Advanced Counting

李昂生

Discrete Mathematics
U CAS
31 May, 2018

Outline

1. Generating functions
2. Applications
3. Inclusion-Exclusion
4. Combinatorics and probability
5. Expanding graphs
6. Lovász local lemma
7. Exercises

General view

- The **merging** of **combinatorics and probability** is powerful
- Enjoy the power of:
  Combinatorics + Probability
  Why?
  Nature evolving = Natural selection + Random variations
  Species evolution = Heredity + Variation
- Applications of the principles

Definition of generating functions

Definition 1

Given a sequence $a_0, a_1, \cdots$ of real numbers, the **generating function** of the sequence is the infinite series, given by

$$G(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{k=0}^{\infty} a_k x^k. \tag{1}$$

- Any **finite restriction** of $G(x)$ is a polynomial. Thus, generating function is the extension of polynomials
- The generating function of a finite sequence $a_0, a_1, \cdots, a_n$ is a **polynomial**

$$G(x) = a_0 + a_1 x + \cdots + a_n x^n. \tag{2}$$

Useful Facts

$$(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i = G(x) \tag{3}$$

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots, \qquad |x| < 1 \tag{4}$$

$$\frac{1}{1-ax} = 1 + ax + (ax)^2 + \cdots, \qquad |ax| < 1. \tag{5}$$

Operations

If $f(x) = \sum_{k=0}^{\infty} a_k x^k$, and $g(x) = \sum_{k=0}^{\infty} b_k x^k$, then,

$$f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k, \tag{6}$$

and

$$f(x)g(x) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) x^k. \tag{7}$$

Note: **Convergence** of the infinite series is necessary.

Extended binomial coefficients

Definition 2

Let a be a real number and k a non-negative integer. Then **the extended binomial coefficient** $\binom{a}{k}$ is defined by

$$\binom{a}{k} = \begin{cases} \frac{a(a-1)\cdots(a-k+1)}{k!}, & \text{if } k > 0 \\ 1, & \text{otherwise.} \end{cases} \tag{8}$$

The Extended Binomial Theorem

Theorem 3

Let a be a real number. Then for any real number x with $|x| < 1$,

$$(1+x)^a = \sum_{k=0}^{\infty} \binom{a}{k} x^k. \tag{9}$$

Proof.

Using Maclaurin series. □

Generating functions using binomial coefficients

$$\begin{aligned}\binom{-n}{r} &= \frac{(-n)(-n-1)\cdots(-n-r+1)}{r!} \\ &= \frac{(-1)^r(n+r-1)\cdots(n)}{r!} \\ &= (-1)^r\binom{n+r-1}{r}. \qquad (10)\end{aligned}$$

$$\begin{aligned}(1+x)^{-n} &= \sum_{k=0}^{\infty}\binom{-n}{k}x^k \\ &= \sum_{k=0}^{\infty}(-1)^k\binom{n+k-1}{k}x^k. \qquad (11)\end{aligned}$$

$$(1-x)^{-n} = \sum_{k=0}^{\infty}\binom{n+k-1}{k}x^k. \qquad (12)$$

Generating functions - continued

$$\begin{aligned}
\frac{1}{(1-x)^2} &= \sum_{k=0}^{\infty} \binom{2+k-1}{k} x^k \\
&= \sum_{k=0}^{\infty} \binom{k+1}{k} x^k \\
&= \sum_{k=0}^{\infty} (k+1) x^k. \qquad (13)
\end{aligned}$$

Constrained equation

Find the number of solutions of equation

$$y_1 + y_2 + y_3 = 17$$

subject to:
(i) $2 \leq y_1 \leq 5$,
(ii) $3 \leq y_2 \leq 6$, and
(iii) $4 \leq y_3 \leq 7$.

Solution 4

The number of solutions of the constrained equation is the coefficient of the term x^{17} in the expansion of the following function:

$$(x^2 + x^3 + x^4 + x^5)(x^3 + x^4 + x^5 + x^6)(x^4 + x^5 + x^6 + x^7).$$

Solving recurrence by generating functions

Let

$$\begin{cases} a_n = 8a_{n-1} + 10^{n-1}, \\ a_1 = 9. \end{cases} \tag{14}$$

Set $a_0 = 1$ and $G(x) = \sum_{n=0}^{\infty} a_n x^n$.

Then,

$$\begin{aligned} G(x) - 1 &= \sum_{n=1}^{\infty} a_n x^n \\ &= \sum_{n=1}^{\infty} (8a_{n-1} + 10^{n-1}) x^n \\ &= 8x \sum_{n=1}^{\infty} a_{n-1} x^{n-1} + x \sum_{n=1}^{\infty} 10^{n-1} x^{n-1} \\ &= 8xG(x) + \frac{x}{1 - 10x}. \end{aligned}$$

Solving recurrence - continued

Solving for $G(x)$,

$$\begin{aligned} G(x) &= \frac{1-9x}{(1-8x)(1-10x)} \\ &= \frac{1}{2}\left(\frac{1}{1-8x} + \frac{1}{1-10x}\right) \\ &= \frac{1}{2}\left(\sum_{n=0}^{\infty} 8^n x^n + \sum_{n=0}^{\infty} 10^n x^n\right) \\ &= \sum_{n=0}^{\infty} \frac{8^n + 10^n}{2} x^n. \end{aligned}$$

We thus have

$$a_n = (8^n + 10^n)/2.$$

Proving identity by generating functions

Prove

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

Consider $(1+x)^{2n}$. $\binom{2n}{n}$ is the coefficient of the term x^n in the expansion of $(1+x)^{2n}$.

$$\begin{aligned} (1+x)^{2n} &= ((1+x)^n)^2 \\ &= (\sum_{k=0}^{n} \binom{n}{k} x^k)^2. \end{aligned}$$

The coefficient of the term x^n is

$$\sum_{i+j=n} \binom{n}{i}\binom{n}{j} = \sum_{k=0}^{n} \binom{n}{k}^2.$$

The Principle of Inclusion-Exclusion

Theorem 5

Let $A_1, A_2, \cdots, A_n$ be finite sets. Then, for $A = \cup_{i=1}^{n} A_i$,

$$\begin{aligned} |A| &= \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| \\ &\quad + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots + \\ &\quad (-1)^{n+1} |A_1 \cap \cdots \cap A_n|. \end{aligned}$$

Continued

$$|\mathbf{A}| = \sum_{\mathbf{k=1}}^{\mathbf{n}} (-\mathbf{1})^{\mathbf{k+1}} \cdot \sum_{\mathbf{1 \le i_1 < i_2 < \cdots < i_k \le n}} |\mathbf{A_{i_1}} \cap \cdots \cap \mathbf{A_{i_k}}|. \qquad (15)$$

Proof

We show that every element $a \in A$ contributes exactly 1 to the right-hand side of Equation (15).
Fix $a \in A$, suppose without loss of the generality that for r with $1 \leq r \leq n$,
(i) for each i with $1 \leq i \leq r$, $a \in A_i$, and
(ii) for each j with $r < j \leq n$, $a \notin A_j$.
Then for $k = 1$, the element a contributes $(-1)^2 \binom{r}{1}$ to the first term $(-1)^{1+1} \sum_{1 \leq i_1 \leq n} |A_{i_1}|$.
Generally, for $k \leq r$, the element a contributes exactly $(-1)^{k+1} \binom{r}{k}$ to the term

$$(-1)^{k+1} \cdot \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} |A_{i_1} \cap \cdots \cap A_{i_k}|. \tag{16}$$

Proof - continued

Let

$$\mathbf{I(a) = \sum_{k=1}^{r} (-1)^{k+1} \binom{r}{k}}. \tag{17}$$

Then $I(a)$ **is the contribution of element** a **to the right-hand side of Equation (15)**. Note that

$$0 = (1-1)^r = \sum_{k=0}^{r} (-1)^k \binom{r}{k} = \binom{r}{0} - I(a). \tag{18}$$

Therefore,

$$\mathbf{I(a) = \binom{r}{0} = 1}. \tag{19}$$

The theorem follows.

Counting of **onto maps**

Theorem 6

Let m and n be positive integers with $m \geq n$. Then, there are

$$\sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} (n-k)^m, \tag{20}$$

onto maps from $[m]$ to $[n]$.

Proof

For every r with $0 \leq r \leq n$, the number of functions from $[m]$ to $[r]$ is r^m.
For each i, $1 \leq i \leq n$, let B_i be the set of functions f from $[m]$ to $[n]$ such that $f^{-1}(i) = \emptyset$, i.e., the i-th box is empty.
Let $B = B_1 \cup \cdots \cup B_n$. Then

- The number of onto maps from $[m]$ to $[n]$ is $|\bar{B}|$.
- The number of functions from $[m]$ to $[n]$ is n^m.

Proof - continued

By the Inclusion-Exclusion principle,

$$\begin{aligned} |B| &= \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |B_{i_1} \cap \cdots \cap B_{i_k}| \\ &= \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)^m. \end{aligned}$$

Therefore, the number of onto maps is

$$\begin{aligned} N &= n^m - \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)^m \\ &= \sum_{k=0}^{n} (-1)^{k} \binom{n}{k} (n-k)^m. \end{aligned}$$

Stirling Number of the Second Type

- $S(m, n)$:
  The number of ways to distribute m **distinguishable** objects into n **indistinguishable** boxes so that no box is empty.
- $M(m, n)$:
  The number of onto maps from $[m]$ to $[n]$.

$$M(m, n) = n! \cdot S(m, n). \tag{21}$$

$$S(m, n) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \frac{(n-k)^m}{n!}. \tag{22}$$

Derangements

Definition 7

A *derangement* is a permutation of objects that leaves no object in its original position.

Let D_n be the number of derangements of n objects.

Theorem 8

Set $0! = 1$.

$$D_n = n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!} \tag{23}$$

Proof

Given $[n]$, for each $i \in [n]$, let A_i be the set of permutations p such that $p(i) = i$, and let $A = A_1 \cup \cdots \cup A_n$.
By the Inclusion-Exclusion principle,

$$|A| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < \cdots < i_k \le n} |A_{i_1} \cap \cdots \cap A_{i_k}|.$$

For $i_1 < \cdots < i_k$,

$$|A_{i_1} \cap \cdots \cap A_{i_k}| = (n-k)!.$$

Therefore,

$$\begin{aligned} |A| &= \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)! \\ &= n! \sum_{k=1}^{n} (-1)^{k-1} \frac{1}{k!}. \end{aligned}$$

Proof - continued

$$\begin{aligned} D_n &= n! - |A| \\ &= n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!}. \end{aligned}$$

$\phi(n)$

Given natural number $n > 1$, let

$$n = p_1^{l_1} \cdots p_k^{l_k}$$

be a prime factoring of n such that all p_i's are distinct. Then

$$\phi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}).$$

Proof

For each i, $1 \leq i \leq k$, let A_i be the set of natural numbers m such that $1 \leq m < n$ and $p_i | m$, and let $A = A_1 \cup \cdots \cup A_k$. Then for every x, $1 \leq x \leq n$, x and n coprime if and only if for all i, $x \notin A_i$, i.e., $x \notin A$. Therefore,

$$\phi(n) = n - |A|. \tag{24}$$

Proof - continued

By the Inclusion-Exclusion principle,

$$\begin{aligned}
|A| &= \sum_{l=1}^{k}(-1)^{l-1} \sum_{1\le i_1<\cdots<i_l\le k} |A_{i_1}\cap\cdots\cap A_{i_l}| \\
&= \sum_{l=1}^{k}(-1)^{l-1} \sum_{1\le i_1<\cdots<i_l\le k} \left\lfloor \frac{n}{p_{i_1}\cdots p_{i_l}} \right\rfloor \\
&= n\left[\sum_{l=1}^{k}(-1)^{l-1} \sum_{1\le i_1<\cdots<i_l\le k} \frac{1}{p_{i_1}\cdots p_{i_l}}\right] \\
&= n\left[\sum_{l=1}^{k}(-1)^{l-1} \sum_{1\le i_1<\cdots<i_l\le k} \frac{1}{p_{i_1}\cdots p_{i_l}}\right].
\end{aligned}$$

Proof - continued

$$
\begin{aligned}
\phi(n) &= n - |A| \\
&= n + n\left[\sum_{l=1}^{k}(-1)^l \sum_{1\le i_1<\cdots<i_l\le k} \frac{1}{p_{i_1}\cdots p_{i_l}}\right] \\
&= n\left(1 + \sum_{1\le i_1<\cdots<i_l\le k}(-1)^l \frac{1}{p_{i_1}\cdots p_{i_l}}\right) \\
&= n\prod_{l=1}^{k}(1-\frac{1}{p_l}).
\end{aligned}
$$

The power of the merging of combinatorics and probability

- The power comes from the merging of combinatorics and probability
- The future source for CS

Randomized Polynomial Time Algorithms RP

A language $L \subset \Sigma^*$ is in **RP**, if there is randomized polynomial time algorithm A such that A runs in polynomial time and for every instance $x \in \Sigma^*$,

- (Completeness) If $x \in L$, then

$$\Pr_r[A(x, r) = 1] \geq \frac{1}{2}$$

- (Soundness) If $x \notin L$, then

$$\Pr_r[A(x, r) = 1] = 0,$$

where r is the random bits used by the algorithm A such that $|r| = n^{O(1)}$, $n = |x|$.

Restate of **RP**

Let Σ be an alphabet and L be a language over Σ. Suppose that A is a randomized polynomial time algorithm that decides L. Then, there is a prime p such that for every $x \in \Sigma^*$,

(1) If $x \in L$, $A(x, r)$ holds for at least half of the possible values of $r \in \mathbb{Z}_p$.

(2) If $x \notin L$, then for any $r \in \mathbb{Z}_p$, $A(x, r) = 0$.

Therefore, for a randomly chosen $r \in \mathbb{Z}_p$,

- If $A(x, r) = 1$, then $x \in L$ and r is a *witness* (or *certificate*) of $x \in L$.
- If $A(x, r) = 0$, then r is an *evidence* that it is possible that $x \notin L$.

Amplifying Probability

The fact is: if $x \in L$, then

- For a randomly chosen $r \in \mathbb{Z}_p$, it is possible that $A(x, r) = 0$, in which case, an *error* occurs.
- However, the probability that an error occurs is at most $\frac{1}{2}$.

To reduce the probability of errors, we repeat the algorithms independently for a number of times. The randomized algorithm with repetition, denoted by $\mathcal{A}$, proceeds as follows: Let $t > 1$ be a number,

1. Pick t random values $r_1, r_2, \cdots, r_t$ independently and randomly from $\mathbb{Z}_p$,
2. If there is an i, $1 \leq i \leq t$ such that $A(x, r_i) = 1$, then accept, and reject, otherwise.

Proof

Completeness: $x \in L$. Then,

$$\Pr[\mathcal{A} \text{ accepts}] \geq 1 - \frac{1}{2^t}.$$

Note: to make sure that $1 - \frac{1}{2^t} \approx 1$, we may take $t = n$, where $n = |x|$.

Soundness: $x \notin L$. Then,

$$\Pr[\mathcal{A} \text{ accepts}] = 0.$$

However, the number of random bits used is:

$$O(t \cdot \log p),$$

where p is usually a prime of length $m = n^{O(1)}$.

Question: How to reduce the number of random bits?

Why? Is RP=P? A big challenge.

Possible approach: for the typical problems that are currently known to be in RP, try to prove they are actually in P.

Pairwise Independence

We may reduce the number of bits based on a pairwise independency.

1. Pick independently and randomly $a, b \in \mathbb{Z}_p$.
2. For i, $1 \leq i \leq t$, let

$$r_i = a \cdot i + b, \quad i \in \mathbb{Z}_p.$$

3. If there is an i such that $A(x, r_i) = 1$, then accept, and reject, otherwise.

The number of random bits used is:

$$2 \log p.$$

Proof

Lemma 9

1. $\{r_1, r_2, \cdots, r_t\}$ *are pairwise independent.*
2. $\{A(x, r_i) \mid 1 \leq i \leq t\}$ *are pairwise independent.*

Proof

For the first item: given $i \neq j$, y_i and y_j,
If

$$a \cdot i + b = y_i$$

and

$$a \cdot j + b = y_j$$

we can solve a and b.

Proof - continued

For any α, β, let S be the set of all r such that $A(x, r) = \alpha$, and T be the set of all r such that $A(x, r) = \beta$.
Let $p_\alpha = \frac{|S|}{p}$ and $p_\beta = \frac{|T|}{p}$.
The probability that $r_i = a \cdot i + b$ and $A(x, r_i) = \alpha$ is

$$p_\alpha \frac{1}{p}$$

By the same reason, the probability that for $r_j = aj + b$, $A(x, r_j) = \beta$ is

$$p_\beta \frac{1}{p}$$

By item 1, the probability that for $r_i = ai + b$ and $r_j = aj + b$, $A(x, r_i) = \alpha$ and $A(x, r_j) = \beta$ hold simultaneously, is that

$$p_\alpha p_\beta \frac{1}{p^2}.$$

Proof - continued

Let $Y = \sum_{i=1}^{t} A(x, r_i)$.

Assume $x \in L$. Then,

$$E[A(x, r_i)] \geq \frac{1}{2}, \quad E[Y] \geq \frac{t}{2}.$$

$$\sigma_Y^2 = \sum_{i=1}^{t} \sigma_{A(x,r_i)}^2 \leq \frac{1}{4}t,$$

$$\sigma_Y \leq \frac{\sqrt{t}}{2}.$$

By the Chehyshev inequality, the probability that x is rejected is

$$\Pr[Y = 0] = \Pr[|Y - E[Y]| \geq \frac{t}{2}] \leq \frac{1}{t}.$$

(n, d, α, c)-Concentrator

Definition 10

An (n, d, α, c)-*concentrator* is a bipartite multigraph $G = (L, R, E)$ with $|L| = |R| = n$, where L and R are independent sets such that

1. For every $v \in L$, the degree of v is $d(v) \leq d$.
2. For any $S \subset L$, if $|S| \leq \alpha n$, then

$$|E(S, R)| \geq c \cdot |S|,$$

where $E(X, Y)$ is the set of edges between vertices in X and the vertices in Y.

Background: Telephone switching networks

Existence of concentrator

Theorem 11

There exist constants d, α, c and n_0, such that for any $n > n_0$, there is an (n, d, α, c)-concentrator.

The construction

The construction of G proceeds as follows:

1. Let L and R be sets of n vertices.
2. For every vertex $x \in L$, pick randomly and uniformly d vertices $y_1, \cdots, y_d$ in R, create links (x, y_i) for each i, $1 \leq i \leq d$.
3. Keep one copy for all multiple edges.

We will show that G is an (n, d, α, c)-concentrator for some d, α and c and for sufficiently large n.
For s with $1 \leq s \leq n$, define

$$\mathcal{E}_s$$

to be the subset of s vertices of L that has fewer than cs neighbors in R.

Proof

For any subset $S \subset L$ of size s and any subset $T \subset R$ of size cs.

- The number of subsets $S \subset L$ of size s is $\binom{n}{s}$.
- The number of subsets $T \subset R$ of size cs is $\binom{n}{cs}$.
- The probability that T contains all the neighbors of the vertices in S is

$$(\frac{cs}{n})^{ds}.$$

Proof - continued

Therefore, the probability that all the edges from a subset of L of size s fall within a set of R of size $< cs$, is bounded by

$$\begin{aligned}
\Pr[\mathcal{E}_s] &\leq \binom{n}{s}\binom{n}{cs}\left(\frac{cs}{n}\right)^{ds} \\
&\leq \left(\frac{ne}{s}\right)^{s}\cdot\left(\frac{ne}{cs}\right)^{cs}\cdot\left(\frac{cs}{n}\right)^{ds}, \text{ using } \binom{n}{k} \leq \left(\frac{ne}{k}\right)^{k} \\
&= \left[\left(\frac{s}{n}\right)^{d-c-1}\cdot e^{1+c}\cdot c^{d-c}\right]^{s} \\
&\leq \left[\left(\frac{1}{3}\right)^{d-c-1}\cdot e^{1+c}\cdot c^{d-c}\right]^{s}, \text{ using } s \leq \alpha n.
\end{aligned}$$

Proof - continued

Choosing c and d such that

$$(\frac{1}{3})^{d-c-1} \cdot e^{1+c} \cdot c^{d-c} = r < \frac{1}{2}.$$

Then

$$\Pr[\mathcal{E}_s] \leq r^s.$$

Hence,

$$\sum_{s \geq 1} \Pr[\mathcal{E}_s] \leq \sum_{s \geq 1} r^s = \frac{r}{1-r} < 1.$$

Therefore, with probability $p > 0$ such that for any $S \subset L$, if $|S| = s \leq \alpha n$, then

$$|E(S, R)| > c|S|.$$

Stronger version of concentrators

Theorem 12

For n sufficiently large, there is a bipartitle graph $G = (L, R, E)$ satisfying:

(1) $|L| = n$, $|R| = 2^{\log^2 n}$.

(2) *Every subset $S \subset L$, if $|S| = \frac{n}{2}$, then*

$$|\Gamma(S)| \geq 2^{\log^2 n} - n,$$

where $\Gamma(X)$ is the set of neighbor vertices of the vertices in X.

(3) *For every $y \in R$, the degree of y is $d(y) \leq 12 \log^2 n$.*

The construction of G

1. Fix n nodes in L, $2^{\log^2 n}$ nodes in R.
2. For every $x \in L$, create $d = \frac{2^{\log^2 n} \cdot 4 \log^2 n}{n}$ edges from x to nodes in R, each of which is chosen independently at random.

Let G be a random graph generated as above. Then,
(i) The probability that (2) fails to hold is $< \frac{1}{2}$.
(ii) The probability that (3) fails to hold is $< \frac{1}{2}$.

For (2)

The probability that (2) fails to hold is at most

$$
\begin{aligned}
\Pr[\text{(2) fails}] &\leq \binom{n}{\frac{n}{2}} \binom{2^{\log^2 n}}{n} (1 - \frac{n}{2^{\log^2 n}})^{d \cdot \frac{n}{2}} \\
&\leq (\frac{ne}{\frac{n}{2}})^{\frac{n}{2}} (\frac{2^{\log^2 n} e}{n})^n (\exp(-n/2^{\log^2 n}))^{d\frac{n}{2}} \\
&= (2e)^{\frac{n}{2}} \cdot (\frac{e \cdot 2^{\log^2 n}}{n})^n e^{-\frac{n}{2^{\log^2 n}} d \frac{n}{2}}, \text{ using } 1 - x \leq e^{-x} \\
&= \left[2e \cdot (\frac{e \cdot 2^{\log^2 n}}{n})^2 \cdot e^{-\frac{n}{\log^2 n} \cdot d} \right]^{\frac{n}{2}} \\
&< \frac{1}{2}.
\end{aligned}
$$

For (3)

For every $y \in R$,

$$\mu = E[d(y)] = 4\log^2 n.$$

By Chernoff bound, for $\delta = 2$,

$$\begin{aligned} \Pr[d(y) > (1+2)\mu] &< \left[\frac{e^{\delta}}{(1+2)^{1+2}}\right]^{\mu} \\ &= \left[\frac{e^2}{3^3}\right]^{4\log^2 n} \\ &< \frac{1}{2}. \end{aligned}$$

Probability Amplification

1) Pick randomly a vertex $y \in R$, using $\log^2 n$ bits,
2) Let $r_1, r_2, \cdots, r_k$ be all the neighbors of y that are in L.
3) If there is an i such that $A(x, r_i) = 1$, then accept, else, reject.

Note:

$$k \leq 12 \log^2 n.$$

Proof

Assume $x \in L$.
Let S be the set of witnesses r such that $A(x, r) = 1$. Then $|S| \geq \frac{n}{2}$. Therefore, there are at least $2^{\log^2 n} - n$ elements in R. each of which has a neighbor in L that is a witness of $x \in L$. Therefore, the probability that the algorithm rejects is at most

$$1 - \frac{2^{\log^2 n} - n}{2^{\log^2 n}} = \frac{n}{2^{\log^2 n}}.$$

Intuition

Suppose that we have n events, each of which occurs with probability at most $\frac{1}{2}$.
If the events are all independent, then with probability $\geq 2^{-n}$, none of them occurs.
The Lovász local lemma generalises this fact so that the condition can be relaxed as:
Each event is independent of all but a small number of other events.

Dependency Graph

Let $\mathcal{E}_i$, $1 \leq i \leq n$, be events in a probability space.
Recall that $\mathcal{E}_i$ is mutually independent of a set S of events, if:

$$\Pr[\mathcal{E}_i \mid \cap_{i \in T} \mathcal{E}_j] = \Pr[\mathcal{E}_i],$$

for any subset $T \subseteq S^+$, where $S^+ = \{\mathcal{E}_j, \bar{\mathcal{E}}_j \mid \mathcal{E}_j \in S\}$.
The *dependency graph* $G = (V, E)$ is defined as follows:

1) $v \in V$ represents an event $\mathcal{E}_i$.
2) For any $\mathcal{E}_i$, $\mathcal{E}_j$, if $\{\mathcal{E}_i, \mathcal{E}_j\} \notin E$, then $\mathcal{E}_i$ is mutually independent of $\mathcal{E}_j$.

The Lemma

Theorem 13

(Lovász local lemma) Let $G = (V, E)$ be a dependency graph for events $\mathcal{E}_1, \cdots, \mathcal{E}_n$ in a probability space. Suppose that there are $x_i \in [0, 1]$ for all i with $1 \leq i \leq n$ such that for each i

$$\Pr[\mathcal{E}_i] \leq x_i \prod_{(i,j)\in E} (1 - x_j).$$

Then,

$$\Pr[\cap_{i=1}^{n} \bar{\mathcal{E}}_i] \geq \prod_{i=1}^{n} (1 - x_i).$$

Proof

First, we show the following:
For any $S \subseteq [n]$ and any $i \notin S$,

$$\Pr[\mathcal{E}_i \mid \cap_{j \in S} \bar{\mathcal{E}}_j] \leq x_i.$$

By induction on $|S|$.
$|S| = 0$. By the assumption.
For $S \neq \emptyset$ and $i \notin S$.
Let

$$S_1 = \{j \in S \mid (i,j) \in E\}$$

$$S_2 = S \setminus S_1.$$

Proof - continued

By the definition of conditional probability,

$$\Pr[\mathcal{E}_i \mid \cap_{j\in S} \bar{\mathcal{E}}_j] = \frac{\Pr[\mathcal{E}_i \cap (\cap_{j\in S_1} \bar{\mathcal{E}}_j) \mid \cap_{m\in S_2} \bar{\mathcal{E}}_m]}{\Pr[\cap_{j\in S_1} \bar{\mathcal{E}}_j \mid \cap_{m\in S_2} \bar{\mathcal{E}}_m]}.$$

For the numerator,

$$\begin{aligned}
& \Pr[\mathcal{E}_i \cap (\cap_{j\in S_1} \bar{\mathcal{E}}_j) \mid \cap_{m\in S_2} \bar{\mathcal{E}}_m] \\
\leq\ & \Pr[\mathcal{E}_i \mid \cap_{m\in S_2} \bar{\mathcal{E}}_m] \\
=\ & \Pr[\mathcal{E}_i], \text{ since } \mathcal{E}_i \text{ is mutually independent of events in } S_2 \\
\leq\ & x_i \prod_{(i,j)\in E} (1 - x_j).
\end{aligned}$$

Proof - continued

For the denominator, let $S_1 = \{j_1, j_2, \cdots, j_r\}$.
If $r = 0$, $\Pr[\cap_{j \in S_1} \bar{\mathcal{E}}_j \mid \cap_{m \in S_2} \bar{\mathcal{E}}_m] = 1$.
If $r > 0$, then by inductive hypothesis,

$$\begin{aligned} & \Pr[\cap_{j \in S_1} \bar{\mathcal{E}}_j \mid \cap_{m \in S_2} \bar{\mathcal{E}}_m] \\ = \; & \Pr[\bar{\mathcal{E}}_{j_1} \mid \cap_{m \in S_2} \bar{\mathcal{E}}_m] \cdot \Pr[\bar{\mathcal{E}}_{j_2} \mid \bar{\mathcal{E}}_{j_1} \cap \cap_{m \in S_2} \bar{\mathcal{E}}_m] \cdots \\ & \Pr[\bar{\mathcal{E}}_{j_r} \mid \bar{\mathcal{E}}_{j_1} \cap \cdots \cap \bar{\mathcal{E}}_{j_{r-1}} \cap (\cap_{m \in S_2} \bar{\mathcal{E}}_m)] \\ \geq \; & (1 - x_{j_1}) \cdots (1 - x_{j_r}) \geq \prod_{(i.j) \in E} (1 - x_j). \end{aligned}$$

Proof - continued

Therefore,

$$\Pr[\mathcal{E}_i \mid \cap_{j\in S}\bar{\mathcal{E}}_j] \leq \frac{x_i \prod_{(i,j)\in E}(1-x_j)}{\prod_{(i,j)\in E}(1-x_j)} = x_i.$$

Finally,

$$\begin{aligned} & \Pr[\cap_{i=1}^{n}\bar{\mathcal{E}}_i] \\ = \; & \Pr[\bar{\mathcal{E}}_1]\cdot\Pr[\bar{\mathcal{E}}_2 \mid \bar{\mathcal{E}}_1]\cdot\cdots\Pr[\bar{\mathcal{E}}_n \mid \bar{\mathcal{E}}_{n-1},\cdots,\bar{\mathcal{E}}_2,\bar{\mathcal{E}}_1] \\ \geq \; & (1-x_1)(1-x_2)\cdots(1-x_n) \\ = \; & \prod_{i=1}^{n}(1-x_i). \end{aligned}$$

Exercises - 1

(1) Prove the inclusion-exclusion principle by using mathematical induction.

(2) Let D_n be the number of derangements of n objects. Show that: For $n \geq 1$,

a)

$$D_n = (n-1)(D_{n-1} + D_{n-2})$$

b)

$$D_n = nD_{n-1} + (-1)^n$$

Exercises - 2

(3) Show that for a natural number n,

$$n! = \sum_{i=0}^{n} \binom{n}{i} \cdot D_{n-i},$$

where D_k is the number of derangements of k objects.

(4) Describe a formula to count the number of primes not exceeding the natural number n by using the inclusion-exclusion principle.

(5) Solve the recurrence relation

$$a_n = a_{n-1}^3 \cdot a_{n-2}^2,$$
$$a_0 = 2,\ a_1 = 2.$$

谢谢！