Discrete mathematics

1 | Generating functions and recurrence relations

Generating functions

Definition 1.1. Let (a_n) be a sequence of real numbers. We define its *ordinary generating function* as the following formal power series:

$$a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots = \sum_{n=0}^{\infty} a_n x^n.$$

Proposition 1.2. Let $\sum_{n=0}^{\infty} a_n x^n, \sum_{n=0}^{\infty} b_n x^n$ be two formal power series. Then:

- $\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n)x^n$.
- $\lambda \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} \lambda a_n x^n$.
- $\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty} (a_0b_n + a_1b_{n-1} + \cdots + a_nb_0)x^n$.
- $\left(\sum_{n=0}^{\infty} a_n x^n\right)' = \sum_{n=1}^{\infty} na_n x^{n-1}$.

Proposition 1.3 (Closed forms). We can write the following ordinary generating functions with their corresponding closed forms:

- $\sum_{n=0}^{N} x^n = \frac{1 - x^{N+1}}{1 - x}$.
- $\sum_{n=0}^{\infty} x^n = \frac{1}{1 - x}$.
- $\sum_{n=0}^{\infty} \binom{n+k-1}{n} x^n = \left(\frac{1}{1-x}\right)^k$.

Proposition 1.4. Suppose A and B are two finite disjoint sets. We set some restrictions for the non-ordered selection of elements of $A \cup B$. For every $n \geq 0$, let:

- a_n be the number of non-ordered selection of n elements of A satisfying the restrictions,
- b_n be the number of non-ordered selection of n elements of B satisfying the restrictions,
- c_n be the number of non-ordered selection of n elements of $A \cup B$ satisfying the restrictions.

And let $f(x)$, $g(x)$, $h(x)$ be the ordinary generating functions of (a_n), (b_n), (c_n), respectively. Then we have:

$$h(x) = f(x)g(x).$$

Definition 1.5. Let (a_n) be a sequence of real numbers. We define its *exponential generating function* as the following formal power series:

$$a_0 + a_1x + a_2\frac{x^2}{2!} + a_3\frac{x^3}{3!} + \cdots = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}.$$

Definition 1.6. Let (a_n) be a sequence of real numbers such that $a_i = 1\ \forall i$. Then its exponential generating function associated is the so called *exponential series*:

$$\mathrm{e}^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Proposition 1.7. The exponential series has the following properties:

1. $\mathrm{e}^{x+y} = \mathrm{e}^x\mathrm{e}^y\ \forall x, y \in \mathbb{R}$.
2. $(\mathrm{e}^x)^n = \mathrm{e}^{nx}\ \forall x, n \in \mathbb{R}$.

Proposition 1.8. Suppose A and B are two finite disjoint sets. We set some restrictions for the ordered selection of elements of $A \cup B$. For every $n \geq 0$, let:

- a_n be the number of ordered selection of n elements of A satisfying the restrictions,
- b_n be the number of ordered selection of n elements of B satisfying the restrictions,
- c_n be the number of ordered selection of n elements of $A \cup B$ satisfying the restrictions.

And let $f(x)$, $g(x)$, $h(x)$ be the exponential generating functions of (a_n), (b_n), (c_n), respectively. Then we have:

$$h(x) = f(x)g(x).$$

Recurrence relations

Definition 1.9. Let (a_n) be a sequence of real numbers. A *recurrence relation of order k for (a_n)* is an expression that express a_n in terms of k consecutive terms of the sequence, $a_{n-1}, \ldots, a_{n-k}$, for $k \leq n$. We say a sequence is *recurrent* if it satisfies a recurrence relation or, equivalently, if it's a solution of the recurrence relation.

Definition 1.10. The *initial values* of a recurrence relation of order k are the values of the first k terms for which the recurrence relation is still not valid, that is, the values $a_0, a_1, \ldots, a_{k-1}$.

Lemma 1.11. The solution of a recurrence relation of order k with k initial conditions is unique.

Definition 1.12. A *linear recurrence relation of order k* is a recurrence relation that can be written as the form

$$a_n + c_1a_{n-1} + \cdots c_ka_{n-k} = g(n)$$

where $c_1, \ldots c_k \in \mathbb{R}, c_k \neq 0$ and $g : \mathbb{N} \to \mathbb{N}$ is an arbitrary function.

Definition 1.13. We say a linear recurrence relation is *homogeneous* if $g(n) = 0$, that is, if it's of the form:

$$a_n + c_1 a_{n-1} + \cdots c_k a_{n-k} = 0, \quad \text{with } c_k \neq 0.$$

Proposition 1.14. The general solution to a recurrence relation

$$a_n + c_1 a_{n-1} + \cdots c_k a_{n-k} = g(n)$$

can be expressed as

$$(a_n^{\text{part}}) + (a_n^{\text{hom}}),$$

where (a_n^{part}) is a particular solution of the recurrence relation and (a_n^{hom}) is the general solution of its associated homogeneous recurrence relation.

Proposition 1.15. Given $c_1, \ldots, c_k \in \mathbb{R}$, the set of sequences that are solution of the homogeneous linear recurrence relation $a_n + c_1 a_{n-1} + \cdots + c_k a_{n-k} = 0$ form a real vector space.

Definition 1.16. Let $a_n + c_1 a_{n-1} + \cdots + c_k a_{n-k} = 0$ be a homogeneous linear recurrence relation of order k. The *characteristic polynomial* of the recurrence is:

$$x^k + c_1 x^{k-1} + \cdots + c_k = 0.$$

Proposition 1.17. Consider an homogeneous linear recurrence relation with characteristic polynomial

$$(x - r_1)(x - r_2) \cdots (x - r_k) = 0$$

where $r_1, \ldots, r_k \in \mathbb{C}$ are different complex numbers. Then the general term of the sequences that satisfy the recurrence relation is

$$a_n = \lambda_1 r_1^n + \cdots + \lambda_k r_k^n$$

for arbitrary numbers $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$.

2 | Graph theory

Definition 1.18. A *graph* G is an structure based on a set $V(G)$ of vertices and a set $E(G)$ of edges, which are non-ordered pairs of vertices.

Definition 1.19. Let G be a graph. The *order of* G is $n = |V(G)|$ and the *size of* G is $m = |E(G)|$.

Definition 1.20. Let G be a graph. Two vertices $a, b \in V(G)$ are said to be *adjacent* to one another if exists an edge $e \in E(G)$ that connects them. In this case we say the edge e is *incident* on vertices a and b.

Definition 1.21. An edge that connects a vertex with itself is called a *loop*.

Definition 1.22. Two or more edges incidents with the same vertices are called *multiple edges*.

Definition 1.23. A graph G is *finite* if $V(G)$ and $E(G)$ are finite.

Definition 1.24. A graph is *simple* if it has neither multiples edges nor loops.

Definition 1.25. A *complete graph* is a graph in which each pair of different vertices is joined by an edge. We denote by K_n the complete graph of order n.

Definition 1.26. Let G be a finite graph. The *degree of a vertex* is the number of edges that are incident to it. If $v \in V(G)$ we denote the degree of v by $\deg v$ or $\deg_G v$[1].

Lemma 1.27 (Handshaking lemma). For every graph G we have:

$$\sum_{v \in V(G)} \deg v = 2|E(G)|.$$

Corollary 1.28. In any graph, the number of odd-degree vertices is even.

Definition 1.29. Let G be a graph with $V(G) = \{v_1, \ldots, v_n\}$. The *degree sequence of* G is the decreasing sequence

$$(\deg v_{i_1}, \ldots, \deg v_{i_n}).$$

Definition 1.30. We say a graph G is k*-regular* if $\deg v = k \ \forall v \in V(G)$.

Definition 1.31. Let G be a graph. A graph F is an *induced subgraph of* G if $V(F) \subseteq V(G)$ and $E(F) \subseteq E(G)$.

Definition 1.32. A *walk of length* k in a graph G is a sequence of vertices $(u_1, \ldots, u_k)$ where $u_i u_{i+1} \in E(G)$ for $i = 1, \ldots, k-1$.

Definition 1.33. A walk in a graph is *closed* if it starts and ends in the same vertex.

Definition 1.34. A walk in a graph is a *trail* if all the edges of the walk are distinct.

Definition 1.35. A walk in a graph is a *path* if all the vertices (and therefore the edges) of the walk are distinct.

Definition 1.36. A closed walk in a graph is a *closed trail* if all the edges of the closed walk are distinct.

Definition 1.37. A closed path is called a *cycle*.

Proposition 1.38. Let G be a graph. Given $u, v \in V(G)$, there exists a walk between u and v if and only if there exists a path between u and v.

Definition 1.39. Let G be a graph. Given $u, v \in V(G)$, we say that u and v are connected if there is a path in G between u and v.

Proposition 1.40. The relation $u \sim v$ if and only if u and v are connected is an equivalence relation. The equivalent classes are the *connected components of* G.

Definition 1.41. A graph G is *connected* if $\forall u, v \in V(G)$, u and v are connected.

Definition 1.42. A graph G is *bipartite* if $V(G) = X \sqcup Y$ and $\forall e \in E(G)$ we have $e = xy$ with $x \in X$ and $y \in Y$.

Definition 1.43. Let G be a graph such that $E(G) \neq \emptyset$. Take an edge $e \in E(G)$. We denote by $G - e$ the induced graph of G such that

$$V(G - e) = V(G) \qquad E(G - e) = E(G) \setminus \{e\}.$$

[1] Observe that with this definition every loop counts as two edges.

Definition 1.44. Given a connected graph G, we say that $e \in E(G)$ is a *bridge of* G if $G - e$ is non-connected.

Proposition 1.45. Let G be a connected graph. $e \in E(G)$ is a bridge if and only if e doesn't belong to any cycle of G.

Definition 1.46. Let G be a connected graph. An *Eulerian trail* in G is a trail that contain all the edges of G. An *Eulerian circuit* in G is a closed Eulerian trail. G is called *Eulerian* if it admits an eulerian circuit.

Theorem 1.47 (Euler theorem). Let G be a connected graph. G is Eulerian $\iff \deg v = 2k\ \forall v \in V(G),\ k \in \mathbb{N}$.

Definition 1.48. Let G be a graph of order n with $V(G) = \{v_1, \dots, v_n\}$. We define the *adjacency matrix of* G, $\mathbf{A}(G) \in \mathcal{M}_n(\mathbb{R})$, as a_{ij} to be the number of edges incident with v_i and v_j.

Proposition 1.49. Let G be a graph of order n with $V(G) = \{v_1, \dots, v_n\}$ and let $\mathbf{A}(G) = (a_{ij})$ be the adjacency matrix of G. Then:

1. $\mathbf{A}(G)$ is symmetric.
2. $\displaystyle\sum_{j=1}^{n} a_{jk} = \sum_{j=1}^{n} a_{kj} = \deg v_k, \quad k = 1, \dots, n.$
3. For $k \in \mathbb{N}$, consider $\mathbf{A}(G)^k = (b_{ij}^k)$. Then b_{ij}^k is equal to the number of walks of length k between vertices v_i and v_j.

Definition 1.50. A *tree* is an acyclic connected graph, that is, a connected graph that has no cycles.

Definition 1.51. Let T be a tree. A *leave* of T is a vertex of degree 1.

Definition 1.52. Let G be a graph. A *generator tree* is a induced subgraph T of G such that $|V(G)| = |V(T)|$ and T is a tree.

Proposition 1.53. Let G be a graph such that $|V(G)| = n \geq 2$. The following are equivalent:

1. G is a tree.
2. G is connected and every edge of G is a bridge.
3. G is connected and $|E(G)| = n - 1$.
4. G is acyclic and $|E(G)| = n - 1$.
5. For $v_i, v_j \in V(G)$, $i \neq j$, there exists a unique path between v_i, v_j.
6. G is acyclic but adding a new edge creates exactly one cycle.

Definition 1.54. Let G be a connected graph. G is called *traversable* if admits an Eulerian trail.

Theorem 1.55. Let G be a connected graph. G is traversable if and only if G has exactly to odd-degree vertices.

Definition 1.56. Two graphs G, H are said to be *isomorphic* if exists a bijective map $f : V(G) \to V(H)$ such that $vv' \in E(G) \iff f(v)f(v') \in E(H)$.

Proposition 1.57. Two finite isomorphic graphs have the same order, size and degree sequence.

Theorem 1.58. Two graphs G, H are isomorphic if and only if exists a permutation matrix $\mathbf{P}$ such that

$$\mathbf{P}\mathbf{A}(G)\mathbf{P}^{\mathrm{T}} = \mathbf{A}(H)$$

where $\mathbf{A}(G)$, $\mathbf{A}(H)$ are adjacency matrices of G, H, respectively.

3 | Linear programming

Definition 1.59. Given vectors $\mathbf{c}, \mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, $\mathbf{b} \in \mathbb{R}^m$ and a matrix $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$, we define the *linear programming to maximize*[2] as

$$\text{LP} = \begin{cases} \text{max :} & z = \mathbf{c}^{\mathrm{T}}x & \textit{(objective function)} \\ \text{subject to :} & \mathbf{A}x \lesseqqgtr \mathbf{b} & \textit{(restrictions)} \\ & \mathbf{u} \leq x \leq \mathbf{v} & \end{cases}$$

Definition 1.60. Given vectors $\mathbf{c}, \mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, $\mathbf{b} \in \mathbb{R}^m$ and a matrix $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$, we define the *canonical form of a linear programming to maximize* as

$$\text{LP} = \begin{cases} \text{max :} & z = \mathbf{c}^{\mathrm{T}}x & \textit{(objective function)} \\ \text{subject to :} & \mathbf{A}x \leq \mathbf{b} & \textit{(restrictions)} \\ & \mathbf{u} \leq x \leq \mathbf{v} & \end{cases}$$

Analogously we define the *canonical form of a linear programming to minimize* as

$$\text{LP} = \begin{cases} \text{min :} & z = \mathbf{c}^{\mathrm{T}}x \\ \text{subject to :} & \mathbf{A}x \geq \mathbf{b} \\ & \mathbf{u} \leq x \leq \mathbf{v} \end{cases}$$

Definition 1.61. Given a linear program, the *feasible region* of the program is the set

$$\mathfrak{F} = \{x \in \mathbb{R}^n : \mathbf{A}x \lesseqqgtr \mathbf{b}, \mathbf{u} \leq x \leq \mathbf{v}\}.$$

That is, the set of the points that satisfy the conditions of the problem.

Proposition 1.62. Given an $x \in \mathbb{R}^n$, x is a *feasible solution* of the linear program if and only if $x \in \mathfrak{F}$.

Definition 1.63. A *polyhedron* P is a set of $\mathbb{R}^n$ that can be expressed as an intersection of a finite collection of half-spaces, that is

$$P = \{x \in \mathbb{R}^n : \mathbf{A}x \geq \mathbf{b}, \mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R}), \mathbf{b} \in \mathbb{R}^m\}.$$

A *polytope* is a non-empty and bounded polyhedron. The feasible region of any linear program is a polyhedron.

Definition 1.64. Let $P \subset \mathbb{R}^n$ be a polyhedron. A point $x \in \mathbb{R}^n$ is an extreme point of P if there is neither a pair of points $y, z \in P$, nor a scalar $\lambda \in [0, 1]$ such that $x = \lambda y + (1 - \lambda)z$.

[2] Analogously we can define a *linear programming to minimize* changing the objective function to a minimize function.

Definition 1.65. Let LP be a linear program. We define the *standard form of LP* as

$$\mathrm{LP} = \left\{ \begin{array}{rl} \min: & z = \mathbf{c}^{\mathrm{T}} x \\ \text{subject to}: & \mathbf{A}x = \mathbf{b} \\ & x \geq 0 \end{array} \right.$$

Definition 1.66. Let $\mathrm{LP} = \min_{x \in \mathbb{R}^n} \{\mathbf{c}^{\mathrm{T}} x : \mathbf{A}x = \mathbf{b}, x \geq 0\}$. Feasible solution in which free variables or non-basic variable equal zero with respect to basis of basic variables are called *basic feasible solutions*.

Proposition 1.67. If a linear program admits feasible solutions, exists a basic feasible solution. If a linear program admits an optimal solution, exists an optimal basic feasible solution.

Theorem 1.68. Let P be a non-empty polyhedron of a linear program in standard form with maximum rank and let $x \in P$. Then x is an extreme point of P if and only if x is a basic feasible solution.

Definition 1.69 (Simplex method: Phase I). Given a linear program in standard form

$$\mathrm{LP} = \left\{ \begin{array}{rl} \min: & z = \mathbf{c}^{\mathrm{T}} x \\ \text{subject to}: & \mathbf{A}x = \mathbf{b} \\ & x \geq 0 \end{array} \right.$$

its associated problem in phase I (LP_1) is

$$\mathrm{LP}_1 = \left\{ \begin{array}{rl} \min: & w = \displaystyle\sum_{i=1}^{m} y_i \\ \text{subject to}: & \mathbf{A}x + \mathbf{I}_m y = \mathbf{b} \\ & x, y \geq 0 \end{array} \right.$$

A condition necessary for LP having basic feasible solutions is that the optimal solution of LP_1 must be $w = 0$. In fact, if $w \neq 0$, then the original linear program has no feasible solutions[3].

Proposition 1.70 (Simplex method: Phase II). Suppose in a simplex table with positive pivots and therefore independent-terms vector $\mathbf{d} \geq 0$, there is a coefficient $c_j < 0$.

$$\left(\begin{array}{c|c} * & \mathbf{d}^{\mathrm{T}} \\ \hline \mathbf{c} & z - z_0 \end{array} \right).$$

To find a basic feasible solution with lower cost, we make the following change of variable:

1. The variable in column j becomes a basic variable.
2. The variable in row i such that
$$\frac{d_i}{a_{ij}} = \min \left\{ \frac{d_k}{a_{kj}} : a_{kj} > 0 \right\}$$
becomes a non-basic variable. If this variable does not exists, that is, $a_{kj} \leq 0 \ \forall k$ then the linear program is not bounded.

Definition 1.71 (Dual program). Let $\mathrm{LP} = \min_{x \in \mathbb{R}^n} \{\mathbf{c}^{\mathrm{T}} x : \mathbf{A}x \geq \mathbf{b}, x \geq 0\}$. We define the *dual program of LP* as

$$\mathrm{LP}^* = \left\{ \begin{array}{rl} \max: & z = \mathbf{b}^{\mathrm{T}} y \\ \text{subject to}: & \mathbf{A}^{\mathrm{T}} y \leq \mathbf{c} \\ & y \geq 0 \end{array} \right.$$

The linear program LP is called *primal*.

Theorem 1.72 (Weak duality theorem). Let x be a feasible solution of the primal linear program and y a feasible solution of the dual linear program. Then we have:

- $\mathbf{c}^{\mathrm{T}} x \leq \mathbf{d}^{\mathrm{T}} y$ if the primal linear program is in canonical form to maximize.
- $\mathbf{c}^{\mathrm{T}} x \geq \mathbf{d}^{\mathrm{T}} y$ if the primal linear program is in canonical form to minimize.

Corollary 1.73. Let x, y be feasible solutions of the primal and dual linear programs respectively such that $\mathbf{c}^{\mathrm{T}} x = \mathbf{d}^{\mathrm{T}} y$. Then x and y are optimal solutions.

Theorem 1.74 (Strong duality theorem). Any linear program has an optimal solution if and only if its dual linear program does, and in this case, the values coincide.

Theorem 1.75 (Complementary property). Suppose that the optimal table of the primal linear program is of the form

$$\left(\begin{array}{c|c} * & \mathbf{d}^{\mathrm{T}} \\ \hline \mathbf{c} & z - z_0 \end{array} \right),$$

where $\mathbf{c} = (c_1, \ldots, c_{n+m})$ and $\mathbf{d} = (d_1, \ldots, d_m)$ with $c_i \geq 0$, $i = 1, \ldots, n+m$. If $(y_1, \ldots y_m, t_1^*, \ldots, t_n^*)$ is the optimal solution of the dual linear program, expressed in standard form, then

$$c_1 = t_1^*, \ldots, c_n = t_n^*, c_{n+1} = y_1, \ldots, c_{n+m} = y_m.$$

[3] This phase is useful to find, if there is, an initial basic feasible solution.