{3}{2}$ ways to choose the location of the 1's in $\mathbf{a}$. Thus

$$Pr(\sum_{i=1}^{l} x_i a_i = 0) = (1-\alpha)^3 + \binom{3}{2}\alpha^2(1-\alpha).$$

Similarly, when $wt(\mathbf{x}) = 4$, then

$$Pr(\sum_{i=1}^{l} x_i a_i = 0) = (1-\alpha)^4 + \binom{4}{2}\alpha^2(1-\alpha)^2 + \alpha^4.$$

A pattern is now becoming evident. The key to finding these probabilities is exactly what we have used before. Since addition is over $\mathbb{F}_2$, the number of 1's that $\mathbf{x}$ and $\mathbf{a}$ have in common must be even. We use this in the following proof.

Lemma 3.4 *Fix $\mathbf{x} \in \mathbb{F}_2^l$ with weight r. Fix α and let $\mathbf{a} = (a_1, a_2, \ldots, a_l)$ such that $Pr(a_i = 1) = \alpha$. Then*

$$Pr(\mathbf{x}^T\mathbf{a} = 0) = \frac{1 + (1-2\alpha)^r}{2}.$$

Proof: In order to have $\mathbf{x}^T\mathbf{a} = 0$ over $\mathbb{F}_2$, $\mathbf{x}$ and $\mathbf{a}$ must have an even number of ones in common, i.e. they can have no 1's in common, two 1's in common, four 1's in common, and so on. Suppose $\mathbf{x}$ and $\mathbf{a}$ have $2m$ common 1's, where $0 \leq m \leq \lfloor r/2 \rfloor$. Then $\mathbf{a}$ must have 0's in the locations corresponding to the $r - 2m$ remaining 1's in $\mathbf{x}$. Since there are $\binom{r}{2m}$ ways to choose the locations of the common 1's in $\mathbf{a}$, the probability that $\mathbf{x}^T\mathbf{a} = 0$ when $\mathbf{x}$ and $\mathbf{a}$ have $2m$ 1's in common is

$$\binom{r}{2m}\alpha^{2m}(1-\alpha)^{r-2m}.$$

Since $0 \leq m \leq \lfloor r/2 \rfloor$, we have

$$Pr(\mathbf{x}^T\mathbf{a} = 0) = (1-\alpha)^r + \binom{r}{2}\alpha^2(1-\alpha)^{r-2} + \cdots + \binom{r}{2\lfloor r/2 \rfloor}\alpha^{2\lfloor r/2 \rfloor}(1-\alpha)^{r-2\lfloor r/2 \rfloor}.$$

The last term in the sum is α^r if r is even and $\alpha^{r-1}(1-\alpha)$ if r is odd. We use the binomial theorem to find a closed form for this probability.

$$\begin{aligned}
Pr\left(\sum_{i=1}^{l} x_i a_i = 0\right) &= (1-\alpha)^r + \binom{r}{2}\alpha^2(1-\alpha)^{r-2} + \ldots \\
&= \frac{1}{2}\left(\sum_{j=0}^{r}\binom{r}{j}\alpha^j(1-\alpha)^{r-j} + \sum_{j=0}^{r}(-1)^j\binom{r}{j}\alpha^j(1-\alpha)^{r-j}\right) \\
&= \frac{1}{2}\left(((1-\alpha)+\alpha)^r + ((1-\alpha)-\alpha)^r\right) \\
&= \frac{1+(1-2\alpha)^r}{2}
\end{aligned}$$

Thus the claim is true. □

In this lemma, we considered only one column of the matrix A. In order to find the expected size of the left null space of A, we must know the probability that the vector $\mathbf{x}$ is in the left null space, $Pr(\mathbf{x}^T A = \mathbf{0})$. To find the matrix product $\mathbf{x}^T A$, we simply multiply $\mathbf{x}$ by each column of A. By definition, the probability that an entry in the j^{th} column is 1 is α_j, so Lemma 3.4 gives

$$Pr(\mathbf{x}^T\mathbf{a}_j = 0) = \frac{1 + (1 - 2\alpha_j)^r}{2}$$

where $\mathbf{a}_j$ is the j^{th} column and $\mathbf{x}$ has weight r. Finally, since each column of A is independent of the others, the probability that $\mathbf{x}$ is in the left null space is the product of the probabilities that $\mathbf{x}$ times each column is 0. We have just shown the following lemma.

Lemma 3.5 *Fix $\mathbf{x} \in \mathbb{F}_2^l$ with weight r. Let $A = (a_{ij})$, where $Pr(a_{ij} = 1) = \alpha_j$. Then*

$$Pr(\mathbf{x}^T A = \mathbf{0}) = \prod_{j=1}^{k} \frac{1 + (1 - 2\alpha_j)^r}{2}.$$

This lemma gives the probability that a given vector of weight r is in the left null space of A. Notice the similarity to the w^{th} term of $E(2^t)$ found earlier. With this probability, we can now use linearity of expectation to find the expected size of the left null space.

Theorem 3.3

$$E(2^s) = \sum_{r=0}^{l} \binom{l}{r} \prod_{j=1}^{k} \frac{1 + (1 - 2\alpha_j)^r}{2}$$

Proof: Let $\{\mathbf{x}_i\}_{i=1}^{2^l}$ be the set of all vectors in $\mathbb{F}_2^l$ and define the random variable Y_i to be

$$Y_i = \begin{cases} 1 & \text{if } \mathbf{x}_i^T A = \mathbf{0} \\ 0 & \text{otherwise.} \end{cases}$$

Then we have

$$|\{\mathbf{x}_i | \mathbf{x}_i^T A = \mathbf{0}\}| = \sum_{i=0}^{2^l} Y_i,$$

and, by linearity of expectation,

$$\begin{aligned} E(2^s) &= E\left(\sum_{i=0}^{2^l} Y_i\right) \\ &= \sum_{i=0}^{2^l} E(Y_i) \\ &= \sum_{i=0}^{2^l} Pr(\mathbf{x}_i^T A = \mathbf{0}). \end{aligned}$$

Regrouping the vectors and summing over the weight of the $\mathbf{x}_i$, we use the probability found in Lemma 3.5 that a fixed vector of weight r is in the left null space:

$$\begin{aligned} E(2^s) &= \sum_{i=0}^{2^l} Pr(\mathbf{x}_i^T A = \mathbf{0}) \\ &= \sum_{r=0}^{l} \binom{l}{r} Pr(\text{vector of weight } r \text{ is in left null space of } A) \\ &= \sum_{r=0}^{l} \binom{l}{r} \prod_{j=1}^{k} \frac{1+(1-2\alpha_j)^r}{2}. \end{aligned}$$

Hence

$$E(2^s) = \sum_{r=0}^{l} \binom{l}{r} \prod_{j=1}^{k} \frac{1+(1-2\alpha_j)^r}{2}$$

is the expected size of the left null space of A. □

Observe that we have verified equation (3.3), that is

$$E(2^s) = 2^{l-k} E(2^t).$$

In fact, unlike the results with fixed weight vectors, we have found the same expression for both $E(2^s)$ and $2^{l-k}E(2^t)$. Additionally, in finding the size of the left null space, we have also found a combinatorial interpretation for the terms of the sum. Here, the index r represents the weight of the vectors and the summand is the probability that a vector of weight r is in the left null space, or the probability that a subset of r vectors, $\mathbf{v}_i$, sum to the zero vector. To find a threshold theorem, we must find when $E(2^s)$ is close to 1 so that we only expect one vector in the left null space, the zero vector. Since the zero vector is in the null space with probability 1, the 0^{th} term of $E(2^s)$ should be 1. This is easily verified by the expression given. Therefore, the remaining terms must contribute a negligible amount to the sum, implying the probability that there are vectors of weight $r > 0$ in the left null space is very small. In Chapter 4, we will use this idea to analyze a specific probability model.

CHAPTER 4

Exploring a Probability Model

4.1 Introduction

Dependency among vectors is a monotone property: if a set of vectors is dependent, adding one more vector to the set will not change that fact. We also expect that the more vectors there are in a set, the more likely they are to be dependent. In fact, as soon as the number of vectors exceeds the length of the vectors, we are assured a dependency. Thus it is reasonable to expect to find threshold behavior in any set of random vectors when considering dependence, that is, we expect to be able to find a threshold function for dependence. We will be searching for a function, $l^*(k)$, such that

(i) if $l(k)/l^*(k) \to 0$, then $l = l(k)$ vectors are almost surely independent, and

(ii) if $l(k)/l^*(k) \to \infty$, then $l = l(k)$ vectors are almost surely dependent.

This threshold behavior is illustrated by the graph in Figure 4.1. The position on the plot marked by l_m shows where we might begin to see the probability of dependence approaching 0. The position marked by l_M shows a value where the probability of dependence is approaching 1.

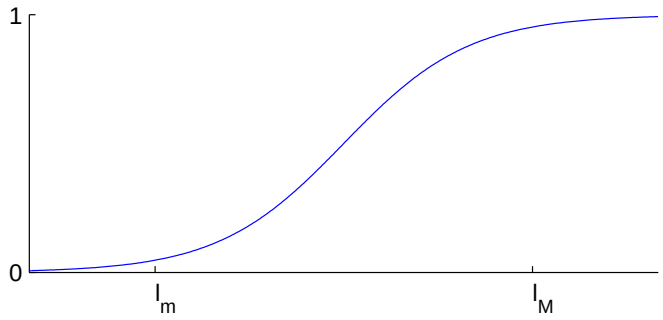

Figure 4.1 General Threshold Graph

The desire with a threshold property is to determine how sharp the threshold is. If the threshold is sharp, the desired property goes from highly unlikely to almost surely present with the addition of just a few objects. A graph for a sharp threshold may look like what we see in Figure 4.2.Often, though, the provable behavior is more like what we see in Figure 4.1, either because this actually is the truth or because this is what our methods allow us to prove.

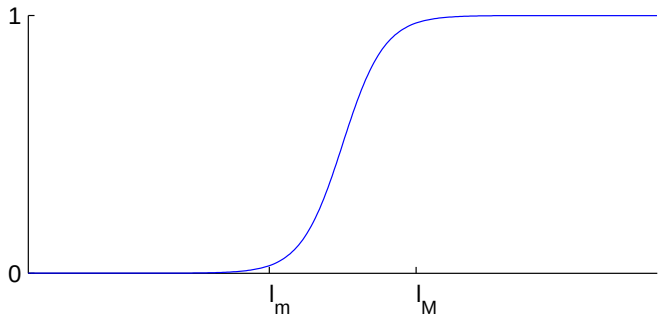

Figure 4.2 Sharp Threshold Graph

We have discussed quite a few threshold theorems related to our main question for vectors of fixed or bounded weight over various finite fields. The theorems we have shown have given the lower bound, l_m, on the number of vectors needed before we expect to see dependency. Although there are some results on upper bounds, we will concentrate on a lower bound for vectors chosen under a different probability model. In the the remainder of this chapter, we will choose vectors, $\mathbf{v}$, so that

$$Pr(\mathbf{v}[j] = 1) = \frac{c}{j}$$

where c is a constant between 0 and 2/5. In the last chapter, we discussed how we could use the size of the left null space of a matrix to determine when a set of vectors are dependent with high probability. We will use this idea in this chapter;

we will first analyze $E(2^s)$ and find an asymptotic for the size of the r^{th} term and then use this to determine when $E(2^s)$ is close to 1.

4.2 What To Expect

The results found using this probability model will be interesting in applications involving vectors that are heavier at the beginning than at the the end. Since the probability of seeing a 1 in the first positions of the vectors is so much greater than a 1 in the last positions, the majority of the 1's will be in the beginning entries. As $k \to \infty$, the probability of having a nonzero entry later in the vector is very small. Therefore the vectors chosen under this model will be very sparse. If a random vector has few nonzero entries compared to its length, we can, in essence, regard it as a vector of smaller dimension. The number of vectors needed to generate a dependent set of vectors increases as the dimension of those vectors increases. Because of this, we expect to see dependency occur much earlier, or with fewer vectors, than we saw in the fixed weight case.

To analyze $E(2^s)$, we will first investigate a few plots of its terms. From Chapter 3 with $\alpha_j = c/j$, we find $E(2^s)$ under this probability model to be

$$E(2^s) = \sum_{r=0}^{l} \binom{l}{r} \prod_{j=1}^{k} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2} . \tag{4.1}$$

We let T_r, $0 \leq r \leq l$, be the r^{th} term of $E(2^s)$, giving

$$T_r = \binom{l}{r} \prod_{j=1}^{k} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2} . \tag{4.2}$$

With extensive plotting of the terms for various combinations of c, l, and k we can identify two different behaviors of T_r, the terms of $E(2^s)$. The first plots below, Figures 4.3 and 4.4, are the terms of $E(2^s)$ for $k = 1000$, $c = 1/4$, and two different values of l, $l = 6$ and $l = 10$.Although we see two different general shapes in Figures 4.3 and 4.4, observe that they are both unimodal, that is they only have one maximum. The maximum term in Figure 4.3 is the 0^{th} term while the maximum term in Figure 4.4 is at $r = 1$. We see a similar trend in Figures 4.5 and 4.6 when $k = 1000$ and $c = 1/3$ for two different l, $l = 10$ and $l = 100$. Again, both plots are

unimodal, but when l is small, $l = 10$, T_0 is the largest term. In the plot on the right, when $l = 100$, the maximum term occurs for larger r. Also notice that the size of the terms in Figure 4.6 is very large, indicating that the size of the terms grows quickly as l grows.

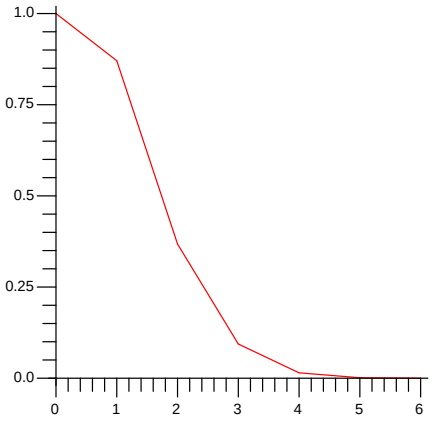

Figure 4.3 $k = 1000$, $l = 6$, $c = 1/4$

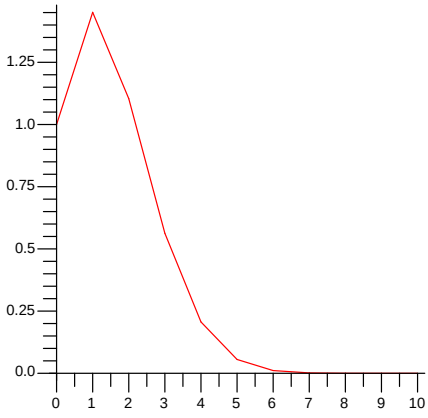

Figure 4.4 $k = 1000$, $l = 10$, $c = 1/4$

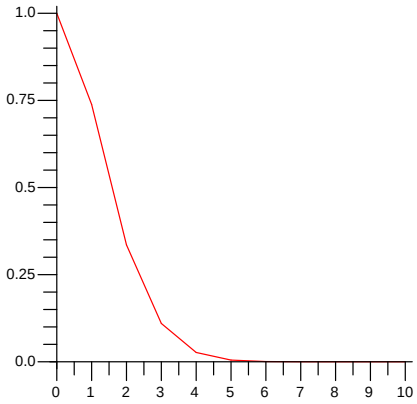

Figure 4.5 $k = 1000$, $l = 10$, $c = 1/3$

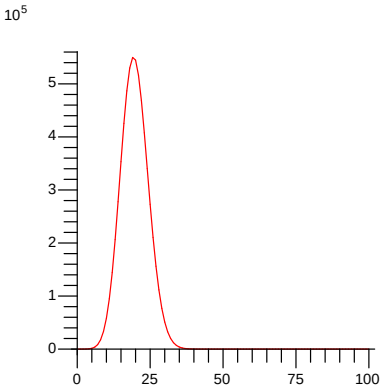

Figure 4.6 $k = 1000$, $l = 100$, $c = 1/3$

We should mention here why we restrict the constant c to be between 0 and 2/5. All of the plots we have seen so far have been unimodal. This is an extremely useful property to have when analyzing $E(2^s)$. If we were to know the maximum term of $E(2^s)$, and that all other terms were less than this maximum, we could use this to aid in estimating the size of the sum. This would, of course, require proving the unimodal property. This idea motivated us to only look at values of c such that the terms of $E(2^s)$ are unimodal. Observe the plots shown in Figures 4.7 and 4.8. Figure 4.7 plots T_r for $k = 1000$, $l = 200$, and $c = 3/4$. Notice that although T_0 is the largest term, there is more than one maximum. Figure 4.8 shows the first 10 terms of $E(2^s)$ for $k = 1000$, $l = 46$, and $c = 0.48$. Observe again that this plot is not unimodal. In addition, $T_1 < 1$ while $T_2 > T_1$. Much of the work we will do in this chapter hinges on the fact that $T_2 < T_1$ whenever $T_1 < 1$, so it is imperative to restrict c so that this is true.

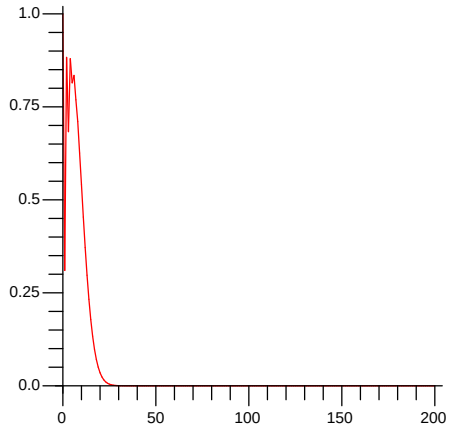

Figure 4.7 $k = 1000$, $l = 200$, $c = 3/4$

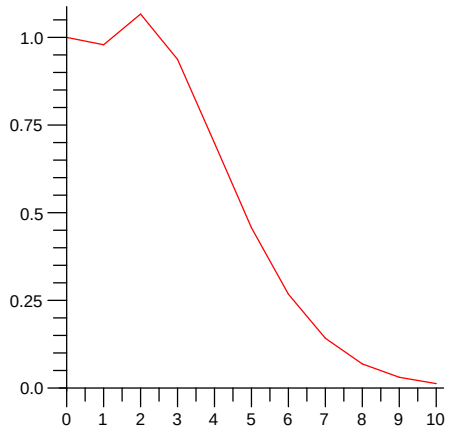

Figure 4.8 $k = 1000$, $l = 46$, $c = 0.48$

Therefore we will only take c between 0 and 2/5. In fact, our calculations show that the results we give are true for $0 < c < 9/20$, but our methods only allow us to prove the theorems for $0 < c < 2/5$. Many of the lemmas and theorems in this

chapter are actually shown for $0 < c < 1/2$. This allows us to give neater bounds and estimates. However, the final theorems and bounds will require $0 < c < 2/5$.

Returning now to the earlier discussion, we're interested in the behavior shown in Figures 4.3 and 4.5. As outlined in Chapter 3, we can determine when $E(2^s)$ is close to 1 by considering the terms of the sum. Since

$$T_0 = \binom{l}{0} \prod_{j=1}^{k} \frac{1 + \left(1 - \frac{2c}{j}\right)^0}{2} = 1,$$

$E(2^s)$ approaches 1 only when T_0 is the largest term and the remaining terms are very small. By the figures above, we make two observations:

(i) For fixed c, T_0 is the maximum term when l is small. As l increases, it appears that the maximum occurs for some $r > 0$.

(ii) As c decreases, the value of l needed to have the appropriate graph seems to also decrease.

These observations imply that T_0 is the maximum term when l is small compared to k and that the critical value of l also depends on c.

We have also discussed that not only must the 0^{th} term of $E(2^s)$ be the largest term, but the sum of the remaining terms must be negligible in order for $E(2^s)$ to approach 1. Thus we want to determine not only when T_0 is the largest term, but also when T_r is small for $r > 0$.

The remainder of the chapter will be devoted to finding a threshold function:

Goal: Find a function $l^* = l^*(k)$ such that

(i) if $l(k)/l^*(k) \to 0$, then $E(2^s) \to 1$, and

(ii) if $l(k)/l^*(k) \to \infty$, then $E(2^s) \to \infty$.

Since we are analyzing $E(2^s)$, the threshold function that we find will describe the behavior of this sum rather than the probability of dependence.

To begin, since l is a function of k and $l < k$, we set $l = dk$, $d < 1$. We will estimate the size of both T_1 and T_2 and determine the critical value of d for which $1 > T_1 > T_2$. The critical d value will lead to the threshold function $l^*(k)$ and we will then show that the sum of T_0, T_1, T_2, and the remaining terms is bounded above by a geometric series that converges to 1 for a given function $l = l(k)$. This will lead us to the threshold theorem we desire.

4.3 The First Term, T_1

We start by determining when $T_1 < T_0 = 1$. This will give us an idea of where we should expect the remaining terms to be very small. We mentioned that the plots above are unimodal. Although we will not show that this is true here, we will show that when $T_1 < 1$, the remaining terms are also decreasing for a given l. In this section we will first estimate T_1 and use the asymptotic with $l = dk$ to determine the critical value, d_1, where $T_1 < 1$ when $d < d_1$ and $T_1 > 1$ otherwise.

4.3.1 An Asymptotic for T_1

By equation (4.2), we see that the first term of $E(2^s)$ is

$$T_1 = \binom{l}{1} \prod_{j=1}^{k} \frac{1 + \left(1 - \frac{2c}{j}\right)}{2} = l \prod_{j=1}^{k} \left(1 - \frac{c}{j}\right). \tag{4.3}$$

We wish to determine the behavior of this term as $k \to \infty$ to find the values of l for which it is less than 1. Clearly, the behavior of T_1 is largely determined by the product. We set $t_1(c, k)$ to be this product. Since we regard k to be fixed, we will simply write this as $t_1(c)$, thus

$$t_1(c) = \prod_{j=1}^{k} \left(1 - \frac{c}{j}\right). \tag{4.4}$$

Before finding when $T_1 < 1$, we will need to estimate $t_1(c)$. The asymptotic analysis of $t_1(c)$ will use estimates derved from the bounds summarized in the lemmas stated below. The proofs of these lemmas are standard and will be given after the proof of the theorem. The first lemma gives upper and lower bounds on the k^{th} harmonic number.

Lemma 4.1 *Let $\gamma = 0.5772\ldots$ be the Euler-Mascheroni constant. Then for $0 < c < 1/2$ and $k \geq 1$,*

$$\log k + \gamma + \frac{1}{2k} - \frac{1}{12k^2} \leq \sum_{j=1}^{k} \frac{1}{j} \leq \log k + \gamma + \frac{1}{2k} - \frac{1}{12k^2} + \frac{1}{60k^4}. \tag{4.5}$$

Notice that since we are adding a finite number of terms above that are $O(k^{-1})$, this inequality tells us that

$$\sum_{j=1}^{k} \frac{1}{j} = \log k + \gamma + O\left(\frac{1}{k}\right).$$

This is a standard estimate for the harmonic number, H_k, that we will use in the proof of Theorem 4.1. The more explicit bounds given above will be needed in Section 4.3.3 for the error analysis of the theorem that will give tighter bounds on $t_1(c)$.

We will also need the following inequality.

Lemma 4.2 *Let $k \geq 1$ and $m \geq 2$. Then*

$$\begin{aligned}
&\zeta(m) - \frac{1}{(m-1)k^{m-1}} + \frac{1}{2k^m} - \frac{m}{12k^{m+1}} \\
&\quad \leq \sum_{j=1}^{k} \frac{1}{j^m} \\
&\quad \leq \zeta(m) - \frac{1}{(m-1)k^{m-1}} + \frac{1}{2k^m} - \frac{m}{12k^{m+1}} + \frac{m(m+1)(m+2)}{15 \cdot 4! k^{m+3}}
\end{aligned} \tag{4.6}$$

where $\zeta(m)$ is the Riemann zeta function.

From this lemma, we will be using the estimate

$$\sum_{j=1}^{k} \frac{1}{j^m} = \zeta(m) + O\left(\frac{1}{k^{m-1}}\right)$$

in the analysis of $t_1(c)$. Again, the more precise bounds will be used in the error analysis of Theorem 4.1.

Finally, we will need

Lemma 4.3 *Let $0 < c < 1/2$ and $k \geq 1$. Then*

$$\frac{c^2}{2k} < \sum_{m=2}^{\infty} \frac{c^m}{m(m-1)k^{m-1}} < \frac{2c^2}{3k}.$$

It will be sufficient to use the estimate

$$\sum_{m=2}^{\infty} \frac{c^m}{m(m-1)k^{m-1}} = O\left(\frac{1}{k}\right)$$

in the proof of Theorem 4.1.

We are now ready to find an asymptotic for $t_1(c)$. These lemmas will become necessary throughout the proof.

Theorem 4.1 *Let $0 < c < 1/2$. Then as $k \to \infty$,*

$$t_1(c) = \prod_{j=1}^{k} \frac{1 + (1 - \frac{2c}{j})}{2} \sim k^{-c} e^{-c\gamma - h_\zeta(c)}, \tag{4.7}$$

where $h_\zeta(c) = \sum_{m=2}^{\infty} \frac{c^m}{m} \zeta(m)$.

Proof: We begin by rewriting the product as an exponential function.

$$\begin{aligned} t_1(c) &= \prod_{j=1}^{k} \frac{1 + (1 - \frac{2c}{j})}{2} \\ &= \prod_{j=1}^{k} \left(1 - \frac{c}{j}\right) \\ &= \exp\left\{ \sum_{j=1}^{k} \log\left(1 - \frac{c}{j}\right) \right\} \end{aligned}$$

To expand the exponent, we use the Taylor series for log,

$$\begin{aligned} t_1(c) &= \exp\left\{ \sum_{j=1}^{k} \log\left(1 - \frac{c}{j}\right) \right\} \\ &= \exp\left\{ \sum_{j=1}^{k} \left(- \sum_{m=1}^{\infty} \left(\frac{c}{j}\right)^m \frac{1}{m} \right) \right\}. \end{aligned}$$

We now partially expand the double sum to a single sum on which we can apply the first lemma above as well as a double sum which we will need to analyze further.

$$\begin{aligned} t_1(c) &= \exp\left\{ \sum_{j=1}^{k} \left(- \sum_{m=1}^{\infty} \left(\frac{c}{j}\right)^m \frac{1}{m} \right) \right\} \\ &= \exp\left\{ - \sum_{j=1}^{k} \frac{c}{j} - \sum_{j=1}^{k} \sum_{m=2}^{\infty} \left(\frac{c}{j}\right)^m \frac{1}{m} \right\} \end{aligned} \tag{4.8}$$

At this point, we have two sums that we must estimate in order to obtain the result we desire. The first sum is simply the k^{th} harmonic number which we bounded in Lemma 4.1. By the comment immediately following the lemma, we know

$$\sum_{j=1}^{k} \frac{1}{j} = \log k + \gamma + O\left(\frac{1}{k}\right). \tag{4.9}$$

By using the big-O term, we are introducing a certain amount of error. Along with another $O(k^{-1})$ term introduced later, we must be careful that the error incurred is in fact small enough to be ignored. The exact bounds given in the lemmas give the error check that we need. These lemmas show that the sums that appear in $t_1(c)$ are $O(k^{-1})$, implying the error is bounded. Therefore we use the estimate (4.9) in equation (4.8) to obtain

$$\begin{aligned} t_1(c) &= \exp\left\{-\sum_{j=1}^{k}\frac{c}{j}-\sum_{j=1}^{k}\sum_{m=2}^{\infty}\left(\frac{c}{j}\right)^m\frac{1}{m}\right\} \\ &= \exp\left\{-c\log k-c\gamma+O\left(\frac{1}{k}\right)-\sum_{j=1}^{k}\sum_{m=2}^{\infty}\left(\frac{c}{j}\right)^m\frac{1}{m}\right\}. \end{aligned}$$

We can now concentrate on the double sum. Notice that

$$\sum_{j=1}^{k}\sum_{m=2}^{\infty}\left(\frac{c}{j}\right)^m\frac{1}{m}<\sum_{j=1}^{k}\sum_{m=2}^{\infty}\left(\frac{c}{j}\right)^m.$$

Since $c/j<1$, the series on the right is convergent. Since the series on the left is positive and bounded above by a convergent series, the original sum is absolutely convergent. Therefore we may switch the order of summation to get

$$\begin{aligned} t_1(c) &= \exp\left\{-c\log k-c\gamma+O\left(\frac{1}{k}\right)-\sum_{j=1}^{k}\sum_{m=2}^{\infty}\left(\frac{c}{j}\right)^m\frac{1}{m}\right\} \\ &= \exp\left\{-c\log k-c\gamma+O\left(\frac{1}{k}\right)-\sum_{m=2}^{\infty}\frac{c^m}{m}\sum_{j=1}^{k}\frac{1}{j^m}\right\}. \end{aligned} \tag{4.10}$$

From Lemma 4.2, we have

$$\sum_{j=1}^{k}\frac{1}{j^m}=\zeta(m)+O\left(\frac{1}{k^{m-1}}\right).$$

Substituting this into (4.10) and separating the exponent we find

$$\begin{aligned} t_1(c) &= \exp\left\{-c\log k-c\gamma+O\left(\frac{1}{k}\right)-\sum_{m=2}^{\infty}\frac{c^m}{m}\sum_{j=1}^{k}\frac{1}{j^m}\right\} \\ &= k^{-c}e^{-c\gamma+O\left(\frac{1}{k}\right)}\exp\left\{-\sum_{m=2}^{\infty}\frac{c^m}{m}\zeta(m)\right\}\exp\left\{-\sum_{m=2}^{\infty}\frac{c^m}{m}O\left(\frac{1}{k^{m-1}}\right)\right\}. \end{aligned} \tag{4.11}$$

The first sum above converges to a constant depending on c. To see this, note that $\zeta(m)$ decreases with m, so that for $m \geq 2$,

$$\zeta(m) \leq \frac{\pi^2}{6}\,,$$

giving an upper bound for the infinite series,

$$\sum_{m=2}^{\infty} \frac{c^m}{m}\zeta(m) < \frac{\pi^2}{6}\sum_{m=2}^{\infty}\frac{c^m}{m}\,.$$

We find that the sum on the right converges also. In fact, this is the Taylor expansion for $-c - \log(1-c)$. Thus

$$\frac{\pi^2}{6}\sum_{m=2}^{\infty}\frac{c^m}{m} = \frac{\pi^2}{6}(-\log(1-c) - c).$$

Since the original sum of positive terms is bounded above by a convergent series, we know that it converges and set

$$h_\zeta(c) = \sum_{m=2}^{\infty}\frac{c^m}{m}\zeta(m).$$

This gives

$$\begin{aligned} t_1(c) &= k^{-c}e^{-c\gamma+O\left(\frac{1}{k}\right)}\exp\left\{-\sum_{m=2}^{\infty}\frac{c^m}{m}\zeta(m)\right\}\exp\left\{\sum_{m=2}^{\infty}\frac{c^m}{m}\,O\left(\frac{1}{k^{m-1}}\right)\right\} \\ &= k^{-c}e^{-c\gamma-h_\zeta(c)+O\left(\frac{1}{k}\right)}\exp\left\{\sum_{m=2}^{\infty}\frac{c^m}{m}\,O\left(\frac{1}{k^{m-1}}\right)\right\}. \end{aligned} \tag{4.12}$$

Lemma 4.3 gives bounds on the remaining series and we use the estimate

$$\sum_{m=2}^{\infty}\frac{c^m}{m}\frac{1}{(m-1)k^{m-1}} = O\left(\frac{1}{k}\right).$$

Substituting this expression in (4.12), we obtain

$$\begin{aligned} t_1(c) &= k^{-c}e^{-c\gamma-h_\zeta(c)+O\left(\frac{1}{k}\right)}\exp\left\{\sum_{m=2}^{\infty}\frac{c^m}{m}\,O\left(\frac{1}{k^{m-1}}\right)\right\} \\ &= k^{-c}e^{-c\gamma-h_\zeta(c)}e^{O\left(\frac{1}{k}\right)} \\ &= k^{-c}e^{-c\gamma-h_\zeta(c)}\left(1+O\left(\frac{1}{k}\right)\right). \end{aligned}$$

The last expression is found using the first two terms of the Taylor expansion of e. This gives

$$\frac{t_1(c)}{k^{-c}e^{-c\gamma-h_\zeta(c)}} = 1 + O\left(\frac{1}{k}\right).$$

Since $1 + O(k^{-1}) \to 1$ as $k \to \infty$, this implies

$$t_1(c) = \prod_{j=1}^{k} \frac{1 + (1 - \frac{2c}{j})}{2} \sim k^{-c}e^{-c\gamma-h_\zeta(c)}.$$

□

Knowing the behavior of $t_1(c)$, we can use this in equation (4.3) to find that the first term of $E(2^s)$ is approximately

$$T_1 \sim lk^{-c}e^{-c\gamma-h_\zeta(c)}. \tag{4.13}$$

We see that the dominant factor here is k^{-c} so that the asymptotic behavior of T_1 depends heavily on both k and c. We will use (4.13) shortly to determine what l must be in order to ensure that T_1 is less than 1.

4.3.2 Proofs of the Lemmas

We will first prove the three lemmas used in the proof of Theorem 4.1. In Section 4.3.3, we will check the error introduced by using these lemmas to estimate the sums. We use Euler Maclaurin summation to prove the results of the necessary lemmas. The general formula and a brief explanation is given below.

Euler Maclaurin Summation Formula *For any integers a, b and $n \geq 0$ and any function f in $C^{n+1}[a, b]$, we have*

$$\begin{aligned}\sum_{a<i\leq b} f(i) &= \int_a^b f(t)\,dt + \sum_{r=0}^{n} \frac{(-1)^{r+1}B_{r+1}}{(r+1)!}(f^{(r)}(b) - f^{(r)}(a)) \\ &\quad + \frac{(-1)^n}{(n+1)!}\int_a^b B_{n+1}(t)f^{(n+1)}(t)\,dt,\end{aligned}$$

where B_r is the r^{th} Bernoulli number and $B_r(t)$ is the corresponding periodic extension of the r^{th} Bernoulli polynomial.

The periodic functions $B_r(t)$ are extensions of the the Bernoulli polynomials, $b_r(t)$, and are used to control the error encountered by the integral approximation

of the series. The Bernoulli polynomials are defined on the interval $[0,1]$ by the following three conditions:

$$\begin{aligned} b_0(t) &:= 1 \\ b_r'(t) &:= r b_{r-1}(t), \quad r \geq 1 \\ \int_0^1 b_r(t)\, dt &= 0, \quad r \geq 1. \end{aligned}$$

The first five Bernoulli polynomials are as follows.

$$\begin{aligned} b_0(t) &= 1 \\ b_1(t) &= t - \frac{1}{2} \\ b_2(t) &= t^2 - t + \frac{1}{6} \\ b_3(t) &= t^3 - \frac{3}{2}t^2 + \frac{1}{2}t \\ b_4(t) &= t^4 - 2t^3 + t^2 - \frac{1}{30} \end{aligned}$$

The r^{th} Bernoulli function, $B_r(t)$, is then defined to be the function with period 1 that agrees with $b_r(t)$ on $[0,1)$. Observe that the integral condition on the Bernoulli polynomials requires $b_r(0) = b_r(1)$ for $r > 1$. This implies that the extension, $B_r(t)$, is a continuous differentiable function over the entire range of the integral. Furthermore, set

$$B_r := B_r(0) = b_r(0)$$

to be the r^{th} Bernoulli number. The sequence of Bernoulli numbers begins

$$B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_3 = 0,\ B_4 = -\frac{1}{30}, \ldots$$

It is a fact that $B_{2r+1} = 0$ for all $r \geq 1$.

The Euler Maclaurin formula is extremely powerful in approximating sums. The first integral and following sum give a function that estimates the desired series and the final integral in the formula provides an error bound for the asymptotic formula. We will now use Euler Maclaurin to prove the three lemmas stated earlier.

Lemma 4.1 *Let $\gamma = 0.5772\ldots$ be the Euler-Mascheroni constant. Then for $k \geq 1$,*

$$\log k + \gamma + \frac{1}{2k} - \frac{1}{12k^2} \leq \sum_{j=1}^{k} \frac{1}{j} \leq \log k + \gamma + \frac{1}{2k} - \frac{1}{12k^2} + \frac{1}{60k^4}\,. \tag{4.14}$$

Proof: Let $f(x) = x^{-1}$. By Euler Maclaurin summation,

$$\begin{aligned}\sum_{j=1}^{k} \frac{1}{j} &= 1 + \int_1^k \frac{dx}{x} + \sum_{r=0}^{n} \frac{(-1)^{r+1} B_{r+1}(0)}{(r+1)!}(f^{(r)}(b) - f^{(r)}(a)) \\ &\quad + \frac{(-1)^n}{(n+1)!}\int_a^b B_{n+1}(t) f^{(n+1)}(t)\, dt.\end{aligned}$$

Choosing $n = 3$ will give enough accuracy for our purposes.

$$\begin{aligned}\sum_{j=1}^{k} \frac{1}{j} &= 1 + \int_1^k \frac{dx}{x} - B_1\left(\frac{1}{k} - 1\right) + \frac{B_2}{2!}\left(\frac{-1}{k^2} + 1\right) + \frac{B_4}{4!}\left(\frac{-3!}{k^4} + 3!\right) \\ &\quad - \frac{4!}{4!}\int_1^k B_4(t)\frac{dt}{t^5} \\ &= 1 + \log k + \frac{1}{2k} - \frac{1}{2} - \frac{1}{12k^2} + \frac{1}{12} + \frac{1}{120k^4} - \frac{1}{120} - \int_1^k B_4(t)\frac{dt}{t^5} \\ &= \log k + \frac{1}{2k} - \frac{1}{12k^2} + \frac{1}{120k^4} + \frac{1}{2} + \frac{1}{12} - \frac{1}{120} - \int_1^k B_4(t)\frac{dt}{t^5} \qquad (4.15)\end{aligned}$$

The Euler-Mascheroni constant is defined as

$$\gamma = \lim_{n\to\infty}\left(\sum_{j=1}^{n} \frac{1}{j} - \log n\right).$$

Letting k go to infinity in (4.15), we find that

$$\gamma = \frac{1}{2} + \frac{1}{12} - \frac{1}{120} - \int_1^\infty B_4(t)\frac{dt}{t^5}\,.$$

We can substitute this definition of γ back into (4.15) to find that

$$\sum_{j=1}^{k} \frac{1}{j} = \log k + \gamma + \frac{1}{2k} - \frac{1}{12k^2} + \frac{1}{120k^4} + \int_k^\infty B_4(t)\frac{dt}{t^5}\,. \tag{4.16}$$

Finally, observe that the Bernoulli polynomial $b_4(t) = t^4 - 2t^3 + t^2 - \frac{1}{30}$ satisfies $|b_4(t)| \leq \frac{1}{30}$ when $t \in [0,1]$. We can easily check that $b_4(t)$ has critical points at $t = 0, 1/2$, and 1 and that $b_4(0) = b_4(1) = \frac{1}{30}$ and $b_4(1/2) = \frac{7}{240} < \frac{1}{30}$. Therefore, since $B_4(t)$ is the periodic extension of $b_4(t)$, it is also true that $|B_4(t)| \leq \frac{1}{30}$ for all

t. Thus

$$\begin{aligned}\left|\int_k^\infty B_4(t)\frac{dt}{t^5}\right| &\leq \int_k^\infty |B_4(t)|\,\frac{dt}{t^5}\\ &\leq \frac{1}{120k^4}\,.\end{aligned}$$

Using this with (4.16), we get

$$\left|\sum_{j=1}^{k}\frac{1}{j}-\log k-\gamma-\frac{1}{2k}+\frac{1}{12k^2}-\frac{1}{120k^4}\right|\leq\frac{1}{120k^4}\,.$$

Writing out the absolute value gives (4.5). □

We will use Euler Maclaurin summation often throughout this chapter to find asymptotic functions and to bound the resulting error as we have done here. The result seen in this and the following lemmas is typical of results by this method. The final big-O term in Theorem 4.1 required the following two lemmas.

Lemma 4.2 *Let $k \geq 1$ and $m \geq 2$. Then*

$$\begin{aligned}&\zeta(m)-\frac{1}{(m-1)k^{m-1}}+\frac{1}{2k^m}-\frac{m}{12k^{m+1}}\\ &\quad\leq\sum_{j=1}^{k}\frac{1}{j^m}\\ &\quad\leq\zeta(m)-\frac{1}{(m-1)k^{m-1}}+\frac{1}{2k^m}-\frac{m}{12k^{m+1}}+\frac{m(m+1)(m+2)}{15\cdot 4!k^{m+3}}\end{aligned}$$

where $\zeta(m)$ is the Riemann zeta function.

Proof: Let $f(x)=x^{-m}$ and let $n=3$. By the Euler Maclaurin summation formula,

$$\begin{aligned}\sum_{j=1}^{k}\frac{1}{j^m} &= 1+\int_1^k\frac{dx}{x^m}-B_1\left(\frac{1}{k^m}-1\right)+\frac{m(m+1)(m+2)B_4}{4!}\left(\frac{-1}{k^{m+3}}+1\right)\\ &\quad+\frac{mB_2}{2!}\left(\frac{-1}{k^{m+1}}+1\right)-\frac{m(m+1)(m+2)(m+3)}{4!}\int_1^k B_4(t)\frac{dt}{t^{m+4}}\\ &= 1-\frac{1}{(m-1)k^{m-1}}+\frac{1}{m-1}+\frac{1}{2k^m}-\frac{1}{2}-\frac{m}{12k^{m+1}}+\frac{m}{12}\\ &\quad+\frac{m(m+1)(m+2)}{30\cdot 4!\,k^{m+3}}-\frac{m(m+1)(m+2)}{30\cdot 4!}-\binom{m+3}{4}\int_1^k B_4(t)\frac{dt}{t^{m+4}}\\ &= \frac{-1}{(m-1)k^{m-1}}+\frac{1}{2k^m}-\frac{m}{12k^{m+1}}+\frac{m(m+1)(m+2)}{30\cdot 4!\,k^{m+3}}+\frac{1}{2}+\frac{1}{m-1}\\ &\quad+\frac{m}{12}-\frac{m(m+1)(m+2)}{30\cdot 4!}-\binom{m+3}{4}\int_1^k B_4(t)\frac{dt}{t^{m+4}}\,.\end{aligned}$$

Letting $k \to \infty$ in this equation, the left side becomes $\zeta(m)$ and we find

$$\zeta(m) = \sum_{j\geq 1} \frac{1}{j^m} = \frac{1}{2} + \frac{1}{m-1} + \frac{m}{12} - \frac{m(m+1)(m+2)}{30 \cdot 4!} - \binom{m+3}{4} \int_1^\infty B_4(t) \frac{dt}{t^{m+4}} \,.$$

Substituting this expression for $\zeta(m)$ into the above equation,

$$\begin{aligned} \sum_{j=1}^{k} \frac{1}{j^m} &= \zeta(m) - \frac{1}{(m-1)k^{m-1}} + \frac{1}{2k^m} - \frac{m}{12k^{m+1}} + \frac{m(m+1)(m+2)}{30 \cdot 4!\, k^{m+3}} \\ &\quad + \binom{m+3}{4} \int_k^\infty B_4(t) \frac{dt}{t^{m+4}} \,. \end{aligned} \tag{4.17}$$

Using the fact that $|B_4(t)| \leq 1/30$ for all t as shown in the previous proof, we have

$$\begin{aligned} \left| \binom{m+3}{4} \int_k^\infty B_4(t) \frac{dt}{t^{m+4}} \right| &\leq \binom{m+3}{4} \int_k^\infty |B_4(t)| \frac{dt}{t^{m+4}} \\ &\leq \frac{m(m+1)(m+2)}{30 \cdot 4!\, k^{m+3}} \,. \end{aligned}$$

Substituting this back into (4.17), we now have

$$\begin{aligned} &\left| \sum_{j=1}^{k} \frac{1}{j^m} - \zeta(m) + \frac{1}{(m-1)k^{m-1}} - \frac{1}{2k^m} + \frac{m}{12k^{m+1}} - \frac{m(m+1)(m+2)}{30 \cdot 4!\, k^{m+3}} \right| \\ &\quad \leq \frac{m(m+1)(m+2)}{30 \cdot 4!\, k^{m+3}} \,, \end{aligned}$$

thus giving the desired inequalities. □

The final lemma can be proved without Euler Maclaurin summation.

Lemma 4.3 *Let $0 < c < 1/2$ and $k \geq 1$. Then*

$$\frac{c^2}{2k} < \sum_{m=2}^{\infty} \frac{c^m}{m(m-1)k^{m-1}} < \frac{2c^2}{3k} \,.$$

Proof: Observe that the lower bound given above is simply the first term of the series. Since the terms are all nonnegative, then the sum of any bounded number of these terms gives a lower bound. To find the upper bound, we first pull out the first term. This gives

$$\sum_{m=2}^{\infty} \frac{c^m}{m(m-1)k^{m-1}} = \frac{c^2}{2k} + \sum_{m=3}^{\infty} \frac{c^m}{m(m-1)k^{m-1}} \,.$$

Rewriting the series on the right to begin with $m = 0$, we have

$$\begin{aligned}\sum_{m=2}^{\infty} \frac{c^m}{m(m-1)k^{m-1}} &= \frac{c^2}{2k} + \frac{c^3}{k^2} \sum_{m=0}^{\infty} \frac{c^m}{(m+3)(m+2)k^m} \\ &< \frac{c^2}{2k} + \frac{c^3}{6k^2} \sum_{m=0}^{\infty} \left(\frac{c}{k}\right)^m \\ &= \frac{c^2}{2k} + \frac{c^3}{6k^2} \frac{1}{1-c/k}\,.\end{aligned}$$

Since $c < 1/2$, then for any $k \geq 1$,

$$\frac{1}{1-c/k} < 2,$$

giving

$$\sum_{m=2}^{\infty} \frac{c^m}{m(m-1)k^{m-1}} < \frac{c^2}{2k} + \frac{c^3}{3k^2}\,.$$

Again using the fact that $c < 1/2$, we find that

$$\sum_{m=2}^{\infty} \frac{c^m}{m(m-1)k^{m-1}} < \frac{c^2}{2k} + \frac{c^2}{6k} = \frac{2c^2}{3k}\,,$$

giving the result. □

In Theorem 4.1, the results of these lemmas provided big-O terms that allowed us to find an asymptotic expression for $t_1(c)$. In the next section, we use the inequalities found in each lemma to give an even tighter asymptotic for $t_1(c)$.

4.3.3 Error Analysis for Theorem 4.1

In the proof of Theorem 4.1, we made extensive use of asymptotic notation. This is extremely useful in seeing how $t_1(c)$ behaves, but each introduction of a big-O term incurs a certain amount of error. It is very important to be sure that the error is under control when using estimates as we are. If we are adding a fixed number of terms that are all $O(k^{-1})$, then the sum of these terms is, in fact, $O(k^{-1})$ and the approximations made are valid. On the other hand, if we are adding an unbounded number of terms that behave in this way, we must be careful that the sum isn't larger than $O(k^{-1})$. If the number of terms added is actually a function of k, it is possible that the sum could be, for example, $O(k^{-1/2})$, or worse, the error could be unbounded as $k \to \infty$. If this were true, the error would be more significant than claimed and possibly be a dominant term in the the asymptotic.

Although we added an unbounded number of terms that were $O(k^{-1})$ in Theorem 4.1, the inequalities given in the lemmas show that we can actually reduce this to the sum of only two $O(k^{-1})$ terms, implying the error is bounded. In this section, we use the inequalities in Lemmas 4.1, 4.2, and 4.3 to find a tighter estimate for $t_1(c)$.

Notice that the first equation in the proof of Theorem 4.1, equation (4.8), is an exact expression:

$$t_1(c) = \exp\left\{ -\sum_{j=1}^{k} \frac{c}{j} - \sum_{j=1}^{k} \sum_{m=2}^{\infty} \left(\frac{c}{j}\right)^m \frac{1}{m} \right\}.$$

We then used the fact that

$$\sum_{j=1}^{k} \frac{1}{j} = \log k + \gamma + O\left(\frac{1}{k}\right)$$

to replace the harmonic sum above. The result of Lemma 4.1 gives precise upper and lower bounds for the product, namely

$$\begin{aligned} &\exp\left\{ -c\log k - c\gamma - \frac{c}{2k} + \frac{c}{12k^2} - \frac{c}{60k^4} - \sum_{j=1}^{k} \sum_{m=2}^{\infty} \left(\frac{c}{j}\right)^m \frac{1}{m} \right\} \\ \leq\ & t_1(c) \\ \leq\ & \exp\left\{ -c\log k - c\gamma - \frac{c}{2k} + \frac{c}{12k^2} - \sum_{j=1}^{k} \sum_{m=2}^{\infty} \left(\frac{c}{j}\right)^m \frac{1}{m} \right\}. \end{aligned} \tag{4.18}$$

By inequality (4.18) we see that the upper and lower bounds are extremely close, differing only by a factor of $e^{-c/60k^4}$. As $k \to \infty$, the two bounds become even closer.

We now must handle the double sum. Recall that we were able to switch the order of summation so that

$$\sum_{j=1}^{k} \sum_{m=2}^{\infty} \left(\frac{c}{j}\right)^m \frac{1}{m} = \sum_{m=2}^{\infty} \frac{c^m}{m} \sum_{j=1}^{k} \frac{1}{j^m}.$$

We may now use the result of Lemma 4.2 on the inside sum on the right to eliminate the double sum.

$$\begin{aligned}
&\exp\left\{-c\log k - c\gamma - \frac{c}{2k} + \frac{c}{12k^2} - \frac{c}{60k^4} - h_\zeta(c) + \sum_{m=2}^{\infty}\frac{c^m}{m}\frac{1}{(m-1)k^{m-1}}\right.\\
&\qquad\left. - \sum_{m=2}^{\infty}\frac{c^m}{m}\left(\frac{1}{2k^m} - \frac{m}{12k^{m+1}} + \frac{m(m+1)(m+2)}{15\cdot 4!\,k^{m+3}}\right)\right\}\\
&\leq\ t_1(c)\\
&\leq\ \exp\left\{-c\log k - c\gamma - \frac{c}{2k} + \frac{c}{12k^2} - h_\zeta(c) + \sum_{m=2}^{\infty}\frac{c^m}{m}\frac{1}{(m-1)k^{m-1}}\right.\\
&\qquad\left. - \sum_{m=2}^{\infty}\frac{c^m}{m}\left(\frac{1}{2k^m} - \frac{m}{12k^{m+1}}\right)\right\} \qquad (4.19)
\end{aligned}$$

Here we are using the previous definition of $h_\zeta(c)$,

$$h_\zeta(c) = \sum_{m=2}^{\infty}\frac{c^m}{m}\zeta(m).$$

We now use Lemma 4.3 to find another set of inequalities bounding the product.

$$\begin{aligned}
&\exp\left\{-c\log k - c\gamma - \frac{c}{2k} + \frac{c}{12k^2} - \frac{c}{60k^4} - h_\zeta(c) + \frac{c^2}{2k}\right.\\
&\qquad\left. - \sum_{m=2}^{\infty}\frac{c^m}{m}\left(\frac{1}{2k^m} - \frac{m}{12k^{m+1}} + \frac{m(m+1)(m+2)}{15\cdot 4!\,k^{m+3}}\right)\right\}\\
&\leq\ t_1(c)\\
&\leq\ \exp\left\{-c\log k - c\gamma - \frac{c}{2k} + \frac{c}{12k^2} - h_\zeta(c) + \frac{2c^2}{3k}\right.\\
&\qquad\left. - \sum_{m=2}^{\infty}\frac{c^m}{m}\left(\frac{1}{2k^m} - \frac{m}{12k^{m+1}}\right)\right\} \qquad (4.20)
\end{aligned}$$

At this point in the proof of Theorem 4.1 we didn't have these remaining terms to deal with. Since we are adding an infinite number of positive terms, we must find bounds on the remaining sums to show that they are small. We summarize this in the following lemmas.

Lemma 4.4 *Let $0 < c < 1/2$ and $k \geq 1$. Then*

$$\frac{c^2}{4k^2} < \frac{1}{2}\sum_{m=2}^{\infty}\left(\frac{c}{k}\right)^m\frac{1}{m} < \frac{c^2}{2k^2}\,.$$

Proof: Proceeding as in Lemma 4.3,

$$\begin{aligned}
\frac{1}{2}\sum_{m=2}^{\infty}\left(\frac{c}{k}\right)^m\frac{1}{m} &= \frac{c^2}{4k^2}+\frac{1}{2}\sum_{m=3}^{\infty}\left(\frac{c}{k}\right)^m\frac{1}{m} \\
&= \frac{c^2}{4k^2}+\frac{c^3}{2k^3}\sum_{m=0}^{\infty}\left(\frac{c}{k}\right)^m\frac{1}{m+3} \\
&< \frac{c^2}{4k^2}+\frac{c^3}{6k^3}\sum_{m=0}^{\infty}\left(\frac{c}{k}\right)^m \\
&= \frac{c^2}{4k^2}+\frac{c^3}{6k^3}\frac{1}{1-c/k} \\
&< \frac{c^2}{4k^2}+\frac{c^3}{3k^3}\,.
\end{aligned}$$

Then since $c < 1/2$ and $k \geq 1$,

$$\frac{1}{2}\sum_{m=2}^{\infty}\left(\frac{c}{k}\right)^m\frac{1}{m} < \frac{c^2}{4k^2}+\frac{c^2}{6k^2} < \frac{c^2}{2k^2}\,.$$

The lower bound is found by pulling out the first term and observing that the remaining sum is positive. □

Lemma 4.5 *Let $0 < c < 1/2$ and $k \geq 1$. Then*

$$\frac{c^2}{12k^3} < \frac{1}{12k}\sum_{m=2}^{\infty}\left(\frac{c}{k}\right)^m < \frac{c^2}{6k^3}\,.$$

Proof: The lower bound comes from the first term of the series. To find the upper bound, observe that

$$\begin{aligned}
\frac{1}{12k}\sum_{m=2}^{\infty}\left(\frac{c}{k}\right)^m &= \frac{c^2}{12k^3}+\frac{c^3}{12k^4}\sum_{m=0}^{\infty}\left(\frac{c}{k}\right)^m \\
&= \frac{c^2}{12k^3}+\frac{c^3}{12k^4}\frac{1}{1-c/k} \\
&< \frac{c^2}{12k^3}+\frac{c^3}{6k^4}\,.
\end{aligned}$$

So

$$\frac{1}{12k}\sum_{m=2}^{\infty}\left(\frac{c}{k}\right)^m < \frac{c^2}{12k^3}+\frac{c^2}{12k^3} = \frac{c^2}{6k^3}$$

as needed. □

Lemma 4.6 *Let $0 < c < 1/2$ and $k \geq 1$. Then*

$$\frac{c^2}{30k^5} < \frac{1}{15\cdot 4!}\sum_{m=2}^{\infty}\frac{c^m(m+1)(m+2)}{k^{m+3}} < \frac{2c^2}{15k^5}\,.$$

Proof: The first term of the series gives the lower bound above. The proof of the upper bound requires the use of the following derivative.

$$\frac{d^2}{dx^2}\left[\frac{1}{x^{m+1}}\right] = \frac{(m+1)(m+2)}{x^{m+3}}$$

We expand as before and use this derivative to get

$$\begin{aligned}
\frac{1}{15\cdot 4!}\sum_{m=2}^{\infty}\frac{c^m(m+1)(m+2)}{k^{m+3}} &= \frac{12c^2}{15\cdot 4!\,k^5} + \frac{1}{15\cdot 4!}\sum_{m=3}^{\infty}\frac{c^m(m+1)(m+2)}{k^{m+3}} \\
&= \frac{c^2}{30k^5} + \frac{1}{15\cdot 4!}\frac{d^2}{dk^2}\left[\frac{c^3}{k^4}\sum_{m=0}^{\infty}\left(\frac{c}{k}\right)^m\right] \\
&= \frac{c^2}{30k^5} + \frac{1}{15\cdot 4!}\frac{2c^3(10-15c/k+6c^2/k^2)}{k^6(1-c/k)^3}\,.
\end{aligned}$$

Then since $c < 1/2$,

$$\begin{aligned}
\frac{1}{15\cdot 4!}\sum_{m=2}^{\infty}\frac{c^m(m+1)(m+2)}{k^{m+3}} &< \frac{c^2}{30k^5} + \frac{1}{15\cdot 4!}\frac{8c^3}{k^6(1-c/k)^3} \\
&< \frac{c^2}{30k^5} + \frac{4\cdot 8c^2}{15\cdot 4!\,k^5} \\
&= \frac{11c^2}{90k^5} \\
&< \frac{2c^2}{15k^5}\,.
\end{aligned}$$

This gives the desired inequality. □

The results of Lemmas 4.4, 4.5, and 4.6 provide the remaining bounds needed for $t_1(c)$. These lemmas imply

$$\begin{aligned}
&\exp\left\{-c\log k - c\gamma - h_\zeta(c) - \frac{c}{2k} + \frac{c}{12k^2} - \frac{c}{60k^4} + \frac{c^2}{2k} - \frac{c^2}{2k^2} + \frac{c^2}{12k^3} - \frac{2c^2}{15k^5}\right\} \\
&\quad\le\ t_1(c) \\
&\quad\le\ \exp\left\{-c\log k - c\gamma - h_\zeta(c) - \frac{c}{2k} + \frac{c}{12k^2} + \frac{2c^2}{3k} - \frac{c^2}{4k^2} + \frac{3c^2}{6k^3}\right\}. \qquad (4.21)
\end{aligned}$$

We now have very accurate bounds on $t_1(c)$. We can use the inequalities in 4.21 to give a more precise estimate for the product:

$$t_1(c) = k^{-c}\exp\left\{-c\gamma - h_\zeta(c) - \frac{c}{2k} + \frac{c}{12k^2}\right\}\left(1 + O\left(\frac{1}{k}\right)\right).$$

Although this estimate is more precise, the asymptotic given in Theorem 4.1 is still very accurate. We will use that asymptotic in our work.

4.3.4 Finding the Critical Value

With an asymptotic for $t_1(c)$ and consequently for T_1, we are now in a position to determine the range of l where $T_1 < 1$. Recall in Section 4.3.1 that we found the first term of $E(2^s)$ to be

$$T_1 \sim lk^{-c}e^{-c\gamma - h_\zeta(c)}. \tag{4.22}$$

Since $l = dk$, we may substitute this into (4.22) to find the new approximation

$$T_1 \sim dk^{1-c}e^{-c\gamma - h_\zeta(c)}. \tag{4.23}$$

To find the critical range for l, we will instead use this asymptotic to determine the range for d where $T_1 < 1$. To do this, we must solve the inequality

$$dk^{1-c}e^{-c\gamma - h_\zeta(c)} < 1. \tag{4.24}$$

Observe that k^{1-c} is the dominant term in (4.23) and $k^{1-c} > 1$. As $k \to \infty$, this term becomes quite large. So d will need to be very small in order to obtain $T_1 < 1$. The inequality in (4.24) is solved easily and we find that

$$d < \frac{e^{c\gamma + h_\zeta(c)}}{k^{1-c}} \tag{4.25}$$

ensures that $T_1 < 1$. We define d_1 to be this critical value, that is

$$d_1 = \frac{e^{c\gamma + h_\zeta(c)}}{k^{1-c}}. \tag{4.26}$$

When $d < d_1$, we know that $T_1 < 1$ and we hope to see that the largest term of $E(2^s)$ is the 0^{th} term. If this is the case and the remaining terms are small enough, then $E(2^s) \to 1$ and the vectors generated are, with high probability, independent. This will mean that $l_1 = d_1 k$ is a lower bound for the number of vectors needed to generate a dependent set. Notice that l_1 is not very large. For example, if $k = 1000$ and $c = 1/3$, this result implies that the first 14 randomly chosen vectors could be independent. This small lower bound may be somewhat surprising when we compare it to the much larger lower bound for the fixed weight vector case. Recall our hypothesis in Section 4.2 that we would need to generate fewer vectors to see dependency with this model than we did in the fixed weight model. Although

this result does not prove that claim, it does make the lower bound less surprising. However, we still must check that the remaining terms are decreasing and that their contribution to $E(2^s)$ is negligible.

4.4 The Second Term, T_2

The plots we saw in Section 4.2 seemed to suggest that the terms of $E(2^s)$ are unimodular. If we knew this to be true, then we would know that T_2 is less than T_1 in the critical range we just found. Since we don't know that the terms are unimodular, we will show that $T_2 < T_1$ whenever $T_1 < 1$ in this section. By (4.2), the second term of $E(2^s)$ is

$$T_2 = \binom{l}{2} \prod_{j=1}^{k} \frac{1 + \left(1 - \frac{2c}{j}\right)^2}{2} \tag{4.27}$$

As with T_1, we see that T_2 consists of two factors: a function of l and a product that depends on k. Let $t_2(c, k) \equiv t_2(c)$ be

$$t_2(c) = \prod_{j=1}^{k} \frac{1 + \left(1 - \frac{2c}{j}\right)^2}{2} \,. \tag{4.28}$$

Before determining the values of l where $T_2 < T_1$, we must determine the behavior of $t_2(c)$. Once we find an asymptotic function describing $t_2(c)$, we will be able to find a critical range for l as we did in the last section.

4.4.1 A Naive Approximation for T_2

A first approach to this problem might be to proceed as we did in the proof of Theorem 4.1. There, we first rewrote $t_1(c)$ as an exponential function. Using this technique, $t_2(c)$ becomes

$$\begin{aligned} t_2(c) &= \prod_{j=1}^{k} \frac{1 + \left(1 - \frac{2c}{j}\right)^2}{2} \\ &= \exp\left\{ \sum_{j=1}^{k} \log\left(1 + \left(1 - \frac{2c}{j}\right)^2\right) - \log 2 \right\}. \end{aligned}$$

Finding bounds for the sum of the logs is difficult with the added exponent. Instead of continuing with this expression, let's rewrite $t_2(c)$.

$$\begin{aligned} t_2(c) &= \prod_{j=1}^{k} \frac{1+\left(1-\frac{2c}{j}\right)^2}{2} \\ &= \prod_{j=1}^{k} \left(1-\frac{2c}{j}\left(1-\frac{c}{j}\right)\right) \end{aligned} \tag{4.29}$$

Continuing now as in Theorem 4.1, the product becomes

$$t_2(c) = \prod_{j=1}^{k} \left(1-\frac{2c}{j}\left(1-\frac{c}{j}\right)\right) = \exp\left\{\sum_{j=1}^{k} \log\left(1-\frac{2c}{j}\left(1-\frac{c}{j}\right)\right)\right\}$$

and we may now replace the log function with a Taylor series. Bounds for this function are still difficult to obtain due to the extra factor $1-c/j$. Notice, however, that as j grows, $1-c/j$ becomes extremely close to 1. Concentrating on this factor, we can replace it by constant upper and lower bounds, allowing us to find bounds for the product.

To find a good upper bound for $t_2(c)$, we must be sure that the lower bound on $1-c/j$ is close to 1. For all j, $1-c/j \geq 1-c > 1/2$, but we desire an even better bound. As j increases, the lower bound becomes better. Let $\epsilon = c/10$ and observe that

$$1-\frac{c}{j} \geq 1-\epsilon > \frac{19}{20}$$

for all $j \geq 10$. We can then see that

$$\prod_{j=10}^{k} \left(1-\frac{2c}{j}\left(1-\frac{c}{j}\right)\right) \leq \prod_{j=10}^{k} \left(1-\frac{2c(1-\epsilon)}{j}\right).$$

Since this bound is only true for $j \geq 10$, we must separate the first terms and include them in the final bound. To extend this bound to the original product, we first define

$$P = \prod_{j=1}^{9} \left(1-\frac{2c}{j}\left(1-\frac{c}{j}\right)\right).$$

With this, the upper bound for $t_2(c)$ now becomes

$$t_2(c) \leq P \prod_{j=10}^{k} \left(1-\frac{2c(1-\epsilon)}{j}\right).$$

Proceeding as in Theorem 4.1 on the product for $j \geq 10$, we find

$$t_2(c) \leq k^{-2c(1-\epsilon)} P e^{-2c(1-\epsilon)\gamma + \frac{7129}{1260}c(1-\epsilon) - h'_\zeta(2c(1-\epsilon))} \left(1 + O\left(\frac{1}{k}\right)\right) \tag{4.30}$$

where

$$h'_\zeta(z) = \sum_{m=2}^{\infty} \frac{z^m}{m} \left(\zeta(m) - \sum_{j=1}^{9} \frac{1}{j^m}\right).$$

The terms in this bound are similar to what we saw in the asymptotic for $t_1(c)$. However, in finding a better lower bound by pulling out the first nine terms, we have added quite a bit of difficulty to the result.

To find a lower bound that we can compare to the upper bound just found, we factor out the first nine terms. Now observe that $1 - c/j < 1$ for all j, so that

$$t_2(c) > P \prod_{j=10}^{k} \left(1 - \frac{2c}{j}\right).$$

The above product can be analyzed as in Theorem 4.1 to obtain the following lower bound:

$$t_2(c) > k^{-2c} P e^{-2c\gamma + \frac{7129}{1260}c - h'_\zeta(2c)} \left(1 + O\left(\frac{1}{k}\right)\right). \tag{4.31}$$

We again see factors similar to those we found in (4.30) and (4.7). To determine an asymptotic for $t_2(c)$, we would need to take a limit of both the upper and lower bounds. But the factor of $1-\epsilon$ appearing in the upper bound makes it impossible to do this. However, we expect that $t_2(c)$ behaves like the lower bound and will need to find a different method to find the estimate.

What we do see from the bounds above is that it appears as though the $r = 2$ term is roughly the square of the $r = 1$ term with a little "extra" thrown in. To be slightly more precise, the bounds given in (4.30) and (4.31) indicate that $t_2(c)$ is roughly $t_1(2c)$ along with a correction, or error, factor. In the next section, we will use this idea to find a better asymptotic for $t_2(c)$.

4.4.2 A Better Asymptotic for T_2

The basic idea behind the approximation found in this section is the same as in the last section: the factor $1 - c/j$ is very close to 1. This means that as j

increases,

$$1 - \frac{2c}{j}\left(1 - \frac{c}{j}\right)$$

becomes closer to

$$1 - \frac{2c}{j}\,.$$

This motivates us to compare $t_2(c)$ to the product

$$\prod_{j=1}^{k}\left(1 - \frac{2c}{j}\right).$$

Observe that this last expression is actually $t_1(2c)$. In fact, we were already doing this comparison in Section 4.4.1. In this section, we will be more precise, allowing us to write $t_2(c)$ as a function of $t_1(c)$ as well as eliminating the need to separate the initial term of the product. We first define

$$Q_{2,k}(c) = \prod_{j=1}^{k} \frac{1 - \frac{2c}{j}\left(1 - \frac{c}{j}\right)}{1 - \frac{2c}{j}} \tag{4.32}$$

to be the ratio of $t_2(c)$ to $t_1(2c)$ and define $Q_2(c)$ to be the limit of $Q_{2,k}(c)$ as $k \to \infty$. As in Theorem 4.1, we will be using error estimates in this proof. The statements and proofs of these estimates will be delayed until the next section.

Theorem 4.2 *Suppose $0 < c < 1/2$ and define $t_1(c)$ and $t_2(c)$ as follows:*

$$\begin{aligned} t_1(c) &= \prod_{j=1}^{k} \frac{1 + (1 - \frac{2c}{j})}{2}\,, \\ t_2(c) &= \prod_{j=1}^{k} \frac{1 + \left(1 - \frac{2c}{j}\right)^2}{2} = \prod_{j=1}^{k} 1 - \frac{2c}{j}\left(1 - \frac{c}{j}\right). \end{aligned}$$

Then the ratio of the two products,

$$Q_{2,k}(c) = \frac{t_2(c)}{t_1(2c)}\,,$$

converges to $Q_2(c)$ as $k \to \infty$. Furthermore,

$$t_2(c) \sim t_1(2c)Q_2(c). \tag{4.33}$$

Proof: The ratio, $Q_{2,k}(c)$, will allow us to determine how close $t_2(c)$ is to $t_1(2c)$. First observe that

$$\begin{aligned} Q_{2,k}(c) &= \frac{t_2(c)}{t_1(2c)} \\ &= \prod_{j=1}^{k} \frac{1-\frac{2c}{j}\left(1-\frac{c}{j}\right)}{1-\frac{2c}{j}} \end{aligned}$$

as defined in (4.32). Furthermore,

$$\begin{aligned} \prod_{j=1}^{k} \frac{1-\frac{2c}{j}\left(1-\frac{c}{j}\right)}{1-\frac{2c}{j}} &= \prod_{j=1}^{k} \frac{1-\frac{2c}{j}+\frac{2c^2}{j^2}}{1-\frac{2c}{j}} \\ &= \prod_{j=1}^{k} 1+\frac{2c^2}{j^2}\left(1-\frac{2c}{j}\right)^{-1}. \end{aligned} \tag{4.34}$$

Consider the final product given in (4.34). We claim that this converges as $k \to \infty$. From real analysis we know that when $a_j \geq 0$, the infinite product

$$\prod_{j=1}^{\infty}(1+a_j)$$

converges if and only if the series

$$\sum_{j=1}^{\infty} a_j$$

converges. Since $2c < 1$, $2c/j < 1$ also. Thus

$$\frac{2c^2}{j^2}\left(1-\frac{2c}{j}\right)^{-1} \geq 0$$

for all j. Furthermore, when $j > 2$, $1 - 2c/j > 1/2$, so

$$\left(1-\frac{2c}{j}\right)^{-1} < 2.$$

We use this to find the following upper bound for the positive sum,

$$\sum_{j=3}^{\infty} \frac{2c^2}{j^2}\left(1-\frac{2c}{j}\right)^{-1} < \sum_{j=3}^{\infty} \frac{4c^2}{j^2}\,.$$

Since the series on the right is a convergent $p-$series, the sum on the left converges also. Thus as $k \to \infty$, the finite product $Q_{2,k}(c)$ converges to the infinite product

$$\prod_{j=1}^{\infty} \frac{1-\frac{2c}{j}\left(1-\frac{c}{j}\right)}{1-\frac{2c}{j}}\,.$$

We set this limit to be $Q_2(c)$.

Since $Q_2(c)$ converges for fixed c, we can use it to write $t_2(c)$ in terms of $t_1(2c)$. It is simple to write $t_2(c)$ as a function of $Q_{2,k}(c)$ and $t_1(2c)$: by definition,

$$t_2(c) = t_1(2c)Q_{2,k}(c). \tag{4.35}$$

We wish to replace $Q_{2,k}(c)$ above with $Q_2(c)$. However, since $Q_{2,k}(c)$ approaches $Q_2(c)$ as $k \to \infty$, the substitution is not exact. We will need to include an error term to account for the fact that $Q_2(c)$ is an infinite product while $Q_{2,k}(c)$ is finite. This substitution will eliminate the parameter k, and enable us to give an estimate for $t_2(c)$ for fixed c. First observe that

$$\begin{aligned} 1 &< \frac{Q_2(c)}{Q_{2,k}(c)} \\ &= \prod_{j=k+1}^{\infty} \frac{1 - \frac{2c}{j}\left(1 - \frac{c}{j}\right)}{1 - \frac{2c}{j}} \\ &= \prod_{j=k+1}^{\infty} \left(1 + \frac{2c^2}{j^2}\left(1 - \frac{2c}{j}\right)^{-1}\right). \end{aligned}$$

The expression above is the error incurred by replacing $Q_{2,k}(c)$ by $Q_2(c)$. To find an approximation for this error, we bound it above by an exponential function.

$$\begin{aligned} \prod_{j=k+1}^{\infty} \left(1 + \frac{2c^2}{j^2}\left(1 - \frac{2c}{j}\right)^{-1}\right) &< \exp\left\{\sum_{j=k+1}^{\infty} \frac{2c^2}{j^2}\left(1 - \frac{2c}{j}\right)^{-1}\right\} \\ &= \exp\left\{\sum_{j=k+1}^{\infty} \frac{2c^2}{j(j-2c)}\right\} \\ &= \exp\left\{O\left(\frac{1}{k}\right)\right\} \\ &= 1 + O\left(\frac{1}{k}\right) \end{aligned}$$

We will discuss the error found in replacing the sum by the big-O term further in Section 4.4.3, but this gives a relation between $Q_{2,k}(c)$ and $Q_2(c)$ in terms of the difference between the two:

$$Q_2(c) = Q_{2,k}(c)\left(1 + O\left(\frac{1}{k}\right)\right).$$

Since $(1+x)^{-1} = 1 + O(x)$, we may write

$$Q_{2,k}(c) = Q_2(c)\left(1 + O\left(\frac{1}{k}\right)\right),$$

thus giving an expression to substitute for $Q_{2,k}(c)$. Along with (4.35), this gives

$$t_2(c) = t_1(2c)Q_2(c)\left(1 + O\left(\frac{1}{k}\right)\right).$$

Finally, since $1 + O(k^{-1}) \to 1$ as $k \to \infty$, we have shown (4.33). □

As we conjectured from the bounds given in (4.30) and (4.31), this theorem shows that $t_2(c)$ is closely related to $t_1(c)$ and in fact, $t_2(c)$ is $t_1(2c)$ times a little "extra," the convergent product, $Q_2(c)$. To be precise, we now have

$$t_2(c) \sim k^{-2c} e^{-2c\gamma - h_\zeta(2c)} \prod_{j=1}^{\infty} \frac{1 + \left(1 - \frac{2c}{j}\right)^2}{2\left(1 - \frac{2c}{j}\right)}. \tag{4.36}$$

We will soon use this estimation for $t_2(c)$ to determine when $T_2 < T_1$, but will first take a look at the error encountered in the last proof.

4.4.3 Error Analysis for Theorem 4.2

In Theorem 4.2 we use the fact that

$$\sum_{j=k+1}^{\infty} \frac{2c^2}{j(j-2c)} = O\left(\frac{1}{k}\right).$$

Since we are adding an infinite number of terms that are $O(k^{-1})$, we must check that this series is in fact $O(k^{-1})$. The following lemma gives the bounds we need.

Lemma 4.7 *Let $0 < c < 1/2$ and $k \geq 2$. Then*

$$\frac{c^2}{k} < \sum_{j=k+1}^{\infty} \frac{2c^2}{j(j-2c)} < \frac{2c^2}{k}. \tag{4.37}$$

Proof: We find the upper bound first. Observe that since $2c < 1$, $j - 2c > j - 1$ and therefore

$$\sum_{j=k+1}^{\infty} \frac{2c^2}{j(j-2c)} < \sum_{j=k+1}^{\infty} \frac{2c^2}{j(j-1)}. \tag{4.38}$$

In Theorem 4.2 we showed that the infinite series in (4.37) converges. Similarly, we can show that the new series in (4.38) converges. Furthermore, since the terms of the sum are all positive, it is absolutely convergent. Therefore we may rearrange

the terms. The series can be decomposed into the difference of two other sums,

$$\sum_{j=k+1}^{\infty} \frac{2c^2}{j(j-1)} = 2c^2 \left(\sum_{j=k+1}^{\infty} \frac{1}{j-1} - \sum_{j=k+1}^{\infty} \frac{1}{j} \right).$$

We simplify the difference to find the desired upper bound,

$$\sum_{j=k+1}^{\infty} \frac{2c^2}{j(j-2c)} < \frac{2c^2}{k}. \tag{4.39}$$

To find the lower bound, we observe that $j - 2c < j$, so

$$\sum_{j=k+1}^{\infty} \frac{2c^2}{j(j-2c)} > \sum_{j=k+1}^{\infty} \frac{2c^2}{j^2}.$$

Rewriting this series, we see that

$$\sum_{j=k+1}^{\infty} \frac{2c^2}{j^2} = \zeta(2) - \sum_{j=1}^{k} \frac{2c^2}{j^2}.$$

By Lemma 4.2, we find a lower bound to be

$$\sum_{j=k+1}^{\infty} \frac{2c^2}{j^2} > \frac{2c^2}{k} - \frac{c^2}{k^2} + \frac{c^2}{6k^3} - \frac{c^2}{15k^5}.$$

Since $c^2/6k^3 - c^2/15k^5 > 0$, we can simplify this bound and see that

$$\sum_{j=k+1}^{\infty} \frac{2c^2}{j^2} > \frac{2c^2}{k} - \frac{c^2}{k^2}.$$

Finally, since $k > 1$,

$$\sum_{j=k+1}^{\infty} \frac{2c^2}{j^2} > \frac{2c^2}{k} - \frac{c^2}{k} = \frac{c^2}{k}. \tag{4.40}$$

The inequalities in (4.39) and (4.40) prove the result. □

From this lemma, we have the estimate

$$\sum_{j=k+1}^{\infty} \frac{2c^2}{j(j-2c)} = O\left(\frac{1}{k}\right)$$

used to bound the error introduced by replacing $Q_{2,k}(c)$ by $Q_2(c)$ in the proof of Theorem 4.2.

We now have an asymptotic for $t_2(c)$:

$$t_2(c) \sim k^{-2c} e^{-2c\gamma - h_\zeta(2c)} \prod_{j=1}^{\infty} \frac{1 + \left(1 - \frac{2c}{j}\right)^2}{2\left(1 - \frac{2c}{j}\right)}.$$

Consequently, this gives an approximation for T_2,

$$\begin{aligned} T_2 &= \binom{l}{2} t_2(c) \\ &\sim \frac{l(l-1)}{2}\, k^{-2c} e^{-2c\gamma - h_\zeta(2c)} \prod_{j=1}^{\infty} \frac{1+\left(1-\frac{2c}{j}\right)^2}{2\left(1-\frac{2c}{j}\right)}\,. \end{aligned} \tag{4.41}$$

We can now use (4.41) to find a range of l values where $T_2 < T_1$.

4.4.4 Finding the Critical Value

In Section 4.3.4, we found that $T_1 < 1$ when $l < l_1 = d_1 k$ where

$$d_1 = \frac{e^{c\gamma + h_\zeta(c)}}{k^{1-c}}\,.$$

As stated there, we suspect that $T_2 < T_1$ in this range also. With the asymptotic for T_2, we can show that this is true. Substituting $l = dk$, equation (4.41) becomes

$$T_2 \sim \frac{dk(dk-1)}{2}\, k^{-2c} e^{-2c\gamma - h_\zeta(2c)} Q_2(c).$$

To determine when T_2 is less than

$$T_1 \sim dk^{1-c} e^{-c\gamma - h_\zeta(c)},$$

we solve the inequality

$$dk^{1-c} e^{-c\gamma - h_\zeta(c)} > \frac{dk(dk-1)}{2}\, k^{-2c} e^{-2c\gamma - h_\zeta(2c)} Q_2(c). \tag{4.42}$$

Solving this, we find that $T_2 < T_1$ when

$$d < \frac{2}{k^{1-c} Q_2(c)}\, e^{c\gamma + h_\zeta(2c) - h_\zeta(c)} + \frac{1}{k}\,. \tag{4.43}$$

Set d_2 to be the right side of (4.43). If we can show that $d_1 < d_2$, then we will have shown that $T_2 < T_1$ whenever $T_1 < 1$. We do this in the next theorem.

Theorem 4.3 *Let $0 < c < 2/5$ and $l = dk$. If $T_1 < 1$, then $T_2 < T_1$ also.*

Proof: Let $l = dk$ and suppose that $T_1 < 1$. From previous work we know that $T_1 < 1$ when

$$d < d_1 = \frac{e^{c\gamma + h_\zeta(c)}}{k^{1-c}}\,.$$

and that $T_2 < T_1$ when

$$d < d_2 = \frac{2}{k^{1-c}Q_2(c)} e^{c\gamma + h_\zeta(2c) - h_\zeta(c)} + \frac{1}{k}\,.$$

Since $T_1 < 1$ by assumption, $d < d_1$. To show that $T_2 < T_1$, we must prove that $d < d_2$ also. If we can show that $d_1 < d_2$, we will be done. Observe that

$$\begin{aligned} d_2 &= \frac{2}{k^{1-c}Q_2(c)}\, e^{c\gamma + h_\zeta(2c) - h_\zeta(c)} + \frac{1}{k} \\ &= \frac{e^{c\gamma + h_\zeta(c)}}{k^{1-c}}\, \frac{2e^{h_\zeta(2c) - 2h_\zeta(c)}}{Q_2(c)} + \frac{1}{k} \\ &= d_1\, \frac{2e^{h_\zeta(2c) - 2h_\zeta(c)}}{Q_2(c)} + \frac{1}{k}\,. \end{aligned} \tag{4.44}$$

Then $d_1 < d_2$ when

$$d_1 < d_1\, \frac{2e^{h_\zeta(2c) - 2h_\zeta(c)}}{Q_2(c)} + \frac{1}{k}\,.$$

It is sufficient to show that

$$d_1 < d_1\, \frac{2e^{h_\zeta(2c) - 2h_\zeta(c)}}{Q_2(c)}\,,$$

since

$$d_1\, \frac{2e^{h_\zeta(2c) - 2h_\zeta(c)}}{Q_2(c)} < d_1\, \frac{2e^{h_\zeta(2c) - 2h_\zeta(c)}}{Q_2(c)} + \frac{1}{k} = d_2.$$

Thus we would like to show that

$$Q_2(c) e^{2h_\zeta(c) - h_\zeta(2c)} < 2. \tag{4.45}$$

In order to find an upper bound on $Q_2(c)e^{2h_\zeta(c) - h_\zeta(2c)}$, we want to first find an equivalent expression that is more straightforward to analyze. Observe that we can rewrite $2h_\zeta(c) - h_\zeta(2c)$ in terms of logs. By the definition of $h_\zeta(c)$,

$$\begin{aligned} 2h_\zeta(c) - h_\zeta(2c) &= 2\sum_{m=2}^{\infty} \frac{c^m}{m}\zeta(m) - \sum_{m=2}^{\infty} \frac{(2c)^m}{m}\zeta(m) \\ &= 2\sum_{m=2}^{\infty} \frac{c^m}{m} \sum_{j=1}^{\infty} \frac{1}{j^m} - \sum_{m=2}^{\infty} \frac{(2c)^m}{m} \sum_{j=1}^{\infty} \frac{1}{j^m}\,. \end{aligned}$$

Recall that $h_\zeta(c)$ is absolutely convergent when $c < 1$. Rearranging the terms, we see

$$\begin{aligned} 2h_\zeta(c) - h_\zeta(2c) &= 2\sum_{m=2}^{\infty} \frac{c^m}{m} \sum_{j=1}^{\infty} \frac{1}{j^m} - \sum_{m=2}^{\infty} \frac{(2c)^m}{m} \sum_{j=1}^{\infty} \frac{1}{j^m} \\ &= \sum_{j=1}^{\infty} \left(2\sum_{m=2}^{\infty} \left(\frac{c}{j}\right)^m \frac{1}{m} - \sum_{m=2}^{\infty} \left(\frac{2c}{j}\right)^m \frac{1}{m} \right). \end{aligned}$$

Now, recognizing that this is one term away from the Taylor expansion for log, we rewrite this one more time to find

$$\begin{aligned} h_\zeta(2c) - 2h_\zeta(c) &= \sum_{j=1}^{\infty} \left(\sum_{m=2}^{\infty} \left(2\sum_{m=2}^{\infty} \left(\frac{c}{j}\right)^m \frac{1}{m} - \frac{2c}{j} \right)^m \frac{1}{m} \right) \\ &= \sum_{j=1}^{\infty} \left(-2\log\left(1 - \frac{c}{j}\right) - \frac{2c}{j} + \log\left(1 - \frac{2c}{j}\right) + \frac{2c}{j} \right) \\ &= \sum_{j=1}^{\infty} \log\left(\frac{1 - \frac{2c}{j}}{\left(1 - \frac{c}{j}\right)^2} \right). \end{aligned}$$

Substituting this in the exponential function, this becomes

$$\begin{aligned} e^{h_\zeta(2c) - 2h_\zeta(c)} &= \exp\left\{ \sum_{j=1}^{\infty} \log\left(\frac{1 - \frac{2c}{j}}{\left(1 - \frac{c}{j}\right)^2} \right) \right\} \\ &= \prod_{j=1}^{\infty} \frac{1 - \frac{2c}{j}}{\left(1 - \frac{c}{j}\right)^2}. \end{aligned}$$

With this expression, the left side of (4.45) becomes

$$\begin{aligned} Q_2(c) e^{2h_\zeta(c) - h_\zeta(2c)} &= \prod_{j=1}^{\infty} \frac{1 + \left(1 - \frac{2c}{j}\right)^2}{2\left(1 - \frac{c}{j}\right)^2} \\ &= \prod_{j=1}^{\infty} 1 + \frac{c^2}{(j-c)^2}. \end{aligned} \tag{4.46}$$

We now want to show that the product given in (4.46) is less than 2. We will be using the fact that $j - c > j - 1$ to rewrite this expression and as a result will need to be careful of the range of the product. We will separate the initial term of the

product to do this and in order to obtain a sharper result. Observe that

$$\begin{aligned} Q_2(c)e^{2h_\zeta(c)-h_\zeta(2c)} &= \prod_{j=1}^{\infty} 1+\frac{c^2}{(j-c)^2} \\ &= \left(1+\frac{c^2}{(1-c)^2}\right)\exp\left\{\sum_{j=2}^{\infty}\log\left(1+\frac{c^2}{(j-c)^2}\right)\right\} \\ &< \left(1+\frac{c^2}{(1-c)^2}\right)\exp\left\{\sum_{j=2}^{\infty}\frac{c^2}{(j-c)^2}\right\}. \end{aligned}$$

Now, since $j-c>j-1$, we can bound the last expression above by

$$\begin{aligned} \left(1+\frac{c^2}{(1-c)^2}\right)\exp\left\{\sum_{j=2}^{\infty}\frac{c^2}{(j-c)^2}\right\} &< \left(1+\frac{c^2}{(1-c)^2}\right)\exp\left\{\sum_{j=2}^{\infty}\frac{c^2}{(j-1)^2}\right\} \\ &= \left(1+\frac{c^2}{(1-c)^2}\right)\exp\left\{\sum_{j=1}^{\infty}\frac{c^2}{j^2}\right\}. \end{aligned}$$

Finally, since the sum over the squares is $\zeta(2)$, we find that

$$Q_2(c)e^{2h_\zeta(c)-h_\zeta(2c)} < \left(1+\frac{c^2}{(1-c)^2}\right)e^{c^2\pi^2/6}. \tag{4.47}$$

Since this expression is maximized when $c=2/5$, we find that

$$Q_2(c)e^{2h_\zeta(c)-h_\zeta(2c)} < \frac{13}{9}\,e^{2\pi^2/75} < 1.87932\ldots \tag{4.48}$$

Since this is less than 2, we have shown that the inequality in (4.45) is true. Thus $d<d_2$ whenever $d<d_1$ and therefore $T_2<T_1$ when $T_1<1$. □

This theorem supports our expectation that the terms of $E(2^s)$ continue to decrease when $T_1<1$ for $0<c<2/5$. In the following sections, we will check that the remaining terms are decreasing quickly enough to allow $E(2^s)$ to converge to 1.

4.5 The r^{th} Term, T_r

In order for the terms of $E(2^s)$ to be unimodal with the maximum term being the 0^{th} term, we need to know that $T_{r+1}<T_r$ for all $r\geq 0$. We know that this inequality is true for $r=0$ and $r=1$, that is, $T_2<T_1<T_0$ for appropriate values of d. In the next few sections, we will show that this is true for $r\geq 2$. To do this, we will first need an approximation on the size of T_r for $r\geq 3$.

4.5.1 A Heuristic for T_r

In Section 4.2, we set the r^{th} term of $E(2^s)$ to be

$$T_r = \binom{l}{r} \prod_{j=1}^{k} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2}. \tag{4.49}$$

As with T_1 and T_2, the part of T_r that is difficult to analyze is the product. Let $t_r(c,k) \equiv t_r(c)$ be

$$t_r(c) = \prod_{j=1}^{k} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2}. \tag{4.50}$$

In this section, we find a heuristic for the size of $t_r(c)$. Although this heuristic will be valid for a limited number of r values, it will give an idea of the behavior of $t_r(c)$ and enable us to state a more exact theorem in the next section.

As we have seen, it is simpler to deal with sums than with products, so we rewrite the product as

$$t_r(c) = \prod_{j=1}^{k} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2} = \exp\left\{ \sum_{j=1}^{k} \log\left(\frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2} \right) \right\}$$

and look at the new sum

$$\sum_{j=1}^{k} \log\left(\frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2} \right)$$

to give us information about $t_r(c)$.

Now, if $2c/j$ is close to 0, then we can use the approximation

$$\left(1 - \frac{2c}{j}\right)^r \simeq e^{-\theta/j},$$

where $\theta = 2cr$. Since this will just be a heuristic, we will not give a careful analysis of error in this section. Since log is a smooth function, it is natural to estimate our sum with an integral using Euler Maclaurin summation. Thus

$$\begin{aligned} \sum_{j=1}^{k} \log\left(\frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2} \right) &\simeq \sum_{j=1}^{k} \log\left(\frac{1 + e^{-\theta/j}}{2} \right) \\ &\simeq \int_1^k \log\left(\frac{1 + e^{-\theta/x}}{2} \right) dx. \end{aligned} \tag{4.51}$$

Notice that we have only used the integral approximation from Euler Maclaurin. If we were to make this heuristic more exact we would need to include more terms, but this estimate will be sufficient.

As it is written now, the integral in (4.51) is difficult to integrate. So we need to transform it to an integral that is easier to compute. Notice that

$$\frac{1+e^{-\theta}}{2} < \frac{1+e^{-\theta/x}}{2} < 1$$

so that the integral will be negative. The most negative part of the integrand occurs when θ/x is large, or when x is small. But the integrand very quickly approaches 0, making the contribution of small x to the integral minute. Since the integrand is close to 0 for most of the interval, the x values in this range have the most effect on the value of the integral. So we will concentrate on this range to see how much it does contribute. Thus when θ/x is small, or when x is large, we need to determine how the integrand behaves.

Now, when θ/x is small, the Taylor series expansion for $e^{-\theta/x}$ gives $e^{-\theta/x} \simeq 1 - \frac{\theta}{x}$. Thus

$$\frac{1+e^{-\theta/x}}{2} \simeq \frac{1+1-\frac{\theta}{x}}{2} = 1 - \frac{\theta}{2x}\,.$$

Along with the Taylor series expansion for log, this gives the asymptotic

$$\log\left(\frac{1+e^{-\theta/x}}{2}\right) \simeq \log\left(1-\frac{\theta}{2x}\right) \simeq \frac{-\theta}{2x}\,.$$

So we see in the area of interest, the integrand behaves like $-\theta/2x$. Now this function is easy to integrate. We now add and subtract $-\theta/2x$ from the integral to end up with the sum of an integral that we know how to do and another integral that is smaller than the first. The "smaller" integral will be what remains after removing the contribution of $-\theta/2x$ to the integral. We will then need to estimate

the remaining integral. Returning to (4.51), we find

$$\begin{aligned}\int_1^k \log\left(\frac{1+e^{-\theta/x}}{2}\right)\,dx &= \int_1^k \log\left(\frac{1+e^{-\theta/x}}{2}\right)+\frac{\theta}{2x}-\frac{\theta}{2x}\,dx \\ &= \int_1^k \log\left(\frac{1+e^{-\theta/x}}{2}\right)+\frac{\theta}{2x}\,dx-\int_1^k \frac{\theta}{2x}\,dx \\ &= \int_1^k \log\left(\frac{1+e^{-\theta/x}}{2}\right)+\frac{\theta}{2x}\,dx-\frac{\theta}{2}\log k. \quad (4.52)\end{aligned}$$

Combining (4.51) and (4.52), we now have

$$\begin{aligned}\sum_{j=1}^{k}\log\left(\frac{1+\left(1-\frac{2c}{j}\right)^r}{2}\right) &\simeq \int_1^k \log\left(\frac{1+e^{-\theta/x}}{2}\right)\,dx \\ &= -\frac{\theta}{2}\log k+\int_1^k \log\left(\frac{1+e^{-\theta/x}}{2}\right)+\frac{\theta}{2x}\,dx (4.53)\end{aligned}$$

We now consider the last integral above. We use the fact that for fixed θ, the integral

$$\int_1^\infty \log\left(\frac{1+e^{-\theta/x}}{2}\right)+\frac{\theta}{2x}\,dx$$

is convergent. Replacing the definite integral by an improper integral will allow us to write the integral in (4.53) as the sum of an exact value and the tail of the integral. The integrand for large values of x is extremely small so we will be able to find an estimate for the size of the integral tail. Observe that

$$\begin{aligned}&\int_1^k \log\left(\frac{1+e^{-\theta/x}}{2}\right)+\frac{\theta}{2x}\,dx \\ &= \int_1^\infty \log\left(\frac{1+e^{-\theta/x}}{2}\right)+\frac{\theta}{2x}\,dx-\int_k^\infty \log\left(\frac{1+e^{-\theta/x}}{2}\right)+\frac{\theta}{2x}\,dx. \quad (4.54)\end{aligned}$$

Since

$$e^{-\theta/x}<1-\frac{-\theta}{x}+\frac{\theta^2}{2x^2}$$

by the Taylor expansion of e^{-y}, we see that

$$\log\left(\frac{1+e^{-\theta/x}}{2}\right)<\log\left(1-\frac{\theta}{2x}+\frac{\theta^2}{4x^2}\right)<-\frac{\theta}{2x}+\frac{\theta^2}{4x^2}$$

by a standard upper bound for the Taylor expansion of log. Thus we may bound the tail of the integral above and find an estimate as follows.

$$\begin{aligned}\int_k^\infty \log\left(\frac{1+e^{-\theta/x}}{2}\right)+\frac{\theta}{2x}\,dx &< \int_k^\infty -\frac{\theta}{2x}+\frac{\theta^2}{4x^2}+\frac{\theta}{2x}\,dx\\ &= \int_k^\infty \frac{\theta^2}{4x^2}\,dx\\ &= \frac{\theta^2}{4k}\\ &= O\left(\frac{1}{k}\right)\end{aligned}$$

Therefore (4.54) becomes

$$\int_1^k \log\left(\frac{1+e^{-\theta/x}}{2}\right)+\frac{\theta}{2x}\,dx=\int_1^\infty \log\left(\frac{1+e^{-\theta/x}}{2}\right)+\frac{\theta}{2x}\,dx+O\left(\frac{1}{k}\right).$$

We now need to estimate the improper integral. Let $u=x/\theta$. Then

$$\int_1^\infty \log\left(\frac{1+e^{-\theta/x}}{2}\right)+\frac{\theta}{2x}\,dx=\theta\int_{1/\theta}^\infty \log\left(\frac{1+e^{-1/u}}{2}\right)+\frac{1}{2u}\,du.$$

Since the latter integral grows as θ increases, we will decompose the integral and express it as the sum of a convergent integral and an integral whose limits depend on θ. So we get

$$\begin{aligned}&\theta\int_{1/\theta}^\infty \log\left(\frac{1+e^{-1/u}}{2}\right)+\frac{1}{2u}\,du\\ &\quad=\theta\int_1^\infty \log\left(\frac{1+e^{-1/u}}{2}\right)+\frac{1}{2u}\,du+\theta\int_{1/\theta}^1 \log\left(\frac{1+e^{-1/u}}{2}\right)+\frac{1}{2u}\,du.\end{aligned}$$

The first integral converges to give

$$D_1=\int_1^\infty \log\left(\frac{1+e^{-1/u}}{2}\right)+\frac{1}{2u}\,du=0.123329\ldots$$

On the interval $(0,1]$, the log function above is close to 0 and its integral converges. Therefore we can rewrite the second integral as

$$\begin{aligned}\theta\int_{1/\theta}^1 \log\left(\frac{1+e^{-1/u}}{2}\right)+\frac{1}{2u}\,du &= \theta\int_{1/\theta}^1 \log\left(\frac{1+e^{-1/u}}{2}\right)\,du+\theta\int_{1/\theta}^1\frac{1}{2u}\,du\\ &= \frac{\theta}{2}\log\theta+\theta\int_{1/\theta}^1 \log\left(\frac{1+e^{-1/u}}{2}\right)\,du.\end{aligned}$$

As $1/\theta \to 0$, this final integral converges to

$$D_2 = \int_0^1 \log\left(\frac{1+e^{-1/u}}{2}\right)\, du = -0.56051\ldots$$

Since the integral converges and is always negative, then for fixed, large θ,

$$\theta \int_{1/\theta}^1 \log\left(\frac{1+e^{-1/u}}{2}\right) + \frac{1}{2u}\, du = \theta D_2 + e_1,$$

where e_1 is an error term depending on θ. So for the improper integral, we have

$$\int_1^\infty \log\left(\frac{1+e^{-\theta/x}}{2}\right) + \frac{\theta}{2x}\, dx = \theta D_1 + \theta D_2 + \frac{\theta}{2}\log\theta + e_1. \tag{4.55}$$

Finally, putting together (4.53) and the estimation of the integral leading to (4.55), we have found

$$\begin{aligned}
&\sum_{j=1}^k \log\left(\frac{1+\left(1-\frac{2c}{j}\right)^r}{2}\right) \\
&\quad\simeq\ -\frac{\theta}{2}\log k + \int_1^k \log\left(\frac{1+e^{-\theta/x}}{2}\right) + \frac{\theta}{2x}\, dx \\
&\quad=\ -\frac{\theta}{2}\log k + \theta D_1 + \theta D_2 + \frac{\theta}{2}\log\theta + e_1 + O\left(\frac{1}{k}\right).
\end{aligned} \tag{4.56}$$

With the asymptotic in (4.56), we return to $t_r(c)$ and find

$$\begin{aligned}
t_r(c) &= \prod_{j=1}^k \frac{1+\left(1-\frac{2c}{j}\right)^r}{2} \\
&= \exp\left\{\sum_{j=1}^k \log\left(\frac{1+\left(1-\frac{2c}{j}\right)^r}{2}\right)\right\} \\
&\simeq \exp\left\{-\frac{\theta}{2}\log k + \theta(D_1+D_2) + \frac{\theta}{2}\log\theta + e_1 + O\left(\frac{1}{k}\right)\right\} \\
&= k^{-\theta/2}\theta^{\theta/2}e^{\theta(D_1+D_2)+e_1+O\left(\frac{1}{k}\right)} \\
&= k^{-rc}(2rc)^{rc}e^{2cr(D_1+D_2)+e_1}\left(1+\left(\frac{1}{k}\right)\right).
\end{aligned}$$

So we see that $t_r(c)$ is similar to the asymptotics we found for $t_1(c)$ and $t_2(c)$: the dominant term is k^{-rc} and there is a natural exponential factor. However, as stated before, we are only using this as a heuristic to begin to understand the behavior of $t_r(c)$. It turns out that the error incurred by our estimates and integrals restricts the values of r for which the work above is valid.

The problem arises from the behavior of

$$\log\left(\frac{1+\left(1-\frac{2c}{j}\right)^r}{2}\right); \tag{4.57}$$

in particular, how quickly it increases to 0. The index, j, does not have to be very large before $\left(1-\frac{2c}{j}\right)^r$ is close to 1. Since the majority of the terms satisfy this, this range contributes the most to the sum. Therefore we want to have a very small absolute error in our approximations for these terms. However, $e^{-2cr/j}$ is an extremely close approximation to $\left(1-\frac{2c}{j}\right)^r$ in this range. So the integral approximation we use in (4.51) is very close to the actual contribution made by the summand here. On the other hand, when $\left(1-\frac{2c}{j}\right)^r$ is very small, or when j is small, we see that (4.57) is very close to $-\log 2$. Since this occurs for so few values of j, we can allow large absolute error because it really does contribute so little to the sum.

But we must analyze the error and we run into problems when we start quantifying it. The measure of error actually relies heavily on r. Let's say $\left(1-\frac{2c}{j}\right)^r$ is small when it is close to $1/k$. Then

$$\left(1-\frac{2c}{j}\right)^r \simeq \frac{1}{k} \Leftrightarrow r \simeq \frac{j\log k}{2c},$$

or when

$$j < \frac{2cr}{\log k}.$$

But this means that r must be larger than $\log k/2c$ for this to be meaningful. So it becomes very difficult to measure error as it is so dependent on r. In fact, the asymptotic given is only valid for large r anyway. When evaluating the integral

$$\theta\int_{1/\theta}^{1}\log\left(\frac{1+e^{-1/u}}{2}\right)du,$$

we made the assumption that $\theta = 2cr$ was large. Since $0 < 2c < 1$, we are really making the assumption that r is large. Furthermore, we are assuming that $1/\theta < 1$. Since we must have $r > 1/2c$ for this to happen, if c is small, r must be quite large to even evaluate this integral as we have. Although this discussion has given us an idea of cases of r where an error analysis of this heuristic would be useful, we

would still need to find an alternate method of analyzing $t_r(c)$ for small r. In the next section, we will approach the problem from a different direction, resulting in an asymptotic that will be valid for all $r \geq 3$.

4.5.2 A Better Asymptotic for T_r

Although the error is difficult to analyze above, we now have a rough idea of what $t_r(c)$ looks like. The factor of k^{-rc} indicates that $t_r(c)$ looks something like $t_1(c)$ with rc substituted for c. This is the behavior we saw when analyzing $t_2(c)$ and we found that $t_2(c)$ behaves similarly to $t_1(2c)$. In this section, we will prove a theorem similar to Theorem 4.2, by comparing

$$t_r(c) = \prod_{j=1}^{k} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2}$$

to the product

$$t_1(rc) = \prod_{j=1}^{k} \frac{1 + (1 - \frac{2rc}{j})}{2} = \prod_{j=1}^{k} 1 - \frac{rc}{j}\,.$$

Observe that if we were to expand the numerator of $t_r(c)$, it would be similar to the numerator given in $t_1(rc)$, further justifying the given comparison. However, we run into problems with the second product when $j < rc$. In this range, $t_1(rc) < 0$, leading us to compare a negative product to a quantity that we know to be positive, resulting in an incorrect asymptotic. To overcome this problem, we will consider the product over this range separately. In fact, it is beneficial to split the product and look at it for $j \leq 2rc$ and the product for $j > 2rc$. When $j > 2rc$, we find

$$\frac{1}{2} < 1 - \frac{rc}{j} < 1,$$

giving less fluctuation in the product we're interested in. So we will write

$$\prod_{j=1}^{k} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2} = \prod_{j \leq 2rc} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2} \prod_{j > 2rc}^{k} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2} \tag{4.58}$$

and analyze each part of (4.58). We look at the product over small j first.

Lemma 4.8 *Let $0 < c < 1/2$ and let $r \geq 3$. Then*

$$\begin{aligned} & 2^{-\lfloor 2rc \rfloor} e^{e^{-2rc-2rc^2/(1-2c)}} e^{2rcC_3 e^{-r/4} - e^{-2}/2 - rcC_2} \\ < & \prod_{j \leq 2rc} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2} \\ < & 2^{-\lfloor 2rc \rfloor} e^{e^{-1}} e^{2rcC_1}. \end{aligned} \tag{4.59}$$

Proof: Rewriting the product above, we find that

$$\begin{aligned} \prod_{j \leq 2rc} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2} &= \exp\left\{ \sum_{j \leq 2rc} \log\left(1 + \left(1 - \frac{2c}{j}\right)^r\right) - \log 2 \right\} \\ &= 2^{-\lfloor 2rc \rfloor} \exp\left\{ \sum_{j \leq 2rc} \log\left(1 + \left(1 - \frac{2c}{j}\right)^r\right) \right\}. \end{aligned} \tag{4.60}$$

We wish to find bounds on the sum in (4.60) to prove the lemma. Starting with an upper bound, we use the Taylor expansion of log to bound the summand as follows.

$$\begin{aligned} \log\left(1 + \left(1 - \frac{2c}{j}\right)^r\right) &< \left(1 - \frac{2c}{j}\right)^r \\ &< e^{-\frac{2rc}{j}} \end{aligned}$$

Thus the sum is bounded above by

$$\sum_{j \leq 2rc} \log\left(1 + \left(1 - \frac{2c}{j}\right)^r\right) < \sum_{j \leq 2rc} e^{-\frac{2rc}{j}}.$$

We bound this exponential sum using Euler-Maclaurin summation.

$$\sum_{j \leq 2rc} e^{-\frac{2rc}{j}} < e^{-2rc} + \int_1^{2rc} e^{-\frac{2rc}{x}}\, dx + \frac{1}{2}(e^{-1} - e^{-2rc}) + \int_1^{2rc} B_1(t) e^{-2rc/t} \frac{2rc}{t^2}\, dt$$

Following the method of Lemma 4.1, we see that

$$\left| \int_1^{2rc} B_1(t) e^{-2rc/t} \frac{2rc}{t^2}\, dt \right| < \frac{1}{2} \int_1^{2rc} e^{-2rc/t} \frac{2rc}{t^2}\, dt = \frac{1}{2}(e^{-1} - e^{-2rc}).$$

This implies that

$$\begin{aligned} \sum_{j \leq 2rc} e^{-\frac{2rc}{j}} &< e^{-1} + \int_1^{2rc} e^{-\frac{2rc}{x}}\, dx \\ &= e^{-1} + 2rc \int_{1/2rc}^1 e^{-1/u}\, du. \end{aligned}$$

The latter integral is obtained using the substitution $x = 2rcu$. Since $1/2rc > 0$ and $e^{-1/u} > 0$, we can bound this integral above by another integral that does not depend on r or c,

$$\int_{1/2rc}^{1} e^{-1/u}\, du < \int_{0}^{1} e^{-1/u}\, du.$$

The final integral converges to $C_1 = 0.1484\ldots$. Thus

$$\begin{aligned} e^{-1} + 2rc \int_{1/2rc}^{1} e^{-1/u}\, du &< e^{-1} + 2rc \int_{0}^{1} e^{-1/u}\, du \\ &= e^{-1} + 2rcC_1. \end{aligned}$$

Combining this with (4.60), we get

$$\begin{aligned} \prod_{j \le 2rc} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2} &< 2^{-\lfloor 2rc \rfloor} \exp\left\{ \sum_{j \le 2rc} e^{-\frac{2rc}{j}} \right\} \\ &< 2^{-\lfloor 2rc \rfloor} e^{e^{-1}} e^{2rcC_1}, \end{aligned}$$

proving the upper bound.

To show that the lower bound is true, we will need the following facts.

$$\log\left(1 + \left(1 - \frac{2c}{j}\right)^r\right) > \left(1 - \frac{2c}{j}\right)^r - \frac{1}{2}\left(1 - \frac{2c}{j}\right)^{2r} \tag{4.61}$$

$$\left(1 - \frac{2c}{j}\right)^r > \exp\left\{ \frac{-2rc}{j} - \frac{2rc^2}{j(j-2c)} \right\} \tag{4.62}$$

$$\left(1 - \frac{2c}{j}\right)^{2r} < \exp\left\{ \frac{-4rc}{j} \right\} \tag{4.63}$$

Putting these facts together, we find the lower bound

$$\begin{aligned} &\sum_{j \le 2rc} \log\left(1 + \left(1 - \frac{2c}{j}\right)^r\right) \\ &> \sum_{j \le 2rc} \left(1 - \frac{2c}{j}\right)^r - \frac{1}{2}\left(1 - \frac{2c}{j}\right)^{2r} \\ &> \sum_{j \le 2rc} \exp\left\{ \frac{-2rc}{j} - \frac{2rc^2}{j(j-2c)} \right\} - \frac{1}{2} \sum_{j \le 2rc} \exp\left\{ \frac{-4rc}{j} \right\}. \end{aligned} \tag{4.64}$$

Euler Maclaurin summation can be used to find bounds on both of the above exponential sums; we begin with the second. The estimations and substitutions used

are similar to those we saw when finding the upper bound.

$$\begin{aligned}\sum_{j\le 2rc}\exp\left\{\frac{-4rc}{j}\right\} &< e^{-2}+\int_1^{2rc} e^{-4rc/x}\,dx\\ &= e^{-2}+2rc\int_{1/2rc}^{1} e^{-2/u}\,du\\ &< e^{-2}+2rc\int_0^1 e^{-2/u}\,du\\ &= e^{-2}+2rcC_2\end{aligned}$$

where C_2 is the convergent integral and

$$C_2 = 0.0375\cdots = \int_0^1 e^{-2/u}\,du.$$

Thus

$$\frac{1}{2}\sum_{j\le 2rc}\exp\left\{\frac{-4rc}{j}\right\} < \frac{1}{2}e^{-2}+rcC_2. \tag{4.65}$$

Before proceeding with the remaining exponential sum, we comment that any integral used to approximate this sum will be difficult to evaluate if the exponent is left in its current form. Thus far, we have been able to use a substitution that gives a convergent integral, but this sum is more difficult because of the added term in the exponent. However, observe that when $j \ge 2$,

$$\frac{2rc^2}{j(j-2c)} \le \frac{rc^2}{2(1-c)}\,.$$

Since the latter expression is increasing in c, we find

$$\frac{rc^2}{2(1-c)} < \frac{r}{4}$$

over the range of interest. Therefore, when $j \ge 2$,

$$\exp\left\{\frac{-2rc}{j}-\frac{2rc^2}{j(j-2c)}\right\} > \exp\left\{\frac{-2rc}{j}-\frac{r}{4}\right\} = e^{-2rc/j}e^{-r/4}.$$

This allows us to replace the exponent of the sum with an expression that is similar to the functions we have already integrated. In fact, we don't even have to use Euler Maclaurin summation: since $e^{-2rc/x}$ is an increasing, concave down function,

we can find a lower bound for the given sum simply by evaluating an integral.

$$\begin{aligned}
&\sum_{j\le 2rc} \exp\left\{\frac{-2rc}{j} - \frac{2rc^2}{j(j-2c)}\right\} \\
&= e^{-2rc-2rc^2/(1-2c)} + \sum_{2\le j\le 2rc} \exp\left\{\frac{-2rc}{j} - \frac{2rc^2}{j(j-2c)}\right\} \\
&> e^{-2rc-2rc^2/(1-2c)} + \sum_{2\le j\le 2rc} \exp\left\{\frac{-2rc}{j} - \frac{r}{4}\right\} \\
&> e^{-2rc-2rc^2/(1-2c)} + e^{-r/4}\int_1^{2rc} e^{-2rc/x}\,dx \\
&= e^{-2rc-2rc^2/(1-2c)} + 2rce^{-r/4}\int_{1/2rc}^1 e^{-1/u}\,du
\end{aligned}$$

Finally, since $j \ge 2$ in the sum estimated by the integral, we note that $2rc \ge j \ge 2$ implies that $1/2rc \le 1/2$. Thus

$$\begin{aligned}
\sum_{j\le 2rc} \exp\left\{\frac{-2rc}{j} - \frac{2rc^2}{j(j-2c)}\right\} &> e^{-2rc-2rc^2/(1-2c)} + 2rce^{-r/4}\int_{1/2rc}^1 e^{-1/u}\,du \\
&> e^{-2rc-2rc^2/(1-2c)} + 2rce^{-r/4}\int_{1/2}^1 e^{-1/u}\,du \\
&= e^{-2rc-2rc^2/(1-2c)} + 2rce^{-r/4}C_3, \qquad (4.66)
\end{aligned}$$

where

$$C_3 = 0.1297\cdots = \int_{1/2}^1 e^{-1/u}\,du.$$

Combining (4.64), (4.65), and (4.66) we find that

$$\sum_{j\le 2rc} \log\left(1 + \left(1 - \frac{2c}{j}\right)^r\right) > e^{-2rc-2rc^2/(1-2c)} + 2rcC_3e^{-r/4} - \frac{1}{2}e^{-2} - rcC_2. \quad (4.67)$$

Substituting this bound into (4.60), we find the lower bound for the original product, proving both the upper and lower bounds given in (4.59). □

The upper and lower bounds for the product over small j given in Lemma 4.8 are similar. When we return to analyzing T_r, we will use the simpler upper bound in our calculations, but we must first look at the remaining part of $t_r(c)$. Recall the earlier determination that $t_r(c)$ behaved like $t_1(rc)$ and the realization that the behavior of $t_1(rc)$ for small j would require splitting this product into two parts. For large j, we will compare the two products over the appropriate range,

$2rc < j \leq k$. We define $t'_1(c)$ and redefine $t_r(c)$ to be

$$t'_1(c) = \prod_{j>2c}^{k} \frac{1+(1-\frac{2c}{j})}{2}, \tag{4.68}$$

$$t_r(c) = \prod_{j>2rc}^{k} \frac{1+\left(1-\frac{2c}{j}\right)^r}{2}. \tag{4.69}$$

This gives

$$t'_1(rc) = \prod_{j>2rc}^{k} \frac{1+(1-\frac{2rc}{j})}{2} = \prod_{j>2rc}^{k} \left(1-\frac{rc}{j}\right) \tag{4.70}$$

as the product that we need to compare to $t_r(c)$. The next theorem is similar to Theorems 4.1 and 4.2. We will show that $t_r(c)$ is approximately $t'_1(rc)$ along with an error term.

Theorem 4.4 *Suppose $0 < c < 1/2$, $r \geq 3$, and define $t'_1(c)$ and $t_r(c)$ as follows:*

$$t'_1(c) = \prod_{j>2c}^{k} \frac{1+(1-\frac{2c}{j})}{2},$$

$$t_r(c) = \prod_{j>2rc}^{k} \frac{1+\left(1-\frac{2c}{j}\right)^r}{2}.$$

Then the ratio of $t_r(c)$ and $t'_1(rc)$,

$$Q_{r,k}(c) = \frac{t_r(c)}{t'_1(rc)},$$

converges to

$$Q_r(c) = \prod_{j>2rc} \frac{1+\left(1-\frac{2c}{j}\right)^r}{2\left(1-\frac{rc}{j}\right)}$$

as $k \to \infty$. Furthermore,

$$t_r(c) \sim t'_1(rc)Q_r(c). \tag{4.71}$$

Proof: First observe that

$$t'_1(rc) = \prod_{j>2rc}^{k} \frac{1+(1-\frac{2rc}{j})}{2} = \prod_{j>2rc}^{k} 1-\frac{rc}{j}.$$

Expanding out the numerator of $t_r(c)$ gives

$$\begin{aligned}
t_r(c) &= \prod_{j>2rc}^{k} \frac{1+\left(1-\frac{2c}{j}\right)^r}{2} \\
&= \prod_{j>2rc}^{k} \frac{1+\sum_{n\geq 0}\binom{r}{n}(-1)^n\left(\frac{2c}{j}\right)^n}{2} \\
&= \prod_{j>2rc}^{k} \frac{1}{2}\left(2-\frac{2rc}{j}+\sum_{n\geq 2}\binom{r}{n}(-1)^n\left(\frac{2c}{j}\right)^n\right) \\
&= \prod_{j>2rc}^{k} \frac{1}{2}\left(2-\frac{2rc}{j}\left(1-\frac{1}{r}\sum_{n\geq 2}\binom{r}{n}(-1)^n\left(\frac{2c}{j}\right)^{n-1}\right)\right) \\
&= \prod_{j>2rc}^{k} \left(1-\frac{rc}{j}\left(1-\frac{1}{r}\sum_{n\geq 2}\binom{r}{n}(-1)^n\left(\frac{2c}{j}\right)^{n-1}\right)\right).
\end{aligned}$$

Then $Q_{r,k}(c)$ can be simplified as follows.

$$\begin{aligned}
Q_{r,k}(c) &= \frac{t_r(c)}{t_1'(rc)} \\
&= \prod_{j>2rc}^{k} \frac{1-\frac{rc}{j}\left(1-\frac{1}{r}\sum_{n\geq 2}\binom{r}{n}(-1)^n\left(\frac{2c}{j}\right)^{n-1}\right)}{1-\frac{rc}{j}} \\
&= \prod_{j>2rc}^{k} 1+\frac{c}{j}\left(1-\frac{rc}{j}\right)^{-1}\sum_{n\geq 2}\binom{r}{n}(-1)^n\left(\frac{2c}{j}\right)^{n-1} \\
&= \prod_{j>2rc}^{k} 1+\frac{2c^2}{j(j-rc)}\sum_{n\geq 0}\binom{r}{n+2}(-1)^n\left(\frac{2c}{j}\right)^n
\end{aligned}$$

We claim that $Q_{r,k}(c)$ converges as $k\to\infty$. Recall from Theorem 4.2 that the infinite product

$$\prod_{j>2rc} 1+a_j$$

converges if and only if the series

$$\sum_{j>2rc} a_j$$

converges absolutely. We first observe that

$$\frac{2c^2}{j(j-rc)} \geq 0$$

if and only if $j > rc$, certainly this is true when $j > 2rc$. Also, the alternating sum

$$\sum_{n\geq 0} \binom{r}{n+2} (-1)^n \left(\frac{2c}{j}\right)^n = \binom{r}{2} - \binom{r}{3}\frac{2c}{j} + \cdots + (-1)^r \left(\frac{2c}{j}\right)^{r-2}$$

will be positive if j is large enough so that the absolute value of the terms decrease. In particular, we need

$$1 > \frac{\binom{r}{t+3}\left(\frac{2c}{j}\right)^{t+1}}{\binom{r}{t+2}\left(\frac{2c}{j}\right)^{t}} = \frac{r-t-2}{t+3} \cdot \frac{2c}{j}\,.$$

Thus the $(t+1)^{st}$ term is less than the t^{th} term when

$$j > 2c \cdot \frac{r-t-2}{t+3}\,.$$

Since the expression on the right decreases as t increases, the maximum value of this quotient occurs when $t = 0$, implying the terms of the sum are decreasing when $j > \frac{2}{3}\, c(r-2)$. Consequently, the sum is positive when j is in this range. Since $j > 2rc > \frac{2}{3}\, c(r-2)$, the alternating sum is positive. Thus

$$\frac{2c^2}{j(j-rc)} \sum_{n\geq 0} \binom{r}{n+2} (-1)^n \left(\frac{2c}{j}\right)^n \geq 0$$

in the range we are interested in. Finally, we note that when $j > 2rc$,

$$\sum_{n\geq 0} \binom{r}{n+2} (-1)^n \left(\frac{2c}{j}\right)^n \leq \binom{r}{2}$$

and $rc/j < 1/2$, implying

$$\frac{2c^2}{j(j-rc)} = \frac{2c^2}{j^2}\left(1 - \frac{rc}{j}\right)^{-1} < \frac{4c^2}{j^2}\,.$$

This enables us to find an upper bound on the alternating series,

$$\sum_{j>2rc} \frac{2c^2}{j(j-rc)} \sum_{n\geq 0} \binom{r}{n+2} (-1)^n \left(\frac{2c}{j}\right)^n < \sum_{j>2rc} \binom{r}{2} \frac{4c^2}{j^2}\,.$$

Since the latter sum is a convergent $p-$series,

$$\sum_{j>2rc} \frac{2c^2}{j(j-rc)} \sum_{n\geq 0} \binom{r}{n+2} (-1)^n \left(\frac{2c}{j}\right)^n$$

is an absolutely convergent series. Therefore

$$\prod_{j>2rc}^{k} 1 + \frac{2c^2}{j(j-rc)} \sum_{n\geq 0} \binom{r}{n+2} (-1)^n \left(\frac{2c}{j}\right)^n$$

converges as $k \to \infty$ to

$$\begin{aligned} Q_r(c) &= \prod_{j>2rc} 1 + \frac{2c^2}{j(j-rc)} \sum_{n\geq 0} \binom{r}{n+2} (-1)^n \left(\frac{2c}{j}\right)^n \\ &= \prod_{j>2rc} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2\left(1 - \frac{rc}{j}\right)}. \end{aligned} \tag{4.72}$$

By definition we have

$$t_r(c) = t_1'(rc) Q_{r,k}(c). \tag{4.73}$$

To eliminate the parameter k in (4.73), we replace $Q_{r,k}(c)$ by $Q_r(c)$ and determine the error introduced by this substitution.

$$\begin{aligned} 1 &< \frac{Q_r(c)}{Q_{r,k}(c)} \\ &= \prod_{j=k+1}^{\infty} 1 + \frac{2c^2}{j(j-rc)} \sum_{n\geq 0} \binom{r}{n+2} (-1)^n \left(\frac{2c}{j}\right)^n \\ &< \exp\left\{ \sum_{j=k+1}^{\infty} \frac{2c^2}{j(j-rc)} \sum_{n\geq 0} \binom{r}{n+2} (-1)^n \left(\frac{2c}{j}\right)^n \right\} \\ &= \exp\left\{ O\left(\frac{1}{k}\right) \right\} \\ &= 1 + O\left(\frac{1}{k}\right). \end{aligned}$$

We will give a proof of this error estimate in Section 4.5.3. Therefore,

$$Q_{r,k}(c) = Q_r(c)\left(1 + O\left(\frac{1}{k}\right)\right),$$

and along with (4.73), this gives

$$t_r(c) = t_1'(rc) Q_r(c)\left(1 + O\left(\frac{1}{k}\right)\right).$$

Finally, since $1 + O(k^{-1}) \to 1$ as $k \to \infty$, we have shown the result. □

This theorem along with Lemma 4.8 is the beginning of an asymptotic for $t_r(c)$. Using the upper bound from Lemma 4.8, we have found that

$$\begin{aligned}\prod_{j=1}^{k}\frac{1+\left(1-\frac{2c}{j}\right)^r}{2} &= \prod_{j\le 2rc}\frac{1+\left(1-\frac{2c}{j}\right)^r}{2}\prod_{j>2rc}^{k}\frac{1+\left(1-\frac{2c}{j}\right)^r}{2}\\ &\sim 2^{-\lfloor 2rc\rfloor}e^{e^{-1}}e^{2rcC_1}t_1'(rc)Q_r(c). \qquad (4.74)\end{aligned}$$

This gives

$$T_r \sim \binom{l}{r}2^{-\lfloor 2rc\rfloor}e^{e^{-1}}e^{2rcC_1}t_1'(rc)Q_r(c) \qquad (4.75)$$

as an approximation for the r^{th} term of $E(2^s)$. We will soon find an asymptotic for $t_1'(rc)$, but first we will check the error from Theorem 4.4.

4.5.3 Error Analysis for Theorem 4.4

In comparing $Q_{r,k}(c)$ to $Q_r(c)$ in Theorem 4.4, we used the fact that the alternating sum is $O(k^{-1})$. The following lemma shows that this error estimation is true.

Lemma 4.9 *Let $0 < c < 1/2$, $k \ge 2$, $r \ge 3$, and let*

$$A_{r,c}(j) = \sum_{n\ge 0}\binom{r}{n+2}(-1)^n\left(\frac{2c}{j}\right)^n.$$

Then

$$0 < \sum_{j=k+1}^{\infty}\frac{2c^2}{j(j-rc)}A_{r,c}(j) < \binom{r}{2}\frac{2c^2r}{k}.$$

Proof: First note that by the definition of $t_r(c)$, $k+1 > k > 2rc$ and by the work in Theorem 4.4, we know that the terms of $A_{r,c}(j)$ are decreasing. Thus

$$0 < \binom{r}{2} - \binom{r}{2}\frac{2c}{j} < A_{r,c}(j) < \binom{r}{2}.$$

Substituting this into the infinite series,

$$0 < \sum_{j=k+1}^{\infty}\frac{2c^2}{j(j-rc)}A_{r,c}(j) < \binom{r}{2}\sum_{j=k+1}^{\infty}\frac{2c^2}{j(j-rc)}. \qquad (4.76)$$

Continuing with the upper bound, since $0 < c < 1/2$, then $j - rc > j - r$. Thus

$$\sum_{j=k+1}^{\infty}\frac{2c^2}{j(j-rc)} < \sum_{j=k+1}^{\infty}\frac{2c^2}{j(j-r)}.$$

Since $j > k \geq r$, the sum on the right is positive and bounded above by a convergent $p-$series. So the sum is absolutely convergent and we can rearrange it. In particular, we find that

$$\begin{aligned}\sum_{j=k+1}^{\infty} \frac{2c^2}{j(j-r)} &= 2c^2 \left(\sum_{j=k+1}^{\infty} \frac{1}{r(j-r)} - \sum_{j=k+1}^{\infty} \frac{1}{rj} \right) \\ &= 2c^2 \left(\sum_{j=k-r+1}^{\infty} \frac{1}{rj} - \sum_{j=k+1}^{\infty} \frac{1}{rj} \right) \\ &= \sum_{j=k-r+1}^{k} \frac{2c^2}{rj} \,.\end{aligned}$$

Combining this with (4.76), we now have

$$0 < \sum_{j=k+1}^{\infty} \frac{2c^2}{j(j-rc)} A_{r,c}(j) < \binom{r}{2} \sum_{j=k-r+1}^{k} \frac{2c^2}{rj} \,. \tag{4.77}$$

Rewriting the sum above to begin with index 0, we find

$$\begin{aligned}\sum_{j=k+1}^{\infty} \frac{2c^2}{j(j-rc)} A_{r,c}(j) &< \binom{r}{2} \sum_{j=k-r+1}^{k} \frac{2c^2}{rj} \\ &= \binom{r}{2} \sum_{i=0}^{r-1} \frac{2c^2}{r(k-i)} \\ &= \binom{r}{2} \frac{1}{k} \sum_{i=0}^{r-1} \frac{2c^2}{r(1-i/k)} \,. \end{aligned} \tag{4.78}$$

The final sum in (4.78) is easy to bound upon observing that since $k \geq r$,

$$\frac{i}{k} \leq \frac{r-1}{k} \leq \frac{r-1}{r} = 1 - \frac{1}{r} \,.$$

Thus, $1 - i/k \geq 1/r$, so

$$\begin{aligned}\sum_{i=0}^{r-1} \frac{2c^2}{r(1-i/k)} &\leq \sum_{i=0}^{r-1} \frac{2c^2 r}{r} \\ &= 2c^2 r.\end{aligned}$$

Using this in (4.78), we have the new upper bound

$$\sum_{j=k+1}^{\infty} \frac{2c^2}{j(j-rc)} A(j) < \binom{r}{2} \frac{2c^2 r}{k} \,, \tag{4.79}$$

proving the result. □

We now continue with the asymptotics given in Section 4.5.2

$$\prod_{j=1}^{k} \frac{1+\left(1-\frac{2c}{j}\right)^r}{2} \sim 2^{-\lfloor 2rc \rfloor} e^{e^{-1}} e^{2rcC_1} t_1'(rc) Q_r(c)$$

and

$$T_r \sim \binom{l}{r} 2^{-\lfloor 2rc \rfloor} e^{e^{-1}} e^{2rcC_1} t_1'(rc) Q_r(c).$$

To further improve these estimations, we must determine how $t_1'(rc)$ behaves. We do this in the next section.

4.5.4 An Asymptotic For $t_1'(rc)$

From the work in Section 4.5.1, we expect to see a factor of k^{-rc} in the asymptotic for T_r. Since we have found bounds for the product part of T_r over small j that do not include this factor, this behavior must come from the latter part of the product that we defined in Theorem 4.4 to be $t_r(c)$. There, we found $t_r(c)$ to be $t_1'(rc)$ times a correction factor $Q_r(c)$, where

$$t_1'(rc) = \prod_{j>2rc}^{k} 1 - \frac{rc}{j}\,.$$

To analyze $t_1'(rc)$, we will, as usual, rewrite it as an exponential function. This gives

$$\begin{aligned} t_1'(rc) &= \exp\left\{ \sum_{j>2rc}^{k} \log\left(1-\frac{rc}{j}\right) \right\} \\ &= \exp\left\{ -\sum_{j>2rc}^{k} \sum_{m\geq 1} \left(\frac{rc}{j}\right)^m \frac{1}{m} \right\} \\ &= \exp\left\{ -\sum_{j>2rc}^{k} \frac{rc}{j} - \sum_{j>2rc}^{k} \sum_{m\geq 2} \left(\frac{rc}{j}\right)^m \frac{1}{m} \right\}. \end{aligned}$$

When finding estimates for the sums in the exponent, we will use approximations similar to those we've seen before, but we must take care to not include the first terms where $j < 2rc$. With this in mind, the analysis of $t_1'(rc)$ breaks into two cases: $2rc < 1$ and $2rc \geq 1$.

Case 1: $2rc < 1$

Observe that when $2rc < 1$, $t_1'(rc)$ is the full product, that is

$$t_1'(rc) = \prod_{j=1}^{k} 1 - \frac{rc}{j}\,.$$

Therefore we may use the asymptotic found for $t_1'(c)$ in Theorem 4.1. Substituting rc into the function there we have

$$t_1'(rc) \sim k^{-rc} e^{-rc\gamma - h_\zeta(rc)}, \tag{4.80}$$

where

$$h_\zeta(rc) = \sum_{m\geq 2} \frac{(rc)^m}{m} \zeta(m).$$

Returning to T_r, we observe that the bounds found in Lemma 4.8 are not necessary as the product for small $j < 2rc$ is empty. Thus the asymptotic for T_r when $2rc < 1$ consists only of the binomial coefficient along with (4.80) and $Q_r(c)$,

$$T_r \sim \binom{l}{r} k^{-rc} e^{-rc\gamma - h_\zeta(rc)} Q_r(c). \tag{4.81}$$

The use of this asymptotic is dependent on whether or not it converges; the question of convergence comes down to $h_\zeta(rc)$. Although not mentioned above, $h_\zeta(rc)$ converges when $2rc < 1$ because $rc < 1$. When $1 \leq 2rc < 2$, it is still true that $rc < 1$, implying that $h_\zeta(rc)$ converges in this case also. Therefore we may still use the asymptotic for $t_1'(rc)$ given in equation (4.80) when $2rc < 2$. So the estimate given for T_r in (4.81) is valid for $r \geq 3$ when $2rc < 2$.

Once $2rc \geq 2$, we may no longer use this asymptotic. Not only does $h_\zeta(rc)$ not converge when $2rc \geq 2$, now $rc \geq 1$ and there are some terms in the product $t_1'(rc)$ that are negative or possibly 0. Therefore the manipulation of $t_1'(rc)$ to rewrite it as an exponential function is no longer valid as there will be terms not in the domain of log. When this happens, we must turn to more careful estimations of sums.

Case 2: $2rc \geq 1$

When $2rc \geq 1$, $t_1'(rc)$ is no longer the full product and we must take this into account in our approximations. The methods used in the next lemma will be similar to what we have done before but the resulting asymptotic will have extra terms due to the missing factors in the product we are looking at.

Lemma 4.10 *Let $0 < c < 1/2$ and $r \geq 3$. Then*

$$\begin{aligned} t_1'(rc) &\sim \left(\frac{k}{\lfloor 2rc \rfloor}\right)^{-rc} \exp\left\{\frac{rc}{2\lfloor 2rc\rfloor} - \frac{rc}{12\lfloor 2rc\rfloor^2} + \frac{rc}{12\lfloor 2rc\rfloor^4}\right\} \\ &\quad * \exp\left\{-rch_1\left(\frac{rc}{\lfloor 2rc\rfloor}\right) + h_2\left(\frac{rc}{\lfloor 2rc\rfloor}\right) - \frac{h_3\left(\frac{rc}{\lfloor 2rc\rfloor}\right)}{\lfloor 2rc\rfloor}\right\}, \quad (4.82) \end{aligned}$$

where

$$\begin{aligned} h_1(x) &= 1 + \frac{(1-x)\log(1-x)}{x}, \\ h_2(x) &= -\frac{1}{2}\log(1-x) - \frac{x}{2}, \\ h_3(x) &= \frac{-x^2}{12(x-1)}. \end{aligned}$$

Proof: As defined in Theorem 4.4,

$$t_1'(rc) = \prod_{j>2rc}^{k} \frac{1 + (1 - \frac{2rc}{j})}{2} = \prod_{j=\lfloor 2rc\rfloor+1}^{k} 1 - \frac{rc}{j}.$$

We can rewrite this expression in terms of an exponential function,

$$\begin{aligned} t_1'(rc) &= \exp\left\{\sum_{j>2rc}^{k} \log\left(1 - \frac{rc}{j}\right)\right\} \\ &= \exp\left\{-\sum_{j>2rc}^{k}\sum_{m\geq 1}\left(\frac{rc}{j}\right)^m \frac{1}{m}\right\} \\ &= \exp\left\{-\sum_{j>2rc}^{k}\frac{rc}{j} - \sum_{j>2rc}^{k}\sum_{m\geq 2}\left(\frac{rc}{j}\right)^m \frac{1}{m}\right\}. \end{aligned}$$

Considering the first sum in the exponent, an application of Euler Maclaurin summation shows

$$\sum_{j>2rc}^{k}\frac{1}{j} = \log k - \log\lfloor 2rc\rfloor - \frac{1}{2\lfloor 2rc\rfloor} + \frac{1}{12\lfloor 2rc\rfloor^2} - \frac{1}{60\lfloor 2rc\rfloor^4} + O\left(\frac{1}{k}\right).$$

Replacing the first sum in the exponential expression with this estimate and switching the order of summation on the double series, we see

$$\begin{aligned} t_1'(rc) &= \exp\left\{-rc\log k + rc\log\lfloor 2rc\rfloor + \frac{rc}{2\lfloor 2rc\rfloor} - \frac{rc}{12\lfloor 2rc\rfloor^2} + \frac{rc}{60\lfloor 2rc\rfloor^4}\right\} \\ &\quad * \exp\left\{-\sum_{m\geq 2}\frac{(rc)^m}{m}\sum_{j>2rc}^{k}\frac{1}{j^m}\right\}\exp\left\{O\left(\frac{1}{k}\right)\right\} \\ &= \left(\frac{k}{\lfloor 2rc\rfloor}\right)^{-rc}\exp\left\{\frac{rc}{2\lfloor 2rc\rfloor} - \frac{rc}{12\lfloor 2rc\rfloor^2} + \frac{rc}{60\lfloor 2rc\rfloor^4}\right\} \\ &\quad * \exp\left\{-\sum_{m\geq 2}\frac{(rc)^m}{m}\sum_{j>2rc}^{k}\frac{1}{j^m}\right\}\left(1+O\left(\frac{1}{k}\right)\right). \end{aligned} \tag{4.83}$$

Another application of Euler Maclaurin shows that

$$\sum_{j>2rc}^{k}\frac{1}{j^m} = \frac{1}{(m-1)\lfloor 2rc\rfloor^{m-1}} - \frac{1}{2\lfloor 2rc\rfloor^m} + \frac{m}{12\lfloor 2rc\rfloor^{m+1}} + O\left(\frac{1}{k^{m-1}}\right).$$

Applying this to the inner sum in (4.83) gives

$$\begin{aligned} &\sum_{m\geq 2}\frac{(rc)^m}{m}\sum_{j>2rc}^{k}\frac{1}{j^m} \\ &= \sum_{m\geq 2}\frac{(rc)^m}{m}\left(\frac{1}{(m-1)\lfloor 2rc\rfloor^{m-1}} - \frac{1}{2\lfloor 2rc\rfloor^m} + \frac{m}{12\lfloor 2rc\rfloor^{m+1}} + O\left(\frac{1}{k^{m-1}}\right)\right) \\ &= \sum_{m\geq 2}\frac{(rc)^m}{m}\left(\frac{1}{(m-1)\lfloor 2rc\rfloor^{m-1}} - \frac{1}{2\lfloor 2rc\rfloor^m} + \frac{m}{12\lfloor 2rc\rfloor^{m+1}}\right) + O\left(\frac{1}{k}\right). \end{aligned}$$

Substituting this back into (4.83), we obtain

$$\begin{aligned} t_1'(rc) &= \left(\frac{k}{\lfloor 2rc\rfloor}\right)^{-rc}\exp\left\{\frac{rc}{2\lfloor 2rc\rfloor} - \frac{rc}{12\lfloor 2rc\rfloor^2} + \frac{rc}{60\lfloor 2rc\rfloor^4}\right\} \\ &\quad * \exp\left\{-\sum_{m\geq 2}\frac{(rc)^m}{m}\left(\frac{1}{(m-1)\lfloor 2rc\rfloor^{m-1}} - \frac{1}{2\lfloor 2rc\rfloor^m}\right)\right\} \\ &\quad * \exp\left\{-\sum_{m\geq 2}\frac{(rc)^m}{m}\frac{m}{12\lfloor 2rc\rfloor^{m+1}}\right\}\left(1+O\left(\frac{1}{k}\right)\right). \end{aligned} \tag{4.84}$$

Finally, we define $h_1(x)$, $h_2(x)$, and $h_3(x)$ as the following infinite sums.

$$\begin{aligned} h_1(x) &= \sum_{m\geq 2} \frac{x^{m-1}}{m(m-1)} = 1 + \frac{(1-x)\log(1-x)}{x} \\ h_2(x) &= \sum_{m\geq 2} \frac{x^m}{2m} = -\frac{1}{2}\log(1-x) - \frac{x}{2} \\ h_3(x) &= \sum_{m\geq 2} \frac{x^m}{12} = \frac{-x^2}{12(x-1)} \end{aligned}$$

Letting $x = rc/\lfloor 2rc \rfloor$ and substituting $h_1(x)$, $h_2(x)$, and $h_3(x)$ into (4.84), we have the result. □

The analyses of the error terms encountered here are similar to the analyses done in Sections 4.4.3 and 4.5.3 and will therefore be omitted. We can now use Lemmas 4.8 and 4.10 with Theorem 4.4 to give an asymptotic for the r^{th} term of $E(2^s)$ when $2rc \geq 1$. We summarize the results of this section and Section 4.5.4 in the next theorem.

Theorem 4.5 *Let $0 < c < 1/2$ and $r \geq 3$. The behavior of the r^{th} term of $E(2^s)$ can be summarized in two cases.*

(i) When $2rc < 1$,

$$T_r \sim \binom{l}{r} k^{-rc} e^{-rc\gamma - h_\zeta(rc)} Q_r(c),$$

where

$$Q_r(c) = \prod_{j\geq 1} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2\left(1 - \frac{rc}{j}\right)}.$$

(ii) When $2rc \geq 1$,

$$\begin{aligned} T_r \sim\ & \binom{l}{r} \left(\frac{k}{\lfloor 2rc \rfloor}\right)^{-rc} 2^{-\lfloor 2rc \rfloor} e^{e^{-1}} e^{2rcC_1} Q_r(c) \\ & * \exp\left\{ \frac{rc}{2\lfloor 2rc \rfloor} - \frac{rc}{12\lfloor 2rc \rfloor^2} + \frac{rc}{60\lfloor 2rc \rfloor^4} \right\} \\ & * \exp\left\{ -rch_1\left(\frac{rc}{\lfloor 2rc \rfloor}\right) + h_2\left(\frac{rc}{\lfloor 2rc \rfloor}\right) - \frac{h_3\left(\frac{rc}{\lfloor 2rc \rfloor}\right)}{\lfloor 2rc \rfloor} \right\}, \end{aligned}$$

where C_1, $h_1(x)$, $h_2(x)$, and $h_3(x)$ are defined as before and

$$Q_r(c) = \prod_{j > 2rc} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2\left(1 - \frac{rc}{j}\right)}.$$

Recall that although the first case is stated for $2rc < 1$, we can also use this asymptotic when $1 \leq 2rc < 2$. The two approximations for T_r in this range are slightly different, but we will find use for both of them later in the chapter.

4.6 Comparing Consecutive Terms

With an asymptotic expression for T_r, $r \geq 3$, we are now prepared to return to determining the values of $l = dk$ for which $E(2^s)$ approaches 1. Recall that we have shown that $T_1 < 1$ when

$$d < d_1 = \frac{e^{c\gamma + h_\zeta(c)}}{k^{1-c}}$$

and $0 < c < 2/5$. We have also shown that $T_2 < T_1$ in this range. To show that $E(2^s)$ approaches 1 for these values of d, we must show that the sum of the remaining terms is negligible. Since the factor k^{-rc} appears in the asymptotic of T_r, it seems reasonable to expect $E(2^s)$ to behave like a geometric series. In fact, the terms are decreasing when $d < d_1$ and we will show that they are bounded above by a geometric series that converges to 1 for a given function $l = l(k)$.

One approach to this would be to find the sequence of d_r, $r \geq 1$, such that $T_{r+1} < T_r$. If this sequence is increasing as r increases, then the sequence of terms, T_r, is decreasing. We have already found d_1 and d_2 and have seen that $d_1 < d_2$, showing that $T_2 < T_1$ for l greater than what is even needed to have $T_1 < 1$. One advantage to this approach is showing that the sequence d_r strictly increases would imply the terms are unimodal. However, we would still need to prove that the sum of the remaining terms is small and $E(2^s)$ approaches 1.

On the other hand, we know the range for d we're interested in; we know that d must be less than d_1 before T_1 is small enough to possibly see $E(2^s)$ approach 1. If we show that $T_{r+1} < T_r$ when $d < d_1$, then we will be showing that the terms are decreasing in the range of interest. To do this, we may determine if

$$\frac{T_{r+1}}{T_r} < 1$$

in the critical range. This is a more direct approach than the latter and will have the result of giving an upper bound on the ratio of consecutive terms. The advantage

of this approach is that this upper bound enables us to bound $E(2^s)$ above by a geometric series, not only showing that the terms are decreasing, but giving an upper bound on the sum itself.

4.6.1 The Range of Interest

Since the asymptotics for T_r depend on l, we must be sure to compare approximations with the correct values of l substituted in to find an upper bound on the ratio of consecutive terms. To narrow down the range we are interested in, observe that the numerator of d_1 is increasing in c. Then since $0 < c < 2/5$,

$$1 < e^{c\gamma + h_\zeta(c)} < e^{2\gamma/5 + h_\zeta(2/5)} < 1.4893.$$

This allows us to bound d_1,

$$k^{c-1} < d_1 < 1.4893k^{c-1}.$$

Setting $l_1 = d_1 k$ to be the critical l value such that $T_1 < 1$ when $l < l_1$, this implies that

$$k^c < l_1 < 1.4893k^c. \tag{4.85}$$

Certainly, if $l \leq k^c$, l is in the range where $T_1 < 1$. We will concentrate our remaining work in this area. We will first look at the ratio of consecutive terms when $l = k^c$.

4.6.2 The Ratio of Consecutive Terms, $l = k^c$

We will be using the asymptotics given in Theorem 4.5 to find an upper bound for the ratio

$$\frac{T_{r+1}}{T_r}\,.$$

In this section, we will take $l = k^c$. Since the asymptotic we use for T_r changes depending on the size of $2rc$, we will need to consider three different cases based on the values of $2rc$ and $2(r+1)c$:

Case 1: $2rc < 2(r+1)c < 1$;

Case 2: $2rc < 1$, $1 \leq 2(r+1)c < 2$;

Case 3: $1 \leq 2rc < 2(r+1)c$.

The cases are broken up in this way so that we will be able to compare similar asymptotics. Cases 1 and 2 will use the approximation given in part *(i)* of Theorem 4.5 for both T_r and T_{r+1} while the comparisons for case 3 will use part *(ii)* of the theorem. It is necessary to have case 2 as what we might call a "crossover" comparison between the two different asymptotics. It is certainly possible in case 2 to use part *(i)* for T_r and *(ii)* for T_{r+1} in the ratio, but the resulting expression will be very difficult to analyze. Since both estimations we have found for T_r are valid when $1 \leq 2rc < 2$, we use similar expressions to simplify our work. We also observe that this is the only case that needs to be set up this way. Since $2c < 1$,

$$2(r+1)c < 2rc + 1,$$

thus it is never possible to have the case when $2rc < 1$ while $2(r+1)c \geq 2$.

This also brings up the fact that $\lfloor 2rc \rfloor$ may not be equal to $\lfloor 2(r+1)c \rfloor$. The impact of this will arise in case 3 where we will need to decompose the case even further according to the value of the two floors.

Case 1: $2rc < 2(r+1)c < 1$

We first consider the case when $2rc$ and $2(r+1)c$ are both small. By Theorem 4.5, the r^{th} term of $E(2^s)$ is

$$T_r \sim \binom{l}{r} k^{-rc} e^{-rc\gamma - h_\zeta(rc)} Q_r(c) \tag{4.86}$$

while the $(r+1)^{st}$ term is

$$T_{r+1} \sim \binom{l}{r+1} k^{-(r+1)c} e^{-(r+1)c\gamma - h_\zeta((r+1)c)} Q_{r+1}(c). \tag{4.87}$$

We wish to find an upper bound on the ratio of these two terms. Taking the ratio of (4.86) and (4.87) and simplifying, we find that

$$\begin{aligned} \frac{T_{r+1}}{T_r} &\sim \frac{\binom{l}{r+1}}{\binom{l}{r}} k^{-c} e^{-c\gamma - h_\zeta((r+1)c) + h_\zeta(rc)} \frac{Q_{r+1}(c)}{Q_r(c)} \\ &= \frac{l-r}{r+1} k^{-c} e^{-c\gamma - h_\zeta((r+1)c) + h_\zeta(rc)} \frac{Q_{r+1}(c)}{Q_r(c)}\,. \end{aligned} \tag{4.88}$$

We will divide the analysis of this ratio into three parts: the ratio of binomial coefficients along with the factor k^{-c}, the natural exponential function, and the remaining infinite product.

We are assuming right now that $l = k^c$. Since $r \leq l$, we may write $r = \alpha l = \alpha k^c$, where $\alpha \leq 1$. Substituting this into the first part of the expression, we have

$$\begin{aligned} \frac{l-r}{r+1}\, k^{-c} &= \frac{k^c - \alpha k^c}{k^c} \cdot \frac{1}{r+1} \\ &= \frac{1-\alpha}{r+1} \\ &< \frac{1}{r+1}\,. \end{aligned}$$

Finally, since $r \geq 3$,

$$\frac{l-r}{r+1}\, k^{-c} < \frac{1}{4}\,. \tag{4.89}$$

Moving on to the exponential function, we can show that it is less than 1. First observe that

$$h_\zeta(y) = \sum_{m \geq 2} \frac{y^m}{m}\, \zeta(m)$$

increases with the argument. If $y_1 < y_2$, then for $m \geq 2$,

$$\frac{y_1^m}{m}\, \zeta(m) < \frac{y_2^m}{m}\, \zeta(m).$$

Therefore, $h_\zeta(y_1) < h_\zeta(y_2)$. Then since $rc < (r+1)c$,

$$h_\zeta(rc) < h_\zeta((r+1)c).$$

This implies that the exponent, $-c\gamma - h_\zeta((r+1)c) + h_\zeta(rc)$, is negative. Thus,

$$e^{-c\gamma - h_\zeta((r+1)c) + h_\zeta(rc)} < e^0 = 1. \tag{4.90}$$

Equations (4.89) and (4.90) together give an upper bound so far to be

$$\frac{l-r}{r+1} k^{-c} e^{-c\gamma - h_\zeta((r+1)c) + h_\zeta(rc)} \frac{Q_{r+1}(c)}{Q_r(c)} < \frac{1}{4} \frac{Q_{r+1}(c)}{Q_r(c)}\,.$$

If the remaining product is less than 4, then the ratio of consecutive terms will be less than 1. This will imply that we may bound the sum of T_r, $r \geq 3$, above by a convergent geometric series when $2rc < 2(r+1)c < 1$.

The remaining ratio requires more work. Recall that

$$Q_r(c) = \prod_{j>2rc} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2\left(1 - \frac{rc}{j}\right)}$$

was the accumulated error from replacing $t_r(c)$ by $t_1'(rc)$. In this case, both $Q_r(c)$ and $Q_{r+1}(c)$ are over $j \geq 1$. The ratio we are looking at here is

$$\frac{Q_{r+1}(c)}{Q_r(c)} = \prod_{j\geq 1} \frac{1 + \left(1 - \frac{2c}{j}\right)^{r+1}}{1 + \left(1 - \frac{2c}{j}\right)^r} \cdot \frac{1 - \frac{rc}{j}}{1 - \frac{(r+1)c}{j}} \,. \tag{4.91}$$

We expect this product to be close to 1; consider the first fraction above,

$$\frac{1 + \left(1 - \frac{2c}{j}\right)^{r+1}}{1 + \left(1 - \frac{2c}{j}\right)^r} \,,$$

for fixed j. Since $0 < 1 - 2c/j < 1$, the difference between having an exponent r or an exponent $r+1$ is minimal, especially as $j \to \infty$. Therefore the numerator and denominator of this fraction are very close. The denominator is only slightly larger than the numerator, so this ratio is less than 1 for all j and approaches 1 as $j \to \infty$. On the other hand,

$$\frac{1 - \frac{rc}{j}}{1 - \frac{(r+1)c}{j}}$$

is greater than 1 since $(r+1)c/j > rc/j$ for all j. So the product of these two fractions approaches 1 as $j \to \infty$. But since one ratio is slightly larger than 1 while the other is slightly smaller, we can't determine whether their product is greater or less than 1 with the information we have.

We can, however, bound their product for fixed j using the expansion of the binomial term. Observe that since $j > 2rc$,

$$1 - \frac{2rc}{j} < \left(1 - \frac{2c}{j}\right)^r < 1 - \frac{2rc}{j} + \frac{2r(r-1)c^2}{j^2} \,.$$

With these bounds,

$$\begin{aligned}\frac{1+\left(1-\frac{2c}{j}\right)^{r+1}}{1+\left(1-\frac{2c}{j}\right)^{r}}\cdot\frac{1-\frac{rc}{j}}{1-\frac{(r+1)c}{j}} &< \frac{1-\frac{(r+1)c}{j}+\frac{(r+1)rc^2}{j^2}}{1-\frac{rc}{j}}\cdot\frac{1-\frac{rc}{j}}{1-\frac{(r+1)c}{j}}\\ &= \frac{1-\frac{(r+1)c}{j}+\frac{(r+1)rc^2}{j^2}}{1-\frac{(r+1)c}{j}}\\ &= 1+\frac{(r+1)rc^2}{j^2}\cdot\frac{1}{1-\frac{(r+1)c}{j}}\,.\end{aligned}$$

Since $j > 2(r+1)c$, observe that

$$\frac{1}{1-\frac{(r+1)c}{j}} < 2.$$

We use this in the bound found above to see for fixed j,

$$\frac{1+\left(1-\frac{2c}{j}\right)^{r+1}}{1+\left(1-\frac{2c}{j}\right)^{r}}\cdot\frac{1-\frac{rc}{j}}{1-\frac{(r+1)c}{j}} < 1+\frac{2(r+1)rc^2}{j^2}\,. \tag{4.92}$$

We substitute this back into (4.91) to find that

$$\begin{aligned}\frac{Q_{r+1}(c)}{Q_r(c)} &< \prod_{j\geq 1} 1+\frac{2(r+1)rc^2}{j^2}\\ &= \exp\left\{\sum_{j\geq 1}\log\left(1+\frac{2(r+1)rc^2}{j^2}\right)\right\}\\ &< \exp\left\{\sum_{j\geq 1}\frac{2(r+1)rc^2}{j^2}\right\}\end{aligned}$$

by the Taylor expansion for log. Now, the sum over the squares in the exponent is $\zeta(2) = \pi^2/6$. This, along with the fact that $2rc < 2(r+1)c < 1$, gives

$$\begin{aligned}\frac{Q_{r+1}(c)}{Q_r(c)} &< \exp\left\{\sum_{j\geq 1}\frac{2(r+1)rc^2}{j^2}\right\}\\ &= \exp\{2(r+1)rc^2\zeta(2)\}\\ &< e^{\pi^2/12}.\end{aligned} \tag{4.93}$$

Applying this in (4.88) with the earlier bounds, we now have that

$$\begin{aligned}\frac{T_{r+1}}{T_r} &\sim \frac{l-r}{r+1}k^{-c}e^{-c\gamma-h_\zeta((r+1)c)+h_\zeta(rc)}\frac{Q_{r+1}(c)}{Q_r(c)} \\ &< \frac{1}{4}\,e^{\pi^2/12} \\ &= 0.56902\ldots \end{aligned} \tag{4.94}$$

This upper bound is exactly what we had hoped for. Not only have we found a constant upper bound, we have shown that the ratio of consecutive terms is less than 1. This means that we can bound the portion of $E(2^s)$ where $2rc < 2(r+1)c < 1$ by a partial geometric series. In the next cases, we will apply similar techniques to find upper bounds on this same ratio. Case 2, when $2rc < 1$ and $1 \leq 2(r+1)c < 2$, will be similar to what we have done here, although we will need to take more care with the infinite product. Case 3, when $2(r+1)c > 2rc > 1$, will be more tedious since there are more factors to analyze. The ratio of $Q_{r+1}(c)$ to $Q_r(c)$ will again be a difficult step as the upper bound given in this section will not be valid there.

Case 2: $2rc < 1$, $1 \leq 2(r+1)c < 2$

In order to compare similar expressions for the case where $2rc < 1$ and $1 \leq 2(r+1)c < 2$, we use part *(i)* of Theorem 4.5 for both T_r and T_{r+1}. Recall the earlier discussion in Section 4.5.4 on the validity of using this expression when $1 \leq 2(r+1)c < 2$. Therefore T_r and T_{r+1} in this case will be

$$T_r \sim \binom{l}{r}k^{-rc}e^{-rc\gamma-h_\zeta(rc)}Q_r(c), \tag{4.95}$$

$$T_{r+1} \sim \binom{l}{r+1}k^{-(r+1)c}e^{-(r+1)c\gamma-h_\zeta((r+1)c)}Q_{r+1}(c). \tag{4.96}$$

This gives the ratio of T_{r+1} to T_r to be

$$\frac{T_{r+1}}{T_r} \sim \frac{l-r}{r+1}k^{-c}e^{-c\gamma-h_\zeta((r+1)c)+h_\zeta(rc)}\frac{Q_{r+1}(c)}{Q_r(c)}\,, \tag{4.97}$$

as in equation (4.88). Since these are the same asymptotics used in the last section, much of the work here will be identical to the work seen there. In fact, any estimates in the last section that did not require the use of the bounds on $2rc$ or $2(r+1)c$ will follow through in this case. Thus the bounds from (4.89) and (4.90) hold and

we know that

$$\frac{l-r}{r+1}k^{-c}e^{-c\gamma-h_\zeta((r+1)c)+h_\zeta(rc)} < \frac{1}{4}\,. \tag{4.98}$$

All that remains is to find the upper bound on the ratio of $Q_{r+1}(c)$ to $Q_r(c)$,

$$\frac{Q_{r+1}(c)}{Q_r(c)} = \prod_{j\geq 1} \frac{1+\left(1-\frac{2c}{j}\right)^{r+1}}{1+\left(1-\frac{2c}{j}\right)^{r}} \cdot \frac{1-\frac{rc}{j}}{1-\frac{(r+1)c}{j}}\,.$$

The bound we found earlier for this ratio was highly dependent on the upper bound of 1 for both $2rc$ and $2(r+1)c$. When we extend the range of $2(r+1)c$, the work on this ratio is no longer valid. In particular, the analysis breaks down when finding an upper bound for the product factors for fixed j. There, we used the fact that $2(r+1)c < 1$ to show that

$$\frac{1}{1-\frac{(r+1)c}{j}} < 2$$

for all j, enabling us to find the final upper bound given. In case 2, we now have $(r+1)c < 1$. When $j = 1$, this implies that

$$\frac{1}{1-(r+1)c} < \infty.$$

Clearly this is not a useful bound. But $j = 1$ is the only problem; when $j \geq 2$, $(r+1)c/j < 1/2$. This means

$$\frac{1}{1-\frac{(r+1)c}{j}} < 2$$

for all $j \geq 2$, indicating that it will be useful to handle the first term of the infinite product separately and analyze the remaining product as before. We rewrite this ratio as

$$\frac{Q_{r+1}(c)}{Q_r(c)} = \frac{1+(1-2c)^{r+1}}{1-(r+1)c} \cdot \frac{1-rc}{1+(1-2c)^r} \prod_{j\geq 2} \frac{1+\left(1-\frac{2c}{j}\right)^{r+1}}{1+\left(1-\frac{2c}{j}\right)^{r}} \cdot \frac{1-\frac{rc}{j}}{1-\frac{(r+1)c}{j}}\,.$$

Then following the steps leading to (4.92), we find that

$$\frac{1+\left(1-\frac{2c}{j}\right)^{r+1}}{1+\left(1-\frac{2c}{j}\right)^{r}} \cdot \frac{1-\frac{rc}{j}}{1-\frac{(r+1)c}{j}} < 1 + \frac{2(r+1)rc^2}{j^2}$$

when $j \geq 2$. This leads to

$$\begin{aligned}\prod_{j\geq 2} \frac{1+\left(1-\frac{2c}{j}\right)^{r+1}}{1+\left(1-\frac{2c}{j}\right)^{r}} \cdot \frac{1-\frac{rc}{j}}{1-\frac{(r+1)c}{j}} &< \prod_{j\geq 2} 1+\frac{2(r+1)rc^2}{j^2} \\ &< \exp\left\{\sum_{j\geq 2}\frac{2(r+1)rc^2}{j^2}\right\}\end{aligned}$$

as before. Now we find that $2(r+1)rc^2 < 1$ and the sum over the squares is $\zeta(2)-1$. Thus

$$\exp\left\{\sum_{j\geq 2}\frac{2(r+1)rc^2}{j^2}\right\} < e^{\pi^2/6-1}. \tag{4.99}$$

Returning to the initial term of the ratio, we use the standard upper bound for $(1-2c)^{r+1}$ to see that

$$\frac{1+(1-2c)^{r+1}}{1-(r+1)c} < \frac{2(1-(r+1)c)}{1-(r+1)c} < 2. \tag{4.100}$$

Also, since $0 < 1-rc < 1$ and $1+(1-2c)^r > 1$, we have

$$\frac{1-rc}{1+(1-2c)^r} < 1. \tag{4.101}$$

Then, combining equations (4.99), (4.100), and (4.101), we finally have

$$\frac{Q_{r+1}(c)}{Q_r(c)} < 2e^{\pi^2/6-1}. \tag{4.102}$$

We are now able to find an upper bound for the ratio of consecutive terms:

$$\begin{aligned}\frac{T_{r+1}}{T_r} &\simeq \frac{l-r}{r+1}k^{-c}e^{-c\gamma-h_\zeta((r+1)c)+h_\zeta(rc)}\frac{Q_{r+1}(c)}{Q_r(c)} \\ &< \frac{1}{2}\,e^{\pi^2/6-1} \\ &= 0.95293\ldots\end{aligned} \tag{4.103}$$

We have again shown that the ratio of consecutive terms is less than 1 in this case. As r increases, this upper bound becomes even smaller. We may therefore bound the terms of $E(2^s)$ where $2rc < 1$ and $1 \leq 2(r+1)c < 2$ above by a convergent geometric series.

Case 3: $2(r+1)c > 2rc \geq 1$

Case 3 considers the remaining possibilities for $2rc$ and $2(r+1)c$. By Theorem 4.5, when $2rc \geq 1$, the r^{th} term of $E(2^s)$ is approximately

$$\begin{aligned} T_r &\sim \binom{l}{r}\left(\frac{k}{\lfloor 2rc\rfloor}\right)^{-rc} 2^{-\lfloor 2rc\rfloor} e^{e^{-1}} e^{2rcC_1} Q_r(c) \\ &\quad * \exp\left\{\frac{rc}{2\lfloor 2rc\rfloor} - \frac{rc}{12\lfloor 2rc\rfloor^2} + \frac{rc}{60\lfloor 2rc\rfloor^4}\right\} \\ &\quad * \exp\left\{-rch_1\left(\frac{rc}{\lfloor 2rc\rfloor}\right) + h_2\left(\frac{rc}{\lfloor 2rc\rfloor}\right) - \frac{h_3\left(\frac{rc}{\lfloor 2rc\rfloor}\right)}{\lfloor 2rc\rfloor}\right\} \end{aligned}$$

where C_1, $h_1(x)$, $h_2(x)$, and $h_3(x)$ are defined in Lemmas 4.8 and 4.10 as

$$\begin{aligned} C_1 &= 0.1484\cdots = \int_0^1 e^{-1/u}\, du, \\ h_1(x) &= \sum_{m\geq 2} \frac{x^{m-1}}{m(m-1)} = 1 + \frac{(1-x)\log(1-x)}{x}, \\ h_2(x) &= \sum_{m\geq 2} \frac{x^m}{2m} = -\frac{1}{2}\log(1-x) - \frac{x}{2}, \\ h_3(x) &= \sum_{m\geq 2} \frac{x^m}{12} = \frac{-x^2}{12(x-1)}, \end{aligned}$$

and

$$Q_r(c) = \prod_{j>2rc} \frac{1 + \left(1 - \frac{2c}{j}\right)^r}{2\left(1 - \frac{rc}{j}\right)}.$$

Similarly, since $2(r+1)c \geq 1$, we have

$$\begin{aligned} T_{r+1} &\sim \binom{l}{r+1}\left(\frac{k}{\lfloor 2(r+1)c\rfloor}\right)^{-(r+1)c} 2^{-\lfloor 2(r+1)c\rfloor} e^{e^{-1}} e^{2(r+1)cC_1} Q_{r+1}(c) \\ &\quad * \exp\left\{\frac{(r+1)c}{2\lfloor 2(r+1)c\rfloor} - \frac{(r+1)c}{12\lfloor 2(r+1)c\rfloor^2} + \frac{(r+1)c}{60\lfloor 2(r+1)c\rfloor^4}\right\} \\ &\quad * \exp\left\{-(r+1)ch_1\left(\frac{(r+1)c}{\lfloor 2(r+1)c\rfloor}\right) + h_2\left(\frac{(r+1)c}{\lfloor 2(r+1)c\rfloor}\right)\right\} \\ &\quad * \exp\left\{-\frac{h_3\left(\frac{(r+1)c}{\lfloor 2(r+1)c\rfloor}\right)}{\lfloor 2(r+1)c\rfloor}\right\}. \end{aligned}$$

Comparing these two expressions is possible, but it is extremely difficult to show what we need with the exponential functions written as they are above. The ratio of consecutive terms becomes more manageable if we return to a more exact expression

for T_r and T_{r+1}. We will instead be using the asymptotic

$$T_r \sim \binom{l}{r} 2^{-\lfloor 2rc \rfloor} e^{e^{-1}} e^{2rcC_1} t_1'(rc) Q_r(c) \tag{4.104}$$

for T_r rather than substituting the approximation to $t_1'(rc)$ found in Lemma 4.10. Similarly,

$$T_{r+1} \sim \binom{l}{r+1} 2^{-\lfloor 2(r+1)c \rfloor} e^{e^{-1}} e^{2(r+1)cC_1} t_1((r+1)c) Q_{r+1}(c). \tag{4.105}$$

With these approximations, we will need to look at the ratio

$$\frac{t_1((r+1)c)}{t_1'(rc)}$$

as well as the ratio of $Q_{r+1}(c)$ to $Q_r(c)$ as in the previous two cases.

The analyses of these two ratios are challenging due to the values of $2rc$ and $2(r+1)c$. Although we have eliminated almost all of the floor functions in T_r by returning to a more exact expression, we must still be careful with the range of the two product ratios. To be more precise, since

$$t_1'(rc) = \prod_{j>2rc}^{k} 1 - \frac{rc}{j},$$

then the ratio of $t_1((r+1)c)$ to $t_1'(rc)$ is

$$\frac{t_1((r+1)c)}{t_1'(rc)} = \frac{\prod_{j>2(r+1)c}^{k} \left(1 - \frac{(r+1)c}{j}\right)}{\prod_{j>2rc}^{k} \left(1 - \frac{rc}{j}\right)}.$$

If $\lfloor 2rc \rfloor = \lfloor 2(r+1)c \rfloor$, the range of each product is the same and this ratio is simply

$$\frac{t_1((r+1)c)}{t_1'(rc)} = \prod_{j>2rc}^{k} \frac{1 - \frac{(r+1)c}{j}}{1 - \frac{rc}{j}} = \prod_{j>2(r+1)c}^{k} \frac{1 - \frac{(r+1)c}{j}}{1 - \frac{rc}{j}}.$$

On the other hand, if $\lfloor 2rc \rfloor \neq \lfloor 2(r+1)c \rfloor$, then the denominator has extra terms. However, since $2c < 1$ we must have $\lfloor 2rc \rfloor + 1 = \lfloor 2(r+1)c \rfloor$ and $t_1'(rc)$ only has one additional term. Therefore, we see

$$\frac{t_1((r+1)c)}{t_1'(rc)} = \left(1 - \frac{rc}{\lfloor 2rc \rfloor + 1}\right)^{-1} \prod_{j>2(r+1)c}^{k} \frac{1 - \frac{(r+1)c}{j}}{1 - \frac{rc}{j}}.$$

The same anomaly occurs with $Q_{r+1}(c)/Q_r(c)$. This requires us to decompose case 3 even further to consider T_r and T_{r+1} where (a) $\lfloor 2rc \rfloor = \lfloor 2(r+1)c \rfloor$ and (b) $\lfloor 2rc \rfloor \neq \lfloor 2(r+1)c \rfloor$.

Before continuing, we present two lemmas that will aid in analyzing T_{r+1}/T_r. The proofs of these lemmas appear in the next section. The first gives an upper bound for a product related to $t_1((r+1)c)/t_1'(rc)$.

Lemma 4.11 *Suppose* $2(r+1)c > 2rc \geq 1$. *Then*

$$\prod_{j>2(r+1)c}^{k} \frac{1-\frac{(r+1)c}{j}}{1-\frac{rc}{j}} < \left(\frac{k}{\lfloor 2(r+1)c \rfloor}\right)^{-c} \exp\left\{\frac{c}{\lfloor 2(r+1)c \rfloor}\right\}.$$

The second lemma will be used in bounding $Q_{r+1}(c)/Q_r(c)$. In cases 1 and 2, we used the inequality

$$\prod_j \frac{1+\left(1-\frac{2c}{j}\right)^{r+1}}{1+\left(1-\frac{2c}{j}\right)^{r}} \cdot \frac{1-\frac{rc}{j}}{1-\frac{(r+1)c}{j}} < \exp\left\{\sum_j \frac{2(r+1)rc^2}{j^2}\right\}$$

where the product and sum are over the appropriate range for j. The key to obtaining the final upper bound on the product was in the upper bounds on $2rc$ and $2(r+1)c$. In this case, we no longer have these bounds. Therefore it is necessary to find an alternate upper bound for the infinite product. The next lemma will aid in finding this bound.

Lemma 4.12 *Suppose* $2(r+1)c > 2rc \geq 1$. *Then*

$$\prod_{j>2(r+1)c} \frac{1+\left(1-\frac{2c}{j}\right)^{r+1}}{1+\left(1-\frac{2c}{j}\right)^{r}} \cdot \frac{1-\frac{rc}{j}}{1-\frac{(r+1)c}{j}} < \exp\left\{\frac{8rc^2}{\lfloor 2(r+1)c \rfloor}\right\}.$$

With these lemmas, we will be able to complete the desired analysis. From (4.104) and (4.105), the ratio of consecutive terms is asymptotically

$$\frac{T_{r+1}}{T_r} \sim \frac{l-r}{r+1} 2^{\lfloor 2rc \rfloor - \lfloor 2(r+1)c \rfloor} e^{2cC_1} \frac{t_1((r+1)c)}{t_1'(rc)} \frac{Q_{r+1}(c)}{Q_r(c)}. \tag{4.106}$$

We first observe that $2cC_1 < C_1$, so that

$$e^{2cC_1} < e^{C_1}.$$

This implies that

$$\frac{T_{r+1}}{T_r} < \frac{l-r}{r+1} 2^{\lfloor 2rc \rfloor - \lfloor 2(r+1)c \rfloor} e^{C_1} \frac{t_1((r+1)c)}{t_1'(rc)} \frac{Q_{r+1}(c)}{Q_r(c)} . \tag{4.107}$$

At this point, we must divide our analysis into two parts. We first consider the state when $\lfloor 2rc \rfloor = \lfloor 2(r+1)c \rfloor$. When this is true, we see that

$$2^{\lfloor 2rc \rfloor - \lfloor 2(r+1)c \rfloor} = 1,$$

giving

$$\frac{T_{r+1}}{T_r} < \frac{l-r}{r+1} e^{C_1} \frac{t_1((r+1)c)}{t_1'(rc)} \frac{Q_{r+1}(c)}{Q_r(c)} . \tag{4.108}$$

Since $\lfloor 2rc \rfloor = \lfloor 2(r+1)c \rfloor$, the products $t_1((r+1)c)$ and $t_1'(rc)$ are over the same range of j. Therefore we know that

$$\begin{aligned} \frac{t_1((r+1)c)}{t_1'(rc)} &= \prod_{j>2(r+1)c}^{k} \frac{1-\frac{(r+1)c}{j}}{1-\frac{rc}{j}} \\ &< \left(\frac{k}{\lfloor 2(r+1)c \rfloor} \right)^{-c} \exp\left\{ \frac{c}{\lfloor 2(r+1)c \rfloor} \right\} \end{aligned}$$

by Lemma 4.11. $Q_{r+1}(c)$ and $Q_r(c)$ are also over the same values of j and Lemma 4.12 implies

$$\begin{aligned} \frac{Q_{r+1}(c)}{Q_r(c)} &= \prod_{j>2(r+1)c} \frac{1+\left(1-\frac{2c}{j}\right)^{r+1}}{1+\left(1-\frac{2c}{j}\right)^{r}} \cdot \frac{1-\frac{rc}{j}}{1-\frac{(r+1)c}{j}} \\ &< \exp\left\{ \frac{8rc^2}{\lfloor 2(r+1)c \rfloor} \right\}. \end{aligned}$$

Replacing $\lfloor 2(r+1)c \rfloor$ by $\lfloor 2rc \rfloor$ and substituting these inequalities into (4.108), we find that

$$\frac{T_{r+1}}{T_r} < e^{C_1} \frac{l-r}{r+1} \left(\frac{k}{\lfloor 2rc \rfloor} \right)^{-c} \exp\left\{ \frac{c}{\lfloor 2rc \rfloor} \right\} \exp\left\{ \frac{8rc^2}{\lfloor 2rc \rfloor} \right\}. \tag{4.109}$$

This expression can now be bounded above by a constant. Consider first the ratio

$$\frac{l-r}{k^c} .$$

With $l = k^c$ and $r = \alpha l$, we find that

$$\frac{l-r}{k^c} = 1 - \alpha < 1$$

as in cases 1 and 2. Since $\lfloor 2rc \rfloor < 2rc < r < r+1$,

$$\frac{\lfloor 2rc \rfloor^c}{r+1} < \frac{(r+1)^c}{r+1} = (r+1)^{c-1}.$$

Furthermore, $r \geq 3$ and $c < 2/5$ implies that

$$\frac{\lfloor 2rc \rfloor^c}{r+1} < \frac{1}{4^{3/5}}\,.$$

Moving on to the exponential functions, we recall that $\lfloor 2rc \rfloor \geq 1$ to see that

$$\exp\left\{\frac{c}{\lfloor 2rc \rfloor}\right\} < e^{2/5}.$$

Finally, since $2rc < \lfloor 2rc \rfloor + 1$, we have that $2rc/\lfloor 2rc \rfloor < 1 + 1/\lfloor 2rc \rfloor$. Therefore,

$$\exp\left\{\frac{8rc^2}{\lfloor 2rc \rfloor}\right\} < \exp\left\{4c\left(1 + \frac{1}{\lfloor 2rc \rfloor}\right)\right\} < e^{16/5}.$$

Applying these results to (4.109), we have shown that when $2(r+1)c > 2rc \geq 1$ and $\lfloor 2rc \rfloor = \lfloor 2(r+1)c \rfloor$, then the ratio of consecutive terms is bounded above by

$$\begin{aligned} \frac{T_{r+1}}{T_r} &< \frac{1}{4^{3/5}}\, e^{18/5 + C_1} \\ &< 18.4806\ldots \end{aligned} \tag{4.110}$$

Certainly this is not quite as low of an upper bound as we hoped for, but it decreases quickly as r, $2rc$, and $2(r+1)c$ grow. In fact, when $2rc \geq 2$, this bound is already reduced to $6.7986\ldots$

We must also look at T_{r+1}/T_r when $\lfloor 2rc \rfloor \neq \lfloor 2(r+1)c \rfloor$. In this case, all the work leading up to (4.107) still holds, and we begin with the inequality

$$\frac{T_{r+1}}{T_r} < \frac{l-r}{r+1} 2^{\lfloor 2rc \rfloor - \lfloor 2(r+1)c \rfloor} e^{C_1} \frac{t_1((r+1)c)}{t_1'(rc)} \frac{Q_{r+1}(c)}{Q_r(c)}\,.$$

Here, $\lfloor 2rc \rfloor + 1 = \lfloor 2(r+1)c \rfloor$, so that

$$2^{\lfloor 2rc \rfloor - \lfloor 2(r+1)c \rfloor} = \frac{1}{2}\,,$$

modifying the above bound to be

$$\frac{T_{r+1}}{T_r} < \frac{e^{C_1}}{2} \frac{l-r}{r+1} \frac{t_1((r+1)c)}{t_1'(rc)} \frac{Q_{r+1}(c)}{Q_r(c)}\,. \tag{4.111}$$

Although the remaining ratios will involve more work to analyze, they will lead to a better bound for T_{r+1}/T_r. Per the discussion leading to Lemma 4.11, we may write

$$\frac{t_1((r+1)c)}{t_1'(rc)} = \left(1 - \frac{rc}{\lfloor 2rc \rfloor + 1}\right)^{-1} \prod_{j>2(r+1)c}^{k} \frac{1 - \frac{(r+1)c}{j}}{1 - \frac{rc}{j}}\,.$$

Observe again that $2rc < \lfloor 2rc \rfloor + 1$. This implies that

$$\frac{rc}{\lfloor 2rc \rfloor + 1} < \frac{1}{2}$$

and therefore,

$$\left(1 - \frac{rc}{\lfloor 2rc \rfloor + 1}\right)^{-1} < 2.$$

Along with the result of Lemma 4.11, this gives

$$\frac{t_1((r+1)c)}{t_1'(rc)} < 2\left(\frac{k}{\lfloor 2(r+1)c \rfloor}\right)^{-c} \exp\left\{\frac{c}{\lfloor 2(r+1)c \rfloor}\right\}.$$

$Q_r(c)$ also has more factors than $Q_{r+1}(c)$, so

$$\frac{Q_{r+1}(c)}{Q_r(c)} = \frac{1 - \frac{rc}{\lfloor 2rc \rfloor + 1}}{1 + \left(1 - \frac{2c}{\lfloor 2rc \rfloor + 1}\right)^{r}} \prod_{j>2(r+1)c} \frac{1 + \left(1 - \frac{2c}{j}\right)^{r+1}}{1 + \left(1 - \frac{2c}{j}\right)^{r}} \cdot \frac{1 - \frac{rc}{j}}{1 - \frac{(r+1)c}{j}}\,.$$

Another inequality for $\lfloor 2rc \rfloor$ will enable us to bound the initial term. Since the denominator of this factor is strictly greater than 1,

$$\frac{1 - \frac{rc}{\lfloor 2rc \rfloor + 1}}{1 + \left(1 - \frac{2c}{\lfloor 2rc \rfloor + 1}\right)^{r}} < 1 - \frac{rc}{\lfloor 2rc \rfloor + 1}\,.$$

Then $\lfloor 2rc \rfloor \leq 2rc$ gives the inequality

$$\frac{rc}{\lfloor 2rc \rfloor + 1} \geq \frac{1}{2}\frac{\lfloor 2rc \rfloor}{\lfloor 2rc \rfloor + 1}\,.$$

Finally, since $\lfloor 2rc \rfloor \geq 1$,

$$1 - \frac{rc}{\lfloor 2rc \rfloor + 1} \leq 1 - \frac{1}{2}\frac{\lfloor 2rc \rfloor}{\lfloor 2rc \rfloor + 1} \leq \frac{3}{4}\,.$$

Then this result with Lemma 4.12 shows

$$\begin{aligned}\frac{Q_{r+1}(c)}{Q_r(c)} &= \frac{1-\frac{rc}{\lfloor 2rc\rfloor+1}}{1+\left(1-\frac{2c}{\lfloor 2rc\rfloor+1}\right)^r}\prod_{j>2(r+1)c}\frac{1+\left(1-\frac{2c}{j}\right)^{r+1}}{1+\left(1-\frac{2c}{j}\right)^r}\cdot\frac{1-\frac{rc}{j}}{1-\frac{(r+1)c}{j}}\\ &< \frac{3}{4}\exp\left\{\frac{8rc^2}{\lfloor 2(r+1)c\rfloor}\right\}.\end{aligned}$$

Returning to the ratio of consecutive terms, the inequality given in (4.111) becomes

$$\begin{aligned}\frac{T_{r+1}}{T_r} &< \frac{3}{4}e^{C_1}\frac{l-r}{r+1}\left(\frac{k}{\lfloor 2(r+1)c\rfloor}\right)^{-c}\\ &\quad *\exp\left\{\frac{c}{\lfloor 2(r+1)c\rfloor}\right\}\exp\left\{\frac{8rc^2}{\lfloor 2(r+1)c\rfloor}\right\}. \qquad (4.112)\end{aligned}$$

The remaining non-constant factors can be handled as before. With $l = k^c$ and $r = \alpha l$,

$$\frac{l-r}{k^c} < 1.$$

The fact that $\lfloor 2(r+1)c\rfloor \le 2(r+1)c$ gives

$$\frac{\lfloor 2(r+1)c\rfloor^c}{r+1} < (r+1)^{c-1} < \frac{1}{4^{3/5}}.$$

Now, since $\lfloor 2(r+1)c\rfloor = \lfloor 2rc\rfloor + 1$ and $\lfloor 2rc\rfloor \ge 1$,

$$\exp\left\{\frac{c}{\lfloor 2(r+1)c\rfloor}\right\} < e^{1/5}.$$

Finally, since $2rc < \lfloor 2(r+1)c\rfloor$,

$$\exp\left\{\frac{8rc^2}{\lfloor 2(r+1)c\rfloor}\right\} < e^{4c} < e^{8/5}.$$

We apply these bounds to (4.112) to find the final upper bound of

$$\begin{aligned}\frac{T_{r+1}}{T_r} &< \frac{3}{4}\frac{1}{4^{3/5}}e^{9/5+C_1}\\ &< 2.2911\ldots \qquad (4.113)\end{aligned}$$

When $2rc \ge 2$, this constant upper bound decreases to $1.9052\ldots$

Proofs of the Lemmas

We have now shown that the ratio of T_{r+1} to T_r can be bounded above by a constant in each of the three cases. Before summarizing the results found in the last sections and commenting on them, we prove the lemmas used in the last section.

Lemma 4.11 gives a necessary partial bound on the ratio of $t_1((r+1)c)$ to $t_1'(rc)$. Since the same product appears both when $\lfloor 2rc \rfloor = \lfloor 2(r+1)c \rfloor$ and $\lfloor 2rc \rfloor \neq \lfloor 2(r+1)c \rfloor$, we needed to find an upper bound on this product. The following proof will first find an upper bound on the product factors for fixed j and use this to give the final result.

Lemma 4.11 *Suppose* $2(r+1)c > 2rc \geq 1$. *Then*

$$\prod_{j>2(r+1)c}^{k} \frac{1-\frac{(r+1)c}{j}}{1-\frac{rc}{j}} < \left(\frac{k}{\lfloor 2(r+1)c \rfloor}\right)^{-c} \exp\left\{\frac{c}{\lfloor 2(r+1)c \rfloor}\right\}.$$

Proof: To find an upper bound on the factors of the product, we first observe that the ratio

$$\frac{1-\frac{(r+1)c}{j}}{1-\frac{rc}{j}} \tag{4.114}$$

is very close to 1 for all $j > 2(r+1)c$. In fact, since $(r+1)c > rc$, this ratio is slightly less than 1. We can find an upper bound for the ratio by finding a lower bound on the distance between 1 and (4.114). Subtracting the ratio from 1, we see

$$1 - \frac{1-\frac{(r+1)c}{j}}{1-\frac{rc}{j}} = \frac{c/j}{1-rc/j}\,.$$

Since $1 - rc/j < 1$ for all $j > 2(r+1)c$, we find that

$$\frac{1-\frac{(r+1)c}{j}}{1-\frac{rc}{j}} > \frac{c}{j}\,.$$

Therefore

$$\frac{1-\frac{(r+1)c}{j}}{1-\frac{rc}{j}} < 1 - \frac{c}{j} \tag{4.115}$$

for all $j > 2(r+1)c$. We apply this bound to the original product to see that

$$\prod_{j>2(r+1)c}^{k} \frac{1-\frac{(r+1)c}{j}}{1-\frac{rc}{j}} < \prod_{j>2(r+1)c}^{k} 1 - \frac{c}{j}\,. \tag{4.116}$$

This product can be rewritten as an exponential function,

$$\prod_{j>2(r+1)c}^{k} 1 - \frac{c}{j} = \exp\left\{ \sum_{j>2(r+1)c}^{k} \log\left(1 - \frac{c}{j}\right) \right\}.$$

By the Taylor expansion of log, we know that $-\log(1-x) > x$, so that

$$\exp\left\{ \sum_{j>2(r+1)c}^{k} \log\left(1 - \frac{c}{j}\right) \right\} < \exp\left\{ \sum_{j>2(r+1)c}^{k} -\frac{c}{j} \right\}.$$

An application of Euler Maclaurin summation will show that

$$\sum_{j>2(r+1)c}^{k} \frac{1}{j} > \log k - \log\lfloor 2(r+1)c \rfloor + \frac{1}{k} - \frac{1}{\lfloor 2(r+1)c \rfloor}.$$

Substituting this into the inequality above and simplifying, this gives

$$\exp\left\{ \sum_{j>2(r+1)c}^{k} -\frac{c}{j} \right\} < \left(\frac{k}{\lfloor 2(r+1)c \rfloor} \right)^{-c} \exp\left\{ -\frac{c}{k} + \frac{c}{\lfloor 2(r+1)c \rfloor} \right\}.$$

We bound this final expression to obtain the result

$$\prod_{j>2(r+1)c}^{k} \frac{1 - \frac{(r+1)c}{j}}{1 - \frac{rc}{j}} < \left(\frac{k}{\lfloor 2(r+1)c \rfloor} \right)^{-c} \exp\left\{ \frac{c}{\lfloor 2(r+1)c \rfloor} \right\},$$

as desired. □

Recall that the asymptotic for $t_1'(rc)$ found in Section 4.5.4 contains a factor of k^{-rc} and the asymptotic for $t_1((r+1)c)$ contains $k^{-(r+1)c}$. The ratio of these two asymptotics would have a factor of k^{-c}, as the upper bound given above does. This supports the result of Lemma 4.11 and tells us that this bound is correct.

The next lemma was needed in order to look at the ratio of $Q_{r+1}(c)$ to $Q_r(c)$. Since the upper bound on this ratio used in cases 1 and 2 was so dependent on $2rc$ and $2(r+1)c$ being bounded above, we needed another result that didn't depend on this.

Lemma 4.12 *Suppose* $2(r+1)c > 2rc \geq 1$. *Then*

$$\prod_{j>2(r+1)c} \frac{1 + \left(1 - \frac{2c}{j}\right)^{r+1}}{1 + \left(1 - \frac{2c}{j}\right)^{r}} \cdot \frac{1 - \frac{rc}{j}}{1 - \frac{(r+1)c}{j}} < \exp\left\{ \frac{8rc^2}{\lfloor 2(r+1)c \rfloor} \right\}.$$

Proof: As in the proof of Lemma 4.11, we first find an upper bound on one factor of the product. To simplify notation slightly, define $x = c/j$. Then

$$\frac{1+\left(1-\frac{2c}{j}\right)^{r+1}}{1+\left(1-\frac{2c}{j}\right)^{r}} \cdot \frac{1-\frac{rc}{j}}{1-\frac{(r+1)c}{j}} = \frac{1+(1-2x)^{r+1}}{1+(1-2x)^{r}} \cdot \frac{1-rx}{1-(r+1)x} .$$

Set $f(r,x)$ to be this expression. We know that this ratio is close to 1. Subtracting 1 from $f(r,x)$ and simplifying, we obtain

$$f(r,x) - 1 = \frac{x(1-(1-2x)^r(1-2rx))}{(1-(r+1)x)(1+(1-2x)^r)} .$$

Since this ratio, call it $g(r,x)$, is positive, then an upper bound for it will give an upper bound for $f(r,x)$, which is what we desire.

Consider the denominator of $g(r,x)$. Observe first that since $j > 2(r+1)c$, we have that $(r+1)x < 1/2$. Therefore

$$1-(r+1)x > \frac{1}{2} .$$

Furthermore, $1+(1-2x)^r > 1$, so that the denominator of $g(r,x)$ is greater than $1/2$. Thus,

$$g(r,x) < 2x(1-(1-2x)^r(1-2rx)).$$

Using the standard lower bound, $(1-2x)^r > 1-2rx$, we now have

$$\begin{aligned} g(r,x) &< 2x(1-(1-2x)^r(1-2rx)) \\ &< 2x(1-(1-2rx)^2) \\ &= 8rx^2(1-rx) \\ &< 8rx^2. \end{aligned}$$

This implies that

$$f(r,x) < 1 + 8rx^2.$$

Returning to the original notation and applying this to the product, we have

$$\prod_{j>2(r+1)c} \frac{1+\left(1-\frac{2c}{j}\right)^{r+1}}{1+\left(1-\frac{2c}{j}\right)^{r}} \cdot \frac{1-\frac{rc}{j}}{1-\frac{(r+1)c}{j}} < \prod_{j>2(r+1)c} 1 + \frac{8rc^2}{j^2} .$$

We rewrite this as an exponential function and bound it above using an upper bound on the exponent.

$$\begin{aligned}\prod_{j>2(r+1)c} 1+\frac{8rc^2}{j^2} &= \exp\left\{\sum_{j>2(r+1)c}\log\left(1+\frac{8rc^2}{j^2}\right)\right\}\\ &< \exp\left\{\sum_{j>2(r+1)c}\frac{8rc^2}{j^2}\right\}\end{aligned}$$

Since $1/x^2$ is decreasing and concave up, we can find an upper bound on the last sum above by evaluating the corresponding integral from $\lfloor 2(r+1)c\rfloor$ to infinity. So

$$\begin{aligned}\sum_{j>2(r+1)c}\frac{8rc^2}{j^2} &< \int_{\lfloor 2(r+1)c\rfloor}^{\infty}\frac{8rc^2}{x^2}\,dx\\ &= \frac{8rc^2}{\lfloor 2(r+1)c\rfloor}\,.\end{aligned}$$

Substituting this into the exponential function gives the desired result. □

The bound found in this lemma is actually the reason that the constant upper bound for T_{r+1}/T_r is larger than we would like. Although this bounding function becomes very close to the actual truth as r increases, this is not the case for small r. A better bound, however, would require different methods.

Summary of Cases

In each of the outlined cases, we have shown that the ratio of consecutive terms of $E(2^s)$ is bounded above by the constant 19, better in most cases. The bounds found for Cases 1, 2, and 3 are summarized in the next theorem.

Theorem 4.6 *Suppose $r \geq 3$. Let T_r be the r^{th} term of $E(2^s)$ and T_{r+1} the $(r+1)^{st}$ term.*

(i) When $2rc < 2(r+1)c < 1$,

$$\frac{T_{r+1}}{T_r} < \frac{1}{4}\,e^{\pi^2/12} < 0.5690\ldots;$$

(ii) When $2rc < 1$ and $1 \leq 2(r+1)c < 2$,

$$\frac{T_{r+1}}{T_r} < \frac{1}{2}\,e^{\pi^2/6-1} < 0.9529\ldots;$$

(iii) When $2(r+1)c > 2rc \geq 1$ *and* $\lfloor 2rc \rfloor = \lfloor 2(r+1)c \rfloor$,

$$\frac{T_{r+1}}{T_r} < \frac{1}{4^{3/5}}\, e^{18/5+C_1} < 18.4806\ldots;$$

(iv) When $2(r+1)c > 2rc \geq 1$ *and* $\lfloor 2rc \rfloor + 1 = \lfloor 2(r+1)c \rfloor$,

$$\frac{T_{r+1}}{T_r} < \frac{3}{4}\frac{1}{4^{3/5}}\, e^{9/5+C_1} < 2.2911\ldots$$

As discussed in the work for Case 1 and Case 2, since the bounds found for these two cases are less than 1, we can bound the terms of $E(2^s)$ above by a convergent geometric series while $2rc$ and $2(r+1)c$ fall into one of these categories. On the other hand, although the upper bounds improve in the last two cases above and even fall below 1 when r is large enough, we cannot initially bound the terms in this range by a convergent geometric series. What this means is that our methods will not allow us to prove what we want with the assumptions we have now on l. Recall that we chose $l = k^c$ as a result of determining when $T_1 < 1$. Although we cannot show that $E(2^s)$ can be entirely bounded above by a geometric series with our results, we will be able to show that this can be done for smaller l. Therefore, $l = k^c$ will serve as the threshold function that we have been searching for. In the next section, we will show that $E(2^s)$ approaches 1 for smaller l, and that it approaches infinity for larger l.

4.7 The Threshold Theorems

We can determine how much smaller l needs to be before we can show that $E(2^s)$ approaches 1 by the bounds given in Theorem 4.6. That theorem tells us that for $r \geq 3$,

$$\frac{T_{r+1}}{T_r} = \frac{\binom{l}{r+1} t_{r+1}(c)}{\binom{l}{r} t_r(c)} < 19.$$

As previously mentioned, the upper bound is, in fact, better than this for most cases considered, but we take the largest bound to take care of all cases. We also know that this bound is true for $r < 3$ as well. Since $T_1 < 1$ when $l < d_1 k = k^c e^{c\gamma + h_\zeta(c)}$, then

$$\frac{T_1}{T_0} = T_1 < 1$$

when $l = k^c < k^c e^{c\gamma + h_\zeta(c)}$. Then since $T_2 < T_1$ whenever $T_1 < 1$ by Theorem 4.3, we know

$$\frac{T_2}{T_1} < 1$$

when $l = k^c$. Our goal is still to bound $E(2^s)$ above by a geometric series that converges to 1. To do this, we must choose l small enough to force the largest upper bound of 19 to instead be less than 1. Set $\epsilon < 1/19$ and $l = \epsilon k^c$. Observe that choosing l this way gives $l < k^c$. Consider the ratio of consecutive terms for $r \geq 3$,

$$\begin{aligned} \frac{T_{r+1}}{T_r} &= \frac{\binom{l}{r+1} t_{r+1}(c)}{\binom{l}{r} t_r(c)} \\ &= \frac{l-r}{r+1} \cdot \frac{t_{r+1}(c)}{t_r(c)}. \end{aligned}$$

With $l = \epsilon k^c$ and $r = \alpha l$, this ratio can be bounded above by

$$\begin{aligned} \frac{T_{r+1}}{T_r} &= \frac{l-r}{r+1} \cdot \frac{t_{r+1}(c)}{t_r(c)} \\ &< \epsilon \left(\frac{k^c - \alpha k^c}{r+1} \cdot \frac{t_{r+1}(c)}{t_r(c)} \right) \\ &< 19\epsilon \\ &< 1. \end{aligned}$$

Therefore, when $\epsilon < 1/19$, the ratio of consecutive terms for all r is less than 1. Furthermore, as $\epsilon \to 0$, the ratio decreases. This gives a function for l for which we can bound $E(2^s)$ above by a geometric series. We are now prepared to state the threshold theorem we have been searching for.

Theorem 4.7 *Suppose* $0 < c < 2/5$ *and* $l = l(k)$.

(i) If $l/k^c \to 0$, *then* $E(2^s) \to 1$.

(ii) If $l/k^c \to \infty$, *then* $E(2^s) \to \infty$.

Proof: Much of the work to prove part *(i)* has been done already. We will complete the proof of part *(i)* here and prove part *(ii)* as well.

(i) Suppose $l = \epsilon k^c$ where $\epsilon \to 0$. We will show that we can bound

$$E(2^s) = \sum_{r=0}^{l} T_r = \sum_{r=0}^{l} \binom{l}{r} t_r(c)$$

above by a geometric series that converges to 1 as $\epsilon \to 0$. Observe that

$$\frac{T_1}{T_0} = lt_1(c) = \epsilon k^c t_1(c) < \epsilon$$

by the results from Section 4.3.4. Theorem 4.3 also implies that

$$\begin{aligned} \frac{T_2}{T_1} &= \frac{l-1}{2}\frac{t_2(c)}{t_1(c)} \\ &< \epsilon\frac{k^c}{2}\frac{t_2(c)}{t_1(c)} \\ &< \epsilon. \end{aligned}$$

A careful analysis similar to the one leading to Theorem 4.6 will show that $T_3/T_2 < 1.1988\ldots$ when $l = k^c$. As we saw in that discussion, we must consider the case when $2rc < 1$ as well as when $2rc \geq 1$ for $r = 3$. The methods of Section 4.6.2 can be used for both cases. Then for $l = \epsilon k^c$,

$$\frac{T_3}{T_2} < 1.2\epsilon.$$

Finally, when $r \geq 3$,

$$\begin{aligned} \frac{T_{r+1}}{T_r} &= \frac{l-r}{r+1} \cdot \frac{t_{r+1}(c)}{t_r(c)} \\ &< \epsilon\left(\frac{k^c - \alpha k^c}{r+1} \cdot \frac{t_{r+1}(c)}{t_r(c)}\right) \\ &< 19\epsilon \end{aligned}$$

by Theorem 4.6. Therefore, for all $r \geq 0$,

$$\frac{T_{r+1}}{T_r} < 19\epsilon. \tag{4.117}$$

Beginning with $r = 0$, equation (4.117) implies that $T_1/T_0 < 19\epsilon$, so that

$$T_1 < 19\epsilon.$$

Similarly, by equation (4.117), $T_2 < 19\epsilon T_1$, so that

$$T_2 < (19\epsilon)^2.$$

Continuing in this manner, we see that $T_{r+1} < 19\epsilon T_r$, thus

$$T_{r+1} < (19\epsilon)^{r+1}$$

for all $0 \leq r < l$. Applying this to the sum $E(2^s)$, we find

$$\begin{aligned} E(2^s) &= \sum_{r=0}^{l} T_r \\ &< \sum_{r=0}^{l} (19\epsilon)^r \\ &< \sum_{r=0}^{\infty} (19\epsilon)^r \\ &= \frac{1}{1-19\epsilon}\,. \end{aligned} \tag{4.118}$$

Then as $\epsilon \to 0$,

$$E(2^s) \to 1.$$

(ii) Suppose that $l = Mk^c$, where $M \to \infty$. We want to show that $E(2^s)$ approaches infinity also. We have seen that $T_1 < 1$ when $l < k^c$. When l is larger than the critical value, roughly when $l > 1.4892k^c$, we know that $T_1 > 1$. We use this fact to show the desired result. Observe that

$$\begin{aligned} E(2^s) &= \sum_{r=0}^{l} T_r \\ &> T_1 \\ &\sim lk^{-c}e^{-c\gamma - h_\zeta(c)} \end{aligned}$$

since $T_r > 0$ for all r. Then substituting Mk^c in for l, we see that

$$E(2^s) > Me^{-c\gamma - h_\zeta(c)}.$$

Then for fixed c,

$$E(2^s) \to \infty$$

as $M \to \infty$. □ We can restate Theorem 4.7 more precisely to make the limits clearer.

Theorem 4.8 *Suppose* $0 < c < 2/5$ *and* $l = l(k)$.

(i) If $l < \epsilon k^c$, then

$$E(2^s) < 1 + \frac{19\epsilon}{1 - 19\epsilon}\,.$$

(ii) If $l > Mk^c$, then

$$E(2^s) > Me^{-c\gamma - h_\zeta(c)}.$$

Observe that as $\epsilon \to 0$ above, $E(2^s) \to 1$. Similarly, $E(2^s) \to \infty$ as $M \to \infty$. The bounding functions come directly from the previous proof and we can see that Theorem 4.7 is also a consequence of this theorem.

We now have the threshold function that describes the behavior of $E(2^s)$ for this model. Theorem 4.7 tells us when l is small compared to $l^*(k) = k^c$, in particular when $l < \epsilon k^c$, then $E(2^s)$ approaches 1. Then when l is large with respect to $l^*(k)$, the sum approaches infinity. Thus $l = \epsilon k^c$ is a lower bound for the number of vectors needed before $E(2^s)$ increases above 1.

4.8 Conclusion

We return now to the application we are interested in. Recall our question, introduced in Chapter 1:

Question: Choose l vectors randomly from a vector space based on a given probability distribution. How large must l be to ensure with high probability that a subset of the l vectors is linearly dependent?

The work in this chapter has been devoted to analyzing the probability model in which the vectors chosen have probability c/j of having a 1 in the j^{th} position. That is, if $\mathbf{v}$ is a vector generated under this model, then

$$Pr(\mathbf{v}[j] = 1) = \frac{c}{j}$$

where $0 < c < 2/5$. Our goal was to find a lower bound on the number of vectors needed in order to ensure that a subset of those vectors is linearly dependent with high probability. In this chapter, we have identified the threshold function discussed in the introduction, $l^*(k)$, which desribes the behavior of the sum $E(2^s)$.

Theorem 4.8 gives critical values for fixed k for which $E(2^s)$ approaches 1 and infinity. Recall that $E(2^s)$ is the expected size of the left null space of the matrix whose j^{th} row is the j^{th} vector chosen. When the expected size of the left null space

is 1, we only expect there to be 1 vector in the null space, the zero vector. If this is the case, the vectors chosen are almost surely independent. By Theorem 4.8, we see that when $l < \epsilon k^c$, the expected size of the left null space is close to 1, implying that the probability the l vectors generated are dependent is close to 0. Therefore we must generate at least ϵk^c vectors before we can expect to see dependence among the vectors.

On the other hand, when the size of the left null space becomes very large, it becomes more likely that the vectors chosen are dependent. Unfortunately we are not able to use the results of the theorem to predict when the probability of dependence is close to 1. Since the threshold function describes the expected size of the left null space rather than the expected dimension, it merely tells us when $E(2^s)$ approaches infinity, and 2^s grows much more quickly than s, the dimension of the left null space. The threshold function describing the behavior of $E(2^s)$ certainly provides a lower bound for the threshold function describing the probability of dependence. However, the actual probability threshold results may be better than what we have shown here. For future work, we would like to determine a threshold function for the probability of dependence. This will be a function, $l^*(k)$, such that when $l(k)/l^*(k)$ approaches 0, the probability of dependence is very small. Then when $l(k)/l^*(k)$ approaches infinity, the probability of dependence approaches 1, that is, the vectors are almost surely dependent.

Figure 4.9 shows the threshold graph representing our results.Observe that the probability that the vectors are dependent is small when $l < \epsilon k^c$. Calculations of $E(2^s)$ seem to show that it approaches 1 for values of l closer to k^c than our results imply. This would mean that l vectors are almost surely independent for a larger range of l than what we have shown. We also believe these results to be true for $0 < c < 9/20$. However, we will need a different approach or different method to prove these statements. Finally, since we don't have an upper bound for the number of vectors needed for dependency, we are not able determine how sharp the threshold is. Finding an upper bound for l will require further study.

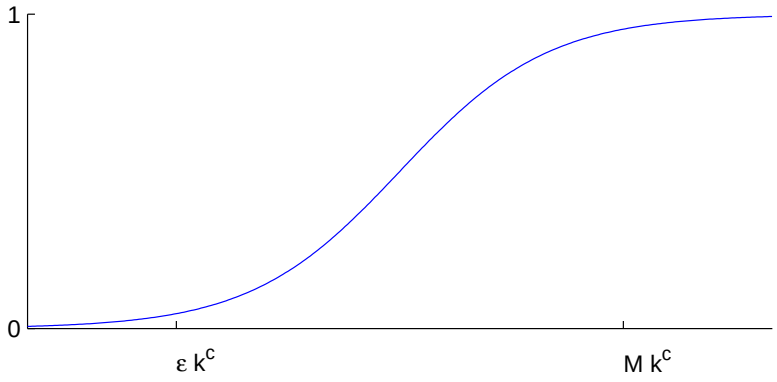

Figure 4.9 Threshold Graph for c/j Model

We have now given a lower bound for the number of vectors we need to generate before it is possible for dependence to occur. In Section 4.2, we claimed that the number of vectors needed should be less under this model than under the fixed weight vector model since these vectors are very sparse. Our results do not prove this statement, but seem to indicate that it is true. We have shown that we need to generate at least ϵk^c vectors under this probability model to ensure with high probability that the vectors are dependent.

BIBLIOGRAPHY

1. N. Alon and J.H. Spencer, *The Probabilistic Method*, Wiley (2000).

2. G.V. Balakin, V.F Kolchin, and V.I. Khokhlov, Hypercycles in a Random Hypergraph, *Diskretnaya Matematika* **3** 3 (1991), 102-108 (in Russian).

3. B. Bollobás, *Random Graphs*, Cambridge Univ. Press (2001).

4. R.P. Brent, S. Gao, and A.G.B. Lauder, Random Krylov Spaces Over Finite Fields, *SIAM J. Discrete Math.* **16** 2 (2003), 276-287.

5. N.J. Calkin, Dependent Sets of Constant Weight Binary Vectors, *Combinatorics, Probability and Computing* **6** (1997), 263-271.

6. N.J. Calkin, Dependent Sets of Constant Weight Vectors in $GF(q)$, *Random Structures and Algorithms* **9**, Nos. 1 and 2 (1996), 49-53.

7. C. Cooper, Asymptotics for Dependent Sums of Random Vectors, *Random Structures and Algorithms* **14** 3, (1999), 267-292.

8. R.L. Graham, D.E. Knuth, and O. Patashnik, *Concrete Mathematics*, Addison Wesley, 2^{nd} Edition, (1994).

9. V.F. Kolchin, Random Graphs and Systems of Linear Equations in Finite Fields, *Random Structures and Algorithms* **5**, No. 1 (1994), 135-146.

10. V.F. Kolchin, A Threshold Effect For Systems of Random Equations in Finite Fields, *Discrete Math. Appl.* **9**, No. 4 (1999), 355-364.

11. V.F. Kolchin and V.I. Khokhlov, On the Number of Cycles in a Non-equiprobably Random Graph, *Diskretnaya Matematika* **2**, No. 3 (1990), 135-146.

12. V.F. Kolchin and V.I. Khokhlov, A Threshold Effect For Systems of Random Equations of a Special Form, *Discrete Math. Appl.* **5**, No. 5 (1995), 425-436.

13. N. Linial and D. Weitz, Random Vectors of Bounded Weight and Their Linear Dependencies, *unpublished manuscript*, (2000).

14. G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge University Press, (1990).

15. H.S. Wilf, *generatingfunctionology*, Academic Press, 2^{nd} Edition, (1994).

16. H.S. Wilf, *Mathematics for the Physical Sciences*, John Wiley & Sons, Inc., (1962).