Matemática Discreta

Resumo

Conteúdo

Capítulo 1

Teoria dos Números

1.1 Conjuntos e Funções

1.1.1 Conjunto Potência

O conjunto potência de X (ou conjunto das partes de X) é dado por:

$$\mathcal{P}(X) = \{A : A \subset X\}$$

Tem-se que $|\mathcal{P}(X)| = 2^{|X|}$
Exemplo: se $X = \{0, 4, \alpha\}$, então:

$$\mathcal{P}(x) = \{\emptyset, \{0\}, \{4\}, \{\alpha\}, \{0, 4\}, \{0, \alpha\}, \{4, \alpha\}, X\}$$

1.1.2 Funções

Uma função $f : X \to Y$ é uma associação em que a cada $x \in X$ corresponde um único $y \in Y$ tal que $y = f(x)$ em que X é o conjunto de partida e Y é o conjunto de chegada.

A imagem de f é $f(X) = \{f(x) \in Y : x \in X\} \subset Y$, logo a imagem de $A \subset X$ é $f(A) = \{f(x) \in Y : x \in A\} \subset Y$. A imagem inversa de $B \subset Y$ é $f^{-1}(B) = \{x \in X : f(x) \in B\} \subset X$

Classificação

Dada uma função $f : X \to Y$:

- f é injetiva se $\forall x, y \in X, x \neq y \Rightarrow f(x) \neq f(y)$
- f é sobrejetiva se $f(X) = f(Y)$
- f é bijetiva se é injetiva e sobrejetiva

Se $|X| > |Y|$ então f não pode ser injetiva e se $|X| < |Y|$ não pode ser sobrejetiva.

1.1.3 Relações de Equivalência

Relação de equivalência em X é uma partição de X em subconjuntos disjuntos em que cada subconjunto fica com os objetos equivalentes.

Exemplo: Se $X = \{x, y, \zeta, \phi\}$ podemos tornar equivalentes as letras do mesmo alfabeto, obtendo a relação $\{\{x, y\}, \{\zeta, \phi\}\}$.

Uma relação $\sim$ é uma relação de equivalência em X se, e só se, para todos os $x, y, z \in X$ é:

- Reflexiva: $x \sim x$
- Simétrica: se $x \sim y$ então $y \sim x$
- Transitiva: se $x \sim y$ e $y \sim z$ então $x \sim z$

1.2 Teorema Fundamental da Aritmética

1.2.1 Divisibilidade

Sejam $a, b \in \mathbb{N}$, com $a > b > 1$. A divisão inteira de a por b é a representação:

$$a = q \cdot b + r$$

onde $r \in \{0, 1, 2, ..., b-1\}$ é o resto e q o quociente, únicos.

Para $a, b \in \mathbb{Z}$ dizemos que b *divide* a (ou é *divisor*) e escreve-se $b \mid a$ (caso contrário $b \nmid a$) se:

- a é múltiplo de b
- $\frac{a}{b} \in \mathbb{Z}$
- o resto da divisão de a por b é zero

$$Div(a) = \{n \in \mathbb{N} : n \mid a\}$$

Propriedades

- $0 \nmid a$, $1 \mid a, \forall a \in \mathbb{N}$
- Se $a \mid b$ e $b \mid c$ então $a \mid c$
- Se $b \mid a$ e $a \mid b$ então $|a| = |b|$
- Se $a, b \in \mathbb{N}$ e $a \mid b$, então $a \leq b$ e $a \in Div(b)$
- Se $a \mid b$ então $a \mid bc$
- Se $a \mid b$ e $a \mid c$ então $a \mid (b + c)$ e $a \mid (b - c)$

Um número $p \in \mathbb{N}$ é primo se $Div(p) = \{1, p\}$

1.2.2 MDC e Algoritmo de Euclides

O máximo divisor comum entre $a, b \in \mathbb{N}$ é o maior elemento $(a, b) = mdc(a, b)$ do conjunto:

$$Div(a) \cap Div(b)$$

Para determinar (a, b), fazemos uma sucessão de divisões inteiras, começando com $a = d_0, b = d_1$ (supondo $a > b$):

$$d_0 = q_1 d_1 + d_2 \tag{1.1}$$
$$d_1 = q_2 d_2 + d_3 \tag{1.2}$$
$$\vdots \tag{1.3}$$
$$d_{k-2} = d_{k-1} q_{k-1} + d_k \tag{1.4}$$
$$d_{k-1} = d_k q_k + 0 \tag{1.5}$$

No final, obtém-se $(a, b) = d_k$

Diz-se que $a, b \in \mathbb{N}$ são primos entre si se $(a, b) = 1$

1.2.3 Equação de Bézout

Sejam $a, b \in \mathbb{N}$ e $d = (a, b)$. A equação de Bézout é:

$$ax + by = d$$

Uma solução particular obtém-se do algoritmo de Euclides estendido. Geralmente, temos a equação diofantina:

$$ax + by = c$$

Esta equação tem solução (x_0, y_0) se e só se $d \mid c$ e, quando existem, as soluções são infinitas. A solução geral é:

$$x = x_0 + k\frac{b}{d}, \qquad y = y_0 - k\frac{a}{d}, \qquad k \in \mathbb{Z}$$

Sendo x_0, y_0 solução de $ax + by = c = md$.

Exemplo do Algoritmo de Euclides Estendido

Para determinar todas as soluções de $711x + 132y = 6$, constrói-se a seguinte tabela, em que q_i é obtido ao aplicar o algoritmo de euclides:

d_1	$-q_i$	x_i	y_i
711		1	0
132	-5	0	1
51	-2	1	-5
30	-1	-2	11
21	-1	3	-16
9	-2	-5	27
3		13	-70

Logo, como $(711, 132) = 3$, sabe-se que as soluções de $711x + 132y = 3$ são $x = 13$ e $y = -70$. Dado que $6 = 2 \cdot 3$, tem-se que $711(2 \cdot 13) + 132(2 \cdot (-70)) = 6$ e a solução geral é:

$$x = x_0 - 44k, \qquad y = y_0 + 237k, \qquad k \in \mathbb{Z}.$$

1.2.4 Enunciado do TFA

Seja $n \in \mathbb{N}$.

Versão 1: Existe fatorização:

$$n = p_1 ... p_m, \qquad p_1, ..., p_m \ \ são \ \ primos$$

Versão 2: Existe fatorização:

$$n = p_1^{e_1} ... p_k^{e_k} \qquad p_1, ..., p_k \ \ são \ \ primos \ \ distintos, e_j \in \mathbb{N}$$

Ambas as fatorizações são únicas, a menos de reordenação dos fatores.

Corolário:

Seja $n = p_1^{e_1} ... p_k^{e_k} \in \mathbb{N}$. O conjunto dos divisores positivos de n é:

$$Div(n) = \{p_1^{c_1} ... p_k^{c_k} : c_i \in \{0, ..., e_i\}\}$$

1.3 Congruências

Dado $m \in \mathbb{N} \geq 2, a, b \in \mathbb{Z}$, dizemos que a é congruente com b módulo m

$$a \equiv b \mod m$$

se $m \mid (b - a)$, isto é, $\exists x \in \mathbb{Z} : a = m \cdot x + b$, ou seja, m divide a com resto b.

1.3.1 Invertibilidade

$a \in \mathbb{Z}$ é invertível $\mod m$ ($\exists x \in \mathbb{Z}$ com $ax \equiv 1 \mod m$) se, e só se $(a, m) = 1$.

1.3.2 Equações Lineares

A equação linear modular, de módulo $m \geq 2$ é da forma:

$$ax \equiv b \mod m$$

com $a, b \in \mathbb{Z}$. Seja $d = (a, m)$:

- Não há soluções se $d \nmid b$
- Se $d = 1$ há uma solução: $x_0 \equiv a^{-1} b \mod m$

- Se $d \neq 1$ (e $d \mid b$), resolve-se a equação reduzida (dividir por d):

$$a'x \equiv b' \mod m'$$

em que $a' = \frac{a}{d}, b' = \frac{b}{d}, m' = \frac{m}{d}$. A solução geral é:

$$x = x_0 + km' \mod m$$

com $k \in [d]_0$

Teorema Chinês dos Restos

O Teorema Chinês dos Restos permite resolver sistemas lineares modulares da forma:

$$\begin{cases} x \equiv b_1 \mod m_1 \\ x \equiv b_2 \mod m_2 \\ ... \\ x \equiv b_r \mod m_r \end{cases} \tag{1.6}$$

Se $(m_i, m_j) = 1, \forall i \neq j$, então o sistema tem uma única solução $\mod M = m_1 m_2 ... m_r$:

$$x \equiv b_1 \frac{M}{m_1} y_1 + ... + b_r \frac{M}{m_r} y_r \mod M$$

em que $y_k = \left(\frac{M}{m_k}\right)^{-1} \mod m_k, k = 1, ..., r$.

Pequeno Teorema de Fermat

Se p é primo, e a não é múltiplo de p, então:

$$a^{p-1} \equiv 1 \mod p$$

1.3.3 Função Totiente de Euler

A função totiente é definida por:

$$\varphi(n) = \mid \{x \in [n]_0 : (x, n) = 1\} \mid$$

Trata-se da cardinalidade do conjunto dos números entre 0 e $n-1$ que são primos com n (número de invertíveis em $\mathbb{Z}_n$).

Se p é primo, então $\varphi(p) = p - 1$. Mais geralmente, $\varphi(p^r) = p^r - p^{r-1}, r \geq 1$. Se $(n, m) = 1$ temos $\varphi(nm) = \varphi(n)\varphi(m)$.

Corolário: Sendo $n = p_1^{k_1} ... p_r^{k_r}$, temos:

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) ... \left(1 - \frac{1}{p_r}\right)$$

Teorema de Euler

Euler generalizou o pequeno teorema de Fermat para qualquer módulo:

Se $(a, n) = 1$, então:

$$a^{\varphi(n)} \equiv 1 \mod n$$

Teorema de Daniel Augusto da Silva

Se $n_1, ..., n_r$ são primos entre si, e $n = n_1...n_r$, então:

$$\sum_{i=1}^{r} n_i^{\varphi(n)/\varphi(n_i)} \equiv r - 1 \mod n$$

1.4 Criptografia Clássica

Seja M a mensagem a enviar e C a mensagem codificada.

1.4.1 Cifra de César

Na cifra de césar usam-se números de 0 a 25 (mod 26) para as letras:

$$C = M + k \mod 26$$

1.4.2 Funções de um só sentido

Uma função de um só sentido é uma função $f : X \to Y$ em que $f(x)$ tem uma baixa complexidade computacional $\forall x \in X$, mas $f^{-1}(y)$ possui uma elevada complexidade computacional $\forall y \in Y$.

1.4.3 Algoritmo RSA

Módulo base: São escolhidos p e q, primos distintos e calcula-se $N = pq$.
Módulo expoente: $\varphi(N) = (p - 1)(q - 1)$

Passo 1: O recetor escolhe um número invertível mod $\varphi(N)$, e.

Passo 2: Calcula $d = e^{-1} \mod \varphi(N)$ usando, por exemplo, o algoritmo de Euclides estendido

Passo 3: Publica (N, e), mantendo d, $\varphi(N)$, p e q em segredo

Passo 4: O emissor calcula $C = M^e \mod N$ e envia C (a mensagem codificada)

Passo 5: O recetor calcula $C^d = (M^e)^d$ e descobre que $C^d \equiv M \mod N$ (Teorema de Euler)

Teorema RSA

Sejam p, q primos, $N = pq$ e e, d inversos um do outro mod $\varphi(n)$. Então:

$$x^{ed} \equiv x \mod N \qquad \forall x < min\{p, q\}$$

Exemplo

Sejam $p = 61$ e $q = 53$.
Então $N = pq = 3233$ e $\varphi(N) = 60 \cdot 52 = 3210$.
Escolhe-se $e = 661$ e determina-se $d = e^{-1} \equiv 1501 \mod 3120$.
A chave de encriptação $(N, e) = (3233, 661)$.

Seja então a mensagem a enviar $M = x = 2762$. Ao ser codificada obtém-se $C = y = 2762^{661} \equiv 78 \mod 3233$.
Calcula-se então $78^{1501} \equiv 2762 \mod 3233$, recuperando M.

Capítulo 2

Teoria dos Conjuntos

2.1 Números Binomiais

2.1.1 Arranjos sem Repetição

O número de arranjos sem repetição de n elementos k a k em x é:

$$A_k^n = n(n-1)...(n-k+1) = \frac{n!}{(n-k)!}$$

2.1.2 Combinações

Com $n \geq m \geq 0$ definimos o número binomial (número de combinações de n elementos m a m):

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

Propriedade Fundamental

$$\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m-1}$$

2.1.3 Binómio de Newton

Sendo $n \in \mathbb{N}$, temos a seguinte igualdade de polinómios:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

2.1.4 Números Multinomiais

Sendo $n = n_1 + ... + n_k \in \mathbb{N}$, com $n_1, ..., n_k \geq 1$, definimos:

$$\binom{n}{n_1, ..., n_k} = \frac{n!}{n_1!...n_k!}$$

2.2 Princípios da Combinatória

2.2.1 Princípio da Inclusão-Exclusão

O PIE determina o cardinal de uma união não disjunta de conjuntos. Para 2 conjuntos:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Para 3 conjuntos:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Fórmula Geral

Seja $A_{i_1 i_2 \ldots i_k} = A_{i_1} \cup A_{i_2} \cup \ldots \cup A_{i_k}$. Tem-se:

$$\left| \bigcup_i A_i \right| = \sum_{i=1}^{n} |A_i| - \sum_{i_1 < i_2} |A_{i_1 i_2}| + \ldots + (-1)^{k-1} \sum_{i_1 < \ldots < i_k} |A_{i_1 \ldots i_k}| + \ldots + (-1)^{n-1} |A_{1 \ldots n}|$$

2.2.2 Forma Complementar do PIE

A forma complementar do PIE calcula o cardinal do complementar de uma união:

$$|X \setminus (A_1 \cup A_2 \cup \ldots \cup A_n)| = |A_1^c \cap A_2^c \cap \ldots \cap A_n^c|$$

Onde $A_j^c = X \setminus A_j$. De um modo geral:

$$\left| X \setminus \bigcup_i A_i \right| = \left| \bigcap_i A_i^c \right| = |X| - \sum_{i=1}^{n} |A_i| + \sum_{i_1 < i_2} |A_{i_1 i_2}| - \ldots + (-1)^k \sum_{i_1 \ldots i_k} |A_{i_1 \ldots i_k}| + \ldots + (-1)^n |A_{1 \ldots n}|$$

2.3 Simetria

2.3.1 Permutações

Uma permutação de n elementos é uma bijecção $\pi : [n] \to [n]$. Por exemplo:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$$

Representa $\pi(1) = 2, \ldots, \pi(6) = 5$. S_n representa o conjunto de todas as permutações, $|S_n| = n!$.

Notação cíclica

$$\pi = (123)(56) \in S_6$$

Pois $\pi(1) = 2$, $\pi(2) = 3$, $\pi(3) = 1$ (completando o ciclo) e $\pi(5) = 6$ (esgotando os elementos).

2.3.2 Grupos Finitos

Chama-se grupo finito a um conjunto finito G com operação associativa $\cdot$, elemento neutro e, em que todos os elementos têm inverso.

Diz-se que H é subgrupo de G ($H \subset G$) se $e \in H$, fechado para composição e inverso.

Teorema de Lagrange

Se $H \subset G$ é subgrupo, então:

$$|G| = |H||G/H|$$

Onde G/H é o espaço das classes de equivalência da relação:

$$x \sim y \;\; se \;\; \exists h \in H : y = hx$$

2.3.3 Grupo cíclico $\mathbb{Z}_m$

A ordem de $g \in G$ é o menor número natural k tal que $g^k = e$.

Se $H \subset G$ é subgrupo, então $|H|$ divide $|G|$. A ordem de qualquer elemento de G divide $|G|$.

Pode-se pensar em $\mathbb{Z}_m$ como o grupo de rotações de um polígono com m lados.

Exemplo

$\mathbb{Z}_8$ corresponde às rotações de um octógono com vértices $\{0, 1, ..., 7\}$

$$\mathbb{Z}_8 \cong \{e, (01234567), (0246)(1357), (03614725), (04)(15)(26)(37), ...\}$$

Então $H = \{e, (04)(15)(26)(37)\} \subset \mathbb{Z}_8 = G$ é subgrupo e verifica-se:

$$8 = |G| = |H||G/H| = 2 \cdot 4$$

$$H = \{0, 4\} \subset G = \mathbb{Z}_8$$

Pelo que G/H tem 4 classes.

2.3.4 Ação de um Grupo G num conjunto X

Uma ação de G num conjunto X é uma aplicação:

$$G \times X \to X, \qquad (g, x) \to g \cdot x \in X$$

com $e \cdot x = x$ e $(gh) \cdot x = g \cdot (h \cdot x), \forall g, h \in G, x \in X$

Órbita de x: $G \cdot x = \{g \cdot x : g \in G\} \subset X$

Estabilizador de x: $G_x = \{h \in H : h \cdot x = x\} \subset G$

Conjunto fixo por g: $X^g = \{x \in X : g \cdot x = x\} \subset X$

Teorema da Órbita-Estabilizador

Para todo $x \in X$:

$$|G| = |G \cdot x||G_x|$$

2.3.5 Lema de Cauchy-Frobenius-Burnside

Dada a ação de G em X, o espaço das órbitas é X/G. O lema Burnside determina o número de órbitas $|X/G|$, a partir dos conjuntos de pontos fixos:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Colorações de X

Seja $c(g)$ o número de ciclos de $g \in G$, como permutação de X. O número de colorações do conjunto X, tomando em conta as simetrias dadas por G é:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{|G|} \sum_{g \in G} |X|^{c(g)}$$

2.4 Funções Geradoras e Recorrências

2.4.1 Sucessões e Funções Geradoras

Seja $(u_n)_{n \in \mathbb{N}_0} = (u_o, u_1, ..., u_n, ...)$ uma sucessão de números reais. A função geradora associada a (u_n) é a série:

$$f(x) = \sum_{n=0}^{\infty} u_n x^n = \sum_{x \geq 0} u_n x^n$$

Muitas sucessões em combinatória têm funções geradoras racionais:

$$f(x) = \frac{p(x)}{q(x)} \qquad p(x), q(x) \in \mathbb{R}[x]$$

Sabendo que $p(x)$ é da forma $ax + b$, podemos determinar a e b através das derivadas de $f(x)$, já que $f(0) = u_0$ e $f'(0) = u_1$.

Exemplos

- Série geométrica: $\sum_{n \geq 0} x^n = \frac{1}{1-x}$
- Newton: $\sum_{n \geq 0} \binom{N}{n} x^n = (1+x)^N$
- Derivar: $\left(\frac{1}{1-x}\right)' = \sum_{n \geq 0} n x^{n-1} = \frac{1}{(1-x)^2}$
- Exponencial: $\sum_{n \geq 0} \frac{x^n}{n!} = e^x$

2.4.2 Recorrência Linear

Uma equação de recorrência de ordem $k \in \mathbb{N}$ é:

$$u_{n+k} = F(u_n, u_{n+1}, ..., u_{n+k-1}), n \in \mathbb{N}_0$$

O problema de recorrência de ordem k tem-se quando $u_0 = c_0, ..., u_{k-1} = c_{k-1}$. Uma equação de recorrência linear de ordem k é:

$$u_{n+k} = a_{k-1}u_{n+k-1} + ... + a_1u_{n+1} + a_0u_n + b(n), n \in \mathbb{N}_0$$

Sendo homogénea quando $b(n) = 0, \forall n \in \mathbb{N}$. O polinómio característico desta equação é:

$$p(x) = x^k - a_{k-1}x^{k-1} - ... - a_1x - a_0$$

Independentemente de $b(n)$.

Se λ é raiz do polinómio $p(x)$, então $u_n = \alpha\lambda^n$ é solução da homogénea para qualquer $\alpha \in \mathbb{R}$. Se u_n e v_n são soluções da homogénea, então $\alpha u_n + \beta v_n$ também.

Solução geral dos PRL

Sejam $\lambda_1, \lambda_2, ...$ as raízes com multiplicidades $m_1, m_2, ...$ ($\sum_i m_i = k$):

- Caso homogéneo ($b(n) = 0, \forall n$):

  $$u_n = \alpha_1^{(0)}\lambda_1^n + \alpha_1^{(1)}n\lambda_1^n + ... + \alpha_1^{(m_i-1)}n^{m_i-1}\lambda_1^n + ...$$

  Os coeficientes $\alpha_i^{(j)}$ determinam-se com as condições iniciais.

- Caso não homogéneo:

  $$u_n = v_n + \alpha_1^{(0)}\lambda_1^n + ... + \alpha_1^{(m_i-1)}n^{m_i-1}\lambda_1^n + ...$$

  onde v_n é a solução particular, obtida por substituição

- Função geradora da solução: $f(x) = \frac{q(x)}{x^k p\left(\frac{1}{k}\right)}$, com $q(x)$ de grau $< k$

Capítulo 3

Teoria dos Grafos

3.1 Introdução

Um grafo pode ser representado na forma $\Gamma = (V, A)$, em que cada vértice $v \in V$ e cada aresta $\alpha \in A$. Podem ser classificados da seguinte forma:

- Simples: $\alpha = \{v, \omega\}, A \subset \mathcal{P}_2(V)$
- Multigrafo: arestas diferentes $\alpha_2 \neq \alpha_1 \in A$ podem ligar os mesmos vértices: $\phi : A \to \mathcal{P}_2(V), \phi(\alpha_1) = \phi(\alpha_2)$
- Pseudo-grafo: admite lacetes, $\phi : A \to V \sqcup \mathcal{P}_2(V), \phi(\alpha) = \{v\}$
- Dirigido: cada aresta está orientada $\psi : A \to V^2 = V \times V, \psi(\alpha) = (v, \omega)$, v inicio, ω fim.

Os extremos da aresta $\alpha = \{v, \omega\} \in A$ são v e ω; α incide em v e em ω.
A valência ou grau de $v \in V$ é:

$$d_v = |\{\alpha \in A : v \in \alpha\}|$$

3.1.1 Propriedades

Seja Γ um grafo (ou pseudo-grafo). Tem-se:

$$\sum_{v \in V} d_v = 2|A|$$

Diz-se que $(d_1, d_2, ..., d_n)$ é sequência gráfica se existe um grafo simples $\Gamma = (V, A), |V| = n$, em que d_i é o grau do vértice $v_i \in V$.
Se Γ é um grafo simples com graus $d_1 \leq .. \leq d_n$, então:

- $\sum_{i=1}^{n} d_i$ é par
- $d_n < n$ (implica cada $d_i < n$ e $\sum_{i=1}^{n} d_i \leq n(n-1)$
- $(d_1, ..., d_n, d_{n+1} = \Delta)$ é sequência gráfica se e só se $(d_1, ..., d_k, d_{k+1} - 1, ..., d_n - 1)$ é sequência gráfica, $n = k + \Delta$

3.1.2 Passeios e Caminhos

- Um passeio é uma sequência alternada de vértices e arestas, tal que o elemento seguinte é adjacente/incidente ao anterior, começa e termina em vértices.
- Um caminho é um passeio que não repete vértices nem arestas.
- Um ciclo é um caminho que começa e termina no mesmo vértice.

Um caminho é Hamiltoniano se passa por todos os vértices e um passeio diz-se Euleriano se passa por todas as arestas sem repetição.

3.1.3 Características

Conexidade

Um grafo diz-se conexo se para quaisquer dois vértices existe um passeio/caminho entre eles.

Isomorfismo

Um isomorfismo entre os grafos $\Gamma = (V, A)$ e $\Gamma' = (V', A')$ é uma bijecção $f : V \to V'$ com $\{v_i, v_j\} \in A$ se e só se $\{f(v_i), f(v_j)\} \in A'$.

3.1.4 Árvores

Uma árvore é um grafo conexo e sem ciclos. Uma floresta é um grafo sem ciclos, ou seja, uma união disjunta de árvores.

Numa árvore há um único caminho entre quaisquer dois vértices. $(d_1, ..., d_n)$ é a sequência gráfica de uma árvore se e só se $\sum_{i=1}^{n} d_i = 2n - 2$.

Árvores Geradoras

Uma árvore geradora de um grafo simples Γ é uma árvore em Γ que contém todos os seus vértices.

3.2 Grafos planares

Um grafo é planar se pode ser desenhado num plano sem que as arestas se intersectem. Um grafo planar conexo com v vértices, a arestas e f faces verifica:

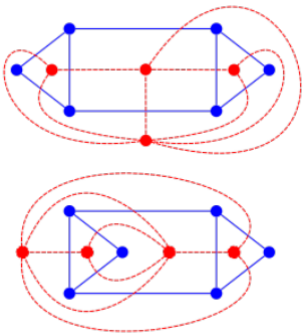
$$v - a + f = 2$$

Contando com a face exterior. Se um grafo é planar conexo com $v > 2$ vértices e a arestas (e faces de ordem > 2) temos:

$$a \leq 3v - 6$$

3.2.1 Grafo Dual

Dado um grafo planar Γ, o grafo dual $\Gamma^\vee$ é obtido trocando os vértices com as faces. Por exemplo:

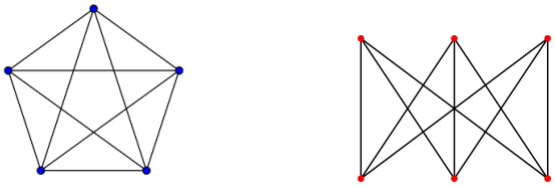


3.2.2 Teorema de Kuratowski

Um subgrafo do grafo simples Γ é $\Gamma' \subset \Gamma$ obtido tomando só algumas arestas e os seus vértices incidentes.

Uma subdivisão de um grafo Γ é um novo grafo Γ' obtido adicionando alguns vértices no meio de arestas de Γ.

Pelo Teorema de Kuratowski, Γ é um grafo planar se e só se não contém nenhum subgrafo que é uma divisão de K_5 ou de $K_{3,3}$



3.3 Matrizes Associadas

3.3.1 Grafos Simples e Multigrafos

Seja $\Gamma = (V, A)$ um grafo simples ou multigrafo, em que $V = \{v_1, ..., v_n\}, A = \{\alpha_1, ..., \alpha_m\}$

Matriz de Incidência

A matriz de incidência é uma matriz $m \times n = |A| \times |V|$ tal que:

$$M_{ij} = \begin{cases} 1, & \text{se } \alpha_i \text{ incide em } v_j \\ 0, & \text{se } \alpha_j \text{ não incide em } v_j, \end{cases} \qquad i \in [m], j \in [n]$$

Matriz de Adjacência

A matriz de adjacência é uma matriz quadrada simétrica $n \times n$:

$$J_{ij} = k$$

Se v_i e v_j estão ligados por k arestas (= 0 se $i = j$).

Matriz de Valência

A matriz de valência é uma matriz diagonal $n \times n$:

$$D = diag(d_{v_1}, ..., d_{v_n})$$

Em que $D_{ij} = 0$ para $i \neq j$.

Teorema: Para um multigrafo, $M^t M = J + D$.

Teorema de Kirchhoff

Uma matriz laplaciana de Γ com n vértices é a matriz quadrada $(n \times n)$ $L = D - J$. Para cada $v \in V$, seja L_v o correspondente cofator de L. Pelo teorema de Kirchhoff, se Γ é conexo então:

- $\det L_v = \det L_w$, para quaisquer $v, w \in V$
- $\det L_v$ é o número de árvores geradoras em Γ

Matriz Estocástica

Um vetor estocástico é $v = (v_1, v_2, ..., v_n)$ com $v_i \geq 0$ e $v_1 + v_2 + ... + v_n = 1$. Uma matriz estocástica $n \times n$ é uma matriz cujas colunas são vetores estocásticos. Se nenhuma entrada for zero, diz-se estocástica positiva.

Sejam A e B matrizes estocásticas:

- AB é estocástica
- $sA + tB$ é estocástica positiva $\forall s, t > 0$ com $s + t = 1$

Seja M uma matriz estocástica positiva, pelo teorema de Perron-Frobenius:

- 1 é o valor próprio de M
- Há um único valor próprio estocástico p de valor próprio 1
- $M^n v$ tende para p, para qualquer v estocástico

p denomina-se o vetor de Perron-Frobenius

3.3.2 Grafos Dirigidos

Seja $\Gamma = (V, A)$ um grafo dirigido, em que $V = \{v_1, ..., v_n\}, A = \{\alpha_1, ..., \alpha_m\}$

Matriz de Incidência

A matriz de incidência é uma matriz $m \times n$ tal que:

$$M_{ij} = \begin{cases} 1, & \textit{se } \alpha_i \textit{ aponta para } v_j \\ -1, & \textit{se } \alpha_i \textit{ sai de } v_j \\ 0, & \textit{se } \alpha_j \textit{ não incide em } v_j, \end{cases} \qquad i \in [m], j \in [n]$$

Matriz de Adjacência/Transferência

A matriz de adjacência/transferência é uma matriz T quadrada não simétrica $n \times n$ com $T_{ij} = 1$ se há seta de v_i para v_j (linha j, coluna i).

Teorema: $(T^n)_{ji}$ é o número de percursos diferentes entre o vértice v_i e v_j com comprimento igual a n

Matriz Estocástica

Sendo $\Gamma = (V, A)$ é um grafo dirigido. Utiliza-se na notação dot para listar todas as flechas: $1 \to \{i, j, ...\}, 2 \to \{k, l, ...\}$.

A matriz estocástica do grafo dirigido com n vértices é uma matriz $n \times n$ que estipula igual probabilidade de seguir as várias flechas de saída e $1/n$ para os vértices sem saída. Por exemplo, para as flechas $1 \to \{2, 3, 4\}; 2 \to \{3, 4\}; 3 \to 1; 4 \to \emptyset$ constrói-se a seguinte matriz:

$$\begin{pmatrix} 0 & 0 & 1 & \frac{1}{4} \\ \frac{1}{3} & 0 & 0 & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{2} & 0 & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{2} & 0 & \frac{1}{4} \end{pmatrix}$$

Proposição: A probabilidade de transição do vértice i para o j em k passos é a entrada da coluna i e linha j da matriz E^k

3.4 Algoritmo PageRank

Supondo que $\Gamma = (V, A)$ com matriz estocástica E é um grafo dirigido que representa a internet, em que os N vértices são páginas e as flechas são links para outras páginas. O algoritmo PageRank calcula o vetor estocástico cuja entrada i é a probabilidade de após n passos estarmos na página i da seguinte forma:

- Escolher vetor estocástico inicial, usualmente $v = \frac{1}{N}(1, 1, ..., 1)$
- Escolher peso $\rho \in]0, 1[$ e calcular $H = (1 - \rho)E + \frac{\rho}{N}1$ (onde 1 é a matriz só com 1's), usualmente $\rho = 0.15$
- Calcular $H^n v$ para n suficientemente grande