Proof by Existence

- Let us now move to a more involved example.
- We start with the definition of an (α, β, n, d)–expander.
- A bipartite graph $G = (V_1 \cup V_2, E)$ on n nodes is an (α, β, n, d) expander if

1) Every vertex in V_1 has degree at most d.
2) For any subset S of vertices from V_1 such that $|S|$ is at most αn, there are at least $\beta|S|$ neighbors in V_2.

- Ideally, d should be small and β as large as possible.

Proof by Existence

- Let us now move to a more involved example.
- We start with the definition of an (α, β, n, d) expander.
- A bipartite graph $G = (V_1 \cup V_2, E)$ on n nodes is an (α, β, n, d) expander if

1) Every vertex in V_1 has degree at most d.
2) For any subset S of vertices from V_1 such that $|S|$ is at most αn, there are at least $\beta|S|$ neighbors in V_2.

- To build such a graph in a deterministic manner is not easy.
- Simple randomized construction with $d = 18$, $\alpha = 1/3$, and $\beta = 2$

Proof by Existence

- A bipartite graph $G = (V_1 \cup V_2, E)$ on n nodes is an (α, β, n, d) expander if

1) Every vertex in V_1 has degree at most d.
2) For any subset S of vertices from V_1 such that $|S|$ is at most αn, there are at least $\beta|S|$ neighbors in V_2.

- Simple randomized construction with $d = 18$, $\alpha = 1/3$, and $\beta = 2$.
- We will actually not use these values until the very end of the proof.

Proof by Existence

- A bipartite graph $G = (V_1 \cup V_2, E)$ on n nodes is an (α, β, n, d) expander if

1) Every vertex in V_1 has degree at most d.
2) For any subset S of vertices from V_1 such that $|S|$ is at most αn, there are at least $\beta|S|$ neighbors in V_2.

- Let each vertex v in V_1 choose d neighbors in V_2 by sampling independently and uniformly at random.
- We can even sample with replacement.
- In other words, the same choice can be made more than once.
- We will still consider only one copy of any multiple choices.

Proof by Existence

- A bipartite graph $G = (V_1 \cup V_2, E)$ on n nodes is an (α, β, n, d) expander if

1) Every vertex in V_1 has degree at most d.

- Let each vertex v in V_1 choose d neighbors in V_2 by sampling independently and uniformly at random.
- By this construction, each vertex in V_1 has degree at most d.
- Next, we show the second condition.

Proof by Existence

- Condition 2: For any subset S of vertices from V_1 such that $|S|$ is at most αn, there are at least $\beta|S|$ neighbors in V_2.
- Let $|V_1| = |V_2| = n$.
- Let each vertex v in V_1 choose d neighbors in V_2 by sampling independently and uniformly at random.
- Fix a parameter s that is at most αn.
- Consider any subset S of V_1 with $|S| = s$.
- Let T be any subset of V_2 of size βs.
- Consider the event that all the neighbors of vertices in S are in T.
- This event occurs with probability at most $(\beta s/n)^{ds}$.

Proof by Existence

- Condition 2: For any subset S of vertices from V_1 such that $|S|$ is at most αn, there are at least $\beta|S|$ neighbors in V_2.
- Let $|V_1| = |V_2| = n$. Let each vertex v in V_1 choose d neighbors in V_2 by sampling independently and uar.
- Consider any subset S of V_1 with $|S| = s$.
- Let T be any subset of V_2 of size βs.
- Consider the event that all the neighbors of vertices in S are in T.
- This event occurs with probability at most $(\beta s/n)^{ds}$.
- We have to now look at all possible S and all possible T.

Proof by Existence

- Condition 2: For any subset S of vertices from V_1 such that $|S|$ is at most αn, there are at least $\beta|S|$ neighbors in V_2.
- Consider the event that all the ds neighbors of vertices in S of size s are in T.
- This event occurs with probability at most $(\beta s/n)^{ds}$.
- Let us use Boole's inequality to upper bound the probability of the event that for some S all its neighbors are in T.
- We have to now look at all possible S and all possible T.
- There are ${}^{n}C_{s}$ ways to choose S and ${}^{n}C_{\beta s}$ ways to choose T.

Proof by Existence

- Condition 2: For any subset S of vertices from V_1 such that $|S|$ is at most αn, there are at least $\beta|S|$ neighbors in V_2.
- This event occurs with probability at most $(\beta s/n)^{ds}$.
- There are ${}^{n}C_{s}$ ways to choose S and ${}^{n}C_{\beta s}$ ways to choose T.
- The probability that for some S all its neighbors are in T is now upper bounded by ${}^{n}C_{s} \,.\, {}^{n}C_{\beta s} \,.\, (\beta s/n)^{ds}$.
- To simplify, let us use the inequality that for any n and k, ${}^{n}C_{k}$ is at most $(en/k)^{k}$.

Proof by Existence

- Condition 2: For any subset S of vertices from V_1 such that $|S|$ is at most αn, there are at least $\beta|S|$ neighbors in V_2.
- The probability that for some S all its neighbors are in T is now upper bounded by ${}^{n}C_{s} \cdot {}^{n}C_{\beta s} \cdot (\beta s/n)^{ds}$.
- To simplify, let us use the inequality that for any n and k, ${}^{n}C_{k}$ is at most $(en/k)^{k}$.
- The probability is at most $(en/s)^{s} \cdot (en/\beta s)^{\beta s} \cdot (\beta s/n)^{ds}$.
- Simplifying we get, $\left[(s/n)^{d-\beta-1}\ e^{1+\beta}\ \beta^{d-\beta}\right]^{s}$.
- Use that s is at most αn, for $\alpha = 1/3$ to simplify to:

Proof by Existence

- Condition 2: For any subset S of vertices from V_1 such that $|S|$ is at most αn, there are at least $\beta|S|$ neighbors in V_2.
- The probability that for some S all its neighbors are in T is now upper bounded by ${}^{n}C_{s} \cdot {}^{n}C_{bs} \cdot (\beta s/n)^{ds}$.
- The probability is at most $(en/s)^{s} \cdot (en/\beta s)^{\beta s} \cdot (\beta s/n)^{ds}$.
- Simplifying we get, $\left[(s/n)^{d-\beta-1} \; e^{1+\beta} \; \beta^{d-\beta}\right]^{s}$.
- Use that s is at most αn, for $\alpha = 1/3$ to simplify the above to $\left[(\beta/3)^{d} \; (3e)^{1+\beta}\right]^{s}$.
- Use $d = 18$ and $\beta = 2$ to simplify to $\left[(2/3)^{18} \; (3e)^{3}\right]^{s}$.

Proof by Existence

- Condition 2: For any subset S of vertices from V_1 such that $|S|$ is at most αn, there are at least $\beta|S|$ neighbors in V_2.
- The probability that for some S all its neighbors are in T is at most $(en/s)^s \cdot (en/\beta s)^{\beta s} \cdot (\beta s/n)^{ds}$.
- Use that s is at most αn, for $\alpha = 1/3$ to simplify the above to $\left[(\beta/3)^d \ (3e)^{1+\beta}\right]^s$.
- Use d = 18 and $\beta = 2$ to simplify to $\left[(2/3)^{18} \ (3e)^3\right]^s$.
- Notice that the term in [ ] is at most 1/2. So, the entire probability is at most $(1/2)^s$.

Proof by Existence

- Condition 2: For any subset S of vertices from V_1 such that |S| is at most αn, there are at least $\beta|S|$ neighbors in V_2.
- The probability that for some S all its neighbors are in T is at most $\left[(2/3)^{18} \ (3e)^3\right]^s$.
- Notice that the term in [ ] is at most 1/2. So, the entire probability is at most $(1/2)^s$.
- We used a specific s. But, we need to show the result for all s between 1 to αn.
- Apply Boole's inequality again to get that

$$\Sigma_{s > 0} \Pr(\text{for some S all its neighbors are in T})$$

$$\leq \Sigma_{s > 0} (1/2)^s < 1$$

Proof by Existence--AnotherExample

- Consider the following claim.
- There is a bipartite graph G = (L, R, E) such that
  - $|L| = n$
  - $|R| = 2^{\log^2 n}$
  - Every subset of n/2 vertices of L has at least $2^{\log^2 n} - n$ neighbors in R.
  - No vertex of R has more than $12\log^2 n$ neighbors.
- We want to use the technique of proof by existence to show the above claim.

Proof by Existence--AnotherExample

- There is a bipartite graph G = (L, R, E) such that
  - $|L| = n$, $|R| = 2^{\log^2 n}$, . Every subset of n/2 vertices of L has at least $2^{\log^2 n} - n$ neighbors in R. No vertex of R has more than $12\log^2 n$ neighbors.
  - Let every vertex of L choose d neighbors in R independently and uniformly at random.
  - Choices are made with replacement.
  - Multiple edges are dropped in favor of one edge.

Proof by Existence--AnotherExample

- There is a bipartite graph G = (L, R, E) such that
  - $|L| = n$, $|R| = 2^{\log^2 n}$, . Every subset of n/2 vertices of L has at least $2^{\log^2 n} - n$ neighbors in R. No vertex of R has more than $12\log^2 n$ neighbors.
  - Let every vertex of L choose d neighbors in R independently and uniformly at random.
  - Let us now estimate the degree of any vertex of R.
  - Let $|R| = r$.
  - We can think of the degree of a vertex v in R as the expectation of the random variable X that indicates how many vertices in L choose v as a neighbor.
  - Each neighbor in L makes d choices, so we have nd choices in all.

Proof by Existence--AnotherExample

- There is a bipartite graph G = (L, R, E) such that
  - $|L| = n$, $|R| = 2^{\log^2 n}$, . Every subset of n/2 vertices of L has at least $2^{\log^2 n} - n$ neighbors in R. No vertex of R has more than $12\log^2 n$ neighbors.
  - Let every vertex of L choose d neighbors in R independently and uniformly at random.
  - Let $|R| = r$.
  - We can think of the degree of a vertex v in R as the expectation of the random variable X that indicates how many vertices in L choose v as a neighbor.
  - Each neighbor in L makes d choices, so we have nd choices in all.
  - Let Xi be a random variable if the ith choice is v.

Proof by Existence--AnotherExample

- Let $|R| = r$.
- We can think of the degree of a vertex v in R as the expectation of the random variable X that indicates how many vertices in L choose v as a neighbor.
- Each neighbor in L makes d choices, so we have nd choices in all.
- Let Xi be a random variable if the ith choice is v.
- $E[X_i] = 1/r$.
- $X = \Sigma X_i$ and so $E[X] = \Sigma E[X_i] = nd/r$.
- Pick $d = r.2\log^2 n /n$ so that $E[X] = 2\log^2 n$.
- Now apply Chernoff bounds on X for the event $X >= 12\log^2 n$.
- Use Boole's inequality to bound the probability of the bad event for every v in R.

Proof by Existence--AnotherExample

- There is a bipartite graph G = (L, R, E) such that
  - $|L| = n$, $|R| = 2^{\log^2 n}$, . Every subset of n/2 vertices of L has at least $2^{\log^2 n} – n$ neighbors in R.
  - Let every vertex of L choose d neighbors in R independently and uniformly at random.
  - We now move to property 1.
  - Let S be any subset of size n/2 from L.
  - Let T be any subset of R of size $2^{\log^2 n} – n$.
  - Consider the event that all the neighbors of S are in T.
  - This happens with a probability of $\left[(2^{\log^2 n} – n)/r\right]^{nd/2}$.

Proof by Existence--AnotherExample

- There is a bipartite graph G = (L, R, E) such that
  - $|L| = n$, $|R| = 2^{\log^2 n}$. Every subset of n/2 vertices of L has at least $2^{\log^2 n} - n$ neighbors in R.
  - Let S be any subset of size n/2 from L.
  - Let T be any subset of R of size $2^{\log^2 n} - n$.
  - Consider the event that all the neighbors of S are in T.
  - This happens with a probability of $\left[(r - n)/r\right]^{nd/2}$.
  - Now, consider all possible choices of S and T. The probability that for any S all its neighbors are in some T is upper bounded by: ${}^{n}C_{n/2} \cdot {}^{r}C_{r-n} \cdot \left[(r - n)/r\right]^{nd/2}$.
  - We will now show that the above probability is at most 1.

Proof by Existence--AnotherExample

- Now, consider all possible choices of S and T. The probability that for any S all its neighbors are in some T is upper bounded by: ${}^{n}C_{n/2}\,.\,{}^{r}C_{r-n}\,.\,\left[(r-n)/r\right]^{nd/2}$.
  - We will now show that the above probability is at most 1.
  - Use the (in)equalities
    - ${}^{n}C_{n-k} = {}^{n}C_{k}$ for k between 0 and n.
    - ${}^{N}c_{k}$ is at most $(en/k)^{k}$.
    - $(1+x)$ is at most e^{x} for any real number x.
  - The required probability is
  - $(2e)^{n/2}.\ (er/n)^{n}.\ (e)^{-n^{2}d/2r}$.
  - Recall that $d = 2\log^{2}n\ .\ r/n$.

Proof by Existence--AnotherExample

- Now, consider all possible choices of S and T. The probability that for any S all its neighbors are in some T is upper bounded by: ${}^{n}C_{n/2} \, . \, {}^{r}C_{r-n} \, . \, \left[(r - n)/r\right]^{nd/2}$.
  - We will now show that the above probability is at most 1.
  - Use the (in)equalities
    - ${}^{n}C_{n-k} = {}^{n}C_{k}$ for k between 0 and n.
    - ${}^{N}c_{k}$ is at most $(en/k)^{k}$.
    - $(1+x)$ is at most e^{x} for any real number x.
  - The required probability is
  - $(2e)^{n/2} . (er/n)^{n} . (e)^{-n^{2}d/2r}$.
  - Recall that $d = 2\log^{2}n \, . \, r/n$ and $\log r = \log^{2}n$ to simplify.