# Maximum Matchings in Random Bipartite Graphs and the Space Utilization of Cuckoo Hash Tables

Alan Frieze[1,*]
[1] Department of Mathematical Sciences
Carnegie Mellon University
Pittsburgh PA 15213
U.S.A.

Páll Melsted[1,2]
[2] Faculty of Industrial Engineering,
Mechanical Engineering and
Computer Science
University of Iceland
Reykjavik
Iceland

**Abstract**

We study the the following question in Random Graphs. We are given two disjoint sets $L, R$ with $|L| = n$ and $|R| = m$. We construct a random graph $G$ by allowing each $x \in L$ to choose $d$ random neighbours in $R$. The question discussed is as to the size $\mu(G)$ of the largest matching in $G$. When considered in the context of Cuckoo Hashing, one key question is as to when is $\mu(G) = n$ **whp**? We answer this question exactly when $d$ is at least three.

## 1 Introduction

For a graph $G$ we let $\mu(G)$ denote the size of a maximum matching in $G$. This paper provides an analysis of $\mu(G)$ in the following model of a random bipartite graph. We have two disjoint sets $L, R$ where $L = [n], R = [m]$ where $n = \alpha m$. Each $v \in L$ independently chooses $d$ random vertices of $R$ as neighbours. Our assumptions are that $\alpha > 0$, $d \geq 3$ are fixed and $n \to \infty$. There is of course the issue as to whether a vertex is allowed to make the same choice twice. We allow this in the paper in order to keep the $d$ choices independent. Keeping the choices distinct makes no essential difference to the final result. One can for example couple the two modes of construction so that the size of the maximum matching is always at least as large when no repetitions are allowed.

After some preliminary analysis we can reduce the question to the following: We have two disjoint sets $L_1, R_1$ of sizes $n_1, m_1$ respectively. Asymptotic expressions for the values of $m_1, n_1$ that hold **whp** are given. Each vertex of $L_1$ chooses $d \geq 3$ random neighbours in $R_1$. The choices are conditioned so that each vertex of $R_1$ is of degree at least two. Let $G_1$ denote the sub-graph of $G$ induced by $L_1, R_1$. We show that

$$\mu(G_1) = \min\{|L_1|, |R_1|\} \ \ \textbf{whp}.$$

This amounts to proving the following theorem:

*Supported in part by NSF Grant DMS0753472.

**Theorem 1** *Let $\Gamma$ be a bipartite graph chosen uniformly from the sets of graphs with bipartition $L, R$, $|L| = n, |R| = m$ such that each vertex of $L$ has degree $d \geq 3$ and each vertex of $R$ has degree at least two. Then* **whp**

$$\mu(\Gamma) = \min\{m, n\}.$$

The proof of this comprises the main technical challenge of the paper. This result has a similar flavour to some classical results. Walkup [30] considered the problem when $|L| = |R| = n$ and each vertex of $L$ chooses $d$ random neighbours in $R$ and each vertex of $R$ chooses $d$ random neighbours in $L$. He showed that a random bipartite graph constructed in this way has a perfect matching **whp** iff $d \geq 2$. Karonski and Pittel [18] considered a refinement where in the first round each vertex of $L \cup R$ first chooses a single random neighbour. Then each vertex not chosen by another vertex in first round gets another random choice. In this way the graph has minimum degree at least two. They show that this graph has a perfect matching **whp**, thus improving on Walkup's theorem.

Another motivation for this study comes from Cuckoo Hashing, see for example Mitzenmacher [26]. Briefly each one of $n$ items $x \in L$ has $d$ possible locations $h_1(x), h_2(x), \ldots, h_d(x) \in R$, where $d$ is typically a small constant and the $h_i$ are hash functions, typically assumed to behave as independent fully random hash functions. (See [25] for some justification of this assumption.) We are thus led to consider the bipartite graph $G$ which has vertex set $L \cup R$ and edge set $\{(x, h_j(x)) : x \in L, j = 1, 2, \ldots, d\}$. Under the assumption that the hash functions are completely random we see that $G$ has the same distribution as the random graph defined in the previous paragraph.

We assume each location can hold only one item. Items are inserted consecutively and when an item $x$ is inserted into the table, it can be placed immediately if one of its $d$ locations is currently empty. If not, one of the items in its $d$ locations must be displaced and moved to another of its $d$ choices to make room for $x$. This item in turn may need to displace another item out of one of its $d$ locations. Inserting an item may require a sequence of moves, each maintaining the invariant that each item remains in one of its $d$ potential locations, until no further evictions are needed. Thus having inserted $k$ items, we have constructed a matching $M$ of size $k$ in $G$. Adding a $(k+1)$-st item is tantamount to constructing an augmenting path with respect to $M$. All $n$ items will be insertable in this way iff $G$ contains a matching of size $n$.

The case of $d = 2$ choices is notably different from that for other values of $d$ and the theory for the case where there are $d = 2$ bucket choices for each item is well understood at this point [10, 23, 28]. We will therefore assume that $d \geq 3$.

We note finally that Theorem 1 can be interpreted in the context of random $d$-uniform hypergraphs for $d \geq 3$. The 2-core of a hypergraph $H$ is the largest set of vertices that induce a sub-graph of minimum degree two. The density of a set of vertices $S$ is the ratio of the number of edges contained entirely in $S$ to the size of $S$ itself. If we interpret the neighbours of a vertex $v \in L$ as an edge of a random $d$-uniform hypergraph then the theorem implies the following: A random $d$-uniform hypergraph contains a set of density at least one, only when the 2-core has density at least one, **whp**. This is a consequence of Hall's theorem for matchings and our result for the case where $n \leq m$. For results on the 2-core of a random hypergraph, see for example Cooper [8] and Molloy [27].

We will now turn to the matchings question referred to in Theorem 1.

## 2 Definitions and Results

This question was studied initially by Fotakis, Pagh, Sanders and Spirakis [15]. They show in the course of their analysis of Cuckoo hashing that the following holds:

**Lemma 2** *Suppose that* $0 < \varepsilon < 1$ *and* $d \geq 2(1+\varepsilon)\log(e/\varepsilon)$. *Suppose also that* $m = (1+\varepsilon)n$. *Then* **whp** $G$ *contains a matching of size* $n$ *i.e. a matching of* $L$ *into* $R$.

□

In particular, if $d = 3$ and $m \approx 1.57n$ then Lemma 2 shows that there is a matching of $L$ into $R$ **whp**.

This lemma is not tight and recently Dietzfelbinger, Goerdt, Mitzenmacher, Montanari, Pagh and Rink [11] observed a connection with a result of Dubois and Mandler on Random 3-XORSAT [13] that enables one to essentially answer the question as to when $\mu(G) \geq n$ for the case $d = 3$. The final version of [11] extends the result of [13] to $d \geq 3$. More recently, Fountoulakis and Panagiotou [16] have also established thresholds for when there is a matching of $L$ into $R$ **whp**, for all $d \geq 3$. It should perhaps be noted that the result of this paper is stronger in the sense that it gives the size of the largest matching when there is no matching of $L$ into $R$.

We begin with a simple observation that is the basis of the Karp-Sipser Algorithm [19, 2]. If $v$ is a vertex of degree one in $G$ and $e$ is its unique incident edge, then there exists a maximum matching of $G$ that includes $e$. Karp and Sipser exploited this via a simple greedy algorithm:

**Algorithm 1** Karp-Sipser Algorithm

```
1:  procedure KSGreedy(G)
2:      M ← ∅, Γ ← G;
3:      while Γ ≠ ∅ do
4:          if Γ has vertices of degree one then
5:              Select a vertex ξ uniformly at random from the set of vertices of degree one
6:              Let e = (ξ, η) be the edge incident to ξ
7:          else
8:              Select an edge e = (v, u) uniformly at random
9:          end if
10:         M ← M ∪ {e}
11:         Γ ← Γ \ {ξ, η}
12:     end while
13:     return M
14: end procedure
```

Phase 1 of the Karp-Sipser Algorithm ends and Phase 2 begins when the graph remaining has minimum degree at least two. So if $\Gamma_1$ denotes the graph $\Gamma$ remaining at the end of Phase 1 and $\tau_1$ is the number of iterations involved in Phase 1 then

$$\mu(G) = \tau_1 + \mu(\Gamma_1). \tag{1}$$

Our approach to estimating $\mu(G)$ is to (i) obtain an asymptotic expression for $\tau_1$ that holds **whp** and then (ii) show that **whp** $\Gamma_1$ has a (near) perfect matching and then apply (1).

We summarise the known results pertaining to the Karp-Sipser algorithm. For proofs of Theorem 3 and parts (a), (b) of Theorem 4 see Luby, Mitzenmacher, Shokrollahi and Spielman [24] or Dembo and Montanari [9] or even an earlier version of this paper [17]: Let $z_1$ satisfy

$$z_1 = \frac{e^{z_1} - 1}{d - 1} \tag{2}$$

and let

$$\alpha^* = \frac{z_1}{d(1 - e^{-z_1})^{d-1}}. \tag{3}$$

**Theorem 3** *If $\alpha \le \alpha^*$ then* **whp** $\mu(G) = \tau_1 = n$.

Thus **whp** Phase 1 of the Karp-Sipser Algorithm finds a (near) maximum matching if $\alpha \le \alpha^*$. In particular, if $d = 3$ then $z_1 \approx 1.251$ and $\alpha_1 \approx .818$ and thus $m \approx 1.222n$ is enough for a matching of $L$ into $R$.

Now consider larger $\alpha$. Let $z^*$ be the largest non-negative solution to

$$\left(\frac{z}{\alpha d}\right)^{\frac{1}{d-1}} + e^{-z} - 1 = 0.$$

**Theorem 4** *If $\alpha > \alpha^*$ then* **whp**

**(a)** $z^* > 0$.

**(b)** $\tau_1 = n\left(1 - \left(\frac{z^*}{\alpha d}\right)^{\frac{d}{d-1}}\right) + o(n)$.

**(c)** *If $d \ge 3$ then*

$$\mu(\Gamma_1) = \min\{|L_1|, |R_1|\} = \min\left\{n - \tau_1, (1 - (1 + z^*)e^{-z^*})m + o(m)\right\}. \tag{4}$$

*Here $L_1 \subseteq L, R_1 \subseteq R$ are the two sides of the bipartition of $\Gamma_1$, after deleting any isolated vertices from the $R$-side.*

Only part (c) needs to be proved here. As already mentioned, parts (a), (b) have already been proven in [9], [24]. It is not easy to extract the precise statements from these papers. An earlier version of this paper was placed on the Arxiv [17]. The interested reader can find a complete proof of (a) and (b) in the first six sections. Alterantively, one can consult Molloy [27] where the precise result is given in terms of hypergraph cores.

The remainder of the paper constitutes a proof of part (c).

# 3 Proof of Theorem 1 (and Theorem 4(c))

Let us summarize what we have to prove. We have a bipartite graph $\Gamma_1$ with partition $L_1, R_1$ and $|L_1| = n_1 = \alpha_1 m_1, |R_1| = m_1$. Each vertex $a \in L_1$ has degree $d_{L_1}(a) = d$ and each vertex $b \in R_1$ has degree $d_{R_1}(b)$ at least 2. The graph $\Gamma_1$ is chosen uniformly from the set of bipartite graphs with these degree properties.

At this point it is convenient to drop the suffix 1. So from now on, $m, n, \alpha, \Gamma$ etc. refer to the graph left at the end of Phase 1.

The degrees of $\Gamma$ satisfy $d_L(a) = d$ for $a \in L$. The degrees of vertices in $R$ are distributed as the box occupancies $X_1, X_2, \ldots, X_m$ in the following experiment. We throw $dn$ balls randomly into $m$ boxes and condition that each box gets at least two balls. In these circumstance the $X_j$'s are independent truncated Poisson, subject to the condition that $X_1 + X_2 + \cdots + X_m = dn$, see Lemma 4 of [2]. Thus for any $S = \{b_1, b_2, \ldots, b_s\} \subseteq R$ and any set of positive integers $k_i \geq 2, i \in S$ we have

$$\mathsf{P}(d_R(b_i) = k_i, i \in S) \leq O(n^{1/2}) \prod_{i \in S} \frac{z^{k_i}}{k_i! f(z)} \tag{5}$$

for $k \geq 2$ where $z$ satisfies

$$\frac{z(e^z - 1)}{f(z)} = \frac{nd}{m} \tag{6}$$

and

$$f(z) = e^z - 1 - z.$$

The $O(n^{1/2})$ term accounts for the conditioning $\sum_{b \in R} d_R(b) = dn$.

We remark that

$$z > 2.$$

It follows from (5) that

$$\mathsf{P}(\exists b \in R : d_R(b) \geq L = \log n) \leq O(n^{3/2}) \frac{z^L}{L! f(z)} = O(n^{-K}) \tag{7}$$

for any positive constant $K$.

### 3.1 Outline of the proof of Theorem 4(c)

At the top level this involves showing that **whp** Hall's condition holds. We will estimate the probability of the existence of sets $A, B$ where $|A| = k$ and $|B| \leq k - 1$ such that $N_\Gamma(A) \subseteq B$. Here $N_\Gamma(S)$ is the set of neighbours of $S$ in $\Gamma$. We call such a pair of sets a *witness* to the non-existence of a matching that covers the smaller of $L, R$. There are two possibilities to consider: (i) *$L$-witnesses*: $A \subseteq L$ and $B \subseteq R$ or (ii) *$R$-witnesses*: $A \subseteq R$ and $B \subseteq L$. We have to deal with both cases in order to deal with the asymmetry between $L$ and $R$. We say this because in the classic case of a binomial random bipartite graph considered by Erdős and Rényi [14] we can get away with only dealing with Case (i). We observe that if there exists a pair $A, B$ then there exists a minimal pair and in this case each $b \in B$ has at least two neighbours in $A$. If $v$ has a unique neighbour $w$ in $A$ then $A \setminus \{w\}, B \setminus \{v\}$ is also a witness.

We first consider $L$-witnesses $A$ where $|A| \leq k_0$ where

$$k_0 = \max\{m, n\}/2.$$

We can restrict out attention to $k \leq k_0$ because if $n \leq m$ and we have an $L$-witness $A \subseteq L$, $|A| = k > k_0$ then $B = R \setminus N_\Gamma(A)$ will be an $R$-witness and $|B| \leq k_0$. The same idea holds for $R$-witnesses $B \subseteq R$.

We begin by proving some lemmas involving the properties of functions that occur throughout the proof. This is the content of Section 3.2. We start the verification of Hall's condition in Section 3.3. In this section we assume that $m$ and $n$ are close, in particular $|m-n| = o(n^{7/8})$. We begin the analysis with $L$-witnesses in Section 3.3.1. When $k = |A|$ is small i.e. at most $n/\log^4 n$ (Case 1.0) we can use a simple bipartite configuration model to prove the non-existence of a witness. This is useful, because it then enables us to "ignore" factors of the order $e^{O(|m-n|)}$ in the main body of the proof.

We then consider larger $k$. This involves a complicated expression (15) for the expected number of $L$-witnesses. The proof continues by making various simplifications to this expression that are valid within different ranges and for different values of $d$. This makes the calculations rather lengthy.

Having dealt with $L$-witnesses we turn to $R$-witnesses in Section 3.3.2. We first produce a complex expression (43). When $k$ is small, now less than $n^{9/10}$ we can make some simplifications. This again allows us to "ignore" factors of the order $e^{O(|m-n|)}$ in the main body of the proof. We are again faced with estimating a rather complex expression which we do by breaking into various sub-cases.

Once we have dealt with $|m-n| = o(n^{7/8})$ we tackle arbitrary $m$ and $n$. We do this by relating the probability of events for the cases $m+s, n$ and $m, n+s$ with the probability of events for the case $m, n$, see (98) and (99). In this way we can reduce the case of arbitrary $m, n$ to the case of $|m-n| = o(n^{7/8})$.

### 3.2 Useful Lemmas

Define the function $\zeta(x), x > 0$ to be the unique solution to

$$\frac{u(e^u-1)}{f(u)} = x. \tag{8}$$

Let $g$ be defined by

$$g(x) = (e^{\zeta(x)}-1)^x f(\zeta(x))^{1-x}. \tag{9}$$

Observe that on replacing $u$ by $\zeta(x)$ in (8) we see that

$$\frac{f(\zeta(x))}{\zeta(x)^x} = \frac{g(x)}{x^x}. \tag{10}$$

**Lemma 5** *The function $g(x)$ is log-concave as a function of $x$.*

**Proof:** We will write $\zeta$ for $\zeta(x)$ and $f$ for $f(\zeta)$ throughout this proof. Now $\frac{\zeta(e^\zeta-1)}{f} = x$ from which we get

$$\frac{d\zeta}{dx} = \frac{f^2}{(e^\zeta-1)^2 - \zeta^2 e^\zeta} \tag{11}$$

and note that $\frac{d\zeta}{dx} > 0$ for $\zeta > 0$, see (13) below. Taking the derivative of $\log(g(x))$ we get

$$\begin{aligned}\frac{d}{dx}\log(g(x)) &= \frac{d}{dx}\left(x\log(e^\zeta-1) + (1-x)\log(e^\zeta-\zeta-1)\right)\\ &= \log\left(\frac{e^\zeta-1}{f}\right) + \frac{d\zeta}{dx}\left(x\frac{e^\zeta}{e^\zeta-1} + (1-x)\frac{e^\zeta-1}{f}\right).\end{aligned}$$

Now $x = \frac{\zeta(e^\zeta - 1)}{f}$ so

$$\begin{aligned} x\frac{e^\zeta}{e^\zeta - 1} + (1-x)\frac{e^\zeta - 1}{f} &= \frac{\zeta e^\zeta}{f} + \frac{f - \zeta(e^\zeta - 1)}{f}\frac{e^\zeta - 1}{f} \\ &= \frac{\zeta e^\zeta(e^\zeta - \zeta - 1) + (e^\zeta - \zeta - 1 - \zeta e^\zeta + \zeta)(e^\zeta - 1)}{f^2} \\ &= \frac{(e^\zeta - 1)^2 - \zeta^2 e^\zeta}{f^2} \\ &= \frac{dx}{d\zeta}. \end{aligned}$$

Thus we have

$$\frac{d}{dx}\log(g(x)) = \log\left(\frac{e^\zeta - 1}{f}\right) + 1. \tag{12}$$

Taking the second derivative we get

$$\begin{aligned} \frac{d^2}{dx^2}\log(g(x)) &= \frac{d}{dx}\left(\log\left(\frac{e^\zeta - 1}{f}\right) + 1\right) \\ &= \frac{f}{e^\zeta - 1}\frac{e^\zeta(e^\zeta - \zeta - 1) - (e^\zeta - 1)^2}{f^2}\frac{d\zeta}{dx} \\ &= \frac{1}{(e^\zeta - 1)f}\frac{d\zeta}{dx}\left(-(\zeta - 1)e^\zeta - 1\right). \end{aligned}$$

Since $-(\zeta - 1)e^\zeta - 1$ is strictly negative for $\zeta > 0$ we get that $g(x)$ is log-concave □

**Lemma 6** *$\zeta(x)$ is concave as a function of $x$.*

**Proof:** We begin with (11). We note that the denominator

$$(e^\zeta - 1)^2 - \zeta^2 e^\zeta = \sum_{k=4}^{\infty}(2^k - 2 - k(k-1))\frac{\zeta^k}{k!} \geq 0. \tag{13}$$

Then we have

$$\frac{d^2\zeta}{dx^2} = \frac{2(1+\zeta) + e^\zeta(-6 - e^{2\zeta}(2 + \zeta(\zeta - 4)) + \zeta^2(5 + \zeta(\zeta + 2)) + e^\zeta(6 - 2\zeta(2\zeta + 3)))}{((e^\zeta - 1)^2 - \zeta^2 e^\zeta)^2}\frac{d\zeta}{dx}.$$

Now let

$$\phi(u) = \sum_{n=0}^{\infty}\phi_n u^n = 2(1+u) + \psi(u)$$

where

$$\psi(u) = \sum_{n=0}^{\infty}\psi_n u^n = e^u(-6 - e^{2u}(2 + u(u-4)) + u^2(5 + u(u+2)) + e^u(6 - 2u(2u+3))).$$

We check that $\psi_0 = -2$ and $\psi_1 = 0$ which implies that $\phi_0 = \phi_1 = 0$. One can finish the argument by checking that

$$\psi_n = -\frac{3^{n-2}(n^2 - 13n + 18) + 2^n(n^2 + 2n - 6) - (n^4 - 4n^3 + 10n^2 - 7n - 6)}{n!} \leq 0$$

for $n \geq 2$. This is simply a matter of checking for small values until the $3^n$ term dominates. $\square$
Next let

$$H(u) = \log f(u) - u - 2\log u = \log\left(\frac{e^u - u - 1}{u^2 e^u}\right)$$

**Lemma 7** *$H(u)$ is convex as a function of $u$.*

**Proof:**

$$\begin{aligned}
\frac{d^2}{du^2}H(u) &= \frac{d}{du}\left(\frac{e^u - 1}{f(u)} - 1 - \frac{2}{u}\right) \\
&= \frac{e^u(e^u - 1 - u) - (e^u - 1)^2}{f(u)^2} + \frac{2}{u^2} \\
&= \frac{e^u - 1 - ue^u}{f(u)^2} + \frac{2}{u^2} \\
&= \frac{u^2(e^u - 1 - ue^u) + 2(e^u - 1 - u)^2}{u^2 f(u)^2} \\
&= \frac{2e^{2u} + u^2e^u + u^2 + 4u + 2 - u^3e^u - 4ue^u - 4e^u}{u^2 f(u)^2}
\end{aligned}$$

Let

$$\phi(u) = 2e^{2u} + u^2e^u + u^2 + 4u + 2 - u^3e^u - 4ue^u - 4e^u = \sum_{n=0}^{\infty} \phi_n u^n.$$

Direct computation gives $\phi_0 = \phi_1 = \phi_2 = 0$ and for $n \geq 3$

$$\phi_n = \frac{1}{n!}(2^{n+1} + n(n-1) - n(n-1)(n-2) - 4n - 4).$$

One can then check that $\phi_3 = \phi_4 = \phi_5 = 0 < \phi_n$ for $n \geq 6$. Thus $\frac{d^2}{du^2}H(u) \geq 0$ implying that $H(u)$ is convex. $\square$

### 3.3 The case $|n - m| = o(n^{7/8})$

We will first prove Theorem 1 under the assumption that $|n - m| = o(n^{7/8})$ and then in Sections 3.4 and 3.5 we will extend the result to arbitrary $m$. We deal first with the existence probability for a minimal $L$-witness and leave $R$-witnesses until Section 3.3.2. We then combine these results to finish the case $|n - m| = o(n^{7/8})$ in Section 3.3.3.

#### 3.3.1 Case 1: $L$-witnesses

For

$$k \leq k_0 \text{ and } \ell \leq k - 1$$

define

$$\pi_L(k, \ell, D) = Pr(\exists A, B : |A| = k, |B| = \ell, N_\Gamma(A) = B, d(B) = D \geq dk, d_A(b) \geq 2, \forall b \in B)$$

where $d(B) = \sum_{b \in B} d_A(b)$. This is the probability of the existence of a minimal $L$-witness $A$ of size of size $k$ that has a neighbour set $B$ of size $\ell$ of total degree $D$.

We observe that if we condition on the degrees $d_b, b \in R$ then we will be able to use a bipartite configuration model for the bipartite graph $\Gamma$. Let $\mathbf{d} = (d_1, d_2, \ldots, d_m)$ be a sequence of non-negative integers with $d_1 + d_2 + \cdots + d_m = M = nd$. Let $W_L, W_R$ be two disjoint copies of $[M]$ and let $W_{i,R} = [d_1 + \cdots + d_{i-1} + 1, d_1 + \cdots + d_i]$, $i \in [m]$, partition $W$ into sets of size $d_1, d_2, \ldots, d_m$. Let $\phi$ be a uniform random bijection between $W_L$ and $W_R$. Given $\phi$ we define the bipartite (multi-)graph $\Gamma_\phi$ as follows: If $\phi(x) = y$ then we add the edge $(\lfloor (x-1)/d \rfloor + 1, i)$ where $y \in W_{i,R}$. This bipartite graph has the same distribution as $\Gamma_1$ conditional on the degrees of the vertices in $R$.

Given this model, we can easily deal with small $k$.

**Case 1.0:** $2 \le k \le n/\log^4 n$.

We have

$$A_{14} = \sum_{\ell<k=2}^{n/\log^4 n} \sum_{D=dk}^{k\log n} \pi_L(k,\ell,D) \le \sum_{D=dk}^{k\log n} \binom{n}{k}\binom{m}{\ell}\left(\frac{D}{dn}\right)^{dk}$$
$$\le \sum_{\ell<k=2}^{n/\log^4 n} \sum_{D=dk}^{k\log n} \left(\frac{ne}{k}\right)^k \left(\frac{me}{\ell}\right)^\ell \left(\frac{k\log n}{n}\right)^{dk} \le \sum_{\ell<k=2}^{n/\log^4 n} \sum_{D=dk}^{k\log n} \left(\frac{e^{2+o(1)}k^{d-2}\log^d n}{n^{d-2}}\right)^k = o(1). \quad (14)$$

The notation $\sum_{\ell<k=r}^{s}$ is short for $\sum_{k=r}^{s}\sum_{\ell=1}^{k-1}$. We use the notation $A_{14}$ so that the reader can easily refer back to the equation giving its definition. $A_{14}$ is the first of several sums that together show the unlikelihood of a witness. We will display them as they become available and use them in Sections 3.3.3, 3.4 and 3.5.

We can restrict our attention to $D \le k\log n$ because of (7).

**Case 1.1:** $n/\log^4 n \le k \le k_0$.

We must work much harder when $k$ is large. We now estimate, with $z$ as defined in (6),

$$\pi_L(k,\ell,D) \le O(n^{1/2})\binom{n}{k}\binom{m}{\ell} \sum_{\substack{2\le x_b\le d_b,\forall b\in[\ell]\\ \sum_b x_b = kd\\ \sum_{b\in[\ell]} d_b = D,\ \sum_{b\notin[\ell]} d_b = dn-D}} \prod_{b=1}^{m} \frac{z^{d_b}}{d_b! f(z)} \prod_{b=1}^{\ell}\binom{d_b}{x_b}\,(kd)! \prod_{i=0}^{dk-1}\frac{1}{dn-i}. \quad (15)$$

**Explanation of** (15)**:** Choose sets $A, B$ in $\binom{n}{k}\binom{m}{\ell}$ ways. Choose degrees $d_b, b \in R$ with probability $O(n^{1/2})\prod_{b=1}^{m}\frac{z^{d_b}}{d_b! f(z)}$ such that $\sum_{b\in B} d_b = D$, $\sum_{b\notin B} d_b = dn - D$ for some $D \ge 2\ell$. Choose the degrees $x_a, a \in A$ in the sub-graph induced by $A \cup B$. Having fixed the degree sequence, we swap to the configuration model

Choose the configuration points associated with the $x_a, a \in A$ in $\prod_{a\in A}\binom{d}{x_a}$ ways. Assign these $D$ choices of points associated with $A$ in $D!$ ways. Then multiply by the probability $(kd)!\prod_{i=0}^{kd-1}\frac{1}{dn-i}$ of a given pairing of points in $A$.

So, after writing $d_b = x_b + y_b$ for $b \in [\ell]$ we get,

$$\pi_L(k,\ell,D) = O(n^{1/2})\binom{n}{k}\binom{m}{\ell}\frac{(d(n-k))!}{(dn)!}\frac{(kd)!z^{dn}}{f(z)^m}\times$$

$$\left(\sum_{\substack{2\le x_b,\forall b\in[\ell]\\ \sum_b x_b=kd}}\prod_{b=1}^{\ell}\frac{1}{x_b!}\right)\left(\sum_{\substack{2\le d_b,\forall b\notin[\ell]\\ \sum_b d_b=dn-D}}\prod_{b=\ell+1}^{m}\frac{1}{d_b!}\right)\left(\sum_{\substack{0\le y_b,\forall b\in[\ell]\\ \sum_b y_b=D-kd}}\prod_{b=1}^{\ell}\frac{1}{y_b!}\right) \tag{16}$$

$$= O(n^{1/2})\binom{n}{k}\binom{m}{\ell}\frac{(d(n-k))!}{(dn)!}\frac{(kd)!z^{dn}}{f(z)^m}\times \left([u^{kd}](e^u-1-u)^{\ell}\right)\left([u^{dn-D}](e^u-1-u)^{m-\ell}\right)\left([u^{D-kd}]e^{u\ell}\right) \tag{17}$$

$$\le O(n^{1/2})e^{O(|m-n|)}\binom{n}{k}\binom{m}{k-1}\frac{(d(n-k))!}{(dn)!}\frac{(kd)!z^{dn}}{f(z)^m}\frac{f(z)^{\ell}}{z^{kd}}\frac{f(\zeta_1)^{m-\ell}}{\zeta_1^{dn-D}}\frac{\ell^{D-dk}}{(D-kd)!}.$$

Here we use the general notation that $[x^r]\phi(x)$ is the coefficient of $x^r$ in the series expansion of $\phi$ around zero. One sees that the expression in (16) can be written as in (17) simply by expanding the various $\phi(u)$ as power series.

If $A(x)=\sum_{n=0}^{\infty}a_nx^n$ where $a_n\ge 0$ for $n\ge 0$ we have $a_n\le A(\zeta)/\zeta^n$ for any positive $\zeta$ and $A(\zeta)/\zeta^n$ is minimised at $\zeta$ satisfying $\zeta A'(\zeta)/A(\zeta)=n$.

Here we take

$$\zeta_1=\zeta(y) \text{ where } y=\frac{dn-D}{n-k}\ge 2-O\left(\frac{|m-n|}{n}\right)$$

due to our minimum degree assumption for $R$. Indeed, our minimum degree assumption implies that

$$dn-D\ge 2(m-\ell)\ge 2(m-k)=2(n-k)+2(m-n). \tag{18}$$

We get an upper bound for any choice of $\zeta_1$, although if $y_0=(dn-D)/(m-\ell)$ then $\zeta_1(y_0)$ (see (8)) gives the smallest upper bound. It is convenient to use $\zeta_1(y)$ instead of this. Later in the proof we choose other values for $\zeta_1$ in this bound, but we will always choose $1<\zeta_1<2<z$.

The term $e^{O(|m-n|)}$ accounts for replacing $\binom{m}{\ell}$ by $\binom{m}{k-1}$ for $k$ exceeding $m/2$. So,

$$\pi_L(k,\ell,D)\le O(n^{1/2}e^{O(|m-n|)})\binom{n}{k}\binom{m}{k-1}\frac{(d(n-k))!}{(dn)!}\frac{(kd)!z^{dn}}{f(z)^m}\frac{f(z)^{\ell}}{z^{kd}}\frac{f(\zeta_1)^{m-\ell}}{\zeta_1^{dn-D}}\frac{(k-1)^{D-dk}}{(D-kd)!}. \tag{19}$$

Observe next that

$$\frac{dn-D}{n-k}-\frac{dn}{m}=\frac{dn(m-n)+(dk-D)n+D(n-m)}{m(n-k)}\le O\left(\frac{|m-n|}{n}\right).$$

Hence

$$f(\zeta_1)\le f(z)+O\left(\frac{|m-n|}{n}\right) \text{ and therefore } f(z)^{\ell}f(\zeta_1)^{m-\ell}\le e^{O(|n-m|)}f(z)^kf(\zeta_1)^{m-k}. \tag{20}$$

Continuing, we find that

$$\pi_L(k,\ell,D)\le O\left(\frac{e^{O(|m-n|)}}{m^{1/2}}\right)\frac{\binom{n}{k}\binom{m}{k}}{\binom{dn}{dk}}\left(\frac{z^d}{f(z)^{\frac{m-k}{n-k}}}\frac{f(\zeta_1)^{\frac{m-k}{n-k}}}{\zeta_1^{\frac{dn-D}{n-k}}}\right)^{n-k}\left(\frac{ek}{D-dk}\right)^{D-dk}. \tag{21}$$

Putting $k = an$ and $m = \beta n$ and $h(u) = u^u(1-u)^{1-u}$ and $x = d - y = \frac{D-dk}{n-k}$ where $0 \le x \le d - 2 + O(|n-m|/n$ we obtain, after substituting $\binom{n}{k} = O\left(\frac{1}{k^{1/2}h(a)^n}\right)$, $\binom{m}{k} = O\left(\frac{1}{k^{1/2}h(a/\beta)^n}\right)$ and $\binom{dn}{dk} = O\left(\frac{1}{k^{1/2}h(a)^{dn}}\right)$, (see (18)),

$$\pi_L(k,\ell,D) \le O\left(\frac{e^{O(|m-n|)}}{n^{1/2}}\right)\left(\frac{h(a)^{d-1}}{h(a/\beta)^\beta}\right)^n\left(\frac{z^d}{f(z)^{\frac{\beta-a}{1-a}}}\frac{f(\zeta_1)^{\frac{\beta-a}{1-a}}}{\zeta_1^{d-x}}\left(\frac{e\frac{a}{1-a}}{x}\right)^x\right)^{n-k}. \tag{22}$$

Because $\beta = 1 + o(n^{-1/8})$, we see that

$$\left(\frac{h(a)}{h(a/\beta)^\beta}\right)^n\left(\frac{f(\zeta_1)^{\frac{\beta-1}{1-a}}}{f(z)^{\frac{\beta-1}{1-a}}}\right)^{n-k} \tag{23}$$

$$= \left(\beta^a\left(1+\frac{a(1-\beta)}{\beta-a}\right)^{1-a}\left(\frac{1}{1-a/\beta}\right)^{\beta-1}\right)^n\left(\frac{f(\zeta_1)}{f(z)}\right)^{(\beta-1)n} \tag{24}$$

$$= e^{o(n^{7/8})}, \tag{25}$$

after using (20).

Thus (22) becomes

$$\pi_L(k,\ell,D) = O\left(\frac{1}{n^{1/2}}\right)e^{o(n^{7/8})}h(a)^{(d-2)n}\left(\frac{z^d}{f(z)}\frac{f(\zeta_1)}{\zeta_1^{d-x}}\left(\frac{e\frac{a}{1-a}}{x}\right)^x\right)^{n-k}. \tag{26}$$

**Case 1.1.1:** $d \ge 5$.

Observe (see (10)) that

$$\frac{z^d}{f(z)}\frac{f(\zeta_1)}{\zeta_1^{d-x}} = \frac{d^d}{g(d)}\frac{g(d-x)}{(d-x)^{d-x}}e^{o(n^{7/8})}$$

where $g(x)$ is as defined in (9). The term $e^{o(n^{7/8})}$ is derived as follows: In (10) $z = \zeta(dn/m)$ and so $z^{dn/m}/f(z) = (dn/m)^{dn/m}/g(dn/m)$ and $e^{o(n^{7/8})}$ is the correction for replacing $z^d/f(z)$ by $d^d/g(d)$.

It follows from (12) that

$$-\log\left(\frac{g(d-x)}{g(d)}\right) = \int_{d-x}^d \frac{d}{dt}\log(g(t))dt \ge \int_{d-x}^d 1dt. \tag{27}$$

Plugging this into the last parenthesis of (26) gives

$$\pi_L(k,\ell,D) = O\left(\frac{1}{n^{1/2}}\right)e^{o(n^{7/8})}\left(h(a)^{d-2}\left(\frac{d^d}{(d-x)^{d-x}}\left(\frac{\frac{a}{1-a}}{x}\right)^x\right)^{1-a}\right)^n. \tag{28}$$

We will use this to prove that

$$A_{29} = \sum_{\ell<k=\varepsilon_L n}^{n(1-2/d)}\sum_{D=dk}^{dk+n^{1/10}}\pi_L(k,\ell,D) \le \sum_{\ell<k=\varepsilon_L n}^{n(1-2/d)}\sum_{D=dk}^{dk+n^{1/10}}O\left(\frac{1}{n^{1/2}}\right)h(a)^{(d-2)n}e^{o(n)} = o(1). \tag{29}$$

where $\varepsilon_L$ is some small constant defined in (33) below.

The bound for $A_{29}$ comes from (28), using the fact that $h(a)$ is bounded away from 1 and $x = o(1)$ in this summation.

The main term $h(a)^{d-2}\left(d^d\frac{1}{(d-x)^{d-x}}\left(\frac{\frac{a}{1-a}}{x}\right)^x\right)^{1-a}$ in (28) is maximized when $x = ad$, provided $ad \le d-2$ or $k \le n\left(1-\frac{2}{d}\right)$. This in turn gives

$$\begin{aligned}
&\pi_L(k,\ell,D)\\
&= O\left(\frac{1}{n^{1/2}}\right)e^{o(n^{7/8})}\left((1+o(n^{-1/8}))h(a)^{d-2}\left((1+o(n^{-1/8}))d^d\frac{1}{(d-ad)^{d-ad}}\frac{1}{((1-a)d)^{ad}}\right)^{1-a}\right)^n\\
&= O\left(\frac{1}{n^{1/2}}\right)e^{o(n^{7/8})}\left((1+o(n^{-1/8}))h(a)^{d-2}\left(\frac{d^d}{d^{d-ad}d^{ad}}(1-a)^{-d}\right)^{1-a}\right)^n\\
&\le O\left(\frac{1}{n^{1/2}}\right)e^{o(n^{7/8})}\left(a^{a(d-2)}(1-a)^{-2(1-a)}\right)^n. \qquad (30)
\end{aligned}$$

The function $\rho_d(a) = a^{a(d-2)}(1-a)^{-2(1-a)}$ is at most 1 and is log-convex in $a$ on $[0, 1-\frac{2}{d}]$. Indeed, if $L_1(a) = \log\rho_d(a)$ then

$$\frac{dL_1}{da} = d + (d-2)\log a + 2\log(1-a). \qquad (31)$$

$$\frac{d^2L_1}{da^2} = \frac{d-2-da}{a(1-a)}. \qquad (32)$$

We have $L_1(0) = 0$ and $L_1'(0) = -\infty$. It follows that for every $K > 0$ there exists a constant $\varepsilon_L(K,d) > 0$ such that

$$\rho_d(a) \le e^{-Ka} \qquad for\ a \le \varepsilon_L(K). \qquad (33)$$

We let $\varepsilon_L = \varepsilon_L(1,d)$. This completes the proof of (29).

In truth we should put

$$\rho_d(a) \le \max\left\{e^{-Ka}, \psi(d)\right\}$$

where

$$\psi(d) = \left(1-\frac{2}{d}\right)^{(d-2)^2/d}\left(\frac{2}{d}\right)^{-4/d}.$$

For small $a < \varepsilon_L(K,d)$, $e^{-Ka} > \psi(d)$ and so it suffices to use (33). Thus

$$A_{34} = \sum_{\ell<k=n/\log^4 n}^{\varepsilon_L n}\sum_{D=dk}^{k\log n}\pi_L(k,\ell,D) = \sum_{\ell<k=n/\log^2 n}^{\varepsilon_L n}\sum_{D=dk}^{k\log n}O\left(\frac{1}{n^{1/2}}\right)e^{-Kk+o(n^{7/8})} = o(1). \qquad (34)$$

The bound for $A_{34}$ comes from (30) and (33).

Now $\psi(d)$ decreases in $d$ and is $< .9$ for $d \ge 5$. So if $d \ge 5$ then for some constant $0 < \xi < 1$ we have

$$A_{35} = \sum_{\ell<k=\varepsilon_L n}^{k_0}\sum_{D=dk+n^{1/10}}^{k\log n}\pi_L(k,\ell,D) = \sum_{\ell<k=\varepsilon_L n}^{k_0}\sum_{D=dk+n^{1/10}}^{k\log n}O\left(\frac{1}{n^{1/2}}\right)e^{o(n^{7/8})}\xi^n = o(1). \qquad (35)$$

The bound for $A_{35}$ comes from (30) and using the fact that $\rho_d(a) \le e^{-a}$.

We have now completed the analysis for $d \geq 5$ and witnesses $A \subseteq L$.

**Case 1.1.2:** $d \in \{3, 4\}$.

Now consider the cases $d = 3, 4$. Putting $\beta_3 = .15$, $\beta_4 = .49$ we note that $\rho_d(\beta_d) \leq .995$ for $d = 3, 4$ and so arguing as above we have

$$A_{36} = \sum_{\ell<k=\varepsilon_L n}^{\beta_d n} \sum_{D=dk+n^{1/10}}^{k\log n} \pi_L(k,\ell,D) = \sum_{\ell<k=\varepsilon_L n}^{\beta_d n} \sum_{D=dk+n^{1/10}}^{\log n} O\left(\frac{\log n}{n^{1/2}}\right) e^{o(n^{7/8})}\xi^n = o(1). \tag{36}$$

Because we can choose any value for $\zeta_1$ in the bound (26) we can simplify matters by choosing $\zeta_1 = \eta > 1$ independent of $x$ to get

$$\pi_L(k,D) = O\left(\frac{1}{n^{1/2}}\right) e^{o(n^{7/8})} h(a)^{(d-2)n} \left(\frac{z^d}{f(z)}\frac{f(\eta)}{\eta^d}\left(\frac{e\eta a}{x(1-a)}\right)^x\right)^{n-k}. \tag{37}$$

Now

$$\left(\frac{\eta e a}{(1-a)x}\right)^x \leq \exp\left\{\frac{\eta a}{1-a}\right\} \tag{38}$$

and so

$$\pi_L(k,D) \leq O\left(\frac{k}{n^{1/2}}\right)\left(h(a)^{d-2}e^{\eta a}e^{o(n^{-1/8})}\left(\frac{z^d}{f(z)}\frac{f(\eta)}{\eta^d}\right)^{1-a}\right)^n. \tag{39}$$

Now the function $L_2(a) = h(a)^{d-2}e^{\eta a}\left(\frac{z^d}{f(z)}\frac{f(\eta)}{\eta^d}\right)^{1-a}$ is log-convex in $a$. Our initial choice of $\eta$ will be 1.5 and we note that with this choice, when $d = 4$, $L_2(.49), L_2(.51) < .9$ and so

$$A_{40} = \sum_{\ell<k=\beta_4 n}^{k_0} \sum_{D=4k}^{k\log n} \pi_L(k,\ell,D) \leq \sum_{\ell<k=\beta_4 n}^{k_0} \sum_{D=4k}^{k\log n} O\left(\frac{\log n}{n^{1/2}}\right) e^{o(n^{7/8})}(.9)^n = o(1). \tag{40}$$

When $d = 3$, with the same choice for $\eta$, we have $L_2(.15), L_2(2/5) < .98$ and so

$$A_{41} = \sum_{\ell<k=.15n}^{2n/5} \sum_{D=3k+n^{1/10}}^{k\log n} \pi_L(k,\ell,D) \leq \sum_{\ell<k=.15n}^{2n/5} \sum_{D=3k+n^{1/10}}^{k\log n} O\left(\frac{\log n}{n^{1/2}}\right) e^{o(n^{7/8})}(.98)^n = o(1). \tag{41}$$

We repeat this idea once more. Putting $\eta = 1.1$ we get $L_2(2/5), L_2(.51) < .98$ from which we deduce that

$$A_{42} = \sum_{\ell<k=2n/5}^{k_0} \sum_{D=3k+n^{1/10}}^{k\log n} \pi_L(k,\ell,D) \leq \sum_{\ell<k=2n/5}^{k_0} \sum_{D=3k+n^{1/10}}^{k\log n} O\left(\frac{\log n}{n^{1/2}}\right) e^{o(n^{7/8})}(.98)^n = o(1). \tag{42}$$

### 3.3.2 Case 2: $R$-witnesses

Now let us estimate the probability of a violation of Hall's condition with $A \subseteq R$. We once again begin with arbitrary $m$.

For

$$k \leq k_0 = \max\{m, n\}/2 \text{ and } \ell \leq k-1$$

define

$$\pi_R(k,\ell,D) =$$
$$\mathsf{P}(\exists A\subseteq R, B\subseteq L:\ |A|=k, |B|=\ell, N_\Gamma(A)\subseteq B, d_A(a)\geq 2, \forall a\in A, d_R(A)=D) \leq$$
$$O(n^{1/2})\binom{m}{k}\binom{n}{\ell} \sum_{\substack{2\leq d_a,\forall a\in[m]\\ 2\leq x_b\leq d,\forall b\in[\ell]\\ \sum_{a\in[k]} d_a=\sum_{b\in[\ell]} x_b=D\\ \sum_{a\notin[k]} d_a=dn-D}} \prod_{a=1}^{m}\frac{z^{d_a}}{d_a!f(z)}\prod_{b=1}^{\ell}\binom{d}{x_b}\, D!\prod_{i=0}^{D-1}\frac{1}{dn-i}. \tag{43}$$

**Explanation of** (43)**:** Choose sets $A, B$ in $\binom{m}{k}\binom{n}{\ell}$ ways. Choose degrees $d_a, a\in R$ with probability $O(n^{1/2})\prod_{a=1}^{n}\frac{z^{d_a}}{d_a!f(z)}$ such that $\sum_{a\in A} d_a = D$, $\sum_{a\notin A} d_a = dn-D$ for some $D\geq 2k$. Choose the degrees $x_b, b\in B$ in the sub-graph induced by $A\cup B$. Having fixed the degree sequence, swap to the configuration model [5]. Choose the configuration points associated with the $x_b, b\in B$ in $\prod_{b\in B}\binom{d}{x_b}$ ways. Then multiply by the probability $D!\prod_{i=0}^{D-1}\frac{1}{dn-i}$ of a given pairing of points in $A$.

So

$$\pi_R(k,\ell,D) =$$
$$O(n^{1/2})\binom{m}{k}\binom{n}{\ell}\frac{z^{dn}D!}{f(z)^m}\frac{(dn-D)!}{(dn)!}$$
$$\times\left(\sum_{\substack{2\leq d_a,\forall a\in[k]\\ \sum_a d_a=D}}\prod_{a=1}^{k}\frac{1}{d_a!}\right)\left(\sum_{\substack{2\leq d_a,\forall a\notin[k]\\ \sum_a d_a=dn-D}}\prod_{a=k+1}^{m}\frac{1}{d_a!}\right)\left(\sum_{\substack{2\leq x_b\leq d,\forall b\in[\ell]\\ \sum_b x_b=D}}\prod_{b=1}^{\ell}\binom{d}{x_b}\right) =$$
$$O(n^{1/2})\binom{m}{k}\binom{n}{\ell}\frac{z^{dn}}{f(z)^m}\frac{1}{\binom{dn}{D}}$$
$$\times\left([u^D](e^u-1-u)^k\right)\left([u^{dn-D}](e^u-1-u)^{m-k}\right)\left([u^D]((1+u)^d-(1+du))^\ell\right)\leq$$
$$O(n^{1/2})e^{2k|m-n|/n}\binom{m}{k}\binom{n}{k-1}\frac{z^{dn}}{f(z)^m}\frac{1}{\binom{dn}{D}}$$
$$\times\left([u^D](e^u-1-u)^k\right)\left([u^{dn-D}](e^u-1-u)^{m-k}\right)\left([u^D]((1+u)^d-(1+du))^k\right)\leq \tag{44}$$
$$O(n^{1/2})e^{2k|m-n|/n}\binom{m}{k}\binom{n}{k-1}\frac{z^{dn}}{f(z)^m}\frac{1}{\binom{dn}{D}}\frac{f(\zeta_1)^k}{\zeta_1^D}\frac{f(\zeta_2)^{m-k}}{\zeta_2^{dn-D}}\binom{dk}{D}. \tag{45}$$

Our choice of $\zeta_1, \zeta_2$ will differ according to circumstances.

**Case 2.0:** $k\leq n^{9/10}$.

In this case we first use a crude bound in place of (44), (45):

$$\pi_R(k,\ell,D=\theta k) \leq \binom{m}{k}\binom{n}{k-1}\left(\frac{k}{n}\right)^{\theta k} \tag{46}$$
$$\leq \frac{2k}{n}\left(\left(\frac{k}{n}\right)^{\theta-2}e^{2+o(n^{-1/8})}\right)^k.$$

To get (46) we choose sets $A \subseteq R, B \subseteq L$ and then use $(k/n)^D$ as an upper bound on the probability that $N_\Gamma(A) \subseteq B$.

Thus if

$$\theta_0 = 2 + \frac{100}{\log n}$$

then

$$B_{47} = \sum_{\ell<k=2}^{n^{9/10}} \sum_{D \geq \theta_0 k} \pi_R(k,\ell,D) = o(1). \tag{47}$$

**Case 2.0.1:** $d \geq 5$.

When $2 \leq \theta \leq \theta_0$ we will use (44). In this case we take $\zeta_1 = \varepsilon$ for small $\varepsilon$ which implies that $f(\zeta_1) = \varepsilon^2/2 + O(\varepsilon^3)$ and $\zeta_2 = z = \zeta(d) + o(1)$. With $\binom{dn}{D} = \left(\frac{den}{2k}\right)^{k+o(k)}$ this gives

$$\begin{aligned}
&\pi_R(k,\ell,D)\\
&\leq O\left(\frac{k}{n^{1/2}}\right)\left((1+O(\varepsilon))\frac{n^2e^2}{k^2}\left(\frac{2k}{den}\right)^2\frac{\zeta(d)^2}{2f(\zeta(d))}\right)^k([u^D]((1+u)^d-(1+du))^k)\\
&= O\left(\frac{k}{n^{1/2}}\right)\left((1+O(\varepsilon))\frac{2}{d^2}\frac{\zeta(d)^2}{f(\zeta(d))}\right)^k([u^D]((1+u)^d-(1+du))^k).
\end{aligned} \tag{48}$$

If we use the bound

$$([u^D]((1+u)^d-(1+du))^k) \leq \binom{dk}{D} \leq \left(\frac{de}{2}\right)^{(2+o(1))k}$$

then (48) becomes

$$\pi_R(k,\ell,D) \leq O\left(\frac{k}{n^{1/2}}\right)\left((1+O(\varepsilon))\frac{\zeta(d)^2e^2}{2f(\zeta(d))}\right)^k. \tag{49}$$

Another calculation shows that if $x \geq 4.5$ then $x^2e^2/2f(x) \leq .89$ and then we have

$$d \geq 5 \text{ implies } \zeta(d) \geq 4.5 \text{ which implies } \pi_R(k,\ell,D) \leq O\left(\frac{k}{n^{1/2}}\right)(.9)^k. \tag{50}$$

So we are only left with $d = 3$ or $4$ for the case of small $k$.

**Case 2.0.2:** $d = 4$

We use

$$\begin{aligned}
[u^D]((1+u)^4-1-4u)^k &= [u^{D-2k}](6+4u+u^2)^k\\
&= 6^k[u^{D-2k}]\left(1+\frac{4}{6}u+\frac{u^2}{6}\right)^k\\
&\leq 6^k[u^{D-2k}]\left(1+\frac{u}{2}\right)^{2k}\\
&= 6^k\frac{\binom{2k}{D-2k}}{2^{D-2k}}.
\end{aligned} \tag{51}$$

Equation (48) now becomes

$$\pi_R(k,\ell,D) \le O\left(\frac{k}{n^{1/2}}\right)\left((1+O(\varepsilon))\frac{12}{16}\frac{\zeta(4)^2}{f(\zeta(4))}\right)^k = O\left(\frac{k}{n^{1/2}2^k}\right) \tag{52}$$

since $3.5 \le \zeta(4) \le 3.6$ and $(3.6)^2/f(3.5) \le 1/2$.

**Case 2.0.3:** $d = 3$

We use

$$\begin{aligned}[u^D]((1+u)^3 - 1 - 3u)^k &= [u^{D-2k}](3+u)^k \\ &= 3^{3k-D}\binom{k}{D-2k}.\end{aligned} \tag{53}$$

In this case (48) becomes

$$\pi_R(k,\ell,D) \le O\left(\frac{k}{n^{1/2}}\right)\left((1+O(\varepsilon))\frac{6}{9}\frac{\zeta(3)^2}{f(\zeta(3))}\right)^k = O\left(\frac{k3^k}{n^{1/2}4^k}\right) \tag{54}$$

since $2.1 \le \zeta(3) \le 2.2$ and $(2.2)^2/f(2.1) < 1$.

It follows from (50), (52) and (53) that

$$B_{55} = \sum_{\ell<k=2}^{n^{9/10}} \sum_{2k\le D\le\theta_0 k} \pi_R(k,\ell,D) = o(1). \tag{55}$$

**Case 2.1:** $k \ge n^{9/10}$.

Going back to (44) we initially take $\zeta_1 = \zeta(D/k)$ and $\zeta_2 = \zeta\left(\frac{dn-D}{n-k}\right)$. It is convenient to use this definition of $\zeta_2$ in place of the more natural $\zeta\left(\frac{dn-D}{m-k}\right)$.

So

$$\begin{aligned}&\pi_R(k,\ell,D)\\ &= O(n^{1/2})e^{2k|m-n|/n}\binom{m}{k}\binom{n}{k}\frac{\binom{dk}{D}}{\binom{dn}{D}}\left(\frac{f(\zeta_1)}{f(z)}\right)^k\left(\frac{f(\zeta_2)}{f(z)}\right)^{m-k}\left(\frac{z}{\zeta_1}\right)^D\left(\frac{z}{\zeta_2}\right)^{dn-D} &(56)\\ &= O\left(\frac{1}{n^{1/2}}\right)e^{2a|m-n|}\left(\frac{h(\theta a/d)^d}{h(a)h(a/\beta)^\beta h(\theta/d)^{ad}}\left(\frac{f(\zeta_1)}{f(z)}\right)^a\left(\frac{f(\zeta_2)}{f(z)}\right)^{\beta-a}\left(\frac{z}{\zeta_1}\right)^{\theta a}\left(\frac{z}{\zeta_2}\right)^{d-\theta a}\right)^n &(57)\\ &= O\left(\frac{1}{n^{1/2}}\right)e^{2a|m-n|}\left(\frac{h(\theta a/d)^d}{h(a)h(a/\beta)^\beta h(\theta/d)^{ad}}\frac{z^d}{f(z)^\beta}\frac{f(\zeta_1)^a}{\zeta_1^{\theta a}}\frac{f(\zeta_2)^{\beta-a}}{\zeta_2^{d-\theta a}}\right)^n, &(58)\end{aligned}$$

where $a = k/n$, $m = \beta n$ and $D = \theta k \le dk$.

We argue as in (25) that

$$\frac{h(a)}{h(a/\beta)^\beta}\frac{f(\zeta_2)^{\beta-1}}{f(z)^{\beta-1}} = e^{o(n^{-1/8})}.$$

Thus, (58) becomes

$$\pi_R(k,\ell,D) \le O\left(\frac{1}{n^{1/2}}\right)\left(e^{o(n^{-1/8})}\frac{h(\theta a/d)^d}{h(a)^2 h(\theta/d)^{ad}}\frac{z^d}{f(z)}\frac{f(\zeta_1)^a}{\zeta_1^{\theta a}}\frac{f(\zeta_2)^{1-a}}{\zeta_2^{d-\theta a}}\right)^n. \tag{59}$$

It follows from Lemma 5 that we can upper bound

$$\begin{aligned}
\frac{z^d}{f(z)}\left(\frac{f(\zeta_1)}{\zeta_1^\theta}\right)^a\left(\frac{f(\zeta_2)}{\zeta_2^{\frac{d-a\theta}{1-a}}}\right)^{1-a} &= \frac{d^d}{g(d)}\frac{g(\theta)^a g\left(\frac{d-a\theta}{1-a}\right)^{1-a}}{\theta^{a\theta}\left(\frac{d-a\theta}{1-a}\right)^{d-a\theta}} \\
&\le \frac{g(a\theta+(1-a)\frac{d-a\theta}{1-a})}{g(d)}\frac{d^d}{\theta^{a\theta}\left(\frac{d-a\theta}{1-a}\right)^{d-a\theta}} \\
&= \frac{a^{a\theta}(1-a)^{d-a\theta}}{\left(\left(\frac{a\theta}{d}\right)^{\frac{a\theta}{d}}(1-\frac{a\theta}{d})^{1-\frac{a\theta}{d}}\right)^d} \\
&= \frac{a^{a\theta}(1-a)^{d-a\theta}}{h\left(\frac{a\theta}{d}\right)^d}.
\end{aligned}$$

Plugging this into (59) gives

$$\pi_R(k,\ell,D) \le O\left(\frac{1}{n^{1/2}}\right)\left(\frac{e^{o(n^{-1/8})}a^{a\theta}(1-a)^{d-a\theta}}{h(a)^2 h\left(\frac{\theta}{d}\right)^{ad}}\right)^n. \tag{60}$$

Now let $R_1(\theta) = \log\left(\frac{a^{a\theta}(1-a)^{d-a\theta}}{h(a)^2 h\left(\frac{\theta}{d}\right)^{ad}}\right)$. Then

$$\begin{aligned}
R_1'(\theta) &= a\log a - a\log(1-a) - a\log\theta + a\log(d-\theta), \\
R_1''(\theta) &= -\frac{ad}{\theta(d-\theta)} < 0.
\end{aligned}$$

Thus $R_1(\theta)$ is concave and is maximized when $\theta = ad$. Because $\theta \ge 2$ we can only use this for $a \ge 2/d$.

**Case 2.1.1:** $k \ge 2n/d$ and $d \ge 5$.

$$\begin{aligned}
\pi_R(k,\ell,D) &\le O\left(\frac{1}{n^{1/2}}\right)\left(\frac{e^{o(n^{-1/8})}a^{a^2d}(1-a)^{d-a^2d}}{h(a)^{2+ad}}\right)^n \\
&= O\left(\frac{1}{n^{1/2}}\right)\left(e^{o(n^{-1/8})}a^{a^2d-a(2+ad)}(1-a)^{d-a^2d-(1-a)(2+ad)}\right)^n \\
&= O\left(\frac{1}{n^{1/2}}\right)\left(e^{o(n^{-1/8})}a^{-2a}(1-a)^{(d-2)(1-a)}\right)^n \\
&= O\left(\frac{1}{n^{1/2}}\right)e^{o(n^{7/8})}\rho_d(1-a)^n
\end{aligned} \tag{61}$$

where the function $\rho_d$ is defined following (30).

We find that

$$\rho_d(1-2/d) = \left(\frac{d^4}{16}\left(1-\frac{2}{d}\right)^{(d-2)^2}\right)^{1/d} \le .9 \text{ for } d \ge 5. \tag{62}$$

Now $\rho_d(1-2/d) < 9/10$ and $\rho_d(.5) < .8$ for $d \geq 5$. So, with the aid of (33),

$$B_{63} = \sum_{\ell<k=2n/d}^{k_0} \sum_{D=2k}^{k\log n} \pi_R(k,\ell,D) \leq \sum_{\ell<k=2n/d}^{k_0} \sum_{D=2k}^{k\log n} O\left(\frac{1}{n^{1/2}}\right) e^{o(n^{7/8})}(.8)^n \qquad \text{for } d \geq 5. \tag{63}$$

We will treat $d=4$ under Case 2.2. In this case we will change the upper bound on the range from $n/2$ to $0.51n$.

**Case 2.2:** $n^{9/10} \leq k \leq 2n/d$.

**Case 2.2.1:** $d \geq 6$.

In this case the expression in (60) (ignoring error terms) is maximized at $\theta = 2$. Then

$$\begin{aligned}
\pi_R(k,D) &\leq O\left(\frac{1}{n^{1/2}}\right)\left(\frac{e^{o(n^{-1/8})}a^{2a}(1-a)^{d-2a}}{h(a)^2 h\left(\frac{2}{d}\right)^{ad}}\right)^n \\
&= O\left(\frac{1}{n^{1/2}}\right)\left(\frac{e^{o(n^{-1/8})}(1-a)^{d-2a-2(1-a)}}{h\left(\frac{2}{d}\right)^{ad}}\right)^n \\
&= O\left(\frac{1}{n^{1/2}}\right)\left(\frac{e^{o(n^{-1/8})}(1-a)^{d-2}}{h\left(\frac{2}{d}\right)^{ad}}\right)^n.
\end{aligned}$$

Let $R_2(a) = \log\left(\frac{(1-a)^{d-2}}{h\left(\frac{2}{d}\right)^{ad}}\right)$. Then

$$\begin{aligned}
R_2'(a) &= -\frac{d-2}{1-a} - d\log h(2/d) < 0 \qquad \textit{for } d \geq 6, \\
R_2''(a) &= -\frac{d-2}{(1-a)^2} < 0.
\end{aligned}$$

Thus $R_2(a)$ is strict concave and its maximum is taken at $a=0$ and $R_2(a) \leq R_2(0)a$ for all $a \in [0, \frac{2}{d}]$. Furthermore, $R_2(0) < -3/10$ for $d \geq 6$. It follows that if $d \geq 6$ then

$$B_{64} = \sum_{\ell<k=n^{9/10}}^{2n/d} \sum_{D=2k}^{dk} \pi_R(k,\ell,D) \leq \sum_{\ell<k=n^{9/10}}^{2n/d} \sum_{D=2k}^{dk} O\left(\frac{1}{n^{1/2}}\right) e^{-(3k/10-o(n^{7/8}))} = o(1). \tag{64}$$

For $d = 3,4,5$ we use a better bound on $[u^D]((1+u)^d - 1 - du)^k$ in (44).

**Case 2.2.2:** $d=5$.

We use

$$\begin{aligned}
[u^D]((1+u)^5 - 1 - 5u)^k &= [u^D](10u^2 + 10u^2 + 5u^4 + u^5)^k) \\
&= [u^{D-2k}](10 + 10u + 5u^2 + u^3)^k \\
&= 10^k [u^{D-2k}]\left(1 + u + \frac{u^2}{2} + \frac{u^3}{10}\right)^k \\
&\leq 10^k [u^{D-2k}]\left(1 + \frac{u}{2}\right)^{3k} \\
&= 10^k \frac{\binom{3k}{D-2k}}{2^{D-2k}}.
\end{aligned}$$

Replacing the $\frac{1}{h\left(\frac{\theta}{d}\right)^{ad}}$ factor in (60) which comes from $\binom{dk}{D}$ gives, for $d=5$,

$$\begin{aligned}\pi_R(k,D) &\le O\left(\frac{k}{n^{1/2}}\right)\left(\frac{e^{o(n^{-1/8})}a^{a\theta}(1-a)^{5-a\theta}}{h(a)^2}\right)^n\left(\frac{10}{2^{\theta-2}h\left(\frac{\theta-2}{3}\right)^3}\right)^k\\ &= O\left(\frac{k}{n^{1/2}}\right)\left(\frac{e^{o(n^{-1/8})}10^a a^{a(\theta-2)}(1-a)^{5-2-a(\theta-2)}}{\left(2^{\theta-2}h\left(\frac{\theta-2}{3}\right)^3\right)^a}\right)^n\\ &= O\left(\frac{k}{n^{1/2}}\right)\left(e^{o(n^{-1/8})}10^a(1-a)^3\left(\frac{\left(\frac{a}{1-a}\right)^{\frac{\theta-2}{3}}}{2^{\frac{\theta-2}{3}}h\left(\frac{\theta-2}{3}\right)}\right)^{3a}\right)^n. \end{aligned} \tag{65}$$

Let $p(x)=\frac{q^x}{h(x)}$ for any $x\in[0,1]$, note that if $P(x)=\log p(x)$ then

$$\begin{aligned}P'(x) &= \log q-\log x+\log(1-x).\\ P''(x) &= -\frac{1}{x}-\frac{1}{1-x}<0.\end{aligned}$$

So $p(x)$ is maximized when $\log q=\log\left(\frac{x}{1-x}\right)$ or $x=\frac{q}{1+q}$ and the maximum value is $1+q$

Thus from (65) we get

$$\pi_R(k,\ell,D)\le O\left(\frac{k}{n^{1/2}}\right)\left(e^{o(n^{-1/8})}10^a(1-a)^3\left(1+\frac{a}{2(1-a)}\right)^{3a}\right)^n.$$

Let $R_3(a)=\log\left(10^a(1-a)^3\left(1+\frac{a}{2(1-a)}\right)^{3a}\right)$. Then

$$\begin{aligned}R_3'(a) &= \log 10-\frac{6}{2-a}+3\log\left(\frac{2-a}{2-2a}\right),\\ R_3''(a) &= \frac{3a}{(2-a)^2(1-a)}>0.\end{aligned}$$

So $R_3(a)$ is convex on $[0,\frac{2}{5}]$. We have $R_3(0)=0$ and $R_3'(0)=\log 10-3\le -3/4$ and $R_3(2/5)<-1/4$. It follows that

$$B_{66}=\sum_{\ell<k=n^{9/10}}^{2n/5}\sum_{D=2k}^{5k}\pi_R(k,\ell,D)\le\sum_{\ell<k=n^{9/10}}^{2n/5}\sum_{D=2k}^{5k}O\left(\frac{1}{n^{1/2}}\right)e^{-(3k/4-o(n^{7/8}))}=o(1). \tag{66}$$

**Case 2.2.3:** $d=4$.

Using (51) we get

$$\begin{aligned}\pi_R(k,\ell,D) &\le O\left(\frac{1}{n^{1/2}}\right)\left(\frac{e^{o(n^{-1/8})}a^{a\theta}(1-a)^{4-a\theta}}{h(a)^2}\right)^n\left(\frac{6}{2^{\theta-2}h\left(\frac{\theta-2}{2}\right)^2}\right)^k\\ &= O\left(\frac{1}{n^{1/2}}\right)\left(e^{o(n^{-1/8})}6^a a^{a(\theta-2)}(1-a)^{2-a(\theta-2)}\left(\frac{1}{2^{\frac{\theta-2}{2}}h\left(\frac{\theta-2}{2}\right)}\right)^{2a}\right)^n\\ &= O\left(\frac{1}{n^{1/2}}\right)\left(e^{o(n^{-1/8})}6^a(1-a)^2\left(\frac{\left(\frac{a}{1-a}\right)^{\frac{\theta-2}{2}}}{2^{\frac{\theta-2}{2}}h\left(\frac{\theta-2}{2}\right)}\right)^{2a}\right)^n\\ &\le O\left(\frac{1}{n^{1/2}}\right)\left(e^{o(n^{-1/8})}6^a(1-a)^2\left(1+\frac{a}{2(1-a)}\right)^{2a}\right)^n.\end{aligned}$$

Now if $R_4(a)=\log\left(6^a(1-a)^2\left(1+\frac{a}{2(1-a)}\right)^{2a}\right)$ then

$$\begin{aligned}R_4'(a) &= \log 6-\frac{4}{2-a}+2\log\left(\frac{2-a}{2-2a}\right),\\ R_4''(a) &= \frac{2a}{(2-a)^2(1-a)}>0.\end{aligned}$$

Thus $R_4$ is convex on $[0,.51]$. We have $R_4(0)=1$ and $R_4'(0)=\log 6-2\le -1/5$ and $R_4(.51)<-1/20$. It follows from this and (33) that

$$B_{67}=\sum_{\ell<k=n^{9/10}}^{k_0}\sum_{D=2k}^{4k}\pi_R(k,\ell,D)\le+\sum_{\ell<k=n^{9/10}}^{k_0}\sum_{D=2k}^{4k}O\left(\frac{1}{n^{1/2}}\right)e^{-(k/5-o(n^{7/8}))}=o(1). \tag{67}$$

**Case 2.2.4:** $d=3$.

Using (54) we get

$$\begin{aligned}\pi_R(k,\ell,D) &\le O\left(\frac{1}{n^{1/2}}\right)\left(\frac{e^{o(n^{-1/8})}a^{a\theta}(1-a)^{3-a\theta}}{h(a)^2}\right)^n\left(\frac{3^{3-\theta}}{h\left(\theta-2\right)}\right)^k\\ &= O\left(\frac{1}{n^{1/2}}\right)\left(e^{o(n^{-1/8})}a^{a(\theta-2)}(1-a)^{1-a(\theta-2)}\left(\frac{3^{3-\theta}}{h(\theta-2)}\right)^a\right)^n\\ &= O\left(\frac{1}{n^{1/2}}\right)\left(e^{o(n^{-1/8})}3^a(1-a)\left(\frac{\left(\frac{a}{3(1-a)}\right)^{\theta-2}}{h(\theta-2)}\right)^a\right)^n\\ &\le O\left(\frac{1}{n^{1/2}}\right)\left(e^{o(n^{-1/8})}3^a(1-a)\left(1+\frac{a}{3(1-a)}\right)^a\right)^n.\end{aligned}$$

Now if $R_5(a)=\log\left(3^a(1-a)\left(1+\frac{a}{3(1-a)}\right)^a\right)$ then

$$\begin{aligned}R_5'(a) &= -\frac{3}{3-2a}+\log\left(\frac{3-2a}{1-a}\right),\\ R_5''(a) &= \frac{4a-3}{(3-2a)^2(1-a)}.\end{aligned}$$

**Case 2.2.4.1:** $\theta \geq 2.0005$ and $0 \leq a \leq a_0 = k_0/n$.

We go back to (59) and make the choice $\zeta_1 = \zeta_2 = z$ and replace $h(\theta/d)^{-ad}$ by $\left(\frac{3^{3-\theta}}{h(\theta-2)}\right)^a$ and consider the function

$$F_1(\theta, a) = \frac{h(\theta a/3)^3 3^{(3-\theta)a}}{h(a)^2 h(\theta-2)^a}$$

so that $\pi_R(k, \ell, D) \leq O\left(\frac{1}{n^{1/2}}\right) F_1(\theta, a)^n$. Let $G_1(\theta, a) = \log(F_1(\theta, a))$. Then

$$\frac{\partial G_1}{\partial a} = \log\left(\frac{27(1-a)^2(\theta-2)^{\theta-2}(a\theta)^\theta}{3^\theta a^2(3-\theta)^{3-\theta}(3-a\theta)^\theta}\right), \tag{68}$$

$$\frac{\partial G_1}{\partial \theta} = a\left(\log\left(\frac{3-\theta}{9}\right) - \log(\theta-2) + \log(a\theta) - \log\left(1-\frac{a\theta}{3}\right)\right), \tag{69}$$

$$\frac{\partial^2 G_1}{\partial a^2} = \frac{(3-a)\theta - 6}{a(1-a)(3-a\theta)}, \tag{70}$$

$$\frac{\partial^2 G_1}{\partial \theta^2} = \frac{((3-a)\theta^2 - 12\theta + 18)a}{\theta(3-a\theta)(\theta-3)(\theta-2)}. \tag{71}$$

It follows from (70) that

$$G_1(\theta, a) \text{ is a convex function of } a \text{ for } 0 \leq a \leq a_\theta = \frac{3\theta-6}{\theta}, \text{ for } \theta \text{ fixed}, 2 \leq \theta \leq 3 \tag{72}$$

and

$$G_1(\theta, a) \text{ is a concave function of } a \text{ for } a_\theta \leq a \leq 1, \text{ for } \theta \text{ fixed}, 2 \leq \theta \leq 3. \tag{73}$$

It follows from (71) that

$$G_1(\theta, a) \text{ is a concave function of } \theta \text{ on } [2,3] \text{ for } a \text{ fixed}, 0 \leq a \leq 1. \tag{74}$$

A calculation shows that if $g_1(\theta) = G_1(\theta, a_\theta)$ then

$$g_1'(\theta) = \frac{3}{\theta^2}\log\left(\frac{144}{3^{\theta^2}(3-\theta)^2}\right), \tag{75}$$

$$g_1''(\theta) = -\frac{6}{\theta^3(3-\theta)}\left(-\theta + 2(3-\theta)\log\left(\frac{12}{3-\theta}\right)\right). \tag{76}$$

Furthermore, if $g_2(\theta) = \frac{\partial G_1}{\partial a}\,|_{a=a_\theta}$ then

$$g_2(\theta) = \log\left(\frac{12}{3^\theta(3-\theta)}\right). \tag{77}$$

**Case 2.2.4.2:** $2.0005 \leq \theta \leq 3$ and $0 \leq a \leq e^{-10000}$.

For $a \leq e^{-10000}$ we have $\frac{\partial G_1}{\partial a} \leq \log 10 - (\theta-2)\log 1/a \leq -2$. So,

$$F_1(\theta, a) \leq e^{-2a} \text{ for } 0 \leq a \leq e^{-10000},\ 2.0005 \leq \theta \leq 3. \tag{78}$$

**Case 2.2.4.3:** $2.46 \leq \theta \leq 3$ and $e^{-10000} \leq a \leq a_0$.

Now $a_\theta > a_0$ for $\theta \geq 2.46$ and so (72) implies that $G_1(\theta, a) \leq \max\left\{G_1(\theta, e^{-10000}), G_1(\theta, a_0)\right\}$ for $2.46 \leq \theta \leq 3$ and $e^{-10000} \leq a \leq a_0$. Now (78) implies that $G_1(2.46, e^{-10000}) < -2e^{-10000}$ and

(69) implies that $\frac{\partial G_1}{\partial \theta} \mid_{\theta=2.46,a=e^{-10000}} < 0$ and so (74) implies that $G_1(\theta, e^{-10000}) \le -2e^{-10000}$ for $2.46 \le \theta \le 3$. Also, by direct calculation, we have $G_1(2.46, a_0) < -.002$ and $\frac{\partial G_1}{\partial \theta} \mid_{\theta=2.46,a=a_0} < 0$ and so $G_1(\theta, a_0) \le -.002$ for $2.46 \le \theta \le 3$. Thus,

$$F_1(\theta, a) \le e^{-2e^{-10000}} \text{ for } e^{-10000} \le a \le a_0 \text{ and } 2.46 \le \theta \le 3.$$

**Case 2.2.4.4:** $2.0005 \le \theta \le 2.25$ and $e^{-1000} \le a \le a_0$.

We take $\zeta_1 = .6$ and $\zeta_2 = 2.1$ in (59) and let

$$F_2(\theta, a) = F_1(\theta, a)\frac{z^3}{f(z)}\frac{f(\zeta_1)^a}{\zeta_1^{\theta a}}\frac{f(\zeta_2)^{1-a}}{\zeta_2^{3-\theta a}} = F_1(\theta, a)e^{\rho_2+\sigma_2 a+\tau_2 a\theta}$$

where

$$e^{\rho_2} = \frac{z^3 f(\zeta_2)}{f(z)\zeta_2^3},\ e^{\sigma_2} = \frac{f(\zeta_1)}{f(\zeta_2)},\ e^{\tau_2} = \frac{\zeta_2}{\zeta_1}.$$

Let $G_2(\theta, a) = \log(F_2(\theta, a))$. $\frac{\partial^2 G_2}{\partial a^2} = \frac{\partial^2 G_1}{\partial a^2}$ and $\frac{\partial^2 G_2}{\partial \theta^2} = \frac{\partial^2 G_1}{\partial \theta^2}$ and so (72),(73) and (74) hold with $G_1$ replaced by $G_2$. Putting $\gamma_2(\theta) = G_2(\theta, a_\theta)$ we see that $\gamma_2''(\theta) = g_1''(\theta) - \frac{12\sigma_2}{\theta^3} > 0$, using (76) ($\sigma_2 < -3.127$). Thus $\gamma_2$ is convex on $2.0005 \le \theta \le 2.25$. Furthermore $\gamma_2(2.0005), \gamma_2(2.25) < -.00003$ and so $\gamma_2(\theta) < -.00003$ for $\theta \in [2.0005, 2.25]$ and therefore $G_2(\theta, a) \le -.00003a/a_\theta < -.00003a$ when $0 \le a \le a_\theta$ and $\theta \in [2.0005, 2.25]$. Next let $\phi_2(\theta) = \frac{\partial G_2}{\partial a} \mid_{a=a_\theta}$. We have $\phi_2(\theta) = g_2(\theta) + \sigma_2 + \tau_2\theta < -.05$ for $2.0005 \le \theta \le 2.25$, using (77) ($\tau_2 < 1.253$). So, $G_2(\theta, a) \le \phi_2(\theta) - .05(a - a_\theta)$ for $a \ge a_\theta$ when $\theta \in [2.0005, 2.25]$. Thus

$$F_2(\theta, a) < e^{-.00003a} \text{ for } e^{-1000} \le a \le a_0 \text{ and } 2.0005 \le \theta \le 2.25.$$

Now suppose that we repeat the idea of the previous paragraph, but this time we take $\zeta_1 = 1.4$ and $\zeta_2 = 3$ in (59) and use the same notation. Putting $\gamma_2(\theta) = G_2(\theta, a_\theta)$ we see that $\gamma_2''(\theta) = g_1''(\theta) - \frac{12\sigma_2}{\theta^3} > 0$, using (76) ($\sigma_2 < -2.27$). Thus $\gamma_2$ is convex on $2.25 \le \theta \le 2.46$. Furthermore $\gamma_2(2.25), \gamma_2(2.46) < -.05$ and so $\gamma_2(\theta) < -.05$ for $\theta \in [2.25, 2.46]$ and therefore $G_2(\theta, a) \le -.05a/a_\theta < -.05a$ when $0 \le a \le a_\theta$ and $\theta \in [2.25, 2.46]$. Next let $\phi_2(\theta) = \frac{\partial G_2}{\partial a} \mid_{a=a_\theta}$. We have $\phi_2(\theta) = g_2(\theta) + \sigma_2 + \tau_2\theta < -.2$ for $2.25 \le \theta \le 2.46$, using (77) ($\tau_2 < .763$). So, $G_2(\theta, a) \le \phi_2(\theta) - .2(a - a_\theta)$ for $a \ge a_\theta$ when $\theta \in [2.25, 2.46]$. Thus

$$F_2(\theta, a) < e^{-.05a} \text{ for } e^{-1000} \le a \le a_0 \text{ and } 2.25 \le \theta \le 2.46.$$

**Case 2.2.4.5:** $2 \le \theta \le 2.0005$ and $e^{-1000} \le a \le a_0$.

For this we simplify our estimate of $\pi_R(k, \ell, D)$ by removing some terms involving $\beta$ from (58).

$$\pi_R(k, \ell, D) \le \mathsf{P}(\exists A \subseteq R, B \subseteq L :\ |A| = k, |B| = k-1, N_\Gamma(A) \subseteq B, d_A(a) \ge 2, a \in A) \le$$

$$O(n^{1/2})\binom{m}{k}\binom{n}{k-1} \sum_{\substack{2\le d_a, a\in[m]\\ 2\le x_b\le d, b\in[k-1]\\ \sum_{a\in[k]} d_a = \sum_{b\in[k-1]} x_b = D}} \prod_{a=1}^{k} \frac{z^{d_a}}{d_a! f(z)} \prod_{b=1}^{k-1} \binom{d}{x_b}\, D! \prod_{i=0}^{D-1} \frac{1}{dn-i} =$$

$$O\left(\frac{k}{m^{1/2}}\right)\binom{n}{k}\binom{m}{k}\frac{z^D D!}{f(z)^k}\frac{(dn-D)!}{(dn)!}\left(\sum_{\substack{2\le d_a, a\in[k]\\ \sum_a d_a = D}} \prod_{a=1}^{k} \frac{1}{d_a!}\right)\left(\sum_{\substack{2\le x_b\le d, b\in[k-1]\\ \sum_b x_b = D}} \prod_{b=1}^{k-1} \binom{d}{x_b}\right) =$$

$$O\left(\frac{k}{m^{1/2}}\right)\binom{n}{k}\binom{m}{k}\frac{z^D}{f(z)^k}\frac{1}{\binom{dn}{D}}\left([u^D](e^u-1-u)^k\right)\left([u^D]((1+u)^d-(1+du))^k\right)\le$$

$$O\left(\frac{k}{m^{1/2}}\right)\binom{n}{k}\binom{m}{k}\frac{z^D}{f(z)^k}\frac{1}{\binom{dn}{D}}\frac{f(\zeta_1)^k}{\zeta_1^D}\binom{dk}{D}=$$

$$O\left(\frac{k}{m^{1/2}}\right)\binom{n}{k}\binom{m}{k}\frac{\binom{dk}{D}}{\binom{dn}{D}}\left(\frac{f(\zeta_1)}{f(z)}\right)^k\left(\frac{z}{\zeta_1}\right)^D$$

$$=O\left(\frac{1}{m^{1/2}}\right)\left(\frac{h(\theta a/d)^d}{h(a)h(a/\beta)^\beta h(\theta/d)^{ad}}\left(\frac{f(\zeta_1)}{\zeta_1^\theta}\frac{z^\theta}{f(z)}\right)^a\right)^n \tag{79}$$

$$=O\left(\frac{1}{m^{1/2}}\right)\left(e^{o(n^{-1/8}a)}\frac{h(\theta a/d)^d}{h(a)^2h(\theta/d)^{ad}}\left(\frac{f(\zeta_1)}{\zeta_1^\theta}\frac{z^\theta}{f(z)}\right)^a\right)^n. \tag{80}$$

Now let

$$F_3(\theta,a)=\frac{h(\theta a/3)^3 3^{(3-\theta)a}}{h(a)^2h(\theta-2)^a}\left(\frac{f(\zeta_1)}{\zeta_1^\theta}\frac{z^\theta}{f(z)}\right)^a.$$

We take $\zeta_1=.0001$ and then

$$\frac{f(\zeta_1)}{\zeta_1^\theta}\frac{z^\theta}{f(z)}<.e^{-.86}$$

for $2\le\theta\le 2.0005$. Keeping some slack, we define

$$F_4(\theta,a)=\frac{h(\theta a/3)^3 3^{(3-\theta)a}e^{-.85a}}{h(a)^2h(\theta-2)^a}$$

and $G_4(\theta,a)=\log(F(\theta,a))$. Now let $\gamma_4(\theta)=G_4(\theta,a_\theta)$. We have $\gamma_4'(\theta)=g_1'(\theta)-\frac{5.1}{\theta^2}$ and $\gamma_4''(\theta)=g_1''(\theta)+\frac{10.2}{\theta^3}$ and we find from (76) that $\gamma_4$ is concave on $2\le\theta\le 2.0005$. Furthermore $\gamma_4(2)=0$ and using (75) we see that $\gamma_4'(2)<-.8$ and so $g_1(\theta)<-.8(\theta-2)$ for $\theta\in[2,2.0005]$. So $G_4(\theta,a)\le -.8a(\theta-2)/a_\theta\le -.8a(\theta-2)$ for $0\le a\le a_\theta$. Next let $\phi_4(\theta)=\frac{\partial G_4}{\partial a}\mid_{a=a_\theta}=g_2(\theta)-.85$. We see from (77) that $g_2(\theta)<-.5$ for $2\le\theta\le 2.0005$ and thus $G_4(\theta,a)\le -.5(a-a_\theta)$ for $a\ge a_\theta$ when $\theta\in[2,2.0005]$. Replacing $e^{-.85}$ by $e^{-.86}$ in the definition of $F_4(\theta,a)$ we get $F_4(\theta,a)<e^{-(4(\theta-2)a/5+a/100)}$ for $0\le a\le a_0$ when $2\le\theta\le 2.0005$. So, for some small constant $c>0$,

$$B_{81}=\sum_{\ell<k=2}^{k_0}\sum_{D=2k}^{3k}\pi_R(k,\ell,D)\le\sum_{\ell<k=2}^{k_0}\sum_{D=2k}^{3k}e^{-ck}=o(1). \tag{81}$$

### 3.3.3 Finishing the case $|n-m|=o(n^{7/8})$

We repeat our observation that the maximum degree $\Delta$ in $\Gamma$ is $o(\log n)$ **whp**. Therefore

$$\mathsf{P}(\mu(\Gamma)<\min\{m,n\})\le o(1)+\begin{cases}A_{14}+A_{29}+A_{34}+A_{35}+B_{47}+B_{55}+B_{63}+B_{64} & d\ge 6\\ A_{14}+A_{29}+A_{34}+A_{35}+B_{47}+B_{55}+B_{63}+B_{66} & d=5\\ A_{14}+A_{29}+A_{34}+A_{36}+A_{40}+B_{47}+B_{55}+B_{67} & d=4\\ A_{14}+A_{29}+A_{34}+A_{36}+A_{41}+A_{42}+B_{47}+B_{55}+B_{81} & d=3\end{cases}$$

where the $o(1)$ term accounts for $\mathsf{P}(\Delta(\Gamma)>\log n)$. We use $A_{14}+A_{29}+A_{34}+A_{35}$ etc. to account for witnesses $A\subseteq L,B$ with $|A|\le k_0$ and $B_{47}+B_{55}+B_{63}+B_{64}$ etc. to account for witnesses

$A \subseteq L, B$ with $|A| > k_0$. This is because if $A' = R \setminus B$ and $B' = L \setminus A$ then $|A'| = m - k + 1$ and $|B'| = n - k$ and $N_\Gamma(A') \subseteq B'$ and there will be a minimal witness $A'', B''$ with $A'' \subseteq A'$. Similarly, we use $B_{47} + B_{55} + B_{63} + B_{64}$ etc. to account for witnesses $A \subseteq R, B$ with $|A| \leq k_0$ and $A_{14} + A_{29} + A_{34} + A_{35}$ etc. to account for witnesses $A \subseteq R, B$ with $|A| > k_0$.

We point out for use in the next section that our computations allow us to claim that we have

$$\sum_{\substack{k=n^{9/10} \\ \ell \leq \min\{k-1, m/2\}}}^{n-n^{9/10}} \sum_{D=dk}^{k \log n} \pi_L(k, \ell, D) = O(e^{-\Omega(n^{9/10})}). \tag{82}$$

One can see this by noting that all of the upper bounds in question are of order $e^{O(|m-n|)}\xi^k$ where $0 < \xi < 1$ is some absolute constant and $k \geq n^{9/10}$.

The same argument allows us to claim that

$$\sum_{\substack{k=n^{9/10} \\ \ell \leq \min\{k-1, n/2\}}}^{n-n^{9/10}} \sum_{D=2k}^{dk} \pi_R(k, \ell, D) = O(e^{-\Omega(n^{9/10})}). \tag{83}$$

### 3.4 The case $n + n^{4/5} \leq m \leq dn/2$

Let $\mathcal{G}(n, m)$ denote the set of bipartite graphs with $|L| = n, |R| = m$ that are $d$-regular on $L$ and degree at least 2 on $R$. The upper bound on $m$ is due to the fact that there are precisely $dn$ edges and the minimum degree in $R$ is at least two. Suppose that $G(n, m)$ is chosen uniformly at random from $\mathcal{G}(n, m)$.

If there is no matching from $L$ to $R$, then let a minimal witness $A, B$ be *small* if $|A| \leq n^{3/4}$ and *large* if $|A| \geq n - n^{3/4}$ and *medium* otherwise.

#### 3.4.1 Small Witnesses

The RHS of (14) remains $o(1)$ for all $C_1 n \leq m \leq C_2 n$, for any constants $0 < C_1 < C_2$.

#### 3.4.2 Large Witnesses

To deal with $k \geq n - n^{9/10}$ we treat this as $k \leq n^{9/10}$ in Section 3.3.2. Indeed, if there is such a witness $A, B$, let $A' = R \setminus B$ and $B' = L \setminus A$. Then $N_\Gamma(A') \subseteq B'$ and $|B'| < \min\{|A'|, n^{3/4}\}$ and so we can find a witness $A'', B''$ with $A'' \subseteq A', B'' \subseteq B'$ and $|A''| \leq n^{9/10}$.

We use (79) for this calculation. Now

$$\frac{h(\theta a/d)^d}{h(a)h(a/\beta)^\beta h(\theta/d)^{ad}} = \frac{\left(\frac{\theta a}{d}\right)^{\theta a}\left(1-\frac{\theta a}{d}\right)^{d-\theta a}}{a^a(1-a)^{1-a}\left(\frac{a}{\beta}\right)^a\left(1-\frac{a}{\beta}\right)^{\beta-a}\left(\frac{\theta}{d}\right)^{\theta a}\left(1-\frac{\theta}{d}\right)^{da-\theta a}} =$$

$$a^{(\theta-2)a}\exp\left\{-(d-\theta a)\sum_{k=1}^{\infty}\frac{\theta^k a^k}{kd^k} + a - \sum_{k=2}^{\infty}\frac{a^k}{k(k-1)} + \frac{a}{\beta} - \sum_{k=2}^{\infty}\frac{a^k}{\beta^{k-1}k(k-1)} + (da-\theta a)\sum_{k=1}^{\infty}\frac{\theta^k}{kd^k}\right\}$$

$$= a^{(\theta-2)a}\exp\left\{a\left(1+\frac{1}{\beta}-(d-\theta)\log(1-\theta/d)-\theta\right)+O(a^2)\right\}. \tag{84}$$

So from (79) we can write

$$\pi_R(k,\ell,D) \leq$$
$$O\left(\frac{1}{m^{1/2}}\right)\left(\left(\frac{az}{\zeta_1}\right)^{\theta-2}\exp\left\{1+\frac{1}{\beta}-(d-\theta)\log(1-\theta/d)-\theta+O(a)\right\}\frac{f(\zeta_1)}{\zeta_1^2}\frac{z^2}{f(z)}\right)^{an}. \tag{85}$$

Now we claim that

$$\zeta_1^{\theta-2} \geq \frac{1}{2} \text{ and that } f(x)x^{-2} \text{ is monotone increasing in } x. \tag{86}$$

First notice that $f(x)x^{-2} = \sum_{i=2}^{\infty}\frac{x^{i-2}}{i!}$ which is clearly monotone increasing. Second note that $\zeta_1 = \zeta(\theta)$ and since $\frac{d\zeta(x)}{dx} > 0$ we have

$$\lim_{x\to\infty}\frac{d\zeta(x)}{dx} = \lim_{x\to\infty}\frac{f(\zeta(x))^2}{(e^{\zeta(x)}-1)^2-\zeta(x)^2e^{\zeta(x)}}$$
$$= \lim_{\zeta\to\infty}\frac{f(\zeta)^2}{(e^{\zeta}-1)^2-\zeta^2e^{\zeta}} = 1$$

and since $\zeta(x)$ is concave we have $\frac{d\zeta(x)}{dx} \geq 1$. This, along with $\lim_{x\to 2^-}\zeta(x) = 0$, implies that $\zeta(x) \geq x-2$. We can then lower bound

$$\zeta_1^{\theta-2} = \zeta(\theta)^{\theta-2} \geq (\theta-2)^{\theta-2} \geq e^{-e^{-1}} \geq 0.69$$

Using this we see from (85) that if

$$\theta \geq \theta_0 = 2 + \frac{4}{\log(1/az)}$$

then

$$\pi_R(k,\ell,D) \leq O\left(\frac{1}{m^{1/2}}\right)e^{-k}.$$

In which case we have

$$\sum_{\ell<k=2}^{n^{9/10}}\sum_{\theta\geq\theta_0}\pi_R(k,\ell,D) \leq O\left(\frac{1}{m^{1/2}}\right)\sum_{k\geq 1}e^{-k} = o(1). \tag{87}$$

When $\theta < \theta_0$ we have $\theta = 2 + o(1), f(\zeta_1)/\zeta_1^2 = 1/2 + o(1)$. Therefore

$$\pi_R(k,\ell,D) \le O\left(\frac{1}{m^{1/2}}\right)\left(\frac{z^2 e^{-(d-2)\log(1-2/d)+o(1)}}{2f(z)}\right)^k. \tag{88}$$

Now for $d \ge 4$ we have

$$\frac{z^2 e^{-(d-2)\log(1-2/d)+o(1)}}{2f(z)} \le \frac{9}{10} \tag{89}$$

and so

$$\sum_{k=1}^{n^{9/10}} \sum_{\theta \le \theta_0} \pi_R(k,\ell,D) \le O\left(\frac{1}{m^{1/2}}\right)\left(\frac{9}{10}\right)^k = o(1). \tag{90}$$

When $d = 3$, the expression on the LHS of (89) is at most 1.26. So in this case we go back to (80) and replace $\frac{1}{h(\theta/d)^{ad}}$ by $\left(\frac{3^{\theta-2}}{h(\theta-2)}\right)^a = e^{o(a)}$. After this (84) is replaced by

$$a^{(\theta-2)a} \exp\left\{a\left(1 + \frac{1}{\beta} + \theta\log(\theta/d) - \theta\right) + o(a)\right\}.$$

And then (88) is replaced by

$$\pi_R(k,\ell,D) \le O\left(\frac{1}{m^{1/2}}\right)\left(\frac{z^2 e^{-2\log(3/2)+o(1)}}{2f(z)}\right)^k \le O\left(\frac{1}{m^{1/2}}\right)\frac{1}{2^k}$$

and so

$$\sum_{k=1}^{n^{9/10}} \sum_{\theta \le \theta_0} \pi_R(k,\ell,D) \le O\left(\frac{1}{m^{1/2}}\right)\frac{1}{2^k} = o(1). \tag{91}$$

### 3.4.3 Medium Witnesses

Let $d_i(n,m)$ denote the number of $R$-vertices of degree $i \ge 2$ in $G(n,m)$ and let $D_i(n,m) = \mathsf{E}(d_i(n,m))$.

We define three events:

$$\mathcal{A}_1(n,m-1) = \left\{G \in \mathcal{G}(n,m-1) :\ \exists i : |d_i(n,m-1) - D_i(n,m-1)| > n^{3/5}/i^3, 2 \le i \le \log^2 n\right\} \tag{92}$$

$$\mathcal{A}_2(n,m) = \left\{G \in \mathcal{G}(n,m) :\ \exists i : d_i(n,m) \ne 0, i > \log^2 n\right\} \tag{93}$$

$$\mathcal{B}(n,m) = \left\{G \in \mathcal{G}(n,m) :\ |d_2(n,m) - D_2(n,m)| > 2n^{3/5}\right\} \tag{94}$$

We argue next that if $\mathcal{A}(n,m) = \mathcal{A}_1(n,m-1) \cup \mathcal{A}_2(n,m)$ then

$$\mathsf{P}(\mathcal{A}(n,m) \cup \mathcal{B}(n,m)) = e^{-\Omega(\log^2 n)}. \tag{95}$$

For any $t > 0$ we have

$$\mathsf{P}(|d_i(n,m-1) - D_i(n,m-1)| > t) \le O(n^{1/2})\mathsf{P}(Bin(m,q_i) > t)$$

where $q_i = \frac{z^i}{i!f(z)}$.

We will now use the following bounds (see for example [1])

$$\mathsf{P}(|Bin(N,p) - Np| \geq t) \leq 2e^{-t^2/N}, \tag{96}$$

$$\mathsf{P}(Bin(N,p) \geq \alpha Np) \leq (e/\alpha)^{\alpha Np}. \tag{97}$$

If $i \leq \log^2 n$ then we can use (96) with $t = n^{3/5}/i^3$ to deal with $\mathcal{A}_1(n,m)$ and also with $\mathcal{B}(n,m)$. If $i \geq \log^2 n$ then $nq_i \leq e^{-\Omega(\log^2 n)}$. We can therefore use (97) with $\alpha = 1/nq_i$ to deal with $\mathcal{A}_2(n,m)$. This concludes the proof of (95).

Now consider a set of pairs $X \subseteq \mathcal{G}(n,m-1) \times \mathcal{G}(n,m)$. We place $(G_1,G_2)$ into $X$ if $G_2$ is obtained from $G_1$ in the following manner: Choose a vertex $x \in R$ of degree at least four in $G_1$. Suppose that its neighbours are $y_i, i = 1,2,\ldots,k$ in any order. To create $G_2$ we (i) replace $x$ by two vertices $x$ and $m$ and then (ii) let the neighbours of $x$ in $G_2$ be $y_1, y_2$ and let the neighbours of $m$ be $y_3,\ldots,y_k$.

For $G \in \mathcal{G}(n,m-1)$ let

$$\pi_1(G) = |\{G_2 : (G,G_2) \in X\}|$$

and for $G \in \mathcal{G}(n,m)$ let

$$\pi_2(G) = |\{G_1 : (G_1,G) \in X\}|.$$

We note that if

$$\Sigma_1 = \sum_{i \geq 4} \binom{i}{2} D_i(n,m-1)$$

then

- $G \notin \mathcal{A}(n,m-1)$ implies that $|\pi_1(G) - \Sigma_1| \leq O(n^{3/5})$.
- $\pi_1(G) \leq \binom{m-1}{2}$ for all $G \in \mathcal{G}(n,m-1)$.
- $G \notin \mathcal{B}(n,m)$ implies that $|\pi_2(G) - D_2(n,m)| \leq n^{3/5}$.
- $\pi_2(G) \leq m$ for all $G \in \mathcal{G}(n,m)$.

We then note that

$$(\Sigma_1 - O(n^{3/5}))|\mathcal{G}(n,m-1)| \leq |X| \leq (D_2(n,m) + n^{3/5} + me^{-\Omega(\log^2 n)})|\mathcal{G}(n,m)|.$$

Now let $\mathcal{P},\mathcal{Q}$ be properties such that if $(G_1,G_2) \in X$ and $G_2 \in \mathcal{Q}$ then $G_1 \in \mathcal{P}$. Let $(G_1,G_2)$ be chosen uniformly from $X$ and let $\mathsf{P}_X$ denote probabilities computed w.r.t. this choice. Then

$$\mathsf{P}_X(G_2 \in \mathcal{Q}) \leq \mathsf{P}_X(G_1 \in \mathcal{P}) \leq \frac{|\mathcal{P}|(\Sigma_1 + O(n^{3/5})) + m|\mathcal{A}(n,m-1)|}{|X|}$$

and

$$\mathsf{P}_X(G_2 \in \mathcal{Q}) \geq \frac{(|\mathcal{Q}| - |\mathcal{B}(n,m)|)(D_2(n,m) - n^{3/5})}{|X|}.$$

So,

$$\frac{(|\mathcal{Q}| - |\mathcal{B}(n,m)|)(D_2(n,m) - n^{3/5})}{|\mathcal{G}(n,m)|(D_2(n,m) + n^{3/5} + me^{-\Omega(\log^2 n)})} \leq \frac{|\mathcal{P}|(\Sigma_1 + O(n^{3/5})) + m|\mathcal{A}(n,m-1)|}{|\mathcal{G}(n,m-1)|(\Sigma_1 - O(n^{3/5}))}.$$

So,

$$\frac{|\mathcal{Q}|}{|\mathcal{G}(n,m)|} \leq (1+O(n^{-2/5}))\frac{|\mathcal{P}|}{|\mathcal{G}(n,m-1)|}.$$

So, if $\mathcal{P}_j$ is a property of $\mathcal{G}(n,j)$ for $j = n, n+1, \ldots, m$,

$$\frac{|\mathcal{P}_m|}{|\mathcal{G}(n,m)|} \leq (1+O(n^{-2/5}))^{m-n}\frac{|\mathcal{P}_{n+n^{4/5}}|}{\mathcal{G}(n,n+n^{4/5})}. \tag{98}$$

We use (98) in the following way: First let $\mathcal{B}_j$, $n+n^{4/5} \leq j \leq m$ be the property that $G \in \mathcal{G}(n,j)$ contains a minimal witness $A, B$ with $A \subseteq L, n^{9/10} \leq |A| \leq n/2$. If $(G_1, G_2) \in X$ and $G_2 \in \mathcal{B}_m$ then $G_1 \in \mathcal{B}_{m-1}$. Indeed $A, B \cap [m-1]$ is a minimal witness in $G_1$. Applying (98) and (82) we see that **whp** $\mathcal{B}_m$ fails to occur. Now let $\mathcal{B}'_j$ be the property that $G \in \mathcal{G}(n,j)$ contains a minimal witness $A, B$ with $A \subseteq R, n^{9/10} \leq |A|, |B| < \min\{|A|-(j-n), n/2\}$. If $(G_1, G_2) \in X$ and $G_2$ has a witness $A, B$ with $A \subseteq L$ and $n/2 < |A| \leq n - n^{9/10}$ then $G_2 \in \mathcal{B}'_m$. Indeed $A' = R \setminus B, B' = L \setminus A$ is also a witness in $G_2$. Now if $G_2 \in \mathcal{B}'_m$ with a witness $A', B'$ then $A' \cap [m-1], B'$ is a witness in $G_1$ and so contains a minimal witness $A'', B''$ where $|A''| > |B''| + m - n > n^{9/10}$ i.e. $G_1 \in \mathcal{B}'_{m-1}$. Applying (98) and (83) we see that **whp** $\mathcal{B}'_m$ fails to occur. This deals with medium witnesses.

## 3.5 The case $m \leq n - n^{4/5}$

We once again consider medium witnesses separately from small or large witnesses.

### 3.5.1 Small Witnesses

We first observe that the RHS of (47) remains $o(1)$ for all $m \leq n$. Then to finish, we can argue as in cases 2.0.1 to 2.0.3 with $m \leq n$ making the calculations easier.

### 3.5.2 Large Witnesses

For $k \geq n - n^{9/10}$ we deal with $\pi_L(k, \ell, D)$ for $k \leq n^{9/10}$. As in Section 3.4.1, we use the fact that the RHS of (14) remains $o(1)$ for all $C_1 n \leq m \leq C_2 n$, for any constants $0 < C_1 < C_2$.

### 3.5.3 Medium Witnesses

Now consider a set of pairs $Y \subseteq \mathcal{G}(n,m) \times \mathcal{G}(n+1,m)$. We place $(G_1, G_2)$ into $Y$ if $G_2$ is obtained from $G_1$ in the following manner: Choose $0 \leq k \leq n$. Replace edges $(\ell, y)$ by $(\ell+1, y)$ for all $\ell > k$ and all $y$. Add vertex $k+1$ and $d$ edges $(k+1, y_j), j = 1, 2, \ldots, d$.

Note that if $(G_1, G_2) \in Y$ and $G_1$ has a matching of $R$ into $L$ then so does $G_2$.

For $G \in \mathcal{G}(n,m)$ let now

$$\pi_1(G) = |\{G_2 : (G, G_2) \in Y\}|$$

and for $G \in \mathcal{G}(n+1,m)$ let

$$\pi_2(G) = |\{G_1 : (G_1, G) \in Y\}|.$$

Let

$$\Sigma_2 = (n+1)\left(1 - \frac{z^2}{2f(z)}\right)^d$$

and for $G \in \mathcal{G}(n+1,m)$ let

$$L_3(G) = |\{v \in L : \text{ all neighbours of } v \text{ have degree at least } 3\}|.$$

Let

$$\mathcal{C}(n+1,m) = \left\{G \in \mathcal{G}(n+1,m) : |L_3(G) - \Sigma_2| \le n^{3/5}\right\}.$$

We note that

- $G \in \mathcal{G}(n,m)$ implies that $\pi_1(G) = (n+1)\binom{m}{d}$.
- $G \notin \mathcal{C}(n,m+1)$ implies that $|\pi_2(G) - \Sigma_2| \le n^{3/5}$.
- $\pi_2(G) \le n+1$ for all $G \in \mathcal{G}(n+1,m)$.

We then note that

$$\frac{|Y|}{|\mathcal{G}(n,m)|} = (n+1)\binom{m}{d}.$$
$$\Sigma_2 - n^{3/5} \le \frac{|Y|}{|\mathcal{G}(n+1,m)|} \le \Sigma_2 + n^{3/5} + (n+1)e^{-\Omega(\log^2 n)}.$$

Now let $\mathcal{P}, \mathcal{Q}$ be properties such that if $(G_1,G_2) \in Y$ and $G_2 \in \mathcal{Q}$ then $G_1 \in \mathcal{P}$. Let $(G_1,G_2)$ be chosen uniformly from $Y$ and let $\mathsf{P}_Y$ denote probabilities computed with respect to this choice. Then

$$\mathsf{P}_Y(G_2 \in \mathcal{Q}) \le \mathsf{P}_Y(G_1 \in \mathcal{P}) = \frac{|\mathcal{P}|(n+1)\binom{m}{d}}{|Y|}$$

and

$$\mathsf{P}_Y(G_2 \in \mathcal{Q}) \ge \frac{(|\mathcal{Q}| - |\mathcal{C}(n+1,m)|)(\Sigma_2 - n^{3/5})}{|Y|}.$$

Arguing as in Section 3.4 we see that if $\mathcal{P}_j$ is a property of $\mathcal{G}(j,m)$ for $j = m, m+1, \dots, n$,

$$\frac{|\mathcal{P}_m|}{\mathcal{G}(n,m)} \le (1 + O(n^{-2/5}))^{n-m} \frac{|\mathcal{P}_{m+n^{4/5}}|}{\mathcal{G}(m+n^{4/5},m)}. \tag{99}$$

First let $\mathcal{B}_j, m + n^{4/5} \le j \le n$ be the property that $G \in \mathcal{G}(j,m)$ contains a minimal witness $A, B$ with $A \subseteq R, n^{9/10} \le |A| \le m/2$. If $(G_1,G_2) \in X$ and $G_2 \in \mathcal{B}_{n+1}$ then $G_1 \in \mathcal{B}_n$. Indeed $A, B \cap [n]$ is a witness in $G_1$. Applying (99) and (83) we see that **whp** $\mathcal{B}_n$ fails to occur. Now let $\mathcal{B}'_j$ be the property that $G \in \mathcal{G}(j,m)$ contains a minimal witness $A, B$ with $A \subseteq R, n^{9/10} \le |A|, |B| \le \min\{|A| - (j-m), m/2\}$. If $(G_1,G_2) \in X$ and $G_2$ has a witness $A, B$ with $A \subseteq R$ and $m/2 < |A| \le m - n^{9/10}$ then $G_2 \in \mathcal{B}'_m$. Indeed $A' = L \setminus B, B' = R \setminus A$ is also a witness in $G_2$. Now if $G_2 \in \mathcal{B}'_m$ with a witness $A', B'$ then $A' \cap [n], B'$ is a witness in $G_1$ and so contains a minimal witness $A'', B''$ where $|A''| > |B''| + n - m > n^{9/10}$ i.e. $G_1 \in \mathcal{B}'_{m-1}$. Applying (99) and (82) we see that **whp** $\mathcal{B}'_m$ fails to occur. This deals with medium witnesses.

## References


[1] N. Alon and J. Spencer, The Probabilistic Method, Wiley-Interscience, 2008.

[2] J. Aronson, A. Frieze, B.G. Pittel. Maximum matchings in sparse random graphs: Karp-Sipser re-visited. *Random Structures and Algorithms*, 12(2):111-178, 1998.

[3] Y. Azar, A. Broder, A. Karlin, and E. Upfal. Balanced Allocations. *SIAM Journal on Computing*, 29(1):180-200, 1999.

[4] T. Bohman, The triangle-free process , *Advances in Mathematics*, 221 (2009) 1653-1677.

[5] B. Bollobás, A probabilistic proof of an asymptotic formula for the number of labelled regular graphs, *European Journal of Combinatorics* 1 (1980) 311-316.

[6] A. Broder and A. Karlin. Multilevel Adaptive Hashing. In *Proceedings of the 1st ACM-SIAM Symposium on Discrete Algorithms* (SODA), pp. 43-53, 1990.

[7] A. Broder and M. Mitzenmacher. Using Multiple Hash Functions to Improve IP Lookups. In *Proceedings of the 20th IEEE International Conference on Computer Communications* (INFOCOM), pp. 1454-1463, 2001.

[8] C. Cooper, The Cores of Random Hypergraphs with a Given Degree Sequence, *Random Structures and Algorithms* 25 (2004) 353-375.

[9] A. Dembo and A. Montanari, Finite size scaling for the core of large random hypergraphs, *Annals of Applied Probability* 18 (2008) 1993-2040.

[10] L. Devroye and P. Morin. Cuckoo hashing: Further analysis. *Information Processing Letters*, 86(4):215-219, 2003.

[11] M. Dietzfelbinger, A. Goerdt, M. Mitzenmacher, A. Montanari, R. Pagh and M. Rink, Tight Thresholds for Cuckoo Hashing via XORSAT. In *Proceedings of the 37th international colloquium conference on Automata, languages and programming* (ICALP), 213-225, 2010 and arXiv:0912.0287v3 [cs.DS]

[12] M. Dietzfelbinger and C. Weidling. Balanced allocation and dictionaries with tightly packed constant size bins. *Theoretical Computer Science*, 380(1-2):47-68, 2007.

[13] O. Dubois and J. Mandler, The 3-XORSAT Threshold, In *Proceedings of the 43rd IEEE Symposium on Foundations of Computer Science* (FOCS '02) 779-788, 2002.

[14] P. Erdős and A. Rényi, On random matrices, *Publ. Math. Inst. Hungar. Acad. Sci.* 5 (1964) 455-461.

[15] D. Fotakis, R. Pagh, P. Sanders, and P. Spirakis. Space Efficient Hash Tables With Worst Case Constant Access Time. *Theory of Computing Systems*, 38(2):229-248, 2005.

[16] N. Fountoulakis and K. Panagiotou, Orientability of Random Hypergraphs and the Power of Multiple Choices. In *Proceedings of the 37th international colloquium conference on Automata, languages and programming* (ICALP ), 348-359, 2010 and arXiv:0910.5147v1 [cs.DS].

[17] A. M. Frieze and P. Melsted, Maximum Matchings in Random Bipartite Graphs and the Space Utilization of Cuckoo Hashtables, arXiv:0910.5535v3 [cs.DS]

[18] M. Karonski and B. Pittel, Existence of a perfect matching in a random $(1+e^{-1})$–out bipartite graph, *Journal of Combinatorial Theory, Series B* 88(1) pp1-16, 2003.

[19] R.M. Karp and M. Sipser, Maximum Matchings in Sparse Random Graphs, *Proceedings of the 22nd Annual IEEE Symposium on Foundations of Computer Science* (1981) 364-375.

[20] A. Kirsch and M. Mitzenmacher. Using a Queue to De-amortize Cuckoo Hashing in Hardware. In *Proceedings of the Forty-Fifth Annual Allerton Conference on Communication, Control, and Computing*, 2007.

[21] A. Kirsch, M. Mitzenmacher, and U. Wieder. More Robust Hashing: Cuckoo Hashing with a Stash. In *Proceedings of the 16th Annual European Symposium on Algorithms*, pp. 611-622, 2008.

[22] A. Kirsch and M. Mitzenmacher. The Power of One Move: Hashing Schemes for Hardware. In *Proceedings of the 27th IEEE International Conference on Computer Communications* (INFOCOM), pp. 565-573, 2008.

[23] R. Kutzelnigg. Bipartite Random Graphs and Cuckoo Hashing. In *Proceedings of the Fourth Colloquium on Mathematics and Computer Science*, 2006.

[24] M. Luby, M. Mitzenmacher, M. Shokrollahi and D. Spielman, Efficient Erasure Correcting Codes, *IEEE Transactions on Information Theory* 47 (2001) 569-584.

[25] M. Mitzenmacher and S. Vadhan. Why Simple Hash Functions Work: Exploiting the Entropy in a Data Stream. In *Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms* (SODA), pp. 746-755, 2008.

[26] M. Mitzenmacher, Some open questions related to cuckoo hashing. In *Proceedings of the 17th Annual European Symposium on Algorithms (ESA)*, pages 1-10, 2009.

[27] M. Molloy, Cores in random hypergraphs and Boolean formulas, *Random Structures and Algorithms* 27 (2005) 124-135.

[28] R. Pagh and F. Rodler. Cuckoo hashing. *Journal of Algorithms*, 51(2):122-144, 2004.

[29] B. Vöcking. How Asymmetry Helps Load Balancing. *Journal of the ACM*, 50(4):568-589, 2003.

[30] David W. Walkup, Matchings in random regular bipartite digraphs, *Discrete Mathematics* 31(1) pp. 59-64, 1980.

[31] N.C. Wormald, The differential equation method for random graph processes and greedy algorithms, in *Lectures on Approximation and Randomized Algorithms* (M. Karonski and H.J. Proemel, eds), PWN, Warsaw, (1999) 73-155.