Summary of "Random Graph Isomorphism" by Babai, Erdos, Selkow
Summary by Caitlin Beecham

April 24, 2019

Source: https://epubs.siam.org/doi/pdf/10.1137/0209047

0.1 Cannonical Labelings

What is a cannonical labeling of a graph H? It is a labeling (bijective function) $l_H : V(G) \to [|V(G)|]$ on the vertices which is deterministically computed given H such that $H \cong H'$ if and only if $H \cong H'$ coincide as labeled graphs via their cannonical labelings l_H and $l_{H'}$. What is an example of a cannonical labeling of a graph H? Given a graph H just take all possible adjacency matrices that arise from all $2^{|V(G)|}$ orderings of the vertices of H. Then, regard each of the these n by n adjacency matrices as a binary vector of length n^2 by filling the vector row by row. Then, out of all $2^{|V(G)|}$ vectors, pick the one who comes first in the standard lexicographic order. The corresponding order of the vertices which gave rise to this adjacency matrix is the cannonical labeling of H. Clearly, this is a valid cannonical labeling as any graph $H' \cong H$ in the same isomorphism class as H has the same set of $2^{|V(G)|}$ adjacency matrices and will have the same unique one which comes first in a lexicographic ordering. Thus, these two adjacency matrices will coincide (literally be the same) which is actually a more precise defintion of what it means for two graphs to coincide as labeled graphs. It means that when one looks at their adjacency matrices corresponding to their labelings, these adjacency matrices are actually the same.

However, it is obviously not possible to compute all $2^{|V(G)|}$ adjacency matrices in practice since one would have to compute all permutation matrices $\sigma \in S_n$. So, these authors have given a good heuristic cannonical labeling algorithm such that if one inputs two graphs and looks at their cannonical labelings, they are isomorphic if and only if they coincide as labeled graphs. I should note that this algorithm only works properly on graphs that the algorithm is able to properly label and insert into the set $\mathcal{X}$ of previously seen cannonically labeled graphs. However, throughout the process of this algorithm, it can happen that an inputted graph X gets rejected by the algorithm because of some properties (namely to do with having multiple vertices of the same degree and similar properties). For these graphs, we are NOT later able to tell whether a future inputted graph Y is isomorphic to the graph X we saw before. It is only for the inputted graphs X which are NOT rejected by our cannonical labeling algorithm and are actually accepted into $\mathcal{X}$ with their new cannonical labeling that we are able to later determine if new unseen graphs are isomorphic to X. However, in such cases, the algorithm does work. Namely, the algorithm has been building up a family $\mathcal{X}$ of graphs it has seen so far which it has accepted and cannonically labeled. Now, at the current point in time, say Y is inputted into this algorithm. Either Y is rejected by the algorithm, in which case we get no information about its isomorphism class, or it is accepted in which cases we know that Y is isomorphic to some previously seen graph $X_i \in \mathcal{X}$ if and only if Y coincides with X_i as labeled graphs, which as I stated before is VERY easy to check. One needs only check that their adjacency matrices (the way we actually store a graph with a cannonical labeling (which makes sense because an adjacency matrix assumes an ordering)) are actually the same. One can do so in $O(|V(G)|^2)$ time.

0.2 Outline of the Algorithm

We take in a graph X. We first single out a portion of vertices of high degree. If any of their degrees coincide we reject this graph X (intuitively we do this because we cannot distinguish these vertices based solely on degree so we cannot come up with a well-defined cannonical labeling this way). Then, we define a generalized degree function and order the remaining vertices based on this function. Once again, if any of these values coincide, we reject this graph X. Barring the above, we now have a cannonical labeling of our graph X which we put into our set of labeled graphs $\mathcal{X}$. Now, as stated before one can take in another graph Y and provided it is not rejected one can determine whether it is isomorphic to any graph $X_i \in \mathcal{X}$ already in our set just by comparing the adjacency matrices which arise from the cannonical labelings of Y and X_i.

1. Set $r = \lceil 3\log_2(n) \rceil$.
2. Pick the r elements of highest degree. Label them $v_1, \ldots, v_r$ in descending degree order (meaning $deg(v_1) \geq deg(v_2) \geq \cdots \geq deg(v_r)$).
3. If $d(v_i) = d(v_{i+1})$ for some $i \in [r]$, then return $x \notin \mathcal{X}$.
4. Compute $f(v_i) = \sum_{j=1}^{\lfloor} n]a(i,j)2^j$ for $i \geq r+1$. (This function is a weighted generalization of the degree function on a vertex. (Note that $deg(v_i) = \sum_{j=1}^{n} a(i,j)$)).
5. Now, order the remaining vertices $v_{r+1}, v_{r+2}, \ldots, v_n$ in decreasing order by their f values. Namely, order them so that $f(v_{r+1}) \geq f(v_{r+2}) \geq f(v_n)$. (The labels used just before are with respect to the new ordering).
6. If any of the last vertices $v_{r+1}, v_{r+2}, \ldots, v_n$ agree on their f values (so namely $f(v_i) = f(v_{i+1})$ for some $i \in \{r+1, \ldots, n-1\}$) return $X \notin \mathcal{X}$.
7. Now, the labeling v_i in the ordering given by the above is the cannonical labeling of X which we now put into the set $\mathcal{X}$.

Theorem 1.2: The probability that a random graph X belongs to our class graphs in the set $\mathcal{X}$ from our cannonically labeling algorithm is greater than $1 - (\frac{1}{n})^{\frac{1}{7}}$.

Proposition 2.1: If $l = \frac{m}{2} + t$ with $0 < t < \frac{m}{2}$ and $f > \frac{r\log(2)}{2}\frac{m}{t}$, then

$$\binom{m}{l+f} < 2^{-r}\binom{m}{l}$$

.

Proof:

$$\frac{\binom{m}{l+f}}{\binom{m}{l}} = \frac{(m-l)\cdots(m-l-f+1)}{(l+f)\cdots(l+1)} < (\frac{m-l}{l+1})^f < (\frac{m-l}{\frac{m}{2}})^f$$
$$= (\frac{1-2t}{m})^f < exp(\frac{-2tf}{m}) < exp(-rlog2) = 2^{-r}.$$

Corollary 2.2: If $l = \frac{m}{2} + t$ with $0 < t < \frac{m}{2}$, then

$$P(m,l)/\binom{m}{l} < \frac{m}{t}.$$

Proof: Let $g = \frac{mlog2}{2t} + 1$. Then, from the above result we know that

$$P(m,l) < \binom{m}{l}(g + \frac{g}{2} + \frac{g}{4} + \ldots) < 2g\binom{m}{l} < \frac{m}{t}\binom{m}{l}.$$

Proposition 2.3: If $l = \frac{m}{2} + t$ (with $0 < t < \frac{m}{2}$ and $0 < f < t$) then

$$\binom{m}{l} > \binom{m}{l-f}(1 - \frac{4tf}{m}).$$

Proof:

$$\begin{aligned}\frac{\binom{m}{l}}{\binom{m}{l-f}} &= \frac{(m-l+f)\cdots(m-l+1)}{l(l-1)\cdots(l-f+1)} > (\frac{m-l}{l})^f \\ &= (\frac{\frac{m}{2}-t}{\frac{m}{2}+t})^f > (\frac{1-2t}{m})^{2f} > 1 - \frac{4tf}{m}.\end{aligned}$$

Corollary 2.4: If $l = \frac{m}{2} + t$ with $2\sqrt{m} < t\frac{m}{30}$ then

$$\frac{P(m,l)}{\binom{m}{l}} > \frac{m}{23t}.$$

Proof: For any $f \in \mathbb{N}$, one has that

$$\frac{P(m,l)}{\binom{m}{l}} > \frac{f\binom{m}{l+f}}{\binom{m}{l}}.$$

Now, Proposition 2.3 tells us that $RHS > 1 - \frac{4tf}{m}$. Let $f = \frac{m}{9t} + 1$. So, $f > \frac{m}{9t}$ and $f < \frac{m}{9t} + 1 < \frac{t}{27}$. Hence, we have

$$\begin{aligned}RHS &= \frac{f\binom{m}{l+f}}{\binom{m}{l}} \\ &= \frac{\frac{m}{9t}+1\binom{m}{l+\frac{m}{9t}+1}}{\binom{m}{l}} \\ &> f(1 - \frac{4(t+f)f}{m}) \\ &= \frac{m}{9t}(1 - \frac{4*28}{9*27} - \frac{4*28}{27}\frac{t}{m}) \\ &> \frac{m}{23t}.\end{aligned}$$

0.3 Expected Value of Indicator Variable Degrees Above Threshold

Set a threshold d. Let $z(x)$ for a vertex $x \in V(G)$ be the indicator variable that is 1 if $deg(x) \geq d$ and 0 otherwise. Now let $z = \sum_{x \in V(G)} z(x)$. We wish to analyze the expected value of z and how it changes as we vary the threshold d. We vary the threshold by increasing t (by increasing ω_m).

Lemma 3.1: Let $m = n - 1$, $d = \frac{m}{2} + t$ where $t = t_0 + \omega_m(\frac{m}{log(m)})^{\frac{1}{2}}$, where

$$t = t_0 + \omega_m(\frac{m}{logm})^{\frac{1}{2}},$$

where

$$t_0 = (\frac{1}{2}mlogm)^{\frac{1}{2}} - \frac{1}{8}(\frac{2m}{logm})^{\frac{1}{2}}loglogm,$$

and

$$\frac{-logm}{\sqrt{2}} < \omega_m < m^{0.7}.$$

If $\omega_m < 0$, then

$$E(z) > c_1 e^{-1.4\omega_m}.$$

If $\omega_m > 0$, then

$$E(z) < c_2 exp(\frac{-2.8\omega_m - 2\omega_m^2}{logm}).$$

If $\frac{\omega_m}{logm} \to \frac{-\epsilon}{\sqrt{2}}$ as $m \to \infty$ where $0 < \epsilon < 1$ (where ϵ is a fixed number) then

$$E(z) > m^{\epsilon(2-\epsilon+o(1))}.$$

Proof: First, note that for any $x \in \mathbb{R}$ with $1 \leq x \leq n$, one has

$$\begin{aligned} E(z) = nE(z_x) &= n2^{-n+1}P(n-1,d) \\ &= (1+o(1))m2^{-m}P(m,d). \end{aligned}$$

Now, using Corollaries 2.2 and 2.4, one obtains θ with $0 < \theta < 1$ such that

$$\begin{aligned} P(m,d) &= \frac{1}{1+22\theta}\binom{m}{d}\frac{m}{t} \\ &= \frac{1+o(1)}{1+22\theta}2^m m\frac{e^{-2t^2/m}}{t(\frac{1}{2}\pi m)^{\frac{1}{2}}}. \end{aligned}$$

Then,

$$log(E(z)) = O(1) + \frac{3logm}{2} - logt - \frac{2t^2}{m}.$$

If one takes $t = t_0$, then the RHS is bounded, which means that in general we get

$$\begin{aligned} log(E(z)) &= O(1) - log(\frac{t}{t_0}) - \frac{2(t^2-t_0^2)}{m} \\ &= O(1) - log(1+\frac{\omega_m\sqrt{2}}{logm}) - 2\omega_m(\sqrt{2} - \frac{\sqrt{2}loglogm}{4logm} + \frac{\omega_m}{logm}). \end{aligned}$$

What's the overall idea here? We're setting $m = n-1$. So $m \simeq n$. Then we set d such that $d > \frac{m}{2} \approx \frac{n}{2}$ which is roughly $\frac{n}{2}$. Then, we'll add something more which is t. Here $t = t_0 + \omega_m(\frac{m}{log(m)})^{\frac{1}{2}}$ where t_0 is an expression in terms of m and ω_m is bounded above and below some functions of m namely on the left by negative logarithm and on the right by $m^{0.17}$ so both grow (or decay for the negative one) slowly. So, intuitively, this seems like a tight bound on ω_m which is some multiplier in the expression for $t = t_0 + \omega_m(\frac{m}{log(m)})^{\frac{1}{2}}$ that varies. Note that all other parts of the expression for t we do not vary. We only change ω_m. Note that ω_m can be positive or negative. If it's less than zero we get a lower bound on $E(z)$ and if its positive we get an upper bound on $E(z)$. These bounds will be useful in applying Chebyshev during our proof of Corollary 3.4 which states roughly speaking that the probability that the number of vertices below some degree threshold dips far below its expected value goes to 0 as the number of vertices n of G tends to ∞.

Corollary 3.2: When $\omega_m > 0$, using the previous Lemma 3.1, one then has that the probability of the event (called E_0) that a random graph X has a vertex of degree at least $t_0 + \omega_m(\frac{m}{logm})^{\frac{1}{2}}$ is

$$Pr(E_0) \leq c_2 exp(-2.8\omega_m - \frac{2\omega_m^2}{logm})$$

where $(\omega_m > 0)$.

Now, to get a similar result for $\omega_m < 0$, one must compute the variance of z. What is that? It is $E[x^2] - E^2[x]$.

Lemma 3.3: Let $m = n - 1$ and $d = \frac{m}{2} + t$, where $2\sqrt{m} < t < \frac{m}{30}$. Then,

$$\frac{Var[z]}{E^2[z]} < \frac{1}{E[z]} + \frac{67t^2}{m^2}.$$

Proof: Notice that for all $x, y \in \mathbb{R}$ with $1 \leq x < y \leq n$, one has

$$Var(z) = E(z^2) - E^2(z) = mA + \binom{n}{2}B,$$

where

$$A = E(z_x)(1 - E(z_x)) \qquad < E(z_x)$$

(since $(1 - E(z_x)) < 1$) and

$$B = E(z_x z_y) - E^2(z_x).$$

Then, the expression for A gives us that $nA < E(z)$.

Now, define conditional probabilities P_1, P_2 as follows.

$$\begin{aligned} P_1 &= Pr((deg(x) > d \text{ and } deg(y) > d) | (x \text{ and } y \text{ are adjacent})) \\ &= 2^{-2n+4} P(n-2, d-1)^2 \\ P_2 &= Pr((deg(x) > d \text{ and } deg(y) > d) | (x \text{ and } y \text{ are not adjacent})) \\ &= 2^{-2n+4} P(n-2, d)^2. \end{aligned}$$

Note that if $x \neq y$, then

$$E(z_x z_y) = Pr(deg(x) > d \text{ and } deg(y) > d) = \frac{P_1 + P_2}{2}.$$

Then, it follows that

$$\begin{aligned} B &= 2^{-2n+2}(2P(n-2, d-1)^2 + 2P(n-2, d)^2 - P(n-1, d)^2) \\ &= 2^{-2n+2}(P(n-2, d-1) - P(n-2, d)^2) \\ &= 2^{-2n+2}\binom{n-2}{d}^2. \end{aligned}$$

Finally, we get that

$$\begin{aligned} \frac{Var(z)}{E^2(z)} &< \frac{1}{E(z)} + \binom{n}{2}\frac{B}{E^2(z)} < \frac{1}{E(z)} + \frac{1}{2}\frac{\binom{n-2}{d}^2}{P(n-1, d)^2} \\ &< \frac{1}{E(z)} + \frac{1}{8}(\frac{\binom{m}{d}}{P(m, d)})^2 < \frac{1}{E(z)} + \frac{1}{8}(\frac{m}{23t})^2 \\ &< \frac{1}{E(z)} + \frac{1}{8}(\frac{23t}{m}) < \frac{1}{E(z)} + \frac{67t^2}{m^2}. \end{aligned}$$

The above block of inequalities follows from Corollary 2.4 and also uses the fact that $\binom{n-2}{d} < \frac{1}{2}\binom{n-1}{d}$ holds for all $d > \frac{n}{2}$.

Corollary 3.4: By varying n (number of vertices of the graph) we can construct an infinite sequence of degree thresholds d indexed by d_n for $n = 0, 1, 2, \ldots$. If this sequence is chosen so that $E[z] \to \infty$ as $n \to \infty$ (recall z is the number of vertices whose degree is less than the degree threshold d_n), then

$$Pr(z < \frac{E[z]}{2}) \to 0. \tag{0.1}$$

Also, (continuing with the notation from Lemma 3.1), for any ω_m with $-log(m\sqrt{2}) < \omega_m < 0$ we have

$$Pr(z < \frac{E(z)}{2}) < c_3 e^{1.4\omega_m}. \tag{0.2}$$

Furthermore, for fixed ϵ in the range $0 < \epsilon < 1$, we have that if $\frac{\omega_m}{logm} \to \frac{\epsilon}{2}$ as $m \to \infty$ (recall that $m = n - 1$ so $m \to \infty$ as $n \to \infty$; they're just shifted by 1), then

$$Pr(z < \frac{E(z)}{2}) < c_4 m^{-\epsilon(2-\epsilon+o(1))}. \tag{0.3}$$

Proof: Recall that Chebyshev's Inequality states that for any random variable z with finite $E(z)$ and finite $Var(z)$ and standard deviation σ, one has

$$Pr(|z - E(z)| \geq k\sigma) < \frac{1}{k^2}.$$

Recall that the standard deviation σ can be computed as the square root of the variance. Namely, $\sigma^2 = Var(z)$.

In the context of our specific problem, how can we apply Chebyshev? Then note $z < \frac{E(z)}{2}$ if and only if $\frac{E(z)}{2} - z > 0$ if and only if

$$\begin{aligned} \frac{E(z)}{2} - z &> 0 \\ \frac{E(z)}{2} + \frac{E(z)}{2} - \frac{E(z)}{2} - z &> 0 \\ E(z) - z - \frac{E(z)}{2} &> 0 \\ E(z) - z &> \frac{E(z)}{2} \end{aligned}$$

Now, $\sigma = \sqrt{Var(z)}$. To apply Chebyshev we want that $E(z) - z > \frac{E(z)}{2} = \sigma k$, so set $k := \frac{E(z)}{2\sigma} = \frac{E(z)}{2\sqrt{Var(z)}}$. Then,

$$\begin{aligned} k^2 &= \frac{1}{4}\frac{E^2(z)}{Var(z)} \\ \frac{1}{k^2} &= 4\frac{Var(z)}{E^2(z)}. \end{aligned}$$

Finally, we can apply Chebyshev by noting that

$$Pr(E(z) - z > \frac{E(z)}{2}) < Pr(|E(z) - z| > \frac{E(z)}{2}) < \frac{1}{k^2} = 4\frac{Var(z)}{E^2(z)}.$$

Now, choose $t \in \mathbb{R}$ such that $2\sqrt{m} < t < \frac{m}{30}$ and $t^2 < mlogm + \frac{2\omega_m^2 m}{logm} = O(\frac{logm}{m})$.

Lemma 3.3 said that for this appropriately chosen t, one has that $\frac{Var(z)}{E^2(z)} < \frac{1}{E(z)} + \frac{67t^2}{m^2}$. Now, we can use Lemma 3.1 to get a bound on $E(z)$ which you'll notice appears in the above expression from Lemma 3.3. In particular, recall that the expression for t was in terms of t_0, ω_m, and m. Lemma 3.1 said that depending on whether $\omega_m < 0$ or $\omega_m < 0$ one gets lower or upper bounds (respectively) on $E(z)$. In this case, we have that $\omega_m < 0$, which gives us $E(z) > c_1 e^{-1.4\omega_m}$ which implies $\frac{1}{E(z)} < \frac{1}{c_1} e^{1.4\omega_m}$. Namely, that implies

$$\frac{1}{E(z)} + \frac{67t^2}{m^2} < \frac{1}{c_1} e^{1.4\omega_m} + \frac{67t^2}{m^2}$$
$$< \frac{1}{c_1} e^{1.4\omega_m} + \frac{67(mlogm + \frac{2\omega_m^2 m}{logm})^2}{m^2}.$$

But now note that $\frac{logm}{m} = exp(loglogm - logm) = o(exp(-1.4\frac{logm}{\sqrt{2}})) = o(e^{-1.4\omega_m})$ and also $e^{-1.4\omega_m} = O(\frac{log(m)}{m})$ which gives us

$$\frac{1}{E(z)} + \frac{67t^2}{m^2} < e^{-1.4\omega_m} + O(\frac{logm}{m})$$

which is exactly the statement of 0.2. We get 0.3 by using the exact same process, namely Lemma 3.3 and Lemma 3.1. Just like above we note that still the same from Lemma 3.3 we have that

$$\frac{Var(z)}{E^2(z)} < \frac{1}{E(z)} + \frac{67t^2}{m^2}$$

(Just a reminder that the whole reason we are interested in bounding $\frac{Var(z)}{E^2(z)}$ is because we want to use Chebyshev and that expression appears on the RHS in our Chebyshev application). Now there is one difference in this case where $\omega_m > 0$ instead of $\omega_m < 0$. Namely, we now get an upper bound on $E(z)$ instead of lower bound. So, applying the analogous argument we get that $Pr(z < \frac{E(z)}{2}) < c_4 m^{-\epsilon(2-\epsilon+o(1))}$ which is exactly the statement of 0.3.

Finally, it remains to prove 0.1. Recall that Lemma 3.3 tells us that $\frac{Var(z)}{E^2(z)} < \frac{1}{E(z)} + \frac{67t^2}{m^2}$. We want to show that if the sequence d_n is chosen such that $E(z) \to \infty$ as $n \to \infty$, then $Pr(z < \frac{E(z)}{2}) \to 0$ as $n \to \infty$. I claim that it suffices to show that $\frac{t}{m} \to 0$ if $E(z) \to \infty$. Why? Because then $\frac{1}{E(z)} + \frac{67t^2}{m^2} \to 0$ as $n \to \infty$. Since $\frac{Var(z)}{E^2(z)} < \frac{1}{E(z)} + \frac{67t^2}{m^2}$ we also get that $\frac{Var(z)}{E^2(z)} \to 0$ as $n \to \infty$. Finally, using Chebyshev, recall that we have

$$Pr(E(z) - z > \frac{E(z)}{2}) < 4\frac{Var(z)}{E^2(z)} \to 0 \text{ as } n \to \infty,$$

concluding the proof.

Lemma 3.5: Let $0 < k < \sqrt{n}$, $\frac{\sqrt{3}}{2} < \alpha < 1$ and $t = \alpha(nlogn)^{\frac{1}{2}}$. Then define event E_1 as the random graph X having two vertices x, y such that $deg(x), deg(y) \geq \frac{n}{2} + t$ and $|deg(x) - deg(y)| < k$. Then,

$$lim_{n\to\infty} Pr(E_1) = o(kn^{\frac{3}{2} - 2\alpha^2}).$$

Proof: Let $a, b \in \mathbb{Z}$ be chosen such that $\frac{n}{2} < a \leq b$. Then, the probability that $deg(x) = a$ and $deg(y) = b$ for distinct vertices $x, y \in V(X)$ is the following expression.

$$\frac{1}{2} \frac{(\binom{n-2}{a}\binom{n-2}{b} + \binom{n-2}{a-1}\binom{n-2}{b-1})}{2^{2n-4}} < 2^{-2n+4}\binom{n-2}{a-1}^2.$$

One then notes that the probability that $a \leq deg(x)$ and $deg(x) \leq deg(y) \leq deg(x) + k$ (call that event E_3)(so we have that $deg(y)$ is sandwiched between expressions in terms of $deg(x)$) is at most

$$k * 2^{-2n+4} \sum_{s=a}^{n-1} \binom{n-2}{s-1}^2.$$

We can apply Proposition 2.1 which said that

$$\binom{m}{l+f} < 2^{-r} \binom{m}{l}$$

. Here we set $m := n-2$ and $l = a-1$ and $f = s-a$. Then, Proposition 2.1 tells us that

$$\binom{n-2}{s-1} < 2^{-r} \binom{n-1}{a-1} < \binom{n-1}{a-1}$$

(noting that for any positive number $r \geq 1$ one has that $2^{-r} < 1$). So, returning to our above expression, we have that

$$k * 2^{-2n+4} \sum_{s=a}^{n-1} \binom{n-2}{s-1}^2 < \frac{n}{a - \frac{n}{2}} \binom{n-2}{a-1}^2.$$

Now, we set $a = \frac{n}{2} + t$ to obtain

$$\begin{aligned} Pr(E_3) &< \frac{\binom{n}{2} k \frac{n}{t} e^{\frac{-4t^2}{n}}}{\frac{1}{2}\pi n(1+o(1))} \\ &= \frac{\sqrt{2}(1+o(1))}{\pi\alpha} n^2 k (nlogn)^{\frac{-1}{2}} n^{-2\alpha^2} \\ &< \frac{k n^{\frac{3}{2}-2\alpha^2}}{logn^{\frac{1}{2}}} \end{aligned}$$

for n sufficiently large.

Theorem 3.6: Let $d_1 \geq d_2 \geq \cdots \geq d_n$ denote the degree sequence of a random graph X on n vertices. Let $k = n^{0.03}$ and $l = n^{0.15}$. Define event E_2 as $d_i - d_j \geq k$ for every i, j satisfying $1 \leq i < j \leq l$. To parse this a little more clearly, one also notes that E_2 happens if and only if the difference between any two CONSECUTIVE terms $d_i - d_{i+1} \geq k$ for all $i \in [l-1]$. Then,

$$Pr(E_2) \geq 1 - n^{-0.15}$$

for n sufficiently large.

Proof: Set $\epsilon = \frac{1}{12}$, $\alpha = 1 - \epsilon$, $t = \frac{\alpha(nlogn)^{\frac{1}{2}}}{\sqrt{2}}$, $d = \frac{n}{2} + t$. Then, continuing with the notation of Lemma 3.1, denote $t = t_0 + \omega_m (\frac{m}{logm})^{\frac{1}{2}}$ where $\frac{\omega_m}{logm} \to \frac{-\epsilon}{\sqrt{2}}$. Then, Lemma 3.1 tells us that

$$E(z) > m^{\epsilon(2-\epsilon+o(1))}.$$

Now, $\epsilon = \frac{1}{12}$ means that $\epsilon(2-\epsilon) = \frac{1}{12}\frac{23}{12} > 0.157$. Hence, we see that we have $\epsilon(2-\epsilon)$ in the exponent on the RHS so we have

$$E(z) > m^{0.157+o(1)} \geq (n-1)^{0.157+o(1)} > n^{0.15}$$

for sufficiently large n. Then clearly also

$$\frac{E(z)}{2} > n^{0.15} = l.$$

Recall Corollary 3.4 says that $Pr(z < \frac{E(z)}{2}) < c_4 m^{-\epsilon(2-\epsilon+o(1))}$. Taking the complement we get $Pr(z < \frac{E(z)}{2}) > 1 - c_4 m^{-\epsilon(2-\epsilon+o(1))}$. Recall that z is the number of vertices whose degree are less than or equal to d_n. So, Corollary 3.4 tells us that the probability that our random graph X on n vertices has at least $\frac{E(z)}{2}$ vertices of degree $> d$ is at least $1 - c_4 m^{-\epsilon(2-\epsilon+o(1))} > 1 - m^{-0.155}$. Finally, by Lemma 3.5 the difference $d(u) - d(w)$ for any u, w with $u \neq w$ and $deg(u), deg(w) > d$ satisfies

$$Pr(|deg(u) - deg(w)| > k) > 1 - kn^{\frac{3}{2}-2\alpha^2} > 1 - n^{0.03+1.5-2\alpha^2} > 1 - n^{-0.1505}.$$

Equivalently put, the probability that our random graph X violates the statement of the theorem is at most $n^{-0.155} + n^{-0.1505} < n^{-0.15}$.

0.4 Uniqueness of the Codes of the Vertices

Let X be a random graph on n vertices. Let $d_1 \geq d_2 \geq \cdots \geq d_n$ be the degree sequence of X and as before let $r = 3log_2(n)$. Let C denote the event that $d_i \geq d_{i+1} + 3$ for $i = 1, \ldots, r+2$. Let X_i be the graph obtained from X by deleting the ith vertex. Let $C(i,j)$ be the event that the degrees of the r highest degree vertices are distinct in $X(i,j)$. Now, note that event C happening implies that event $C(i,j)$ happens for $1 \leq i \leq j \leq n$. Now, let v'_k for $k \in [n-1]$ denote the vertex ordering assigned by our algorithm to the graph X_i and let w_k denote the vertex ordering assigned by our algorithm to the the graph X_j. Finally, let $f_i(v'_k) = \sum_{l=1}^{n-1} a_i(k,l)2^l$ where a_i is the adjacency function in X_i. Similarly let $f_j(w_k) = \sum_{=l1}^{n-1} a_j(k,l)2^l$ be defined on X_j. So, these are just the weighted adjacency functions on X_i, X_j respectively defined as usual. Now, let $A(i,j)$ be the event that either $\overline{C(i,j)}$ or the functions $f_i(v'_k) = f_j(w_k)$ for all $k \in \{r+1, \ldots, n-1\}$ meaning that the respective weighted adjacency functions agree on the respective latter sets of vertices (where both vertex sets are ordered with respect to their cannonical labelings). Then, the probability that X is rejected by our algorithm ($Pr(X \notin \mathcal{X})$) satisfies

$$\begin{aligned}
&Pr(\overline{C}) + Pr(C \text{ and } \exists i,j \text{ with } i \neq j \text{ such that } f(v_i) = f(v_j)) \\
&\leq Pr(\overline{C}) + \sum_{i<j} Pr(C \text{ and } A(i,j)) \\
&\leq Pr(\overline{C}) + \sum_{i<j} Pr(C(i,j) \text{ and } A(i,j)) \\
&\leq Pr(\overline{C}) + \sum_{i<j} Pr(A(i,j)|C(i,j)) \\
&= Pr(\overline{C}) + \binom{n}{2} 2^{-r} + O(\frac{1}{n}).
\end{aligned}$$

That concludes the proof of Theorem 1.2.